On stabiliser techniques and their application to simulation and certification of quantum devices

INAUGURAL-DISSERTATION ZUR
ERLANGUNG DES AKADEMISCHEN GRADES

doctor rerum naturalium (Dr. rer. nat.)

IN THEORETISCHER PHYSIK

der
Mathematisch-Naturwissenschaftlichen Fakultät
der Universität zu Köln

vorgelegt von

MARKUS HEINRICH
aus Offenburg

Köln, 2021

Gutachter:	Prof. Dr. David Gross PD Dr. Rochus Klesse Prof. Dr. Markus Müller
Tag der Disputation:	3. Mai 2021

ABSTRACT

The *stabiliser formalism* is a widely used and successful subtheory of quantum mechanics consisting of *stabiliser states*, *Clifford unitaries* and *Pauli measurements*. The power of the formalism comes from the description of its elements via simple group theory. Although the origins of the formalism lie in quantum error correction and fault-tolerant quantum computing, the utility of the formalism goes beyond that.

The Gottesman-Knill theorem states that the dynamics of stabiliser states under Clifford unitaries and Pauli measurements can be efficiently simulated on a classical computer. This algorithm can be extended to arbitrary states and unitaries in multiple ways at the cost of an increased runtime. This runtime can be seen as a quantification of the non-stabiliser resources needed to implement a quantum circuit. Moreover, as non-stabiliser elements are necessary for universal quantum computing, the runtime provides a way to measure the "non-classicality" of a computation. This is particularly pronounced in the *magic state model* of quantum computing where the only non-stabiliser elements are given by *magic states*. Hence, in the *resource theory of magic*, resources are measured through *magic monotones* which are operationally linked to runtimes of classical simulation algorithms.

In this thesis, I discuss different aspects of the resource theory of magic. The mentioned classical simulation algorithms require the computation of magic monotones which is in general a computationally intractable problem. However, I show that the computational complexity can be exponentially reduced for certain classes of symmetric states, such as copies of magic states. To this end, the symmetries of the convex hull of stabiliser states are characterised and linked to their properties as so-called *designs*. In addition, I study the recently introduced class of *completely stabiliser-preserving channels* (CSP), which is the class of quantum channels unable to generate magic resources. It is shown that this class is strictly larger than the class of stabiliser operations, composed of Clifford unitaries and Pauli measurements. This finding could have several interesting consequences. First, it is likely that CSP is efficiently simulable which would allow classical simulation beyond the Gottesman-Knill theorem. Second, it is possible that optimal magic state distillation rates cannot be achieved via stabiliser operations and this gap is in fact significant.

Further applications of the stabiliser formalism come through *design theory*. A unitary t-design is an ensemble of unitaries which reproduce the first t moments of the Haar measure on the unitary group. *Randomness* in the form of Haar-random unitaries is an essential building block in many quantum information protocols. Implementing such Haar-random unitaries is however often impractical. Here, designs can exhibit considerably lower resource requirements while still being random enough for most applications. Some of the most prominent examples of such protocols concern the certification and characterisation of quantum systems, such as *randomised benchmarking*. Interestingly, the group of Clifford unitaries forms a *unitary 3-design* and is often the prime choice thanks to efficient group operations.

In this thesis, I summarise my recent results obtained with collaborators in constructing *approximate unitary t-designs* from the Clifford group supplemented by only few non-Clifford gates. Intriguingly, this construction uses only $\tilde{O}(t^4)$ single qubit non-Clifford gates and is independent of the number of qubits n. Overall, this yields a gate count of $\tilde{O}(n^2t^4)$ which is a significant improvement over $\tilde{O}(n^2t^{10})$ for the Brandao-Harrow-Horodecki construction based on local random circuits.

To provide context for this result, I review the representation theory of the Clifford group and define the Clifford semigroup. In an attempt to generalise approximations results for the unitary group to the Clifford group, the Clifford semigroup is investigated for suitable approximations of the Clifford twirl.

CONTENTS

INTRODUCTION TO THIS DISSERTATION

The defining goal of quantum information science is to study how information can be manipulated by the quantum-mechanical laws of nature. During the last 30 years, significant progress has been made in developing ideas and methods to store, transmit or process information using quantum effects. Consequently, quantum information science has matured to a broad and prospering field with diverse research directions that reach from quantum communication to quantum computing and the characterisation of quantum processes. Among other things, the research finds that faster and more secure ways of communication as well as more powerful computing is possible with quantum devices. Some of these ideas have already been successfully demonstrated in a series of proof-of-principle experiments [1–6]. Quantum key distribution is arguably the most advanced quantum technology as several networks have demonstrated over the years. Furthermore, researchers have recently claimed the first quantum advantage of a quantum computer over classical computers [5, 6]. Careful voices, however, expect realistic usecases for quantum computers to lie years ahead of us. Nevertheless, these ideas bear the potential to have a technological impact comparable with the silicon revolution of classical computers. Although the development is still in an early stage and high technological barriers have to be overcome, these prospects have already gained a lot of public and political attention.

Due to the sensitivity of quantum systems to their environment, the design of quantum devices is delicate and makes a close collaboration between theory and experiment necessary. On the theoretical side, a number of methods have been developed which allow to *characterise* a quantum system to a varying level of detail [7–16]. This allows to quantify the amount of noise or to determine its form. Furthermore, it can be *certified* that a quantum device is functioning properly. As quantum computations are especially sensitive to noise, these techniques are of special importance there. Besides the characterisation of noise, *benchmarking* the individual components of a quantum computer has become a common method of quantifying its performance [17–23]. At the current state-of-the art, the results of quantum computation can often be *simulated* on a classical computer can be used to certify the function of a quantum computer [24–39].

Many of these methods are based on a special subclass of quantum states and operations with astonishing properties. This subclass consists of *stabiliser states*, *Clifford unitaries*, and *Pauli measurements*, and allows for an efficient description through the so-called *stabiliser formalism*. In particular, the dynamics of stabiliser states under Clifford unitaries and the outcomes of Pauli measurements can be efficiently simulated on a classical computer – a result which is known as the Gottesman-Knill theorem [40]. Nevertheless, this subclass can be used to demonstrate many quantum phenomena. For instance, *stabiliser states* can be highly entangled and have proven useful in studying multipartite entanglement [41–47].

Interestingly, the development of the stabiliser formalism coincided with the discovery of quantum error-correcting codes [40, 48–52]. Calderbank, Shor [49], and Steane [50]

have showed that classical codes can be turned into quantum codes using a simple construction which is now called the CSS construction. As it was quickly realised, the newly found quantum codes belong to the more general family of so-called *stabiliser codes* which can be described using the stabiliser formalism [40, 51–54]. To this date, stabiliser codes are the best-studied quantum codes and almost all known quantum codes are stabiliser codes or are based on them.

The utility of the stabiliser formalism for the mentioned applications is ultimately due to the both powerful and efficient mathematical framework underlying it. This thesis is dedicated to finding a deeper understanding of this framework and the development of advanced stabiliser methods for the simulation and characterisation of quantum devices. In the following, I give a overview of the contents.

Part I: The phase space representation of the stabiliser formalism

The first part of this thesis contains a mathematical treatise of the stabiliser formalism based on the *discrete phase space representation*. In the case of continuous variables, a similar representation lies at the heart of quantum mechanics. It not only ensures that canonical coordinates on classical phase space can be "quantised" to operators on a Hilbert space which fulfil the *canonical commutation relations*, but also shows that canonical, i. e. symplectic, transformations of the classical phase space act in the same way on the so-defined operators. Vice versa, quantum states can be represented on phase space by their *Wigner function*. This representation is almost as old as quantum mechanics itself and goes back to works by Herrmann Weyl who used these ideas to show the equivalence between the Schrödinger and Heisenberg picture.

I treat the case of a finite-dimensional quantum system given by n qudits where we assume that the qudit dimension $q = p^m$ is the power of a prime p. Then, the proper replacement of the continuous phase space $\mathbb{R}^{2n}$ is the discrete phase space $\mathbb{F}_q^{2n}$ for the finite field $\mathbb{F}_q$ with q elements. To develop the formalism, I introduce finite fields and symplectic vector spaces. Then, it is shown how the stabiliser formalism emerges in terms of a unitary representation of phase space on the n-qudit Hilbert space $(\mathbb{C}^q)^{\otimes n}$. Special care is taken in the qubit case $p = 2$ where several mathematical difficulties occur. Many standard results such as the explicit form of stabiliser states and codes or the classical simulation of stabiliser operations are then re-derived via the phase space formalism. Furthermore, I show the advantages of this approach by discussing discrete Wigner functions, mutually unbiased bases and numerical algorithms for sampling and compiling Clifford unitaries.

To the best of my knowledge, this thesis includes the first coherent presentation of the subject. This textbook-style part contains results from numerous research papers which have been reformulated in a uniform and general language. This made the generalisation of some results to prime-power dimensions necessary.

Part II: Classical simulation and the resource theory of magic

As mentioned above, any quantum circuit which applies Clifford unitaries and Pauli measurements to a n-qudit stabiliser state can be simulated on a classical computer in $\mathrm{poly}(n)$ time. Several generalisations of this method are known which allow to go beyond stabiliser states and Clifford unitaries [24–39]. However, the runtime of such an

algorithm typically scales as poly$(n, \Xi(C))$ where $\Xi(C)$ is a function measuring the "non-stabiliserness" of the quantum circuit C. For instance, if C contains k non-Clifford gates, this function typically scales exponentially in k.

Apart from the practical aspect, the simulation of quantum circuits also addresses a fundamental one: What are the necessary resources for a quantum speed-up? Here, the stabiliser perspective is relatively clear. Non-stabiliser elements are necessary to go beyond classical computing and stabiliser-based simulation methods yield a heuristic to quantify these resources by runtime.

The *magic state model* of quantum computing is especially interesting in this context [55]. In this model, a quantum computer is only required to prepare stabiliser states and perform Clifford unitaries and Pauli measurements. Universal quantum computing is then achieved by supplying the quantum computer with so-called *magic states*. The "non-stabiliserness" in this model is concentrated in these magic states and the function Ξ becomes of function of the magic states only. In fact, this has been the starting point of a *resource theory of magic state quantum computing* where the resource is *magic* and measured by the function Ξ, called a *magic monotone* in this context. In this resource theory, stabiliser states are considered "free" and stabiliser operations are "free operations" as they cannot generate any resources.

In the second part of this thesis, I study properties of the resource theory of magic. In Chapter 8, the computability of magic monotones is treated. To this end, I characterise the general symmetries of stabiliser states and show that they are determined by their design properties. This is then used to show that the computation of magic monotones can be exponentially reduced for symmetric inputs such as copies of magic states. Using computer simulations, this is demonstrated for up to 10 copies of common magic states.

In Chapter 9, I discusse the most general class of free operations in the resource theory of magic, the *completely stabiliser-preserving channels* (CSP). The CSP set is characterised and shown to be strictly larger than the set of *stabiliser operations* given by Clifford unitaries, Pauli measurements and the preparation of stabiliser states. Since CSP channels are expected to be efficiently simulable this opens the possibility for new simulation methods beyond the Gottesman-Knill theorem. Moreover, optimal magic state distillation could only be achievable through CSP channels. This could lead to significant gap in the distillation rates when compared to common schemes based on stabiliser operations.

Part III: Exact and approximate unitary designs from the Clifford group

The third and final part of this thesis is dedicated to another aspect of the Clifford group: its statistical properties. Many successful protocols in quantum information theory are based on *randomness* in the form of *Haar-random* states or unitaries. In practice, implementing such a protocol can prove to be difficult due to finite precision errors, circuit depth or limitations of the underlying hardware. Here, the concept of *designs* come into play. Loosely speaking, a t-design is a sub-ensemble of the set of pure states or unitaries which is able to reproduce the first t moments of the Haar measure. Strikingly, the Clifford group forms a unitary 3-design which makes it the prime choice in many quantum information protocols from quantum cryptography [10, 56, 57] to state estimation and characterisation [7–11, 14–16], and randomised benchmarking [17–23].

In Chapter 12, the concept of unitary designs and the design properties of the Clifford group are reviewed. Furthermore, the importance of tensor power representations of the

Clifford group is discussed. In this context, I show that the Kraus operators found for CSP channels in Ch. 9 have another interpretation and form the *Clifford semigroup*.

Afterwards, I address the question why the Clifford group occupies such a prominent role in quantum information theory from the perspective of designs: it is essentially the unique locally generated unitary group design.

Although the Clifford group only forms a 3-design, it can be supplemented by a fixed non-Clifford gate in order to construct approximate t-designs, as shown by my collaborators and I in Ref. [58]. Interestingly, the number of non-Clifford gates only depends on t but not on the number of qubits n. Moreover, the depth of so-constructed circuits is significantly lower than previous constructions based on random gates. These results are summarised in Ch. 14.

Finally, I report on ongoing work in approximating averages over the Clifford group in Ch. 15. The motivation for this comes from the construction of approximate t-designs in Ref. [58]. In an attempt to generalise analogous results for the unitary group, I study approximations which involve the Clifford semigroup. However, it is shown that the situation is more complicated for the Clifford group and closely related to its representation theory. Since the latter subject is still under investigation, this research question remains open.

PART I

THE PHASE SPACE REPRESENTATION OF THE STABILISER FORMALISM

CHAPTER 1

INTRODUCTION

Shortly after stabiliser codes were first discovered [40, 48–52], it was realised that these can be described by symplectic geometry over the binary field $\mathbb{F}_2$ [53, 54]. This is a language similar to the one used in classical coding theory which opened the subject for systematic studies not only by physicists, but also mathematicians and computer scientists [54, 59, 60]. These insights have helped in subsequently generalising the formalism from qubits to systems of arbitrary local dimension – although it works best in the case when the local dimension is a power of a prime.

Interestingly, the formalism has also proven useful beyond quantum error correction. Motivated from optimality results in quantum state reconstruction, mutually unbiased bases (MUBs) have been studied since the dawn of quantum information theory [61]. Although the existence of MUBs in arbitrary dimensions is unknown, there is an explicit construction when the dimension is the power of a prime [61–64]. As it has been realised, these MUBs are exactly the *stabiliser states* described by the generalised stabiliser formalism in prime-power dimension [65]. The study of MUBs and the related symmetric informationally complete positive operator valued measures (SIC-POVMs) has contributed significantly to the understanding of the mathematics behind the stabiliser formalism [11, 66–70] and the relation to complex projective and unitary designs [8, 9, 71].

The phase space representation of quantum mechanics describes quantum states, dynamics and observables as *Wigner functions* and transformations on a classical phase space. In the early years of quantum information theory, a finite-dimensional phase space representation and discrete Wigner function has been developed [72–74] and related to the theory of MUBs [61–64]. But only later, the phase space formulation has been connected to the stabiliser formalism [24, 25, 65, 75, 76].

A central element of the stabiliser formalism is a finite subgroup of the unitary group, called the *Clifford group*. When quantum-error correcting codes had been discovered, this group had emerged in several contexts and plays a prominent role in Gottesman's formulation as the normaliser of the Pauli group [40, 48, 51–54]. However, it was Calderbank, Rains, Shor, and Sloane [53, 54] who introduced the name "Clifford group" into the quantum information community. The name was originally coined by Bolt, Room and Wall [77, 78] who studied symmetries of certain lattices[1]. Calderbank, Rains, Shor, and Sloane realised the relation to stabiliser codes as they were working on related mathematical problems [59, 79–82].

A few years after Bolt, Room and Wall [77, 78] had studied Clifford groups, Weil [83] constructed a representation of the symplectic group $\mathrm{Sp}_{2n}(\mathbb{F})$. In the phase space representation of continuous variable quantum mechanics, this *Weil representation* for $\mathbb{F} = \mathbb{R}$ plays a central role. Intriguingly, by setting $\mathbb{F}$ to a finite field $\mathbb{F}_q$, the Weil representation induces the Clifford group. This is the central element in linking the stabiliser formalism to a discrete phase space.

[1] There is no direct relation to Clifford algebras – although Gottesman attributed one in Ref. [40].

Structure of this part

In this part, I give a mathematical introduction to the stabiliser formalism using its representation on a discrete phase space. The goal is to develop one of the first coherent presentations of the subject in the style of a textbook to make it more accessible to graduate students and researches alike. To this end, results from a multitude of research papers have been collected and reformulated in a uniform and rigorous language. Special emphasis is set on generality – almost all statements are formulated in the general case of prime-power dimensions. In consequence, some literature results have been generalised to align with this idea (e. g. the Clifford sampling algorithm by König and Smolin in Sec. 5.3.1). Special care has been taken in the formulation of the mathematically ill-behaved qubit case. There, I have decided to combine approaches from the physical and mathematical literature [66–68, 84–86] with the goal of finding a balance between rigour and accessibility. The treatise also includes a discussion of the mathematical difficulties in the qubit case and a simplified summary of the mathematical approach in Ref. [86].

This part is structured as follows.

In Chapter 2, we review the standard stabiliser formalism for qubits and show how binary fields and a symplectic structure emerge naturally. Fundamental questions like the form of stabiliser codes or the simulation of stabiliser circuits are then discussed from this perspective.

Motivated by these insights, we proceed by introducing arbitrary finite fields and symplectic vector spaces in Chapter 3. Special emphasis lies on the group of symplectic transformations and its generators. The second half of the chapter is dedicated to a discussion of unitary representations of this symplectic group and their properties.

In Chapter 4, the stabiliser formalism is introduced based on symplectic vector spaces over finite fields and their representation on Hilbert space. We define and characterise stabiliser states and codes and derive explicit formulas, e. g. for their overlaps or the number of stabiliser codes. Finally, a simulation algorithm for stabiliser circuits is given.

Chapter 5 is dedicated to selected applications of the stabiliser formalism. We give an introduction to the discrete Wigner function and MUBs, and summarise the most important results from the literature. Moreover, we present two algorithms based on the finite field formulation, namely the sampling of a random Clifford unitary and the compilation of Clifford unitaries into generators.

This part is concluded by Chapter 6 which treats further topics that are not necessary to understand the main text. There, we describe the construction of Galois fields and rings via polynomial rings. Furthermore, the mathematical intricacies of the qubit case are discussed and the construction of Ref. [86] is reflected.

CHAPTER 2

STABILISER FORMALISM FOR QUBITS

The starting point for the qubit stabiliser formalism is the *Pauli group* which is the group generated by all n-fold tensor products of Pauli operators:

$$\mathcal{P}_n := \langle \{\mathbb{1}, X, Y, Z\}^{\otimes n} \rangle = \left\{ i^k \sigma_1 \otimes \cdots \otimes \sigma_n \;\middle|\; k \in \mathbb{Z}_4,\, \sigma_i \in \{\mathbb{1}, X, Y, Z\} \right\}. \tag{2.1}$$

Here, the Pauli X, Y, and Z operators are defined in the computational basis by

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.2}$$

Given an Abelian subgroup $\mathcal{S}$ of $\mathcal{P}_n$ such that $-\mathbb{1} \notin \mathcal{S}$, we define a *stabiliser code* as the subspace $C_\mathcal{S} \subset (\mathbb{C}^2)^{\otimes n}$ which is stabilised by $\mathcal{S}$:

$$C_\mathcal{S} := \left\{ |\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \;\middle|\; g\,|\psi\rangle = |\psi\rangle \;\forall g \in \mathcal{S} \right\}. \tag{2.3}$$

Suppose $\mathcal{S}$ has a minimal set of l generators $\{g_1, \ldots, g_l\}$. Since $\mathcal{S}$ is Abelian and $-\mathbb{1} \notin \mathcal{S}$, we have $g^2 = \mathbb{1}$ for all $g \in \mathcal{S}$. This implies that every element can be written as $g_1^{x_1} \ldots g_l^{x_l}$ for $x_i \in \{0, 1\}$ and thus $|\mathcal{S}| = 2^l$. Note that $l \leq n$ since there are at most n independent, commuting Pauli operators (we will see an easy proof for this fact later). Finally, it is also simple to compute the dimension of $C_\mathcal{S}$. Clearly, it is the common $+1$ eigenspace of its commuting set of generators and is thus given by the projector

$$P_\mathcal{S} = \prod_{i=1}^{l} \frac{\mathbb{1} + g_i}{2} = \frac{1}{|\mathcal{S}|} \sum_{g \in \mathcal{S}} g. \tag{2.4}$$

Since all $g \in \mathcal{S}$ except for the identity are traceless, the dimension is

$$\dim C_\mathcal{S} = \operatorname{rk} P_\mathcal{S} = \operatorname{tr} P_\mathcal{S} = \frac{\operatorname{tr} \mathbb{1}}{|\mathcal{S}|} = 2^{n-l}. \tag{2.5}$$

Thus, this subspace can be understood as the embedded Hilbert space of $k = n - l$ qubits. In coding theory language, this is called an *encoding* of k qubits into n qubits and $C_\mathcal{S}$ is referred to as a $[[n, k]]$ *stabiliser code*. An important special case of this construction is the maximal one for $l = n$. Then, $C_\mathcal{S}$ is one-dimensional and thus defines a unique pure state, a so-called *stabiliser state*, see Fig. 2.1 for $n = 1$.

Finally, we are interested in the transformations which are compatible with this structure. To this end, we define the *Clifford group*[51, 53] as the unitary normaliser of the Pauli group:

$$\mathrm{Cl}_n = \left\{ U \in U(2^n, \mathbb{Q}[i]) \;\middle|\; U \mathcal{P}_n U^\dagger \subset \mathcal{P}_n \right\}. \tag{2.6}$$

Note that in this definition we added the technical constraint that the unitary matrices should have entries in the complex numbers with rational coefficients $\mathbb{Q}[i]$. When left out, the normaliser becomes an infinite group due to an infinite centre $\simeq U(1)$ of irrelevant

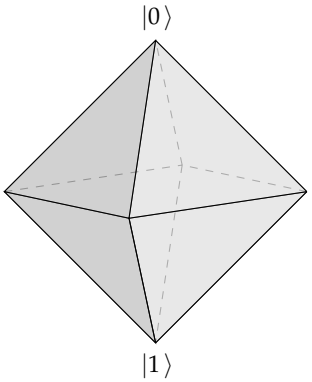


Figure 2.1: Bloch representation of the octahedron spanned by 1-qubit stabiliser states.

phases. Using Def. (2.6), the Clifford group is finite with a minimal centre $Z(\mathrm{Cl}_n) = Z(\mathcal{P}_n) = \langle i\mathbb{1} \rangle \simeq \mathbb{Z}_4$ [60, 87].

By definition, the Clifford group maps Pauli operators to Pauli operators while preserving commutativity and independence. Therefore, properties of stabiliser groups are preserved and $U \in \mathrm{Cl}_n$ maps the code $C_{\mathcal{S}}$ to a code $C_{U\mathcal{S}U^\dagger}$ of the same dimension. In fact, any two stabiliser codes of the same dimension are Clifford-equivalent. This is a straightforward consequence of Witt's theorem 3.1 which we will encounter at a later stage.[1] In particular, this implies that the set of stabiliser states is a Clifford orbit.

Although there is still a lot to say about e. g. error-correcting properties of stabiliser codes, let us focus on the mathematical structure of the formalism. An important feature is its simple and efficient description. As noted earlier, this can be done using geometry over the field $\mathbb{F}_2 \simeq \{0, 1\}$. To this end, we label the computational basis of $(\mathbb{C}^2)^{\otimes n}$ by vectors $x \in \mathbb{F}_2^n$ such that the action of the n-qubit X and Z operators can be written in terms of $a, b \in \mathbb{F}_2^n$ as follows

$$Z(a) \left| x \right\rangle = (-1)^{a \cdot x} \left| x \right\rangle, \quad X(b) \left| x \right\rangle = \left| x + b \right\rangle. \tag{2.7}$$

Note that all operations are over $\mathbb{F}_2$, i. e. they are performed mod 2. In this way, we can write an arbitrary Pauli operator as

$$W(u) = i^{-u_z \cdot u_x \bmod 4} \, Z(u_z) X(u_x), \quad \text{where } u = (u_z, u_x) \in \mathbb{F}_2^{2n}. \tag{2.8}$$

Here, the overall phase comes from the relation $Y = i^{-1} ZX$ and counts the number of Y operators in the tensor product.

As we have seen earlier, the Pauli operators fail to form a group because of additional phase factors which lead to a non-trivial centre $Z(\mathcal{P}_n) = \langle i\mathbb{1} \rangle$. Using the introduced notation, one finds

$$W(u)W(v) = i^{\beta(u,v)} \, W(u + v), \tag{2.9}$$

for some function β which will be discussed in Sec. 3.3. Let us stress at this point that there seems to be a common misunderstanding about the function β in the literature. It is often claimed that β is equal to the function $\Omega(u, v) = u_z \cdot v_x - v_z \cdot u_x \mod 4$. However, this is false, as a comparison with the multiplication table of the single-qubit Pauli operators shows (see Table 2.1).

[1] Alternatively, one can also prove this statement straightforwardly using some algebraic arguments. The logic, however, is the same as in the more general theorem of Witt.

$\times$	Z	Y	X
Z	$\mathbb{1}$	$-iX$	iY
Y	iX	$\mathbb{1}$	$-iZ$
Z	$-iY$	iZ	$\mathbb{1}$

Ω	$(1,0)$	$(1,1)$	$(0,1)$
$(1,0)$	0	1	1
$(1,1)$	-1	0	1
$(0,1)$	-1	-1	0

Table 2.1: Multiplication table of the Pauli operators on the left and the values of $\Omega(u,v) = u_z \cdot v_x - v_z \cdot u_x \mod 4$ on the 3 non-zero points of $\mathbb{F}_2^2$ corresponding to Pauli operators on the right. We see that $i^{\Omega(u,v)}$ does not yield the right phases for the entries marked in red.

By Eq. (2.9), the Pauli group forms a projective representation of the additive group of $\mathbb{F}_2^{2n}$ via the introduced map W. Conversely, the map $\pi : i^k W(u) \mapsto u$ is a group homomorphism with kernel $\ker \pi = Z(\mathcal{P}_n) = \langle i\mathbb{1} \rangle$. It induces an isomorphism $\mathcal{P}_n / Z(\mathcal{P}_n) \simeq \mathbb{F}_2^{2n}$ between the projective Pauli group and the discrete vector space $\mathbb{F}_2^{2n}$.[2] However, the non-Abelian structure of the Pauli group can be encoded in the geometry of $\mathbb{F}_2^{2n}$. Namely, one can show that the group commutator is given by

$$W(u)W(v) = (-1)^{[u,v]} W(v)W(u), \tag{2.10}$$

where

$$[u,v] := \sum_{i=1}^{n} u_i v_{n+i} + u_{n+i} v_i = u^\top J v, \quad \text{with } J = \begin{pmatrix} 0 & \mathbb{1} \\ \mathbb{1} & 0 \end{pmatrix}, \tag{2.11}$$

is the standard symplectic product[3] on $\mathbb{F}_2^{2n}$. Because of this symplectic structure, we refer to $\mathbb{F}_2^{2n}$ as "phase space".

The Clifford group induces an action on phase space by $UW(u)U^\dagger \propto W(Su)$ for some invertible map $S : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$. However, since

$$W(S(u+v)) \propto UW(u+v)U^\dagger \propto UW(u)U^\dagger UW(v)U^\dagger \propto W(S(u))W(S(v)), \tag{2.12}$$

this induced action is additive and thus also linear. As unitaries preserve commutation relations, the induced map S preserves the symplectic product, cp. Eq. (2.10), and is thus an element of the symplectic group:

$$\mathrm{Sp}(\mathbb{F}_2^{2n}) \equiv \mathrm{Sp}_{2n}(2) := \left\{ S \in \mathbb{F}_2^{2n \times 2n} \mid S^\top J S = J \right\} \tag{2.13}$$

By a slight abuse of notation, we will denote this induced action by $\pi : \mathrm{Cl}_n \to \mathrm{Sp}_{2n}(2)$. Similar to the above line of reasoning, one shows that $\pi(U^{-1}) = \pi(U)^{-1}$ and $\pi(UV) = \pi(U)\pi(V)$ and thus π is a group homomorphism. Conversely, given a $S \in \mathrm{Sp}_{2n}(2)$, one can construct a Clifford unitary U_S by defining it on the generators $Z_i = W(e_i)$ and $X_i = W(e_{n+i})$ of the Pauli group,

$$U_S Z_i U_S^\dagger := W(Se_i), \quad U_S X_i U_S^\dagger := W(Se_{n+i}), \tag{2.14}$$

and extend its action to the whole group. The Clifford unitary U_S is well-defined up to a global phase. This shows that π is also surjective. Finally we note that the induced action

[2] In group theoretic terms, this means that the quotient group $\mathcal{P}_n / Z(\mathcal{P}_n)$ is *elementary Abelian*.

[3] A symplectic product is a non-degenerate, alternating bilinear form.

of the Pauli group is always the identity by Eq. (2.10). Since these are the only diagonal channels in the Pauli basis, we have $\ker \pi = \mathcal{P}_n$ and thus $\mathrm{Cl}_n/\mathcal{P}_n \simeq \mathrm{Sp}_{2n}(2)$.

In particular, any Clifford unitary U is completely determined by a tuple (S, u) where $S \in \mathrm{Sp}_{2n}(2)$ and $u \in \mathbb{F}_2^{2n}$. The action of the Clifford unitary can be written as

$$UW(v)U^\dagger = (-1)^{[u,v]}(-1)^{g_S(v)}W(Sv), \tag{2.15}$$

where $g_S : \mathbb{F}_2^{2n} \to \mathbb{F}_2$ is a suitable function depending on S which will be derived later. There, we also show that if we deal with odd-dimensional systems, this function becomes trivial.

Finally, we derive the geometric representation of stabiliser codes. Given a stabiliser subgroup $\mathcal{S} < \mathcal{P}_n$, its projection on phase space is the set

$$M_\mathcal{S} = \pi(\mathcal{S}) = \left\{ u \in \mathbb{F}_2^{2n} \;\middle|\; (-1)^k W(u) \in \mathcal{S} \text{ for some } k \in \mathbb{F}_2 \right\}. \tag{2.16}$$

Note that because π is a group homomorphism, $M_\mathcal{S}$ is actually a linear subspace of $\mathbb{F}_2^{2n}$. In particular, given independent generators $g_1, \ldots, g_l$ of $\mathcal{S}$, their images $b_i = \pi(g_i)$ form a basis of $M_\mathcal{S}$. Moreover, since all elements in $\mathcal{S}$ commute, we find that the symplectic product has to vanish on $M_\mathcal{S}$. Such subspaces are called *isotropic*. One can show that the maximal dimension of an isotropic subspace is n. Such a maximal isotropic subspace is also called a *Lagrangian subspace* and thus corresponds to stabiliser states.

Note that the projection erases the phases of all Pauli operators in $\mathcal{S}$, thus many different stabiliser codes are mapped onto the same isotropic subspace. A natural question at this point is to ask whether all isotropic subspaces correspond to stabiliser codes and what can be said about the phases. We will answer this question in mathematical detail in Ch. 4, but let us state the basic idea at this point. For every isotropic subspace $M \subset \mathbb{F}_2^{2n}$ of dimension l, one fixes a basis $b_1, \ldots, b_l$ and picks a vector $x \in \mathbb{F}_2^l$. The corresponding stabiliser code is defined by the Abelian group $\langle (-1)^{x_1} W(b_1), \ldots, (-1)^{x_l} W(b_l) \rangle$. Moreover, the projector $P_{M,x}$ onto the code space can be written as

$$P_{M,x} := \prod_{i=1}^{l} \frac{1}{2}\left(\mathbb{1} + (-1)^{x_i} W(b_i)\right) = \frac{1}{|M|} \sum_{m \in M} (-1)^{f_x(m)} W(m), \tag{2.17}$$

for a suitable function $f_x : M \to \mathbb{F}_2$ that is completely determined by x and the composition law Eq. (2.9). Clearly, any stabiliser code of dimension 2^{n-l} has this form. Moreover, the projectors $P_{M,x}$ for varying x are actually orthogonal because they disagree in at least one eigenvalue of the generators $W(b_i)$. In particular, a Lagrangian subspace with $l = n$ represents 2^n orthonormal stabiliser states and therefore a basis of $(\mathbb{C}^2)^{\otimes n}$.

At this point, instead of deriving explicit formulas for e. g. the the overlap of stabiliser states, we will postpone this to Ch. 4, after having developed the more general framework. However, as a last remark, let us comment on how to use the phase space representation to efficiently simulate the Clifford dynamics of a stabiliser state ψ. The state is represented by a Lagrangian subspace L given by a basis $b_1, \ldots, b_n$ and a phase vector $x \in \mathbb{F}_2^n$. Any Clifford unitary is represented a symplectic matrix S and some Pauli operator $W(u)$. To compute the image of the state, we compute the basis $Sb_1, \ldots, Sb_n$ of $S(L)$. The signs are accordingly updated as $x \mapsto \tilde{x} = x + \sum_{i=1}^n \left([u, b_i] + g_S(b_i)\right) e_i$. Finally, to computer the expectation value of some Pauli operator $W(v)$, we get

$$\mathrm{tr}\left(U \left|\psi\right\rangle\!\left\langle\psi\right| U^\dagger W(v)\right) = \begin{cases} f_{\tilde{x}}(v) & \text{if } [v, Sb_i] = 0 \quad \forall i \in [n], \\ 0 & \text{else.} \end{cases} \tag{2.18}$$

These operations all involve basic linear algebra on $\mathbb{F}_2^{2n}$ and can be performed in time $O(n^2)$. Note that this procedure is more general than the Gottesman-Knill and Aaronson-Gottesman algorithms [40, 88] which only consider updates of the state with respect to fixed 2-local gates. Since those can be performed constant time, the algorithm scales with $O(n)$. The presented algorithm, however, computes updates with respect to arbitrary n-qubit gates.

CHAPTER 3

SYMPLECTIC STRUCTURES OVER FINITE FIELDS

In this chapter, we reverse the argumentation of the last chapter and start by introducing arbitrary finite fields, discrete symplectic groups and unitary representations thereof. The goal of the following sections is to introduce the mathematical background needed for a deeper understanding of the stabiliser formalism. Based on these concepts, we will see how familiar objects like stabiliser codes and Clifford unitaries emerge in Ch. 4. This can be understood as an axiomatic way of introducing the stabiliser formalism.

3.1 Finite fields and discrete symplectic vector spaces

The subject of finite fields is covered extensively in many textbooks and we refer the reader for more details to e. g. Refs. [89, 90]. An introduction to symplectic vector spaces can be found in textbooks on symplectic geometry, e. g. Refs. [91, 92].

3.1.1 Finite fields in a nutshell

A finite field is a field of finite *order*, i. e. with finitely many elements. The best known examples are finite fields of prime order p. Starting from the residue rings $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ of integers modulo p, it is a standard textbook exercise to show that $\mathbb{Z}_p$ is a field if and only if p is prime. In this sense, prime-order finite fields follow simple arithmetic rules.

However, there are also finite fields with a non-prime number of elements. Indeed, it is a classic result that finite fields exist if and only if their order q is a *prime-power* (i. e. $q = p^m$). Here p is the so-called *characteristic* of the field and m is the *(extension) degree*. Since it turns out that all finite fields of order q are isomorphic, they are unambiguously denoted as $\mathbb{F}_q$. These fields form so-called *Galois extensions* over their *base field* $\mathbb{F}_p$. Here, we omit the technical details of this construction and refer the interested reader to Sec. 6.1.1. Instead, we describe the structure of the *extension field* $\mathbb{F}_q = \mathbb{F}_{p^m}$.

First, $\mathbb{F}_p$ forms a subfield of $\mathbb{F}_q$ given by all elements $x \in \mathbb{F}_q$ such that $x^p = x$. The fact that this set is closed follows from the identity $(x+y)^p = x^p + y^p$ over finite fields of characteristic p.[1] It can be derived from the binomial theorem by noticing that all binomial coefficients – except the first and the last one – are divisible by p and thus vanish.

The additive group $\mathbb{F}_q^+ = (\mathbb{F}_q, +)$ of the field $\mathbb{F}_q$ has the structure of a vector space over $\mathbb{F}_p$ of dimension m. More precisely, the elements of $\mathbb{F}_q$ can be understood as *polynomials* in an element $\theta \in \mathbb{F}_q$ (called *root*) with coefficients in $\mathbb{F}_p$:

$$x = x_0 + x_1\theta + \cdots + x_{m-1}\theta^{m-1}, \qquad x_i \in \mathbb{F}_p. \tag{3.1}$$

In this representation, addition is simple since it only requires to add the coefficients.

The multiplicative group $\mathbb{F}_q^\times = (\mathbb{F}_q \setminus 0, \cdot)$ of $\mathbb{F}_q$ is cyclic, i. e. it is generated by a single element. Since $\mathbb{F}_q^\times$ has $q-1$ elements, this particularly implies that $x^{q-1} = 1$ for

[1] This is sometimes called "Freshman's dream".

any $x \in \mathbb{F}_q$. Any generator λ of the multiplicative group is called a *primitive element* of the field. Using λ, we can express any non-zero element in $\mathbb{F}_q$ by a *power representation* $x = \lambda^k$. The multiplication of two elements in power representation is simple since it only requires adding the exponents modulo $q - 1$.

Let us consider the multiplication by $x \in \mathbb{F}_q$ as a $\mathbb{F}_p$-linear map $M_x(y) = xy$ on the vector space $\mathbb{F}_q^+$. The so-called *field trace* is defined to be the linear trace of this map:

$$\operatorname{tr} x := \operatorname{tr} M_x. \tag{3.2}$$

By definition, this defines a $\mathbb{F}_p$-linear form $\mathbb{F}_q$ to $\mathbb{F}_p$. However, one can show that the field trace can be equivalently written as

$$\operatorname{tr} x = \sum_{j=0}^{m-1} x^{p^j}, \tag{3.3}$$

without referring to the map M_x. Let us verify that this indeed defines a $\mathbb{F}_p$-linear map from $\mathbb{F}_q$ to the subfield $\mathbb{F}_p$. An immediate consequence of the cyclicity of $\mathbb{F}_q^\times$ is that we have the identity $x^q = x$ for all $x \in \mathbb{F}_q$. Thus, we find

$$(\operatorname{tr} x)^p = \left(\sum_{j=0}^{m-1} x^{p^j}\right)^p = \sum_{j=0}^{m-1} x^{p^{j+1}} = \sum_{j=0}^{m-1} x^{p^j} = \operatorname{tr} x, \tag{3.4}$$

for all $x \in \mathbb{F}_q$. Similarly, one shows that $\operatorname{tr}(x + y) = \operatorname{tr} x + \operatorname{tr} y$ and $\operatorname{tr}(\alpha x) = \alpha \operatorname{tr} x$ for $x, y \in \mathbb{F}_q$ and $\alpha \in \mathbb{F}_p$. We can use the field trace to define a symmetric $\mathbb{F}_p$-bilinear form, the *trace inner product*,

$$\langle x, y \rangle := \operatorname{tr}(xy), \tag{3.5}$$

which can be shown to be non-degenerate and turns $\mathbb{F}_q^+$ into an orthogonal vector space.

Finally, we want to discuss the concept of a *field basis*. We have already given an example of such a basis, namely a *polynomial basis* in Eq. (3.1). More generally, given $b_1, \ldots, b_m \in \mathbb{F}_q$, we call them a basis if their $\mathbb{F}_p$-span is $\mathbb{F}_q$, i. e. if we can write any $x \in \mathbb{F}_q$ uniquely as

$$x = \sum_{i=1}^{m} x^i b_i, \quad \text{for some } x^i \in \mathbb{F}_p. \tag{3.6}$$

In other words, a field basis is exactly a $\mathbb{F}_p$-vector space basis for $\mathbb{F}_q^+$. In particular, any choice of basis induces a (non-canonical) vector space isomorphism between the additive group $\mathbb{F}_q^+$ and $\mathbb{F}_p^m$. The theory of vector spaces implies the existence of a *dual basis* $b^1, \ldots, b^m$ which fulfils $\operatorname{tr}(b_i b^j) = \delta_i^j$. Then any element $x \in \mathbb{F}_q$ can be written as

$$x = \sum_{i=1}^{m} x^i b_i = \sum_{i=1}^{m} x_i b^i, \qquad x_i = \operatorname{tr}(x b_i) \in \mathbb{F}_p,\ x^i = \operatorname{tr}(x b^i) \in \mathbb{F}_p. \tag{3.7}$$

We call a basis orthogonal if it is self-dual, i. e. its elements are mutually orthogonal with respect to the trace inner product.

3.1.2 Additive characters

A character of an Abelian group G is a homomorphism $\chi : G \to \mathbb{S}^1$ into the circle group $\mathbb{S}^1$. The set of characters form a group with pointwise multiplication, called the *Pontryagin dual* $\widehat{G}$. There are a lot of analogies with the concept of a dual vector space such as a canonical isomorphism from G into the dual of $\widehat{G}$ given by $g \mapsto (\chi \mapsto \chi(g))$. The characters of an Abelian group G are exactly characters in the representation-theoretic sense since all irreducible representations of G are one-dimensional and thus $\operatorname{tr}\tau \simeq \tau$ is a homomorphism into $\mathrm{U}(1) \simeq \mathbb{S}^1$ for any irrep τ. Moreover, $\widehat{G}$ is a basis for the group algebra $\mathbb{C}[G]$ which is orthonormal with respect to the *character inner product*

$$(\varphi, \psi) := \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)}\psi(g), \qquad \varphi, \psi \in \mathbb{C}[G]. \tag{3.8}$$

In the context of a finite field $\mathbb{F}_q$, with $q = p^m$, we are interested in characters of the additive group $\mathbb{F}_q^+$. Since any element $x \in \mathbb{F}_q$ has additive order p, any character χ has to obey

$$1 = \chi(0) = \chi(px) = \chi(x)^p. \tag{3.9}$$

Thus, the values of χ are in the p-th roots of unity. Given a primitive root, say $\omega = \exp(2\pi i/p)$, we can write $\chi(x) = \omega^{f(x)}$ where the function f has values in $\mathbb{F}_p$ which we can identify with $\mathbb{Z}_p$. For χ to be a homomorphism, the function f has to be additive and is thus a linear form $\mathbb{F}_q^+ \to \mathbb{F}_p$ on $\mathbb{F}_q$ seen as an $\mathbb{F}_p$-vector space. Since the trace inner product is non-degenerate, we can write $f(x) = \operatorname{tr}(ax)$ for some $a \in \mathbb{F}_q$ and hence we have shown that any additive character is of the form

$$\chi(x) = \omega^{\operatorname{tr}(ax)}. \tag{3.10}$$

Similarly one can show that the additive characters of a vector space V over $\mathbb{F}_q$ have the form $\xi(v) = \chi(\varphi(v))$ where χ is a character of $\mathbb{F}_q$ and $\varphi \in V^*$. Note that the linear form φ is uniquely determined by ξ and χ since

$$\chi(\varphi(v)) = \chi(\varphi'(v)) \quad \Rightarrow \quad \varphi(v) - \varphi'(v) \in \ker\chi \quad \forall v \in V, \tag{3.11}$$

which can only be the case if $\chi = 1$ is the trivial character. As above, we can explicitly write the character for some $a \in \mathbb{F}_q$ as:

$$\xi(v) = \omega^{\operatorname{tr}(a\varphi(v))} = \omega^{\operatorname{tr}\varphi(av)} = \omega^{\operatorname{tr}\tilde{\varphi}(v)}. \tag{3.12}$$

If V is equipped with a non-degenerate bilinear form b, we can express the linear form as $\tilde{\varphi}(v) = b(u, v)$ in the usual way.

We will often use characters of subspaces $W \subset V$ which are defined in the same fashion as above, since W is a vector space in its own right. However, there is a slight difference when we want to express a character ξ on W using a bilinear form b on V. In general, b is degenerate when restricted to W, hence there are multiple vectors u such that $\xi(w) = \chi([u, w])$ for all $w \in W$. Any two vectors $u, u' \in V$ define the same character if and only if

$$\forall w \in W : \quad [u - u', w] = 0, \quad \Leftrightarrow \quad u - u' \in W^\perp. \tag{3.13}$$

Hence, the characters $\widehat{W}$ on W are in one-to-one correspondence with the quotient space $V/W^\perp$.

3.1.3 Symplectic vector spaces and the symplectic group

A symplectic vector space is a vector space V over a field $\mathbb{F}$ equipped with a non-degenerate, alternating bilinear form ω. Such a form exists if and only if V is even-dimensional. The prototype of a symplectic space is $E \oplus E^*$ where E is an arbitrary vector space. It can be endowed with a canonical symplectic form τ given by

$$\tau(e \oplus \varepsilon, f \oplus \phi) := \varepsilon(e) - \phi(f). \tag{3.14}$$

In fact, any symplectic vector space (V, ω) is (non-canonically) isomorphic to $(E \oplus E^*, \tau)$ and E can be interpreted as a suitable subspace of V.

Definition 3.1. Given a subspace W of V, the *symplectic complement* of W is

$$W^\perp := \{v \in V \mid \omega(v, w) = 0 \quad \forall w \in W\}. \tag{3.15}$$

The subspace W is called

(i) *symplectic* iff $W^\perp \cap W = \{0\}$,

(ii) *isotropic* iff $W \subset W^\perp$,

(iii) *Lagrangian* iff it is isotropic and $\dim W = \dim V/2$.

Note that $(W^\perp)^\perp = W$. Since $W^\perp$ is defined via $\dim W$ independent linear constraints, its dimension is $\dim V - \dim W$. In particular, we have the dimension formula $\dim W + \dim W^\perp = \dim V$. This bounds the dimension of isotropic subspaces by $\dim V/2$ which motivates the definition of Lagrangian subspaces as maximally isotropic subspaces. Note that this also implies that any isotropic subspace can be extended to a Lagrangian subspace. In general, a subspace W is not a symplectic vector space on its own since the restriction of the symplectic form can be degenerate. This is exactly measured by $\ker \omega|_W = W^\perp \cap W$, thus symplectic subspaces are exactly the subspaces on which the symplectic form is non-degenerate. Their symplectic complements $W^\perp$ are symplectic subspaces, too, and thus we get a direct sum decomposition $V = W \oplus W^\perp$ in symplectic subspaces.

We call an invertible linear map $S : (V_1, \omega_1) \to (V_2, \omega_2)$ an *isometry* or *symplectomorphism* if it is compatible with the symplectic forms $S^*\omega_2 = \omega_1$. If $S \in \mathrm{Aut}(V)$ is an isometric automorphism of V, we call S a *symplectic map* on V. The symplectic maps from a group which is denoted by $\mathrm{Sp}(V, \omega)$. A classical result on isometries of quadratic forms by Witt [93] also applies to symplectic forms and restricts the action of symplectic maps.

Theorem 3.1 (Witt [93])**.** *Suppose $W_1, W_2 \subset V$ are subspaces of a symplectic vector space (V, ω) and $h : W_1 \to W_2$ is a (bijective) isometry. Then, there is a symplectic map $\tilde{h} \in \mathrm{Sp}(V, \omega)$ which extends h, i. e. $\tilde{h}|_{W_1} = h$.*

Note that Witt's theorem has several implications. Take the case where W_1, W_2 are isotropic subspaces of the same dimension k. Then, any bijective linear map $h : W_1 \to W_2$ is an isometry and thus extends to a symplectic map $\tilde{h}$ on V. This means that $\mathrm{Sp}(V, \omega)$ acts transitively on the Grassmannian of k-dimensional isotropic subspaces of V. As we will see in Ch. 4, this directly implies that there is a transitive action of the Clifford group on *stabiliser codes*.

A basis $e_1, \ldots, e_n, f_1, \ldots, f_n$ of V is called *symplectic* or a *Darboux basis* if the following holds:

$$\omega(e_i, e_j) = \omega(f_i, f_j) = 0, \qquad \omega(e_i, f_j) = \delta_{ij}. \tag{3.16}$$

Thus, the subspaces E and F spanned by e_i and f_j, respectively, are Lagrangian. Using the isomorphism $V \to V^*$ introduced by the non-degenerate bilinear form ω, we can interpret the second condition as F being isomorphic to the dual space E^*. Hence, a symplectic basis is a basis choice inducing an explicit symplectic isomorphism $V \simeq E \oplus E^*$ between the symplectic vector space (V, ω) and $(E \oplus E^*, \tau)$ with its canonical form τ. Such a choice of isomorphism is called a *polarisation* of V.

With respect to a symplectic basis, ω is represented by

$$\omega(v, w) = v^\top J w, \qquad J = \begin{pmatrix} 0 & \mathbb{1} \\ -\mathbb{1} & 0 \end{pmatrix}. \tag{3.17}$$

This explicitly gives an isometry between the symplectic vector space (V, ω) and $\mathbb{F}^{2n}$ with its standard symplectic form

$$[v, w] := v^\top J w = \sum_{i=1}^{n} v_i w_{n+i} - w_i v_{n+i}. \tag{3.18}$$

In particular, this shows that the group $\mathrm{Sp}(V, \omega)$ of symplectic maps on V is isomorphic to the standard *symplectic group*:

$$\mathrm{Sp}_{2n}(\mathbb{F}) := \left\{ S \in \mathbb{F}^{2n \times 2n} \;\middle|\; S^\top J S = J \right\}. \tag{3.19}$$

For later reference, we state here the order of the symplectic group for finite fields $\mathbb{F} = \mathbb{F}_q$ [94]:

$$|\mathrm{Sp}_{2n}(\mathbb{F}_q)| = q^{n^2} \prod_{i=1}^{n} \left(q^{2i} - 1 \right). \tag{3.20}$$

3.1.4 An explicit set of generators of the symplectic group

The symplectic group plays a prominent role in the stabiliser formalism, which is why we want to dedicate this section to a brief summary of some properties. For the remaining paper, the following subgroups will be important:

$$S_n(\mathbb{F}) := \left\{ S(R) := \begin{pmatrix} \mathbb{1} & R \\ 0 & \mathbb{1} \end{pmatrix} \;\middle|\; R \in \mathrm{Sym}_n(\mathbb{F}) \right\}, \tag{3.21}$$

$$G_n(\mathbb{F}) := \left\{ G(Q) := \begin{pmatrix} Q^{-\top} & 0 \\ 0 & Q \end{pmatrix} \;\middle|\; Q \in \mathrm{GL}_n(\mathbb{F}) \right\}. \tag{3.22}$$

One readily verifies that these matrices are symplectic and that $S_n(\mathbb{F})$ and $G_n(\mathbb{F})$ correspond to representations of the Abelian group of symmetric matrices $\mathrm{Sym}_n(\mathbb{F})$ and the group of invertible matrices $\mathrm{GL}_n(\mathbb{F})$, respectively. In particular, we have

$$S(R_1)S(R_2)^{-1} = S(R_1 - R_2), \quad G(Q_1)G(Q_2)^{-1} = G(Q_1 Q_2^{-1}). \tag{3.23}$$

From a physical perspective, the subgroup $G_n(\mathbb{F})$ is the group of symplectic transformations induced from transformations of the configuration space $\mathbb{F}^n$ and is sometimes

called "point transformations" in classical mechanics. In the mathematical literature, the group $S_n(\mathbb{F})$ is sometimes called the *Siegel unipotent subgroup* of $\mathrm{Sp}_{2n}(\mathbb{F})$. Note that $G_n(\mathbb{F})$ normalises $S_n(\mathbb{F})$

$$G(Q)^{-1}S(R)G(Q) = S(Q^\top RQ), \tag{3.24}$$

and thus their span is the semidirect product $P_n(\mathbb{F}) := S_n(\mathbb{F}) \rtimes G_n(\mathbb{F})$. The subgroup $P_n(\mathbb{F})$ is called the *Siegel parabolic subgroup* of $\mathrm{Sp}_{2n}(\mathbb{F})$ and is exactly the subgroup which stabilises the Lagrangian subspace spanned by $e_1, \ldots, e_n$. As we saw before, $\mathrm{Sp}_{2n}(\mathbb{F})$ acts transitively on Lagrangian subspaces and thus any stabiliser of a Lagrangian subspace is isomorphic to $P_n(\mathbb{F})$.

The Siegel parabolic subgroup can be equivalently characterised as the group of symplectic matrices with zeros in the lower left block. In particular, J is not an element of $P_n(\mathbb{F})$. However, one can show that $P_n(\mathbb{F}) = S_n(\mathbb{F}) \rtimes G_n(\mathbb{F})$ and J span the whole symplectic group [95]. Thus, a possible set of generators for $\mathrm{Sp}_{2n}(\mathbb{F})$ is given by generators for $S_n(\mathbb{F})$ and $G_n(\mathbb{F})$, supplemented by J. In the later Sec. 5.3.2, we give an algorithm which efficiently decomposes any symplectic matrix into at most two matrices from $S_n(\mathbb{F})$, $G_n(\mathbb{F})$ and J.

Up to now, the introduced concepts were valid for any field $\mathbb{F}$. In order to state explicit generators of the symplectic group, we assume that $\mathbb{F} = \mathbb{F}_q$ for $q = p^m$ and write $\mathrm{Sp}_{2n}(q) \equiv \mathrm{Sp}_{2n}(\mathbb{F}_q)$. Note that since N and G form representations, we can restrict our attention to generators of $\mathrm{Sym}_n(q)$ and $\mathrm{GL}_n(q)$. This set of generators is both natural and motivated from their later interpretation [96]. We denote by $E_{ij} := e_i e_j^\top$ the $n \times n$ matrix having a one in the (i,j)-th entry and zeros elsewhere. Then clearly, the following matrices generate $\mathrm{Sym}_n(q)$:

$$S_i(a) := aE_{ii}, \quad CZ_{ij}(a) := a(E_{ij} + E_{ji}) \quad \forall a \in \mathbb{F}_q. \tag{3.25}$$

Explicitly, any symmetric matrix $R = (r_{ij})$ can be written as

$$R = \sum_{i=1}^{n} S_i(r_{ii}) + \sum_{i<j} CZ_{ij}(r_{ij}). \tag{3.26}$$

Here, we already used a suggestive notation which will become clear in Ch. 4.

Let us now construct generators for $\mathrm{GL}_n(q)$. To this end, consider first the subgroup of invertible lower triangular matrices. Any such matrix can be written as a product of a lower unitriangular matrix (i. e. has ones on the diagonal) and a non-singular diagonal matrix. Lower unitriangular matrices can be decomposed as products of

$$CX_{ij}(a) := \mathbb{1} + aE_{ji}, \quad \text{for } i < j. \tag{3.27}$$

This is because multiplication of lower unitriangular matrices corresponds to the addition of their strictly lower triangular parts. Thus, any lower unitriangular matrix can be written as

$$L = \prod_{i<j} CX_{ij}(L_{ij}). \tag{3.28}$$

By transposition, we get the same decomposition for upper unitriangular matrices in terms of

$$CX_{ij}(a) := \mathbb{1} + aE_{ji}, \quad \text{for } i > j. \tag{3.29}$$

Note that $M_i(a) := CX_{ii}(a-1)$ is the diagonal matrix with a in the i-th entry and ones else ("local multiplication by a"). Those clearly generate all diagonal matrices. This shows that the matrices $CX_{ij}(a)$ generate the group spanned by invertible upper and lower triangular matrices.

To decompose an arbitrary $Q \in \mathrm{GL}_n(q)$, we can make use of a PLDU decomposition,

$$Q = PLDU \tag{3.30}$$

where P is a permutation matrix, L and U are lower and upper unitriangular matrices, respectively, and D is a nonsingular diagonal matrix. We can decompose the permutation P in terms of transpositions π_{ij}, and use the familiar identity

$$\pi_{ij} = CX_{ij}CX_{ji}CX_{ij}, \tag{3.31}$$

where $CX_{ij} \equiv CX_{ij}(1)$. Together with the previous discussion, this shows that any $Q \in \mathrm{GL}_n(q)$ can be written as a product of $CX_{ij}(a)$.

Note that there is a certain redundancy in our definition of generators. Let g be any of the above generators and be $\bullet$ the group operation in $\mathrm{Sym}_n(q)$ or $\mathrm{GL}_n(q)$, respectively. Then we have the identity

$$g(a+b) = g(a) \bullet g(b), \quad \forall a, b \in \mathbb{F}_q. \tag{3.32}$$

In particular, for $x \in \mathbb{F}_p$ in the prime field and $a \in \mathbb{F}_q$, we find

$$g(xa) = g(a + \cdots + a) = g(a) \bullet \cdots \bullet g(a). \tag{3.33}$$

This means that we only have take generators on a *basis* of $\mathbb{F}_q$. The group operations will automatically generate the remaining ones. Let us summarise this result concisely as a proposition:

Proposition 3.1 (Generators of $\mathrm{Sp}_{2n}(q)$)**.** *Let $q = p^m$ for p prime, and let $b_1, \ldots, b_m$ be a basis for $\mathbb{F}_q$. Define $S_i(a), CZ_{ij}(a), M_i(a), CX_{ij}(a)$ as before. Then, the symplectic group $\mathrm{Sp}_{2n}(q)$ is generated by the following matrices for $i \neq j \in [n]$ and $\mu \in [m]$:*

$$J,\ S(S_i(b_\mu)),\ S(CZ_{ij}(b_\mu)),\ G(M_i(b_\mu)),\ G(CX_{ij}(b_\mu)). \tag{3.34}$$

From Sec. 3.1, we know that all non-zero elements in $\mathbb{F}_q$ can be written as powers of a *primitive element*. With this, it is possible to give a reduced set of generators:

Proposition 3.2 (Alternative generators of $\mathrm{Sp}_{2n}(q)$)**.** *Let $\lambda \in \mathbb{F}_q^\times$ be a primitive element. Then, the symplectic group $\mathrm{Sp}_{2n}(q)$ is generated by the following matrices for $i \neq j \in [n]$:*

$$J_i,\ S(S_i(\lambda)),\ G(CX_{ij}),\ G(M_i(\lambda)). \tag{3.35}$$

Here, J_i is the local application of J to the i-th coordinate pair. If q is even, then we can replace $S(S_i(\lambda))$ by $S(S_i)$.

In fact, it is enough for both propositions to have all gates except the CX generators for some index i respectively $i \neq j$, since by using Eq. (3.31), we can implement any transposition via CX to swap the indices to any desired pair.

To show Prop. 3.2, let us compute the action of $M_i(\lambda)$ for an arbitrary $\lambda \in \mathbb{F}_q$ on the generators $S_i(a), CZ_{ij}(a)$ and $CX_{ij}(a)$. Using Eq. (3.24), we find for $i \neq j$:

$$G(M_i(\lambda))^{-1} S(S_i(a)) G(M_i(\lambda)) = S(S_i(a\lambda^2)), \tag{3.36}$$

$$G(M_i(\lambda))^{-1} S(CZ_{ij}(a)) G(M_i(\lambda)) = S(CZ_{ij}(a\lambda)), \tag{3.37}$$

$$M_i(\lambda) CX_{ij}(a) M_i(\lambda)^{-1} = CX_{ij}(a\lambda). \tag{3.38}$$

If we choose $\lambda \in \mathbb{F}_q^\times$ to be primitive, we can write any $a \in \mathbb{F}_q^\times$ as $a = \lambda^r$ and likewise $M_i(\lambda^r) = M_i(\lambda)^r$. Thus, by Eqs. (3.37) and (3.38), we see that $M_i(\lambda)$ together with CZ_{ij} and CX_{ij} generate the last three gate families in Eq. (3.34). However, because of Eq. (3.36), this is generally not true for the S-family since λ^2 may fail to generate $\mathbb{F}_q^\times$. It turns out that this is precisely the case when p is odd due to the following basic group-theoretic fact:

Lemma 3.1. *Let G be a cyclic group. If $a \in G$ has order m, then a^r has order $m/\gcd(m,r)$.*

Given a primitive element $\lambda \in \mathbb{F}_q^\times$, it has order $q-1$, thus λ^2 has order $q-1/\gcd(q-1,2)$ and is primitive if and only if $\gcd(q-1,2) = 1 \Leftrightarrow q$ is even $\Leftrightarrow p = 2$. Thus, if $p = 2$, it is sufficient to supplement the generators evaluated at $a = 1$ with the multiplication gate $M_i(\lambda)$. Furthermore, Lemma 3.1 implies that for $p \neq 2$, there is no $\xi \in \mathbb{F}_q^\times$ such that ξ^2 is primitive since ξ would have order $2(q-1)$. Hence, for $p \neq 2$, we need the generator $S_i(\lambda)$ in addition to $M_i(\lambda)$ for $\lambda \in \mathbb{F}_q^\times$ primitive.

Finally, let us define J_i as the local application of J to the i-th symplectic pair, i. e. J_i acts as $(e_1, \ldots, e_n, f_1, \ldots, f_n) \mapsto (e_1, \ldots, -f_i, \ldots, e_n, f_1, \ldots, e_i, \ldots, f_n)$. Then, we have the identities $J = J_1 \cdots J_n$ and $J_j S(CZ_{ij}) J_j^{-1} = G(CX_{ij})^{-1}$ and hence we can remove CZ as a generator.

3.2 The Weil representation in odd characteristic

In this section, we introduce a unitary representation of the symplectic group $\mathrm{Sp}_{2n}(q)$ on the Hilbert space $\mathbb{C}[\mathbb{F}_2^{2n}] \simeq (\mathbb{C}^q)^{\otimes n}$ which goes back to works by Weil [83]. In fact, André Weil constructed this representation for symplectic groups over an arbitrary local field $\mathbb{F}$. As Weil showed, this representation is a *projective* one which can be lifted to a linear representation of a double cover of the symplectic group, the *metaplectic group*. The Weil representation over the real numbers and its relation to quantum mechanics is extensively discussed in the literature, e. g. in Ref. [97]. For finite fields of odd characteristic, $\mathbb{F} = \mathbb{F}_q$, this *metaplectic* or *Weil representation* can be linearised and descends to the mentioned unitary representation of $\mathrm{Sp}_{2n}(q)$ [98]. However, this construction only works in odd characteristic [86, 99, 100]. In the important qubit case $p = 2$, the structure of the underlying symplectic space changes qualitatively as will be discussed in Sec. 3.3. Then, only a somewhat similar projective representation of a bigger group containing $\mathrm{Sp}_{2n}(2^m)$ can be recovered which eventually leads to a more complicated formalism.

We introduce Weil's important unitary representation of the symplectic group following the explicit construction by Neuhauser [95]. We start by introducing the *Heisenberg group* $\mathrm{H}_n(q)$ of the symplectic vector space $\mathbb{F}_q^{2n}$ as the set $\mathbb{F}_q^{2n} \times \mathbb{F}_q$ with the non-Abelian composition law

$$(v,t) \bullet (w,s) := (v+w,\ t+s+2^{-1}[v,w]). \tag{3.39}$$

From a mathematical point of view, the Heisenberg group $\mathrm{H}_n(q)$ is a *central extension* of the phase space $\mathbb{F}_q^{2n}$ by $\mathbb{F}_q$. This is discussed in detail in Sec. 6.2.2. Since $(v,t)^{-1} = (-v,-t)$, we find

$$(v,t) \bullet (w,s) \bullet (v,t)^{-1} = (w, s + [v,w]). \tag{3.40}$$

Thus, we can deduce that (w,s) is in the centre if and only if $w = 0$, hence $Z(\mathrm{H}_n(q)) \simeq \mathbb{F}_q$. Moreover, we see that the *inner automorphism group* of $\mathrm{H}_n(q)$ can be identified with linear forms $\varphi(w) = [v,w]$ on $\mathbb{F}_q^{2n}$. A straightforward calculation (cp. Sec. 6.2.2) shows that any automorphism of $\mathrm{H}_n(q)$ which fixes its centre has the form $(v,t) \mapsto (g(v), t + \alpha(v))$, where $g \in \mathrm{GL}_{2n}(q)$ and α is a function fulfilling

$$2^{-1}[g(v),g(w)] - 2^{-1}[v,w] = \alpha(v+w) - \alpha(v) - \alpha(w). \tag{3.41}$$

Since the right hand side is symmetric and the left hand side is anti-symmetric it is necessary that

$$[g(v),g(w)] - [v,w] = 0 = 2\left(\alpha(v+w) - \alpha(v) - \alpha(w)\right). \tag{3.42}$$

Thus, we can conclude that g is symplectic, α is a linear form (since since 2 is invertible in odd characteristic), and their choice is independent. Since linear forms correspond to inner automorphisms, the centre-fixing outer automorphisms are given by $\mathrm{Sp}_{2n}(q)$. The total group of (centre-fixing) automorphisms can thus be identified with the *affine symplectic group* $\mathrm{ASp}_{2n}(q) \simeq \mathrm{Sp}_{2n}(q) \ltimes \mathbb{F}_q^{2n}$.

Next, we construct a unitary representation of $\mathrm{H}_n(q)$ on the function space $\mathbb{C}[\mathbb{F}_q^n] \simeq (\mathbb{C}^q)^{\otimes n}$. To this end, let us fix an additive character χ of $\mathbb{F}_q$, i. e. a homomorphism $\chi : \mathbb{F}_q \to \mathbb{S}^1$ of the additive group of $\mathbb{F}_q$. Recall that any such character can be written as $\chi(a) = \omega^{\mathrm{tr}(ax)}$ for $x \in \mathbb{F}_q$ and $\omega = \exp(2\pi i/p)$. Furthermore, we fix a polarisation $\mathbb{F}_q^{2n} = E \oplus F$ which we can without loss of generality assume to be the one induced by the standard symplectic basis, i. e. $E = \langle e_1, \ldots, e_n\rangle$ and $F = \langle f_1, \ldots, f_n\rangle$. In later applications, we will often denote $E =: \mathsf{Z}_n$ and $F =: \mathsf{X}_n$, and call them the Z and X Lagrangian. Let us denote the corresponding coordinates as $z = (z_1, \ldots, z_n)$ and $x = (x_1, \ldots, x_n)$. Then, we define the *Schrödinger representation* (also: *Weyl representation*) as the following unitary representation on $\mathbb{C}[\mathbb{F}_q^n]$:

$$W_\chi(z,x,t)f(u) := \chi(t + z\cdot u + 2^{-1} z\cdot x) f(u+x). \tag{3.43}$$

By definition, we have $W_\chi(z,x,t) = \chi(t) W_\chi(z,x,0)$. We call the operators $W_\chi(z,x) \equiv W_\chi(z,x,0)$ the *Weyl operators* on $\mathbb{C}[\mathbb{F}_q^n]$.[2]

It is easy to see that W_χ is traceless except for the centre $Z(\mathrm{H}_n(q))$, where $W_\chi(0,0,t) = \chi(t)\,\mathrm{id}$. In particular, this implies that W_χ is irreducible since the character inner product is

$$\begin{aligned}(W_\chi, W_\chi) &= \frac{1}{|\mathrm{H}_n(q)|} \sum_{h \in \mathrm{H}_n(q)} |\operatorname{tr} W_\chi(h)|^2 = \frac{1}{q^{2n+1}} \sum_{t \in \mathbb{F}_q} |\chi(t) \operatorname{tr} \mathrm{id}|^2 \\ &= \frac{1}{q^{2n+1}} q q^{2n} = 1.\end{aligned} \tag{3.44}$$

[2] After Herrmann Weyl, who used representations of the Heisenberg group as a basis for the quantisation of phase space.

The orthogonality of two distinct characters $\chi \neq \tilde{\chi}$ implies that $(W_\chi, W_{\tilde{\chi}}) = 0$ and thus the representations are unitarily non-equivalent. Moreover, any representation which *is* unitarily equivalent to W_χ has to agree with it on the centre. Conversely, given an arbitrary irreducible representation ρ of $\mathrm{H}_n(q)$ on $\mathbb{C}[\mathbb{F}_q^n]$, irreducibility implies that on the centre $\rho(0,t) = \gamma(t)\mathrm{id}$, where γ is a character of $\mathbb{F}_q$. Thus, it holds

$$\rho(v,t)\rho(w,s)\rho(v,t)^{-1} = \rho(w, s + [v,w]) = \gamma([v,w])\rho(w,s). \tag{3.45}$$

By taking the trace on both sides, we see that $\operatorname{tr}\rho(w,s) = 0$ for all $w \neq 0$. Hence, the character inner product of ρ with W_γ is analogous to Eq. (3.44) and shows that the two representations are equivalent. In summary, two irreducible representations of $\mathrm{H}_n(q)$ are unitarily equivalent if and only if they agree on the centre. This is the *Stone-von Neumann theorem* for finite fields.

As the symplectic group $\mathrm{Sp}_{2n}(q)$ naturally acts as automorphisms of the Heisenberg group $\mathrm{H}_n(q)$, we obtain from the irreducible Schrödinger representation W of $\mathrm{H}_n(q)$ another irreducible representation $W_g = W \circ g$, which agrees with W on the centre $Z(\mathrm{H}_n(q))$. By the Stone-von Neumann theorem, W_g is unitarily equivalent to W, i. e. there is a unitary operator $\mu(g)$ such that

$$W_g(v,t) = \mu(g)W(v,t)\mu(g)^{-1}, \quad \forall (v,t) \in \mathrm{H}_n(q). \tag{3.46}$$

The operator $\mu(g)$ is uniquely determined up to a phase and thus defines a projective representation of $\mathrm{Sp}_{2n}(q)$, called the *metaplectic* or *Weil representation*. The uniqueness implies that

$$\mu(gh) = c(g,h)\mu(g)\mu(h), \tag{3.47}$$

for all $g, h \in \mathrm{Sp}_{2n}(q)$ and some function $c(g,h) \in S^1$. Note that c has to fulfil the consistency condition $c(g,hk)c(h,k) = c(gh,k)c(g,h)$ for $g,h,k \in \mathrm{Sp}_{2n}(q)$ following from associativity.

It is well known that a projective representation μ can be turned into a faithful unitary representation ν if and only if there exists a function κ such that $c(g,h) = \kappa(g)\kappa(h)\kappa(gh)^{-1}$ and in this case $\nu(g) = \kappa(g)\mu(g)$. We will show in the following, that for the Weil representation such a function κ can be found and give an explicit formula. To this end, we will study the irreducible subrepresentations of μ. For later applications it will be useful to make a concrete choice for μ, although this is not necessary to show the existence of κ. We define μ on the generators introduced in Sec. 3.1.3 as follows.

Theorem 3.2 (Weil representation on generators)**.** *We can choose μ to fulfil*

$$\mu(S(R))f(u) := \chi(2^{-1}u^\top Ru)f(u), \tag{3.48}$$

$$\mu(G(Q))f(u) := f(Qu), \tag{3.49}$$

$$\mu(J)f(u) := \frac{1}{\sqrt{q^n}} \sum_{v \in \mathbb{F}_q^n} \chi(u \cdot v)f(v), \tag{3.50}$$

where $R \in \mathrm{Sym}_n(q)$ and $Q \in \mathrm{GL}_n(q)$.

Proof. This can be checked via direct computation, for instance

$$\begin{aligned}
&\mu(J)W(z,x,t)\mu(J)^{-1}f(u)\\
&= \frac{1}{\sqrt{q^n}}\sum_{v\in\mathbb{F}_q^n}\chi(t+z\cdot v+2^{-1}z\cdot x)\chi(-u\cdot v)\mu(J)f(v+x)\\
&= \frac{1}{q^n}\sum_{w\in\mathbb{F}_q^n}\chi(t+2^{-1}z\cdot x)\chi(x\cdot w)f(w)\sum_{v\in\mathbb{F}_q^n}\chi(w\cdot v)\chi(-(u-z)\cdot v)\\
&= \chi(t+x\cdot u-2^{-1}x\cdot z)f(u-z)\\
&= W(J(z,x),t)f(u).
\end{aligned}$$

□

Lemma 3.2. *The subspaces*

$$\begin{aligned}
V^+ &:= \left\{f\in\mathbb{C}[\mathbb{F}_q^n]\;\middle|\; f(-u)=f(u)\forall u\in\mathbb{F}_q^n\right\},\\
V^- &:= \left\{f\in\mathbb{C}[\mathbb{F}_q^n]\;\middle|\; f(-u)=-f(u)\forall u\in\mathbb{F}_q^n\right\},
\end{aligned}\tag{3.51}$$

are invariant under μ.

Proof. Since $\mu(-\mathbb{1})f(u) = \mu(G(-\mathbb{1}))f(u) = f(-u) = \pm f(u)$ for $f\in V^\pm$, these subspaces are exactly the eigenspaces of $\mu(-\mathbb{1})$. Note that $-\mathbb{1}$ is in the centre of $\mathrm{Sp}_{2n}(q)$. Thus, if $f\in V^\pm$ is an eigenfunction, so is $\mu(g)f\in V^\pm$. This shows that $V^\pm$ are invariant subspaces w.r.t. μ. □

Theorem 3.3. *The Weil representation μ acts irreducibly on $V^\pm$ and these representations are inequivalent.*

Proof. We use Schur's lemma to show that μ acts irreducibly on $V^\pm$. Consider linear operators $T^\pm$ on $V^\pm$ that commute with the restricted representations $\mu^\pm = \mu|_{V^\pm}$. Thus, they define a linear operator on $\mathbb{C}[\mathbb{F}_q^n]$ by $T = T^+\oplus T^-$ which commutes with μ. In particular, T commutes with the action of $S_n(q)$, which yields the following identity when evaluated on the basis $\delta_x \equiv |x\rangle$:

$$\begin{aligned}
&\langle y|\, T\mu(S(R))\,|x\rangle = \langle y|\,\mu(S(R))T\,|x\rangle\\
\Leftrightarrow\;&\chi(-2^{-1}x^\top Rx)T_{yx} = \chi(-2^{-1}y^\top Ry)T_{yx}
\end{aligned}\tag{3.52}$$

Now, assume that y and x are such that $T_{yx}\neq 0$. Then, we will shown that this can only be the case if $y=\pm x$. By assumption, $\chi(-2^{-1}x^\top Rx) = \chi(-2^{-1}y^\top Ry)$ for all $R\in\mathrm{Sym}_n(q)$. Since any non-trivial character is of the form $\chi(a)=\omega^{\mathrm{tr}(ba)}$ for some $b\in\mathbb{F}_q^\times$, we have $\mathrm{tr}(bx^\top Rx) = \mathrm{tr}(by^\top Ry)$ for all $R\in\mathrm{Sym}_n(q)$. However, multiplication by $b\neq 0$ is a bijection on $\mathrm{Sym}_n(q)$ and thus this is equivalent to $\mathrm{tr}(x^\top Rx) = \mathrm{tr}(y^\top Ry)$ for all $R\in\mathrm{Sym}_n(q)$. Repeating the same argument, we can thus deduce that

$$\mathrm{tr}(cx^\top Rx) = \mathrm{tr}(cy^\top Ry),\qquad \forall R\in\mathrm{Sym}_n(q), c\in\mathbb{F}_q^\times.\tag{3.53}$$

By the non-degeneracy of the trace inner product, this is the case if and only if $x^\top Rx = y^\top Ry$ for all $R\in\mathrm{Sym}_n(q)$. Evaluating this expression for $R = e_ie_j^\top + e_je_i^\top$ yields $x_ix_j =$

$y_i y_j$ for all $i, j \in [n]$. Let us assume that $x \neq 0$ and hence there is a k such that $x_k \neq 0$. Taking $i = j = k$ in the former equation, it becomes $x_k^2 = y_k^2$, and thus we also find $y_k \neq 0$. Thus, setting $j = k$, we can invert the equation to obtain $y_i = y_k^{-1} x_k x_i$ for all i. Since $y_k^{-1} x_k \in \{\pm 1\}$, this implies $y = \pm x$. In the case $x = 0$, we have $y = 0$, too, thus this equation holds trivially. In summary, we have shown that T_{yx} can only be non-zero if $y = \pm x$.

Next, let us define a suitable basis for V^+ and V^-. Let X be a set of representatives of $\mathbb{F}_q^n / \{-\mathrm{id}\}$ without 0. Note that since q is odd, $|X| = \frac{1}{2}(q^n - 1)$. Defining $|x^\pm\rangle := \frac{1}{\sqrt{2}}(|x\rangle \pm |-x\rangle)$, an orthonormal basis for V^+ is $B^+ := \{|x^+\rangle \mid x \in X\} \cup \{|0\rangle\}$ and one for V^- is $B^- := \{|x^-\rangle \mid x \in X\}$. This immediately gives $\dim V^+ = \frac{1}{2}(q^n + 1)$ and $\dim V^- = \frac{1}{2}(q^n - 1)$, showing that if the representations are both irreducible, they have to be inequivalent.

The above argumentation implies that $T^\pm$ is diagonal in the respective basis $B^\pm$ with components given by $T^+_{x,x} = \frac{1}{2}(T_{x,x} + T_{x,-x})$ and $T^-_{x,x} = \frac{1}{2}(T_{x,x} - T_{x,-x})$. We compute for $y, x \in X$:

$$\sqrt{q^n}\, \langle y^+ | \, T^+ \mu^+(J) \, |0\rangle = \langle y^+ | \, T^+ \left(|0\rangle + \sum_{x \in X} |x^+\rangle \right) = T^+_{y,y}. \tag{3.54}$$

However, we also find

$$\sqrt{q^n}\, \langle y^+ | \, \mu^+(J) T^+ \, |0\rangle = \sqrt{q^n}\, T^+_{0,0} \, \langle y^+ | \, \mu^+(J) \, |0\rangle = T^+_{0,0}. \tag{3.55}$$

Since T^+ commutes with $\mu^+(J)$, we have $T^+ = T^+_{0,0}\,\mathrm{id}$. Next, we find

$$\begin{aligned} \langle y^+ | \, T^- \mu^-(G(Q)) \, |x^-\rangle &= \langle y^+ | \, T^- \, |Qx^-\rangle = T^-_{y,y} \langle y^+ | Qx^- \rangle, \\ \langle y^+ | \, \mu^-(G(Q)) T^- \, |x^-\rangle &= T^-_{x,x} \langle y^+ | Qx^- \rangle, \end{aligned} \tag{3.56}$$

for all $y, x \in X$. We can assume that $x = Q^{-1} y \in X$ (otherwise $-x$ is), and then find $\langle y | Qx^- \rangle = 1$. This results in $T^-_{y,y} = T^-_{Q^{-1}y, Q^{-1}y}$ for all $Q \in \mathrm{GL}_n(q)$. Since $\mathrm{GL}_n(q)$ acts transitively on $\mathbb{F}_q^n$ this implies that $T^- = t\,\mathrm{id}$ for some $t \in \mathbb{F}_q$.

In summary, we have shown that all linear maps $T^\pm$ on $V^\pm$ which commute with $\mu^\pm$ are proportional to the identity. By Schur's lemma, this can only be the case if $\mu^\pm$ is irreducible. Since the dimensions of V^+ and V^- are different, they can not be equivalent. □

Finally, we explicit construct the function κ which yields a faithful unitary representation $\nu = \kappa\mu$. Note that we have the relation $\mu(gh) = c(g,h)\mu(g)\mu(h)$ as well as the relation $\mu^+(gh) = c(g,h)\mu^+(g)\mu^+(h)$ by restricting to V^+. Taking determinants in both relations results in

$$\begin{aligned} \det \mu(gh) &= c(g,h)^{q^n} \det \mu(g) \det \mu(h), \\ \det \mu^+(gh) &= c(g,h)^{\frac{1}{2}(q^n+1)} \det \mu^+(g) \det \mu^+(h). \end{aligned} \tag{3.57}$$

Division of the square of the second equation by the first one yields

$$c(g,h) = \frac{\det \mu^+(gh)^2}{\det \mu(gh)} \frac{\det \mu(g)}{\det \mu^+(g)^2} \frac{\det \mu(h)}{\det \mu^+(h)^2} = \frac{\kappa(g)\kappa(h)}{\kappa(gh)}, \tag{3.58}$$

for $\kappa(g) = \det \mu(g) \det \mu^+(g)^{-2} = \det \mu^-(g) \det \mu^+(g)^{-1}$.

Remark 3.1. As in Theorem 3.2, it is possible to give explicit formulas for $\nu = \kappa\mu$ on the generators by computing κ. Note that for any $R \in \mathrm{Sym}_n(q)$, the operator $\mu(S(R))$ is diagonal in the computational basis $|x\rangle$. Since its matrix entries do not depend on the sign of x, it is equally diagonal in the (anti-)symmetrised basis $B^{\pm}$ of $V^{\pm}$. Thus, we find:

$$\begin{aligned}\kappa(S(R)) &= \det \mu^-(S(R)) \det \mu^+(S(R))^{-1} \\ &= \prod_{x\in X} \chi(-2^{-1}x^\top Rx) \prod_{x\in X\cup 0} \chi(-2^{-1}x^\top Rx)^{-1} \\ &= 1.\end{aligned} \tag{3.59}$$

Computing κ for the subgroup $G_n(q)$ and J is a bit more involved and can be found in Ref. [95]. Note that both $\mu(G(Q))$ and $\mu^+(G(Q))$ are permutation matrices, thus their determinant is ± 1. Moreover, $\mu(J)^2 = \mu(J^2) = \mu(-\mathbb{1})$, hence $\mu^+(J)^2 = \mathrm{id}$. Recall that we assumed $q = p^m$ for $p > 2$ prime. Then, it holds

$$\begin{aligned}\kappa(G(Q)) = \det(\mu(G(Q))) &= \left(\frac{\det(Q)}{q}\right), \\ \kappa(J) = \det(\mu(J)) &= (-1)^{n(m+1)}(-i)^{\frac{nm}{2}(p-1)}.\end{aligned} \tag{3.60}$$

Here, $(\frac{x}{q})$ is the *Legendre symbol* of $x \in \mathbb{F}_q^\times$ which is 1 if x is a square and -1 else.

3.3 A Weil-like representation in even characteristic

Notably, the construction of the Schrödinger and Weil representations in Sec. 3.2 depends on the *characteristic being not two*. Indeed, the very first Eq. (3.39) invokes the inverse of 2 which does not exist in a field of characteristic two. Since the definition of the Heisenberg group is the foundation for the Weil representation, it is a priori not clear how the phase space formalism should be defined from an axiomatic point of view. To this end, it is instructive to rewrite the Schrödinger representation in Eq. (3.43) as follows

$$W_\chi(z,x,t)f(u) := \chi(t + z\cdot u + 2^{-1}z\cdot x)f(u+x) = \chi(t+z\cdot u)\tilde{\chi}(z\cdot x)f(u+x), \tag{3.61}$$

where $\tilde{\chi}(t) := \chi(2^{-1}t) = \omega^{2^{-1}\,\mathrm{tr}\,t}$. The number $\omega^{2^{-1}}$ is a *square root* of the p-th root of unity ω. Thus, we make the ansatz to replace $\omega^{2^{-1}}$ by a suitable square root of ω in the case $p = 2$. As it turns out, the somewhat different behaviour of the construction is related to the distinct nature of these square roots for even and odd p. Let us choose $\omega = e^{2\pi i/p}$ for concreteness, then its square roots are of the form $\pm e^{\pi i/p}$. Interestingly, the order depends on whether p is even or odd. In the odd case, the "+" square root has order $2p$ and the "-" square root has order p. In particular, $\omega^{2^{-1}} = e^{i\pi(p+1)/p} = -e^{i\pi/p}$ has order p and $\tilde{\chi}$ thus defines an additive character for an extension field over $\mathbb{F}_p$. In the even case, both square roots have order $4 = 2p$. Thus, if want to mimic the behaviour of the Schrödinger representation, one needs to introduce a character $\tilde{\chi}$ of an *extension ring* over $\mathbb{Z}_4$ in the even case.

The following presentation tries to combine approaches from the mathematical literature [86] and from the physical literature [66–68, 84, 85] with the goal of finding a balance between rigour and accessibility. More details on the mathematical background and intricacies can be found in Sec. 6.2 including a discussion of the construction in Ref. [86].

Remark 3.2 ($\mathbb{Z}_4$ phases are necessary)**.** For $p \neq 2$, eliminating the term $\tilde{\chi}(z \cdot x)$ from Eq. (3.61) yields a unitary representation of the Heisenberg group $\mathrm{H}_n(q)$ which is isomorphic to the Schrödinger representation W_χ introduced earlier (see also Sec. 6.2.3). The associated operators are sometimes called the *displacement operators*, thus we call this representation the *displacement representation*. The displacement representation can be equally defined for $p = 2$, however, it has different properties in this case. This is closely related to the fact that the displacement operators are real for $p = 2$. Therefore, the group of displacement operators is also called the *real Heisenberg-Weyl* or *real Pauli group*. However, the real structure is not preserved by all symplectic maps. In fact, this is only the case for the subgroup of *orthogonal maps*. As we will see, this problem is solved by the introduction of $\mathbb{Z}_4$-valued functions.

Before we give the construction of the Heisenberg group, let us briefly state a few fact about the ring $\mathbb{Z}_4$ and its relation to the field $\mathbb{F}_2$. The ring $\mathbb{Z}_4 := \mathbb{Z}/4\mathbb{Z}$ contains a maximal ideal which is generated by $2 \in \mathbb{Z}_4$, this is $(2) = 2\mathbb{Z}/4\mathbb{Z}$. Since the ideal (2) is exactly the set of zero divisors, the quotient $\mathbb{Z}_4/(2)$ is canonically isomorphic to the field $\mathbb{F}_2$ with projection map $\pi : r \mapsto r \mod 2$. Moreover, there is a 2-adic expansion of any element $r \in \mathbb{Z}_4$ as

$$r = r_0 + 2r_1, \qquad r_0, r_1 \in \mathbb{F}_2. \tag{3.62}$$

In this expansion, the projection map acts as $r \mapsto r_0$. We can embed $\mathbb{F}_2$ in $\mathbb{Z}_4$ in two different ways. First, we use the 2-adic expansion to define $\iota : \mathbb{F}_2 \ni x \mapsto x + 2 \cdot 0 \in \mathbb{Z}_4$. However, note that this map is only a multiplicative homomorphism. Likewise, there is an additive homomorphism which acts as $\mathbb{F}_2 \ni x \mapsto 2x \in \mathbb{Z}_4$. The two homomorphisms fulfil the following properties with respect to the projection modulo 2:

$$\iota(x) \mod 2 = x, \qquad 2r = 2(r \mod 2), \quad \forall x \in \mathbb{F}_2, r \in \mathbb{Z}_4. \tag{3.63}$$

3.3.1 The Heisenberg group for $p = 2$

For the sake of presentation, we first consider the case $q = p = 2$ and generalise the construction to arbitrary extension fields at the end of this chapter.

In the light of the previous discussion, we define the *Heisenberg group* $\mathrm{H}_n(2)$ as the central extension $\mathbb{F}_2^{2n} \times \mathbb{Z}_4$ given by the composition law

$$(v, t) \bullet (w, s) := (v + w, s + t + \beta(v, w)), \tag{3.64}$$

where $\beta : \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} \to \mathbb{Z}_4$ is a soon-to-be-defined "lift" of the symplectic form in the sense that $\beta(v, w) \mod 2 = [v, w]$ which fulfils the *cocycle condition* or all $v, w, u \in \mathbb{F}_2^{2n}$:

$$\mathrm{d}\beta(v, w, u) := \beta(w, u) - \beta(v + w, u) + \beta(v, w + u) - \beta(v, w) = 0. \tag{3.65}$$

Note that from the defining equations, we can deduce the following properties

$$\beta(v, v) = \beta(v, 0) = \beta(0, v) = 0, \tag{3.66}$$

$$\beta(v, w) - \beta(w, v) = 2[v, w], \tag{3.67}$$

where the right hand side in the last equation is the additive embedding $\mathbb{F}_2 \hookrightarrow \mathbb{Z}_4, t \mapsto 2t$. Hence, we find that

$$(v, t) \bullet (w, s) \bullet (v, t)^{-1} = (w, s + 2[v, w]). \tag{3.68}$$

Thus, (w, s) is in the centre of $\mathrm{H}_n(2)$ if and only if $w = 0$ and hence $Z(\mathrm{H}_n(2)) \simeq \mathbb{Z}_4$.

Let us fix the standard symplectic basis $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ of $\mathbb{F}_2^{2n}$. Then, we define a function $\gamma : \mathbb{F}_2^{2n} \to \mathbb{Z}_4$ as follows

$$\gamma(v) := \imath(v_z) \cdot \imath(v_x) \equiv v_z \cdot v_x \mod 4. \tag{3.69}$$

Here, the multiplicative homomorphism $\imath$ is applied component-wise and $v = (v_z, v_x)$ with respect to the standard polarisation $\mathbb{F}_2^{2n} = \mathsf{Z}_n \oplus \mathsf{X}_n$ with $\mathsf{Z}_n := \langle e_1, \ldots, e_n \rangle$ and $\mathsf{X}_n := \langle f_1, \ldots, f_n \rangle$. Then, we can define the cocycle β as follows

$$\beta(v, w) = \gamma(v + w) - \gamma(v) - \gamma(w) + 2(v_z \cdot w_x) =: -\mathrm{d}\gamma(v, w) + 2\eta(v, w). \tag{3.70}$$

Here, $\eta(v, w) := v_z \cdot w_x$ is a bilinear form. It is straightforward to verify that β is a cocycle and $\beta \mod 2 = \mathrm{d}\gamma \mod 2 = [\cdot, \cdot]$. To so-constructed cocycle β has the property that it vanishes on the Z and X Lagrangians, i. e. $\beta(e, e') = \beta(f, f') = 0$ for all $e, e' \in \mathsf{X}_n$ and $f, f' \in \mathsf{Z}_n$.

Analogous to Sec. 3.2, the centre-fixing automorphisms of $\mathrm{H}_n(2)$ are given by pairs $(g, \tilde{\alpha})$ where $g \in \mathrm{GL}_{2n}(2)$ and $\tilde{\alpha} : \mathbb{F}_2^{2n} \to \mathbb{Z}_4$ which act as $(v, t) \mapsto (g(v), t + \tilde{\alpha}(v))$. Note that it is necessary that $(g, \tilde{\alpha})$ preserves the order of an element $(v, t) \in \mathrm{H}_n(2)$. In particular, since $(v, 0)^2 = 0$, we find that $2\tilde{\alpha}(v) = 0$ for all $v \in \mathbb{F}_2^{2n}$. This implies that $\tilde{\alpha}$ takes values in $2\mathbb{Z}_4$, and can thus be written as $\tilde{\alpha} = 2\alpha$ for a $\mathbb{F}_2$-valued function α. Using this reparametrisation, the automorphism (g, α) has to fulfil the compatibility condition

$$\beta(g(v), g(w)) - \beta(v, w) = 2\left(\alpha(v + w) - \alpha(v) - \alpha(w)\right) = -2\ \mathrm{d}\alpha(v, w). \tag{3.71}$$

Since the right hand side is symmetric, the left hand side of Eq. (3.71) has to be symmetric, too. Enforcing this condition, we find that $g \in \mathrm{Sp}_{2n}(2)$:

$$0 = \beta(g(v), g(w)) - \beta(g(w), g(v)) - \beta(v, w) + \beta(w, v) = 2\left([g(v), g(w)] - [v, w]\right). \tag{3.72}$$

Crucially, for many $g \in \mathrm{Sp}_{2n}(2)$, the left hand side of Eq. (3.71) does not vanish. This implies that we can not always choose $\alpha = 0$ as a solution, in contrast to the odd case in Sec. 3.2. However, it is still true that any two solutions differ by a linear form $\varphi : \mathbb{F}_2^{2n} \to \mathbb{F}_2$. One way to see this is to note that Eq. (3.71) implies that α is determined by its values on a basis of $\mathbb{F}_2^{2n}$. However, these value assignments are in one-to-one correspondence with linear forms. Note that by Eq. (3.68), these linear forms are exactly given by the inner automorphisms of $\mathrm{H}_n(2)$.

In analogy to Sec. 3.2, we call the group of centre-fixing automorphisms the *affine symplectic group* $\mathrm{ASp}_{2n}(2)$. The above discussion implies that for a given $g \in \mathrm{Sp}_{2n}(2)$, any solution α_g to Eq. (3.71) depends on g. Hence, $\mathrm{ASp}_{2n}(2)$ does not have the structure of a semidirect product, in contrast to the odd case. In this sense, the term "affine symplectic group" might be misleading. However, I decided to adopt it from Gurevich and Hadani [86] nevertheless. This is partially justified by the existence of the double cover by $\mathrm{ASp}_{2n}(\mathbb{Z}_4) \simeq \mathrm{Sp}_{2n}(\mathbb{Z}_4) \ltimes \mathbb{F}_2^{2n}$ which now is a proper semidirect product, see Sec. 6.2.4.

In the even case, the affine symplectic group $\mathrm{ASp}_{2n}(2)$ has the structure of a fibre bundle over $\mathrm{Sp}_{2n}(2)$ with fibre $(\mathbb{F}_2^{2n})^*$. In general, it is not possible to make a consistent choice $g \mapsto \alpha_g$, i. e. to find a global section of this fibre bundle, which is compatible with group multiplication in $\mathrm{Sp}_{2n}(2)$ This is because given (g, α_g) and (h, α_h), the composition of these automorphisms is described by

$$(g, \alpha_g) \circ (h, \alpha_h) = (g \circ h, h^* \alpha_g + \alpha_h), \tag{3.73}$$

where $h^*\alpha_g(v) = \alpha_g(h(v))$ is the usual pullback of the function α_g by the linear map h. This implies that if we e.g. require α_g and α_h to vanish on the standard basis, this is generally not the case for $h^*\alpha_g + \alpha_h$. Instead, we have $h^*\alpha_g + \alpha_h = \alpha_{gh} + \varphi$ where α_{gh} vanishes on the standard basis and φ is a linear form.

3.3.2 Schrödinger and Weil representations

Having defined a suitable Heisenberg group over $\mathbb{F}_2^{2n}$, we can construct unitary representations on $\mathbb{C}[\mathbb{F}_2^{2n}]$ in complete analogy to the odd case. Given an additive character χ_4 of $\mathbb{Z}_4$, this induces an character on $\mathbb{F}_2$ by $\chi(t) = \chi_4(2t)$. With respect to the standard polarisation $\mathbb{F}_2^{2n} = \mathsf{Z}_n \oplus \mathsf{X}_n$, we can then define the Schrödinger representation of $\mathrm{H}_n(2)$ as

$$W_{\chi_4}(z, x, t)f(u) := \chi(z \cdot u)\chi_4(t + \gamma(z, x))f(u + x). \tag{3.74}$$

It is straightforward to check that this indeed defines a unitary representation of $\mathrm{H}_n(2)$.

Along the lines of Sec. 3.2, one can verify the following. W_{χ_4} is traceless outside the centre and is determined thereon by its character, $W_{\chi_4}(0, 0, t) = \chi_4(t)\mathrm{id}$. In particular, W_{χ_4} is irreducible and any two representations W_{χ_4} and $W_{\tilde{\chi}_4}$ are unitarily equivalent if and only if the characters agree, $\chi_4 = \tilde{\chi}_4$. Moreover, any irreducible representation of $H_n(2)$ induces a character on the centre and is thus unitarily equivalent to some W_{χ_4}. Thus, we find that the *Stone-von Neumann theorem* also holds for $H_n(2)$, namely two irreducible representations of $H_n(2)$ are unitarily equivalent if and only if they agree on the centre.

In the following, we consider the character χ_4 to be fixed and write $W \equiv W_{\chi_4}$. The action of a centre-fixing automorphism $(g, \alpha) \in \mathrm{ASp}_{2n}(2)$ induces a representation $W_{(g,\alpha)}(v, t) := W(g(v), t + 2\alpha(v))$ which agrees with W on the centre. Thus, there exists a unitary operator $\mu(g, \alpha)$ such that

$$W_{(g,\alpha)}(v, t) := W(g(v), t + 2\alpha(v)) = \mu(g, \alpha)W(v, t)\mu(g, \alpha)^{-1}. \tag{3.75}$$

Given a linear form $\varphi = [u, \cdot]$, it is straightforward to check that we can choose μ such that

$$\mu(g, \alpha + [u, \cdot]) = \mu(g, \alpha)W(u). \tag{3.76}$$

However, as there is global section $g \mapsto \alpha_g$ compatible with matrix multiplication, μ cannot be turned into a projective representation of $\mathrm{Sp}_{2n}(2)$ alone. In other words, it is not possible to separate the symplectic part from the phase part, since the latter involves "quadratic" dependencies.

Furthermore, the projective representation μ of $\mathrm{ASp}_{2n}(2)$ defined by Eq. (3.75) cannot be linearised. The argument from the odd case, based on Thm. 3.3, cannot be adapted for $p = 2$ since there is only an even parity subspace over $\mathbb{F}_2$ which is the whole space. As a consequence, it is possible to show that μ acts irreducibly on $\mathbb{C}[\mathbb{F}_2^{2n}]$.

Nevertheless, it is possible to extend μ to a faithful unitary representation $\tilde{\mu}$ of an extension of $\mathrm{ASp}_{2n}(2)$ which is the already mentioned double cover $\mathrm{ASp}_{2n}(\mathbb{Z}_4)$. These extensions are discussed in Sec. 6.2.4.

Although the construction of a proper Weil representation in even characteristic seems to be impossible, the above defined projective representation μ of $\mathrm{ASp}_{2n}(2)$ is useful when only the projective action is needed. Calculations can then be performed using the

structure of $\mathrm{ASp}_{2n}(2)$ derived in the last section. Moreover, it will come in handy to define a certain "standard" choice of operators $\mu(g) \equiv \mu(g, \alpha_g)$ which allow to express any other operator as $\mu(g)W(u)$. To this end, we use Thm. 3.2 as a guideline to define these for g in the Siegel parabolic subgroup $P_n(2) = S_n(2) \rtimes G_n(2)$ of $\mathrm{Sp}_{2n}(2)$:

$$\mu(S(R))f(u) := \chi_4(u^\top Ru)f(u), \tag{3.77}$$
$$\mu(G(Q))f(u) := f(Qu). \tag{3.78}$$

Furthermore, we define the following operator

$$\mu(J)f(u) := \frac{1}{\sqrt{2^n}} \sum_{v \in \mathbb{F}_2^n} \chi(u \cdot v)f(v), \tag{3.79}$$

which is commonly known as the *discrete Fourier transform* of the function f.

Note that Eq. (3.78) actually defines a faithful representation of $G_n(2)$ which agrees with the induced representation of $\mathrm{GL}_n(2)$ on $\mathbb{C}[\mathbb{F}_2^n]$. Hence, let us turn to Eq. (3.77). The $\mathbb{Z}_4$-valued quadratic form appearing there is explicitly defined as

$$q(u) := \sum_{i,j=1}^{n} u_i R_{ij} u_j \mod 4. \tag{3.80}$$

It is a quadratic refinement of the $\mathbb{F}_2$-bilinear form $b(u, v) := u^\top Rv$ in the sense that

$$q(u + v) - q(u) - q(v) = 2b(u, v). \tag{3.81}$$

Then, one can check that the operator defined in Eq. (3.77) obeys

$$\mu(S(R))W(z, x)\mu(S(R))^{-1} = \chi(\alpha_R(z, x))W(z + Rx, x), \qquad \alpha_R(z, x) := \sum_{i,j=1}^{n} z_i x_i R_{ij} x_j. \tag{3.82}$$

It is straightforward to see that Eq. (3.77) does not define a projective representation of the subgroup $S_n(2)$. To this end, note that any $\mathbb{F}_2$-valued quadratic form defined as $\bar{q}(u) = u^\top Ru$ fulfills Eq. (3.81), but the RHS vanishes over $\mathbb{F}_2$. Thus, it is actually a linear form which implies that

$$\mu(S(R))\mu(S(R)^{-1})f(u) = \mu(S(R))^2 f(u) = \chi(\bar{q}(u))f(u) = Z(z)f(u), \tag{3.83}$$

for a suitable $z \in \mathbb{F}_2^n$. The RHS is clearly not a multiple of the identity.

Finally, note that the $\mathbb{Z}_4$-valued quadratic form q can also be written as

$$q(u) := \sum_{i=1}^{n} R_{ii} u_i^2 + 2 \sum_{i<j} u_i R_{ij} u_j. \tag{3.84}$$

While the first term is $\mathbb{Z}_4$-quadratic, the second term defines a proper $\mathbb{F}_2$-valued quadratic form. Hence, only symmetric matrices with non-vanishing diagonal induce $\mathbb{Z}_4$-phases by Eq. (3.77).

3.3.3 Generalisation to extension fields

To fully generalise the construction from $\mathbb{F}_2$ to $\mathbb{F}_{2^m}$, it is necessary to define the Heisenberg group as a central extension of the phase space $\mathbb{F}_{2^m}^{2n}$ by a suitable extension of the ring $\mathbb{Z}_4$ of degree m. This extension is the Galois extension for rings, resulting in the *Galois ring* $\mathbb{GR}(4, m)$ with 4^m elements. In the following, we try to avoid the technicalities related to these rings and refer there reader for more details to Sec. 6.1.2.

The additive group of $\mathbb{GR}_{4^m} := \mathbb{GR}(4, m)$ has the structure of a $\mathbb{Z}_4$-module of rank m, i.e. any element in $\mathbb{GR}_{4^m}$ can be written uniquely as

$$t = t_0 + t_1\theta + \ldots t_{m-1}\theta^{m-1}, \qquad t_i \in \mathbb{Z}_4, \tag{3.85}$$

where $\{1, \theta, \ldots, \theta^{m-1}\}$ is a *polynomial ring basis* for $\mathbb{GR}_{4^m}$. In this representation, addition is simply the addition of the coefficients in $\mathbb{Z}_4$.

The multiplicative structure is, however, more involved than in the case of finite fields. Since, $\mathbb{GR}_{4^m}$ is a ring, not all elements are invertible. The *zero divisors* are exactly the elements in the maximal ideal generated by two, which is $(2) := 2\mathbb{GR}_{4^m}$. The invertible elements, or *units*, of $\mathbb{GR}_{4^m}$ can be understood as a suitable lift of the multiplicative group of $\mathbb{F}_{2^m}$ and the principal units $1 + (2)$. Taking the quotient with respect to the zero divisors results in a field, which is $\mathbb{GR}_{4^m}/(2) \simeq \mathbb{F}_{2^m}$.

As for finite fields, there is a *trace map* $\mathrm{tr} : \mathbb{GR}_{4^m} \to \mathbb{Z}_4$ which is a $\mathbb{Z}_4$-linear map on $\mathbb{GR}_{4^m}$. The trace $\mathrm{tr}\, t$ is exactly the trace of the linear map on the $\mathbb{Z}_4$-module R_{4^m} which acts as $x \mapsto t \cdot x$. The additive characters $\chi_4 : \mathbb{GR}_{4^m} \to \mathbb{S}^1$ are exactly of the form

$$\chi_4(t) = i^{\mathrm{tr}(at)}, \tag{3.86}$$

for some $a \in \mathbb{GR}_{4^m}$. Any such character can be turned into a characters of $\mathbb{F}_{2^m}$ as follows. Consider the additive embedding $\mathbb{F}_{2^m} \to 2\mathbb{GR}_{4^m}$, in analogy to $\mathbb{F}_2 \to 2\mathbb{Z}_4$ and define $\chi : \mathbb{F}_{2^m} \to \mathbb{S}^1$ by $\chi(x) := \chi_4(2x)$. Then, one can show that χ has the form

$$\chi(x) = (-1)^{\mathrm{tr}(\bar{a}x)}, \qquad \bar{a} := a \mod 2. \tag{3.87}$$

Adaption for extension fields All constructions can be performed similarly after replacing $\mathbb{F}_2 \mapsto \mathbb{F}_{2^m}$ and $\mathbb{Z}_4 \mapsto \mathbb{GR}_{4^m}$. In particular, the functions γ and β in Eq. (3.69) and (3.70) can be generalised in a straightforward fashion by using the correct generalisation of the lift $\iota : \mathbb{F}_{2^m} \to \mathbb{GR}_{4^m}$ and the projection $\mathbb{GR}_{4^m} \to \mathbb{F}_{2^m}$ modulo 2. As a result, one obtains a Heisenberg group $\mathrm{H}_n(2^m)$ with centre-fixing automorphisms $\mathrm{ASp}_{2n}(2^m)$. Then, the Schrödinger and Weil representations can be defined in the same way as before using an additive character χ_4 of $\mathbb{GR}_{4^m}$ and the induced character χ of $\mathbb{F}_{2^m}$.

CHAPTER 4

STABILISER FORMALISM IN PRIME-POWER DIMENSIONS

The Schrödinger and Weil representations defined in the last chapter act on the Hilbert space $\mathbb{C}[\mathbb{F}_q^n] \simeq (\mathbb{C}^q)^{\otimes n}$ which corresponds to the state space of n q-level systems in quantum information theory. In this chapter, we describe how these representations can be used to define the stabiliser formalism in terms of objects on the discrete phase space $\mathbb{F}_q^{2n}$. This simplifies a lot of computations allows for a systematic treatment. Moreover, this yields a generalisation of the standard qubit stabiliser formalism to the case where the local dimension is a power of a prime.

More details on the relation between symplectic geometry, the stabiliser formalism and quantum error correction can be found in Refs. [54, 75, 85, 101–106].

4.1 The Heisenberg-Weyl and Clifford groups

4.1.1 The odd case

The Schrödinger representation defined in Eq. (3.43) can be written as

$$W(z,x,t) = \chi(t)\chi(-2^{-1}z\cdot x)Z(z)X(x), \tag{4.1}$$

where the Z and X operators are defined in the computational basis as

$$Z(z)\,|u\rangle := \chi(z\cdot u)\,|u\rangle\,, \qquad X(x)\,|u\rangle := |u+x\rangle\,. \tag{4.2}$$

Here and in the following we will use the concrete choice $\chi(t) = \omega^{\mathrm{tr}\,t}$ for $\omega = e^{2\pi i/p}$. The operators $W(z,x,t)$ are called *Weyl operators* and the matrix group formed by them is the *Heisenberg-Weyl group* $\mathrm{HW}_n(q) := W(\mathrm{H}_n(q))$. We will usually write $v = (z,x) \in \mathbb{F}_q^{2n}$ and use the shorthand notation $W(v) \equiv W(v,0)$ for $t = 0$. Recall that we have the relations

$$W(v)W(w) = \chi([v,w])W(w)W(v) = \chi(2^{-1}[v,w])W(v+w). \tag{4.3}$$

Note that this representation canonically factorises with respect to the decomposition $\mathbb{F}_q^{2n} = \mathbb{F}_q^2 \oplus \cdots \oplus \mathbb{F}_q^2$ given by grouping symplectic coordinates (z_i, x_i):

$$W(z,x) = W(z_1,x_1)\otimes\cdots\otimes W(z_n,x_n). \tag{4.4}$$

Let μ be the linearised Weil representation of $\mathrm{Sp}_{2n}(q)$. We have the following *projective* representation of the centre-fixing automorphism of affine symplectic maps $\mathrm{ASp}_{2n}(q) = \mathrm{Sp}_{2n}(q) \ltimes \mathbb{F}_q^{2n}$ [75]:

$$\mu(g,v) := \mu(g)W(v) = W(gv)\mu(g). \tag{4.5}$$

Clearly, this is only a projective representation since $W|_{\mathbb{F}_q^{2n}}$ is. Using the same construction as for the Heisenberg group, this representation can be lifted to a linear one by extending $\mathbb{F}_q^{2n}$ to $H_q(n)$. We call the image of $\mathrm{Sp}_{2n}(q) \ltimes H_q(n)$ under this representation the *Clifford group* $\mathrm{Cl}_n(q) := \mu(\mathrm{Sp}_{2n}(q)) \ltimes \mathrm{HW}_n(q)$. By construction, the Clifford group

normalises $\mathrm{HW}_n(q)$. However, it is in general *not* the full unitary normaliser. As we will explain in Sec. 4.3, the full unitary normaliser is of the form $\mathrm{Cl}_{nm}(p)$ where $q = p^m$ (trivially extended by $U(1)$).

From this definition of the Clifford group, it is straightforward to write down its order. Using Eq. (3.20), we find

$$|\mathrm{Cl}_n(q)| = |\mathrm{Sp}_{2n}(q)||\mathrm{HW}_n(q)| = pq^{2n}q^{n^2}\prod_{i=1}^{n}\left(q^{2i}-1\right). \tag{4.6}$$

4.1.2 The even case

Similar to the odd case, the Schrödinger representation can be reformulated as

$$W(z,x,t) = \chi_4(t - z\cdot x)Z(z)X(x), \tag{4.7}$$

where the Z and X operators are defined in the computational basis as

$$Z(z)\,|u\rangle := \chi(z\cdot u)\,|u\rangle\,, \qquad X(x)\,|u\rangle := |u+x\rangle\,. \tag{4.8}$$

For concreteness, we assume that $\chi_4(t) = i^{\mathrm{tr}\,t}$ and $\chi(t) = (-1)^{\mathrm{tr}\,t}$. Again, the operators $W(z,x) \equiv W(z,x,0)$ are called *Weyl operators* and the group $\mathrm{HW}_n(2^m) = W(\mathrm{H}_n(2^m))$ is the *Heisenberg-Weyl group*. Nevertheless, in the case $p = 2$, the names *Pauli operators* and *Pauli group* are more commonly used. The Weyl operators fulfil the relations

$$W(v)W(w) = \chi([v,w])W(w)W(v) = \chi_4(\beta(v,w))W(v+w), \tag{4.9}$$

where β is defined in Eq. (3.70). As in the odd case, the representation naturally factors as

$$W(z,x) = W(z_1,x_1)\otimes\cdots\otimes W(z_n,x_n). \tag{4.10}$$

The Weil representation μ of $\mathrm{ASp}_{2n}(2^m)$ is a projective representation and thus the operators $\mu(g,\alpha)$ are determined up to a global phase. In principle, this can be lifted to a faithful representation of a central extension of $\mathrm{ASp}_{2n}(2^m)$ which, however, does not exhibit the simple structure of a semidirect product as in the odd case. Instead, we define the *Clifford group* $\mathrm{Cl}_n(2^m)$ to be the smallest finite subgroup of the unitary normaliser $N(\mathrm{HW}_n(2^m))$ such that

$$\mathrm{Cl}_n(2^m)/Z(\mathrm{Cl}_n(2^m)) \simeq \mathrm{ASp}_{2n}(2^m). \tag{4.11}$$

It is possible to show that $\mathrm{Cl}_n(2^m)$ is such that $Z(\mathrm{Cl}_n(2^m)) = Z(\mathrm{HW}_n(2^m)) = \mathbb{Z}_4$ [60, 87].

By construction, we have $\mathrm{Cl}_n(2^m)/\mathrm{HW}_n(2^m) \simeq \mathrm{Sp}_{2n}(2^m)$. In particular, the order of $\mathrm{Cl}_n(2^m)$ is given by

$$|\mathrm{Cl}_n(2^m)| = |\mathrm{Sp}_{2n}(2^m)||\mathrm{HW}_n(2^m)| = 2^{nm+2}2^{mn^2}\prod_{i=1}^{n}\left((2^m)^{2i}-1\right). \tag{4.12}$$

4.1.3 Generators of the Clifford group

Recall that we have introduced the special subgroups $S_n(q)$ and $G_n(q)$ of the symplectic group in Sec. 3.1.4, and have given an explicit formula for their Weil representation in $p \neq 2$ in Thm. 3.2. For $p = 2$, we have argued that there is a somewhat natural way of associating operators with these subgroups which, however, do not form a representation in the case of $S_n(q)$. Combining this with our discussion of generators of the symplectic group in Sec. 3.1.4, we can now give generators of the Clifford group. For the prime case $q = p$, similar sets of generators are given in Refs. [40, 54, 96].

For $p \neq 2$, the Clifford group $\mathrm{Cl}_n(q)$ is a semidirect product of the Weil representation of $\mathrm{Sp}_{2n}(q)$ and the Heisenberg-Weyl group $\mathrm{HW}_n(q)$. Thus, we obtain generators of $\mathrm{Cl}_n(q)$ by using the Weil representation in Thm. 3.2 of the generators introduced in Prop. 3.2, combined with generators of $\mathrm{HW}_n(q)$. This set of *local* generators of the Clifford group is explicitly given by:

$$H := \frac{1}{\sqrt{q}} \sum_{x,y \in \mathbb{F}_q} \chi(x \cdot y) \, |x\rangle\langle y| \,, \qquad M(\lambda) := \sum_{x \in \mathbb{F}_q} |\lambda x\rangle\langle x| \,, \tag{4.13}$$

$$S(\lambda) := \sum_{x \in \mathbb{F}_q} \chi(2^{-1}\lambda x^2) \, |x\rangle\langle x| \,, \qquad CX := \sum_{(x,y) \in \mathbb{F}_q^2} |x, x+y\rangle\langle x, y| \,, \tag{4.14}$$

$$Z = \sum_{x \in \mathbb{F}_q} \chi(x) \, |x\rangle\langle x| \,, \qquad X = \sum_{x \in \mathbb{F}_q} |x+1\rangle\langle x| \,. \tag{4.15}$$

Here, $\lambda \in \mathbb{F}_q^\times$ is a primitive element and it is understood that these single and two-qudit gates can be applied to any qudit or any pair of qudits.

For $p = 2$, we can no longer rely on the Weil representation. Instead, we use the results in Sec. 3.3.2, to associate unitary operators to the generators of $\mathrm{Sp}_{2n}(2^m)$. Combined with generators of $\mathrm{HW}_n(2^m)$, we obtain a similar list of generators:

$$H := \frac{1}{\sqrt{q}} \sum_{x,y \in \mathbb{F}_q} \chi(x \cdot y) \, |x\rangle\langle y| \,, \qquad M(\lambda) := \sum_{x \in \mathbb{F}_q} |\lambda x\rangle\langle x| \,, \tag{4.16}$$

$$S := \sum_{x \in \mathbb{F}_q} \chi_4(x^2) \, |x\rangle\langle x| \,, \qquad CX := \sum_{(x,y) \in \mathbb{F}_q^2} |x, x+y\rangle\langle x, y| \,, \tag{4.17}$$

$$Z = \sum_{x \in \mathbb{F}_q} \chi(x) \, |x\rangle\langle x| \,, \qquad X = \sum_{x \in \mathbb{F}_q} |x+1\rangle\langle x| \,. \tag{4.18}$$

Although this operators affect to correct symplectic transformations, the group generated by them is not necessarily *minimal* as we required in Eq. (4.11). In fact for $q = p = 2$, it is known that the matrix coefficients are in the ring $\mathbb{Q}[\zeta_8]$ where $\zeta_8 = (1+i)/\sqrt{2}$ is a eighth root of unity [54, 60, 107]. This implies that the centre of the generated group is $\mathbb{Z}_8$. This can be corrected for by using an alternative and less standard definition of the *Hadamard* gate H:

$$\tilde{H} := e^{i\pi/4} H = \frac{1+i}{2} \sum_{x,y \in \mathbb{F}_q} \chi(x \cdot y) \, |x\rangle\langle y| \,. \tag{4.19}$$

The generated group now has matrix coefficients in $\mathbb{Q}[i]$ and consequently, its centre is $\mathbb{Z}_4$. This can be directly generalised to the extension field case $q = 2^m$. If m is even, then it is evident that all generators have coefficients in $\mathbb{Q}[i]$ and the centre of the generated

group is $\mathbb{Z}_4$. If m is odd, then we can again use the above redefinition to achieve a minimal centre:

$$\tilde{H} := e^{i\pi/4} H = 2^{-\frac{m-1}{2}} \frac{1+i}{2} \sum_{x,y\in\mathbb{F}_q} \chi(x\cdot y)\, |x\rangle\langle y|\,. \tag{4.20}$$

Although it is not independent from the other generators, let us add the definition of the CZ gate here. The form of the gate is independent of p.

$$CZ := \sum_{(x,y)\in\mathbb{F}_q^2} \chi(xy)\, |x,y\rangle\langle x,y|\,. \tag{4.21}$$

4.2 Stabiliser states and codes

4.2.1 Stabiliser codes as invariant subspaces

In the following, we are interested in Abelian subgroups of the Heisenberg-Weyl group $\mathrm{HW}_n(q)$ as they have a particularly simple representation on Hilbert space. These representations exactly correspond to *stabiliser codes*. For a recent survey on the geometry of stabiliser codes and related constructions, we refer the reader to e.g. Ref. [106].

In the the odd case $p \neq 2$, the composition law Eq. (3.39) implies that any isotropic subspace $M \subset \mathbb{F}_q^{2n}$ induces Abelian subgroups $M \times 0 \subset \mathrm{H}_n(q)$ and $W(M) \subset \mathrm{HW}_n(q)$. In contrast for $p = 2$, an isotropic subspace M does no longer induce a subgroup of $\mathrm{HW}_n(2^m)$ since the function β appearing in the composition law (4.9) is not necessarily zero on M. It is however the case that β vanishes modulo 2 on M. This implies that there is a $\mathbb{F}_{2^m}$-valued function $\bar{\beta}$ such that $2\bar{\beta} = \beta$ and

$$W(v)W(w) = \omega^{\mathrm{tr}\,\bar{\beta}(v,w)} W(v+w), \qquad \forall v, w \in M. \tag{4.22}$$

Thus, for any function $\alpha : M \to \mathbb{F}_{2^m}$ fulfilling

$$\bar{\beta}(v,w) = \alpha(v+w) - \alpha(v) - \alpha(w), \qquad \alpha(0) = 0, \tag{4.23}$$

we find that the following is an Abelian subgroup of $\mathrm{HW}_n(2^m)$:

$$W(M^\alpha) = \left\{\omega^{\mathrm{tr}\,\alpha(v)} W(v) \,|\, v \in M\right\}, \qquad M^\alpha = \left\{(v, 2\alpha(v)) \,|\, v \in M\right\} \subset \mathrm{H}_n(2^m). \tag{4.24}$$

We can treat the two cases simultaneously by noting that the analogous function to $\bar{\beta}$ in the odd case is identically zero and we can thus always choose $\alpha = 0$ for $p \neq 2$.

Because M^α is Abelian, the restricted representation $W|_{M^\alpha}$ decomposed into irreducible representations given by additive characters $\xi : M^\alpha \to \mathbb{S}^1$ of M^α. It is easy to see that the characters of M^α are exactly those of M. Recall from Sec. 3.1.2 that any such character is of the form $\xi = \chi \circ \varphi$ for a unique linear form $\varphi \in M^*$ and that the group of characters has order $|\widehat{M}| = |M| = q^{\dim M}$. The isotypic component $\mathcal{C}(M^\alpha, \xi)$ associated to ξ is the range of the projector

$$P(M^\alpha, \xi) := \frac{1}{|M|} \sum_{v\in M} \overline{\xi}(v) \omega^{\mathrm{tr}\,\alpha(v)} W(v). \tag{4.25}$$

In the even case, the presentation of an isotypic component by the triple (M, α, ξ) is not unique since it is always possible to absorb the character ξ into the phase function α

which does not change Eq. (4.25). Thus, it is convenient to define a standard choice of α. This can be done by selecting a distinguished basis $v_1, \ldots, v_k$ of M and set $\alpha(\lambda v_i) = 0$ for all $\lambda \in \mathbb{F}_q^\times$. In the following, we will implicitly assume that such a choice has been made. Although the presentation is arguably simpler in the odd case, almost any derivation can be performed with some care in any case.

From Eq. (4.25), we can directly compute the dimension of $\mathcal{C}(M^\alpha, \xi)$:

$$\dim \mathcal{C}(M^\alpha, \xi) = \operatorname{tr} P(M^\alpha, \xi) = \frac{\operatorname{tr} \mathbb{1}}{|M|} = q^{n - \dim M}. \tag{4.26}$$

Hence, we have explicitly verified that we have an orthogonal decomposition of Hilbert space into equal-dimensional subspaces $\mathcal{C}(M^\alpha, \xi)$, given by the isotypes of the restricted representation $W|_{M^\alpha}$:

$$(\mathbb{C}^q)^{\otimes n} = \bigoplus_{\xi \in \widehat{M^\alpha}} \mathcal{C}(M^\alpha, \xi) \tag{4.27}$$

In the case that $M = L$ is maximal and hence a Lagrangian subspace, the dimension formula Eq. (4.26) implies that the subspaces $\mathcal{C}(L^\alpha, \xi)$ are one-dimensional and hence irreducible under $W|_{L^\alpha}$. Thus, the projectors define *pure quantum states* which are called *stabiliser states*. The orthogonal decomposition in Eq. (4.27) implies that the $|L| = q^n$ stabiliser states associated to L define an orthonormal basis of the Hilbert space $(\mathbb{C}^q)^{\otimes n}$. We call such a basis a *stabiliser basis*. Stabiliser states have extraordinary properties and thus find various applications throughout quantum information theory. We will discuss some of these in Ch. 5.

In general, an isotypic decomposition as in Eq. (4.27) can be further decomposed into irreducible components in a non-canonical way. Here, this can be achieved by completing an isotropic subspace M to a maximally isotropic, i.e. Lagrangian subspace L (cp. Sec. 3.1.3). The (non-unique) completion of M can be written as $L = M \oplus N$ for some complement N. Since any character $\xi = \varsigma \oplus v$ of L as a direct sum of characters in M and N, we find:

$$\begin{aligned}
\sum_{v \in \widehat{N}} P(L^\alpha, \varsigma \oplus v) &= \sum_{v \in \widehat{N}} \frac{1}{|L|} \sum_{a \in M} \sum_{b \in N} \overline{\varsigma}(a) \overline{v}(b) \omega^{\operatorname{tr} \alpha(a \oplus b)} W(a \oplus b) \\
&= \frac{1}{|L|} \sum_{a \in M} \sum_{b \in N} \overline{\varsigma}(a) \omega^{\operatorname{tr} \alpha(a) + \operatorname{tr} \alpha(b)} W(a) W(b) \sum_{v \in \widehat{N}} \overline{v}(b) \\
&= \frac{1}{|M|} \sum_{a \in M} \overline{\varsigma}(a) \omega^{\operatorname{tr} \alpha(a)} W(a) \frac{1}{|N|} \sum_{b \in N} \omega^{\operatorname{tr} \alpha(b)} W(b) |N| \, \delta_{b,0} \\
&= \frac{1}{|M|} \sum_{a \in M} \overline{\varsigma}(a) \omega^{\operatorname{tr} \alpha(a)} W(a) \\
&= P(M^\alpha, \varsigma).
\end{aligned} \tag{4.28}$$

Here, we used Eqs. (4.22) and (4.23) in the second equation. In the last equation, we used that N is the dual group of $\widehat{N}$, hence the sum over v is a character inner product between b and 0 which are orthogonal if $b \neq 0$. Note that the $P(L^\alpha, \xi)$ are orthogonal as the correspond to different irreducible components of $W(L^\alpha)$. Thus, we have shown that

$$\mathcal{C}(M^\alpha, \varsigma) = \bigoplus_{v \in \widehat{N}} \mathcal{C}(L^\alpha, \varsigma \oplus v). \tag{4.29}$$

In particular, the stabiliser states given by $P(L^\alpha, \varsigma \oplus v)$ form an orthonormal basis of the subspace $\mathcal{C}(M^\alpha, \varsigma)$.

By the dimension formula Eq. (4.26), the subspaces $\mathcal{C}(M^\alpha, \xi)$ can be interpreted as the Hilbert space of $k := n - \dim M$ qudits embedded or *encoded* into the Hilbert space of n qudits. Therefore, we call $\mathcal{C}(M^\alpha, \xi)$ the *code space* of the $[[n, k]]$ *stabiliser code* (M^α, ξ). The name *stabiliser code* originates from the following observation which leads to a more standard way of presenting the subject. Instead of fixing an Abelian subgroup M^α and study its isotypes, we can instead consider the Abelian subgroups $M^{\alpha+\varphi}$ for $\varphi \in M^*$ The function $\alpha + \varphi$ yields another solution to Eq. (4.23) and we can indeed obtain any solution in this way. By Eq. (4.25), we see that the isotype associated with the character $\xi = \chi \circ (-\varphi)$ of $W|_{M^\alpha}$ corresponds exactly to trivial isotype of $W|_{M^{\alpha+\varphi}}$. In other words, the subspace $\mathcal{C}(M^\alpha, \xi)$ is stabilised exactly by the group $W(M^{\alpha+\varphi})$ which is called the *stabiliser group* of $\mathcal{C}(M^\alpha, \xi)$ in this context.

The introduced decomposition in Eq. (4.29) induces a basis for a stabiliser code. A choice of complement N for M such that $M \oplus N = L$ is Lagrangian is called a choice of a *destabiliser group* for the stabiliser codes associated with M. A choice of basis $b_1, \ldots, b_{n-k}$ for N corresponds to a choice of *logical operators* $\overline{Z}(\overline{z}) := W(\overline{z}_1 b_1 + \cdots + \overline{z}_{n-k} b_{n-k})$ for the code as they are used to define a *logical computational basis* $|\overline{x}\rangle$ by their common eigenbasis characterised as (cp. Eq. (4.2)):

$$\begin{aligned} \overline{Z}(\overline{z})\ |\overline{x}\rangle &= \chi(\overline{z} \cdot \overline{x})\ |\overline{x}\rangle\,, \qquad \overline{x}, \overline{z} \in \mathbb{F}_q^{n-k} \\ W(m)\ |\overline{x}\rangle &= \varsigma(m)\ |\overline{x}\rangle\,, \qquad \forall m \in M. \end{aligned} \tag{4.30}$$

Here, $\varsigma \in \widehat{M}$ is the character which singles out a code space $\mathcal{C}(M^\alpha, \varsigma)$. The logical computational basis defined in this way exactly corresponds to the refinement in Eq. (4.29) as $|\overline{x}\rangle\langle\overline{x}| = P(M^\alpha \oplus N^\alpha, \varsigma \oplus v_{\overline{x}})$ where $v_{\overline{x}}$ is the character on N associated with the linear form $\overline{z} \mapsto \overline{z} \cdot \overline{x}$ in the basis $b_1, \ldots, b_{n-k}$.

Stabiliser codes are of major importance for quantum error correction since almost all known quantum codes are stabiliser codes or a based on these. The Heisenberg-Weyl group as an underlying structure makes it possible to analyse these codes in a systematic way. Albeit, even an introduction to quantum error correction is beyond the scope of this work.

Action of the Clifford group (odd case). Consider the action of a Clifford unitary $U = \mu(g)W(v)$ for $g \in \mathrm{Sp}_{2n}(q)$ on a stabiliser code $\mathcal{C}(M, \xi)$. By Eq. (4.25), the image is another stabiliser code of the same dimension and the transformation can be described as $M \mapsto g(M)$ and $\xi \mapsto (\xi\nu) \circ g^{-1}$ where $\nu := \chi([\cdot, v])$. As discussed in Sec. 3.1.3, the action of $\mathrm{Sp}_{2n}(q)$ is *transitive* on isotropic subspaces of the same dimension. This implies that the action of the Clifford group is also transitive on stabiliser codes of the same dimension. In particular, the set $\mathrm{stab}_{n,l}$ of $[[n, n-l]]$ stabiliser codes is a single orbit under the Clifford group. Here, we adopt the somewhat non-standard convention that the rank l of the stabiliser group $W(M, \xi)$, respectively the dimension of the underlying isotropic subspace M, is considered as a parameter of the code rather than the dimension of the code space $\mathcal{C}(M, \xi)$.

Action of the Clifford group (even case). Consider the action of a Clifford unitary U given by $(g, \delta) \in \mathrm{ASp}_{2n}(q)$ on a stabiliser code $\mathcal{C}(M^\alpha, \xi)$. Using Eq. (4.25), the transfor-

mation can be described as $M \mapsto g(M)$, $\xi \mapsto \xi \circ g^{-1}$ and $\alpha \mapsto (\alpha + \delta) \circ g^{-1}$. Note that for all $v, w \in M$ the polarisation identity Eq. (3.71) for (g, δ) becomes

$$\bar{\beta}(g(v), g(w)) - \bar{\beta}(v, w) = \delta(v + w) - \delta(v) - \delta(w). \tag{4.31}$$

Using this and Eq. (4.23) for α on M, we find for all $v, w \in M$:

$$\alpha(v + w) - \alpha(v) - \alpha(w) + \delta(v + w) - \delta(v) - \delta(w) = \bar{\beta}(g(v), g(w)). \tag{4.32}$$

Hence, $\varepsilon := (\alpha + \delta) \circ g^{-1}$ fulfills Eq. (4.23) on $g(M)$ and $(g(M)^{\varepsilon}, \xi \circ g^{-1})$ defines a valid stabiliser code. The transitive action of $\mathrm{Sp}_{2n}(q)$ on isotropic subspaces of the same dimension then again implies that the action of the Clifford group is transitive on stabiliser codes of the same dimension. Again, the set $\mathrm{stab}_{n,l}$ of $[[n, n-l]]$ stabiliser codes is a single orbit under the Clifford group.

Overlaps of stabiliser codes Given two stabiliser codes defined by pairs (M^{α}, ξ) and (N^{δ}, v), we can assume that $\alpha|_{M\cap N} = \delta|_{M\cap N}$ since we can find basis of M and N such that their intersection spans $M \cap N$. Then, we find (cp. Ref. [108]):

$$\begin{aligned}
\operatorname{tr} P(M^{\alpha}, \xi)^{\dagger} P(N^{\delta}, v) &= \frac{1}{|M||N|} \sum_{v\in M} \sum_{w\in N} \xi(v)\overline{v}(w)\omega^{-\operatorname{tr}\alpha(v)+\operatorname{tr}\delta(w)} \operatorname{tr} W(v)^{\dagger} W(w) \\
&= \frac{q^n}{|M||N|} \sum_{v\in M} \sum_{w\in N} \xi(v)\overline{v}(w)\delta_{v,w} \\
&= \frac{q^n}{|M||N|} \sum_{v\in M\cap N} \overline{\xi}(v)v(v) \\
&= \begin{cases} \frac{q^n|M\cap N|}{|M||N|} & \text{if } \xi|_{M\cap N} = v|_{M\cap N}, \\ 0 & \text{else.} \end{cases}
\end{aligned} \tag{4.33}$$

Thus, two stabiliser codes are orthogonal if their characters differ on their common support $M \cap N$. For the Lagrangian case $M = N = L$, this again shows that two distinct stabiliser states associated to the same Lagrangian are orthogonal.

Counting stabiliser codes Using the introduced definition of stabiliser codes, it is straightforward to count the number of $[[n, n-l]]$ stabiliser codes. It is given by

$$|\mathrm{stab}_{n,l}(q)| = q^l \, |\mathrm{Iso}_{n,l}(q)|. \tag{4.34}$$

Here, $\mathrm{Iso}_{n,l}(q)$ is the set of l-dimensional isotropic subspaces in $\mathbb{F}_q^{2n}$ and q^l is the number of characters of a l-dimensional subspace. The number of isotropic subspaces can be determined by a simple counting argument to be [75]

$$|\mathrm{Iso}_{n,l}(q)| = \prod_{i=0}^{l-1} \frac{q^{2(n-i)} - 1}{q^{l-i} - 1}. \tag{4.35}$$

In particular, the number of stabiliser states $\mathrm{stab}_{n,n}(q) \equiv \mathrm{stab}_n(q)$ is

$$|\mathrm{stab}_n(q)| = q^n \prod_{i=1}^{n} (q^i + 1). \tag{4.36}$$

4.2.2 Generator matrices

In the following, we want to make the description of stabiliser states and codes more explicit and relate to the presentation by *generator matrices*, also called *stabiliser tableaux*, which is often used in applications (see e. g. Ref. [109, Ch. 10]).

Although the above introduced concepts are basis-independent, it is sometimes convenient to work in a particular basis $b_1, \ldots, b_k$ of a k-dimensional isotropic subspace $M \subset \mathbb{F}_q^{2n}$. By writing any basis vector b_i in the standard basis of $\mathbb{F}_q^{2n}$, we can form a matrix,

$$G = G(b_1, \ldots, b_k) = \left(b_1 \mid \ldots \mid b_k\right) \in \mathbb{F}_q^{2n \times k}, \tag{4.37}$$

which allows to relate any point $v \in M$ to its coordinates $x \in \mathbb{F}_q^k$:

$$v = G \cdot x. \tag{4.38}$$

The matrix G is called a *generator matrix* for M as its column span is M. Together with a choice of character, G uniquely determines a stabiliser code.

This is particularly pronounced in the prime case $q = p$, where a character is simply determined by its values on the basis $b_1, \ldots, b_k$. Hence, supplementing the generator matrix G with $s_1, \ldots, s_k \in \mathbb{F}_p$ completely fixes the stabiliser code. Thus, it is often the case that another row given by $(s_1, \ldots, s_k)$ is added to G. This matrix is often called the *stabiliser tableaux* of the associated stabiliser code and the basis for many algorithms. The stabiliser tableaux thus corresponds to a choice of generators $\omega^{s_i} W(b_i)$ of the corresponding stabiliser group.

It will prove useful to bring G in a certain normal form. Let us write

$$G = \left(\frac{A}{B}\right), \tag{4.39}$$

for matrices $A, B \in \mathbb{F}_p^{n \times k}$. We can perform arbitary column operations on G since this does not change its column span. Moreoever, we can swap rows, as long as we do in simultaneously in the upper and lower half of G. This corresponding to swapping qudits, but since their labeling is anyway arbitary, we consider this as a valid operation. Let $r := \operatorname{rk} B$, then, we can bring G into the following form by Gaussian elimination and qudit permutations (see e. g. [109, Sec. 10.5.7]):

$$G = \left(\begin{array}{cc} 0 & \mathbb{1}_{k-r} \\ \theta & C \\ \hline D & 0 \\ \mathbb{1}_r & 0 \end{array}\right). \tag{4.40}$$

Although this form is not unique, we refer to any generator matrix in this form as being in *normal form*. Note that isotropicity requires that the $k \times k$ matrix θ is symmetric. The normal form of isotropic subspaces thus depends on the rank r and we will see the significance of that parameter and the matrix θ below.

For the case of *stabiliser states*, the rank r can vary between 0 and n. When the rank is maximal, $r = n$, the generator matrix has the simple form

$$G = \left(\frac{\theta}{\mathbb{1}_n}\right). \tag{4.41}$$

We call such stabiliser states *graph states*. The name comes from the interpretation of the symmetric matrix θ as the adjacency matrix of a (weighted) graph Γ. Usually, it is required that the diagonal of θ is zero and thus the graph is simple, i. e. it does not contain self-loops. In this case, the generators of the stabiliser group have the appealing form

$$K_i := X_i \prod_{j=1}^{n} Z_j^{\theta_{ij}}. \tag{4.42}$$

Moreover, these generators are obtained by acting with the diagonal Clifford unitaries $CZ(\theta_{ij})$ on the generators $X_1, \ldots, X_n$ of the $|+^n\rangle$ state. Thus, the graph θ can be interpreted as a preparation instruction: Take a qudit for any vertex of the graph and prepare them in the superposition $|+^n\rangle$ (e. g. by a global Hadamard gate). Then, act with CZ on every pair of qudits that are connected by an edge.

It is straightforward to extend this to graphs with self-loops by replacing the CZ action with the action of the phase gate S on the corresponding qudit.

Finally, the underlying graph of a graph state encodes its entanglement structure. The state is entangled along a given bipartition if and only if there is an edge crossing it. Moreover, if there are m such edges, then there are local operations which convert the graph state into m copies of a Bell state [45].

Last but not least, it is not difficult to see that an arbitrary generator matrix as in Eq. (4.40) can be converted into graph form (4.41) by local Hadamard transformations. This means that any stabiliser state is locally Clifford-equivalent to a graph state [41]. In particular, the entanglement properties of stabiliser states are determined by the subset of graph states. However, this insight can also be useful outside of entanglement theory, see Ch. 8.

4.2.3 Expansion of stabiliser states in the computational basis

For any Lagrangian $L < \mathbb{F}_q^{2n}$ and character $\xi \in \hat{L}$, there is a canonical way of defining the state vectors $|L, \xi\rangle$ such that $|L, \xi\rangle\langle L, \xi| = P(L^\alpha, \xi)$ (in the following we assume that the phase function α is fixed), see also Refs. [75, 101, 110]. In general, these vectors are defined up to a phase as the normalised solution to the eigenvalue equations

$$\omega^{\mathrm{tr}\,\alpha(v)} W(v)\, |L, \xi\rangle = \xi(v)\, |L, \xi\rangle\,, \qquad \forall v \in L. \tag{4.43}$$

However, it is sufficient to know the solution for $\xi = 1$. To see this, write $\xi(v) = \overline{\chi}([a, v])$ for some $a \in \mathbb{F}_q^{2n}$ (cp. Sec. 3.1.2). Then, $|L, \xi\rangle = W(a)\, |L, 1\rangle$ since $\forall v \in L$:

$$\begin{aligned} \omega^{\mathrm{tr}\,\alpha(v)} W(v)W(a)\, |L, 1\rangle &= \overline{\chi}([a, v])\omega^{\mathrm{tr}\,\alpha(v)} W(a)W(v)\, |L, 1\rangle \\ &= \overline{\chi}([a, v]) W(a)\, |L, 1\rangle\,. \end{aligned} \tag{4.44}$$

Recall that we fixed a polarisation $\mathbb{F}_q^{2n} = \mathsf{Z} \oplus \mathsf{X}$ by the Z and X-Lagrangians. Define the projection $\mathrm{pr}_{\mathsf{X}} : \mathsf{Z} \oplus \mathsf{X} \to \mathsf{X}$ and set $\mathsf{X}_L := \mathrm{pr}_{\mathsf{X}}(L)$. In the standard basis, this projection acts as $\mathbb{F}_q^{2n} \ni (z, x) \mapsto (0, x)$. Note that if $(z, 0) \in \mathsf{Z} \cap L$, then $0 = [(z, 0), (z', x')] = [(z, 0), (0, x')]$ for all $(z', x') \in L$. Regarding X_L as a subspace of $\mathbb{F}_q^n$, we define a bilinear form on $\mathsf{X}_L \subset \mathbb{F}_q^n$ by

$$b_L(x, x') := [(z, x), (0, x')] = z \cdot x', \qquad \text{where } z \in \mathbb{F}_q^n :\ (z, x) \in L. \tag{4.45}$$

Indeed, for any two of such choices z, z', we have $(z, x) - (z', x) = (z - z', 0) \in \mathsf{Z} \cap L$ and thus b_L is well-defined. Note that b_L is symmetric:

$$b_L(x, x') - b_L(x', x) = z \cdot x' - z' \cdot x = [(z, x), (z', x')] = 0, \tag{4.46}$$

since $(z, x), (z', x') \in L$.

We can make this construction more explicit using a generator matrix of L in normal form, cp. Eq. (4.40):

$$G = \left(\begin{array}{cc} 0 & \mathbb{1}_{n-r} \\ \theta & C \\ \hline D & 0 \\ \mathbb{1}_r & 0 \end{array}\right). \tag{4.47}$$

We see that $\mathsf{X}_L \subset \mathbb{F}_q^n$ is an r-dimensional subspace spanned by vectors $b_i = d_i \oplus e_i$ for $i = 1, \ldots, r$ where d_i is the i-th column of the $(n - r) \times r$ matrix D. Let us denote the coordinates in the basis b_i of any x by $\vec{x}$. Then, $z = \theta\vec{x}$ is such that $(z, x) \in L$. Thus, the bilinear form b_L is explicitly given by

$$b_L(x, x') = \vec{x}^\top \theta \vec{x}'. \tag{4.48}$$

In particular, if the rank is maximal $r = n$, then $b_i = e_i$ is the standard basis and the bilinear form is directly given by θ.

Let us first assume that the characteristic is odd, $p \neq 2$, such that we can define an associated quadratic form $q_L(x) := 2^{-1} b_L(x, x)$ on X_L. Then, we define a state vector $|L\rangle$ by its components in the computational basis:

$$\psi_L(x) := |\mathsf{X}_L|^{-\frac{1}{2}} \chi(-q_L(x)) \mathbf{1}_{\mathsf{X}_L}(x) = p^{-\frac{r}{2}} \chi(-2^{-1} \vec{x}^\top \theta \vec{x}) \mathbf{1}_{\mathsf{X}_L}(x) \tag{4.49}$$

Then, it is straightforward to check that ψ_L is fixed by all $W(v)$ for $v = (v_z, v_x) \in L$ (cp. Eq. (3.43)). Here, we use that for any $x \in \mathsf{X}_L$, $x + v_x \in \mathsf{X}_L$.

$$\begin{aligned} W(v_z, v_x)\psi_L(x) &= |\mathsf{X}_L|^{-\frac{1}{2}} \chi(v_z \cdot x + 2^{-1} v_z \cdot v_x) \psi_L(x + v_x) \\ &= |\mathsf{X}_L|^{-\frac{1}{2}} \chi(v_z \cdot x + 2^{-1} v_z \cdot v_x - 2^{-1} b_L(v_x, v_x) - b_L(v_x, x) - 2^{-1} b_L(x, x) \\ &= |\mathsf{X}_L|^{-\frac{1}{2}} \chi(v_z \cdot x + 2^{-1} v_z \cdot v_x - 2^{-1} v_z \cdot v_x - v_z \cdot x - 2^{-1} b_L(x, x)) \\ &= |\mathsf{X}_L|^{-\frac{1}{2}} \chi(-q_L(x, x)) = \psi_L(x). \end{aligned} \tag{4.50}$$

The same derivation can be used to derive the form of stabiliser states with a non-trivial character $\xi(u) = \overline{\chi}([a, u])$ by letting $a = (a_z, a_x) \notin L$. As a convention, we omit the appearing global phase $\chi(-2^{-1} a_z \cdot a_x)$ in the definition of the state vector.

$$\begin{aligned} \psi_{L,a}(x) &:= |\mathsf{X}_L|^{-\frac{1}{2}} \chi(a_z \cdot (x + a_x)) \psi_L(x + a_x) \\ &= |\mathsf{X}_L|^{-\frac{1}{2}} \chi(a_z \cdot (x + a_x) - q_L(x + a_x)) \mathbf{1}_{\mathsf{X}_L - a_x}(x). \end{aligned} \tag{4.51}$$

Hence, the support of $\psi_{L,a}$ is not a *linear* subspace but an *affine* one. The affine shift is given by the x-component of $a = (z, x)$. The coefficients are determined by a quadratic form on the directional vector space, the quadratic part of which depends only on L and the linear part on z.

If the characteristic is even, $p = 2$, then we cannot associate a quadratic form to b_L. Instead, we have to use a quadratic refinement $q_L : \mathsf{X}_L \to \mathbb{Z}_4$ as in Eq. (3.81), i. e. a function fulfilling

$$q_L(x + x') - q_L(x) - q_L(x') = 2b_L(x, x'). \tag{4.52}$$

Concretely, we set $q_L(x) = b_L(x, x) \mod 4$. Then, the above derivation can be repeated to show that the state vector $|L\rangle$ defined by

$$\psi_L(x) := |\mathsf{X}_L|^{-\frac{1}{2}} \chi_4(-q_L(x)) \mathbf{1}_{\mathsf{X}_L}(x), \tag{4.53}$$

is fixed by the stabiliser group $W(L^\alpha)$. To this end, it is enough to check this on a basis of L on which α vanishes:

$$\begin{aligned} W(v_z, v_x)\psi_L(x) &= |\mathsf{X}_L|^{-\frac{1}{2}} \chi(v_z \cdot x)\chi_4(v_z \cdot v_x - q_L(x + v_x)) \\ &= |\mathsf{X}_L|^{-\frac{1}{2}} \chi(v_z \cdot x - b_L(v_x, x))\chi_4(v_z \cdot v_x - q_L(x) - q_L(v_x)) \\ &= |\mathsf{X}_L|^{-\frac{1}{2}} \chi(v_z \cdot x - v_z \cdot x)\chi_4(v_z \cdot v_x - q_L(x) - v_z \cdot v_x) \\ &= \psi_L(x). \end{aligned} \tag{4.54}$$

As above, stabiliser states with a non-trivial character $\xi(u) = \overline{\chi}([a, u])$ are obtained by the action of a Weyl operator:

$$\begin{aligned} \psi_{L,a}(x) &:= |\mathsf{X}_L|^{-\frac{1}{2}} \chi(a_z \cdot (x + a_x))\psi_L(x + a_x) \\ &= |\mathsf{X}_L|^{-\frac{1}{2}} \chi(a_z \cdot (x + a_x))\chi_4(-q_L(x + a_x)) \mathbf{1}_{\mathsf{X}_L - a_x}(x). \end{aligned} \tag{4.55}$$

Remark 4.1. We see that stabiliser state has *full support* in the computational basis if and only if $r = \dim \mathsf{X}_L = n$, i. e. if it is a graph state. In this case, the "wavefunction" has the form of a discrete Gaussian function [75]. If the support is not full and of dimension r, the stabiliser state can be seen to arise from an affine embedding of a full support state on r qudits.

Remark 4.2. The map which takes Lagrangian subspaces to state vectors in a Hilbert space is sometimes called the *quantisation map* in mathematical literature. Clearly, in odd characteristic, the mapping is canonical while it depends on a choice of basis (or α) in even characteristic.

4.3 $\mathbb{F}_q$ versus $\mathbb{F}_p$ structure

In this section, we want to come back to the mentioned fact in Sec. 3.1 that we can find an isomorphism between the additive group of the extension field $\mathbb{F}_q$ for $q = p^m$ and the $\mathbb{F}_p$-vector space $\mathbb{F}_p^m$. As we see shortly, this relates both the symplectic structures on $\mathbb{F}_q^{2n}$ and $\mathbb{F}_p^{2nm}$ and the associated representations on the Hilbert space $(\mathbb{C}^q)^{\otimes n} \simeq (\mathbb{C}^p)^{\otimes nm}$ resulting in an embedding of stabiliser codes and Clifford unitaries (see also Ref. [111]).

From the discussion in Sec. 3.1 we know that the additive group $\mathbb{F}_q^+$ is canonically an orthogonal $\mathbb{F}_p$-vector space and any explicit isomorphism is induced by the choice of a *field basis*. Since the phase space has the structure $V^* \oplus V$ with $V = \mathbb{F}_q^n$, any field basis, together with its *dual basis* induces a $\mathbb{F}_p$-isomorphism on the phase space level. Concretely, let us first consider a 2-dimensional phase space $\mathbb{F}_q^2 = \mathbb{F}_q \times \mathbb{F}_q$. Choose a basis

$b_1, \ldots, b_m$ on the second factor and introduce the corresponding dual basis $b^1, \ldots, b^m$ on the first factor. Clearly, this induces an isomorphism of $\mathbb{F}_p$ vector spaces

$$\begin{aligned} \mathbb{F}_q \times \mathbb{F}_q &\longrightarrow \mathbb{F}_p^m \times \mathbb{F}_p^m, \\ \Big(z = \sum_i z_i b^i, x = \sum_i x^i b_i\Big) &\longmapsto \Big(\vec{z} = (z_1, \ldots, z_m), \vec{x} = (x^1, \ldots, x^m)\Big). \end{aligned} \tag{4.56}$$

This generalises directly to $\mathbb{F}_q^{2n}$ by applying the isomorphism to any symplectic coordinate pair independently. Concretely, any point $\mathbb{F}_q^{2n} \ni (z, x) \equiv (z_1, \ldots, z_n, x^1, \ldots, x^n)$ is mapped to $(\vec{z}, \vec{x}) \equiv (z_{11}, \ldots, z_{nm}, x_{11}, \ldots, x_{nm})$.

It is straightforward to check that under the above isomorphism, the standard symplectic product $[\cdot, \cdot]_p$ on the right hand side corresponds to $\operatorname{tr}[\cdot, \cdot]_q$ on the left hand side. First, we compute

$$\operatorname{tr}(z \cdot x) = \sum_{i=1}^{n} \operatorname{tr}(z_i x^i) = \sum_{i=1}^{n} \sum_{j,k=1}^{m} z_{ij} x^{ik} \operatorname{tr}(b_j b^k) = \sum_{i=1}^{n} \sum_{j=1}^{m} z_{ij} x^{ij} = \vec{z} \cdot \vec{x}. \tag{4.57}$$

From this the claim follows directly:

$$\operatorname{tr}[(z, x), (z', x')]_q = \operatorname{tr}(z \cdot x') - \operatorname{tr}(z' \cdot x) = [(\vec{z}, \vec{x}), (\vec{z}', \vec{x}')]_p \tag{4.58}$$

Any k-dimensional $\mathbb{F}_q$-subspace $M \subset \mathbb{F}_q^{2n}$ inherits a linear $\mathbb{F}_p$-structure from $\mathbb{F}_q^{2n}$ which turns it into a km-dimensional $\mathbb{F}_p$-subspace. Under the above isomorphism, M thus maps to a km-dimensional subspace $\vec{M} \subset \mathbb{F}_p^{2nm}$. By Eq. (4.58), the isomorphism respects symplectic forms and thus maps *isotropic* subspaces M to isotropic subspaces $\vec{M}$.

Since $\mathbb{F}_q$-linear maps are in particular $\mathbb{F}_p$-linear, we get an embedding $\operatorname{End}(\mathbb{F}_q^{2n}) \hookrightarrow \operatorname{End}(\mathbb{F}_p^{2nm})$ under the above isomorphism. As this embedding is compatible with the symplectic structures, restriction symplectic maps yields $\operatorname{Sp}_{2n}(q) \hookrightarrow \operatorname{Sp}_{2nm}(p)$. However, both the endomorphisms and symplectic maps of $\mathbb{F}_p^{2nm}$ are strictly more than those of $\mathbb{F}_q^{2n}$.

It might be worthwhile to point out that the Heisenberg groups on $\mathbb{F}_q^{2n}$ and $\mathbb{F}_p^{2nm}$ are *not* isomorphic, simply because they have different centres $\mathbb{F}_q$ and $\mathbb{F}_p$, respectively $\mathbb{GIR}(q^2)$ and $\mathbb{Z}_4$ for $p = 2$. However, there is a induced surjection $\mathrm{H}_n(q) \twoheadrightarrow \mathrm{H}_{nm}(p)$ given by $(z, x, t) \mapsto (\vec{z}, \vec{x}, \operatorname{tr} t)$.[1]

On the Hilbert space level, the choice of primal basis induces an isomorphism $\mathbb{C}[\mathbb{F}_q^n] \simeq \mathbb{C}[\mathbb{F}_p]^{\otimes nm}$ by identifying any point $x = (x^i) \in \mathbb{F}_q^n$ with its entry-wise components $\vec{x} = (x^{ij})$ in the primal basis. Using the canonical identification $\mathbb{C}[\mathbb{F}_q^n] \simeq (\mathbb{C}^q)^{\otimes n}$ this isomorphism acts on any tensor factor as

$$\mathbb{C}^q \longrightarrow (\mathbb{C}^p)^{\otimes m}, \qquad |x\rangle \longmapsto \otimes_i |x^i\rangle. \tag{4.59}$$

Thus, the induced isomorphism respects Z and X operators in the following sense

$$\begin{aligned} X(x)\,|u\rangle = |u + x\rangle &\simeq |\vec{u} + \vec{x}\rangle = X(\vec{x})\,|\vec{u}\rangle\,, \\ Z(z)\,|u\rangle = \omega^{\operatorname{tr}(z \cdot u)}\,|u\rangle &\simeq \omega^{\vec{z} \cdot \vec{u}}\,|\vec{u}\rangle = Z(\vec{z})\,|\vec{u}\rangle\,. \end{aligned} \tag{4.60}$$

[1] This is precisely a m-fold covering of $\mathrm{H}_{nm}(p)$ by $\mathrm{H}_n(q)$.

And hence we find for $p \neq 2$:

$$W(z,x,t) = \omega^{\mathrm{tr}\, t}\omega^{2^{-1}\,\mathrm{tr}(z\cdot x)}Z(z)X(x) \simeq \omega^{\mathrm{tr}\, t}\omega^{2^{-1}\vec{z}\cdot\vec{x}}Z(\vec{z})X(\vec{x}) = W(\vec{z},\vec{x},\mathrm{tr}\, t). \tag{4.61}$$

However, for $p = 2$, this is not strictly true since the identity $\mathrm{tr}(z_i x^i) = \sum_{j=1}^m z_{ij}x^{ij}$ holds modulo 2 but the according phase is computed modulo 4. Since we have the identity $i^a i^b = i^{(a+b) \mod 2}(-1)^{ab}$ for all $a, b \in \mathbb{F}_2$, we see that this can only result in an additional minus sign on the right hand side. This shows that a choice of field basis eventually leads to equivalent representations over $\mathbb{F}_q$ and $\mathbb{F}_p$.

The above discussion shows that the symplectic structure and its representation over $\mathbb{F}_q$ embeds into the one over $\mathbb{F}_p$. More precisely, any isotropic subspace over $\mathbb{F}_q$ is an isotropic subspace over $\mathbb{F}_p$. The representations of the Heisenberg groups, the *Heisenberg-Weyl groups* $\mathrm{HW}_n(q)$ and $\mathrm{HW}_{nm}(p)$, are isomorphic. In particular, this implies that $\mathbb{F}_q$-stabiliser codes are $\mathbb{F}_p$-stabiliser codes. However, this embedding is not onto, meaning that not all stabiliser codes come from codes over $\mathbb{F}_q$.

A similar statement holds for the automorphisms of the Heisenberg groups. Since $\mathrm{Sp}_{2n}(q) \hookrightarrow \mathrm{Sp}_{2nm}(p)$ is not surjective, we find that the affine symplectic group $\mathrm{ASp}_n(q)$ properly embeds into $\mathrm{ASp}_{nm}(p)$. Although the affine symplectic group $\mathrm{ASp}_n(q)$ is the group of centre-fixing automorphisms of $\mathrm{H}_n(q)$, the automorphisms of its representation $\mathrm{HW}_n(q) \simeq \mathrm{HW}_{nm}(p)$ are thus strictly more and given by $\mathrm{ASp}_{nm}(p)$. Likewise, we have an embedding of Clifford groups $\mathrm{Cl}_n(q) \hookrightarrow \mathrm{Cl}_{nm}(p)$. While the Clifford unitaries in $\mathrm{Cl}_n(q)$ preserve the set of $\mathbb{F}_q$-stabiliser codes and $\mathbb{F}_p$-stabiliser codes individually, the ones in $\mathrm{Cl}_{nm}(p)$ will generally mix them.

At this point let us clarify the nomenclature. The Clifford group is commonly defined as the "finite" normaliser of the Heisenberg-Weyl group. However, over an extension field $\mathbb{F}_q$, this is $\mathrm{Cl}_{nm}(p)$. For this reason, we use a different definition and define the Clifford group $\mathrm{Cl}_n(q)$ as the one which is induced by $\mathrm{ASp}_n(q)$, cp. Eq. (4.11). In the literature, $\mathrm{Cl}_{nm}(p)$ and $\mathrm{Cl}_n(q)$ are sometimes referred to as *"many-particle"* vs. *"single-particle"* Clifford group [75] as well as (*the*) *Clifford group* vs. *restricted Clifford group* [67]. Here, we will call both groups *Clifford groups* and distinguish them by their symbols, respectively whether their action is $\mathbb{F}_p$ or $\mathbb{F}_q$-linear on phase space. We view them as *structure-preserving automorphisms* and thus, depending on whether it is important that this structure is over $\mathbb{F}_p$ or $\mathbb{F}_q$, one or the other Clifford group should be used.

4.4 Simulation of stabiliser circuits

In this section, we argue that the description of stabiliser states and codes, as well as its transformation under Clifford unitaries and Pauli measurements, is efficient in the number of qudits n. Thus, a classical computer is able to efficiently simulate any stabiliser circuit. This remarkable result is often referred to as *Gottesman-Knill theorem* [40]. However, the here presented method is more general since it can deal with arbitrary Clifford unitaries instead of only generators and is formulated for prime-power dimensions.

Stabiliser codes. A $[[n, n-k]]$ stabiliser code of local dimension $q = p^m$ is uniquely determined by a k-dimensional isotropic subspace $M \subset \mathbb{F}_q^{2n}$ and a phase function $\alpha : M \to \mathbb{F}_q$. Note that in order to describe the stabiliser code $\mathcal{C}(M^\alpha)$, it is sufficient to pick a set of independent generators for the associated stabiliser group $W(M^\alpha)$. The latter is

an Abelian group of order $q^k = p^{mk}$ and any element as order p. Thus mk generators are needed to describe the group. Pick a basis $\{v_1, \ldots, v_k\}$ of M and an arbitrary field basis $\{b_1, \ldots, b_m\}$. The mk vectors $v_{ij} := b_i v_j$ determine a set of generators $\omega^{s_{ij}} W(v_{ij})$ with $s_{ij} := \operatorname{tr} \alpha(v_{ij}) \in \mathbb{F}_p$. Note that this procedure effectively treats M as a mk-dimensional subspace over $\mathbb{F}_p$ The possible tuples $(s_{11}, \ldots, s_{mk}) \in \mathbb{F}_p^{mk}$ exactly index the $q^k = p^{mk}$ stabiliser codes associated with M. Thus, we can describe any $[[n, n-k]]$ stabiliser code by the following number of bits:

$$2nk \log_2(q) + m \log_2(q) + mk \log_2(p) = (2nk + m + k) \log_2(q) = O(nk). \tag{4.62}$$

Transformation under Clifford unitaries. In order to describe a Clifford unitary, one needs to store the associated symplectic matrix $g \in \mathrm{Sp}_{2n}(q)$ and the phase function $\delta : \mathbb{F}_q^{2n} \to \mathbb{F}_q$. It is certainly enough to now δ on a basis of $\mathbb{F}_q^{2n}$ and, for $p = 2$, compute other values of δ using the identity Eq. (3.71). This means that we need

$$4n^2 \log_2(q) + 2n \log_2(q) = (4n^2 + 2n) \log_2(q) = O(n^2) \tag{4.63}$$

bits to describe a Clifford unitary.

To compute the transformation of a stabiliser code given by (M, α) under a Clifford unitary described by (g, δ), we simply have to update the basis and signs as

$$v_j \longmapsto g(v_j), \qquad\qquad s_{ij} \longmapsto s_{ij} + \operatorname{tr} \delta(b_i v_j). \tag{4.64}$$

Updating the basis is done via matrix-vector multiplication, which can be done in $O(kn^2)$. The update the mk signs, the δ function has to be evaluated. If $p \neq 2$, δ is linear and thus it is enough to evaluate $\delta(v_j)$ which takes time $O(n)$ each, multiply it with b_i and add it to s_{ij}. In total, this takes time $O(kn + mk)$. For $p = 2$, we have to call $\delta(b_i v_j)$ which needs $O(2n)$ calls to β and the same number of additions. Moreover, any call to β needs time $O(n)$. Thus, the total cost is in this case $O(mkn^2)$. In summary, the cost of applying a Clifford unitary is in any case $O(kn^2)$.

Stabiliser measurements First, let us discuss so-called *Pauli/Weyl measurements*. For $p = q$, the measurement of a Weyl operator $W(a)$ is the projective measurement given by the p projectors P_k onto the eigenspace with eigenvalue ω^k. Since these are stabiliser codes with stabiliser group generated by $\omega^{-k} W(a)$, we can compute the outcome probabilities given a stabiliser state $|\psi\rangle\langle\psi| = P(L, \xi)$ using the overlap formula (4.33). The isotropic subspace associated with the eigenspaces of $W(a)$ is one-dimensional, $M = \langle a \rangle$. Thus, $M \cap L$ is either M or $\{0\}$. Note that we can determine this efficiently by checking whether a commutes with a basis of L. If so, $M \subset L$ and otherwise $M \cap L = \{0\}$. In the case $M \subset L$, we can find a k such that $\omega^{-k} = \xi(a)$. For this k, the character ξ agrees with the character of P_k, and thus the outcome distribution is deterministic: $\langle\psi| P_l |\psi\rangle = \delta_{k,l}$. If M and L only intersect in 0, then the characters have to agree there and hence the outcome distribution is uniform: $\langle\psi| P_l |\psi\rangle = 1/p$.

Note that to determine the type of outcome distribution, one has to evaluate $[a, v_i]$ for a given basis $v_1, \ldots, v_n$ of L which takes time $O(n^2)$. If the outcome is deterministic, the evaluation of $\xi(a)$ takes additional time $O(n)$. The post-measurement state can then be computed as follows. If $M \subset L$, i. e. a commutes with all v_i, the post-measurement state is identical to $|\psi\rangle$. Next, suppose that $[a, v_1] = c \neq 0$. We can assume that a commutes

with the remaining basis, since we can always add a suitable multiple of v_1 to a basis element v_j to ensure that $[a, v_j] = 0$. Having observed outcome k, the post-measurement state is $\sqrt{p}\, P_k \,|\psi\rangle$. This state is described by the Lagrangian $L' = \langle a, v_2, \ldots, v_n\rangle$ and a character ξ' which is given by $\xi'(v_i) = \xi(v_i)$ and $\xi'(a) = \omega^{-k}$. Computation of the post-measurement state thus requires a potential change of basis and re-computation of the phase function on the new basis. For $p \neq 2$ both the change of basis and the computation of phases is $O(n^2)$. For $p = 2$ the update of the phases is $O(n^3)$ similar to the argument for Clifford phases. Thus, the post-measurement state can be computed in time $O(n^2)$ for $p \neq 2$ and $O(n^3)$ for $p = 2$. Note that the actual runtime depends on how many generators need to be adapted. Furthermore, it is possible to improve this result to $O(n^2)$ for any p by extending the description of a stabiliser state by a Lagrangian L^* such that $\mathbb{F}_q^{2n} = L^* \oplus L$ [88].

For the extension case, $q = p^m$, the situation depends on the precise meaning of measuring a Weyl operator $W(a)$. If $W(a)$ is seen as an observable and the POVM is again given by the eigenspace projectors P_k, then this is *not* a stabiliser code over $\mathbb{F}_q$. This is because the dimension of every eigenspace is p^{mn-1} which is not a power of q. However, the eigenspaces are stabiliser codes over $\mathbb{F}_p$. Since any stabiliser state over $\mathbb{F}_q$ is in particular a stabiliser state over $\mathbb{F}_p$, we can again apply the above procedure to compute the outcome distribution. Note that in the case that $W(a)$ commutes with $|\psi\rangle\langle\psi|$, the measurement does not affect the state. In the case that it does not commute, the post-measurement state $\sqrt{p}\, P_k \,|\psi\rangle$ after observing outcome k is *not* a $\mathbb{F}_q$-stabiliser state but a $\mathbb{F}_p$-stabiliser state.

Alternatively, we can associate a different measurement to a Weyl operator $W(a)$ which is again given by the orthogonal projectors associated to $M = \langle a\rangle \subset \mathbb{F}_q^{2n}$. This case is analogous to the case $p = q$.

Finally, let us consider a stabiliser measurement which is given by the q^k orthogonal stabiliser codes associated with a k-dimensional isotropic subspace $M \subset \mathbb{F}_q^{2n}$. In this case, we have to determine the overlap $M \cap L$ with a given Lagrangian subspace M. Since this a subspace, $|M \cap L| = q^l$ for $0 \leq l \leq k$. Then, there are exactly q^{k-l} characters of M which agree with a given character ξ of L on $M \cap L$. Let us call the space of those $\widehat{M}_\xi$. Thus, the outcome distribution is

$$\operatorname{tr} P(M, \varsigma)^\dagger P(L, \xi) = q^{l-k}\, \mathbf{1}_{\widehat{M}_\xi}(\varsigma). \tag{4.65}$$

CHAPTER 5

APPLICATIONS

5.1 Discrete Wigner function

The introduced framework can be used to derive the so-called *phase space representation* of finite-dimensional quantum mechanics. This representation is based on the so-called *discrete Wigner function* which was first introduced by Wootters [72] in 1987 as a finite-dimensional analogue of the better-known Wigner function in continuous-variable systems. A few years later, Leonhardt [73, 74] used a similar Wigner function for quantum state tomography of finite-dimensional systems. With the increasing popularity of quantum information theory in the 2000s, there was renewed interest in the discrete Wigner function which resulted in several works on the discrete Wigner function, positively represented states and mutually unbiased bases [24, 25, 65, 75, 76]. Interestingly, these results are closely tied to theory of quantum computing and contextuality with immediate consequences. We will discuss these aspects in the next section.

The crucial observation is that the Weyl operators, both in even and odd characteristic, define an orthonormal basis for the space of linear operators $L\left((\mathbb{C}^q)^{\otimes n}\right)$ with the normalised *Hilbert-Schmidt* inner product

$$(A, B) := q^{-n} \operatorname{tr}(A^\dagger B), \tag{5.1}$$

since the composition law and tracelessness imply in both cases

$$(W(a), W(b)) \propto \operatorname{tr} W(b-a) = \delta_{a,b}. \tag{5.2}$$

Thus, any operator O can be uniquely written as

$$O = \sum_{a \in \mathbb{F}_q^{2n}} \Xi_O(a)\, W(a), \tag{5.3}$$

where $\Xi_O(a) := (W(a), O)$ is the *characteristic function* of O. Note that for a Hermitian O, the characteristic function is symmetric $\Xi_O(-a) = \Xi_O(a)$. Thus, the *symplectic Fourier transform* of Ξ_O,

$$\mathcal{W}_O(a) := \mathcal{F}\left[\Xi_O\right](a) := q^{-n} \sum_{b \in \mathbb{F}_q^{2n}} \overline{\chi}([a, b])\, \Xi_O(b), \tag{5.4}$$

is in this case a real-valued function on $\mathbb{F}_q^{2n}$. A somewhat dual, but equivalent point of view is to consider the Hermitian operators

$$A(a) := q^{-n} \sum_{b \in \mathbb{F}_q^{2n}} \overline{\chi}([a, b])\, W(b). \tag{5.5}$$

This is a unitary change of basis (w.r.t. the Hilbert-Schmidt inner product), thus the *phase point operators* $A(a)$ form an orthonormal basis, both for the complex vector space of

linear operators and the real vector space of Hermitian operators. Clearly, in this basis, X is given exactly as

$$X = \sum_{a \in \mathbb{F}_q^{2n}} \mathcal{W}_X(a) A(a). \tag{5.6}$$

The function $\mathcal{W}_X = \mathcal{F}[\Xi_X]$ is called the *discrete Wigner function* of X. We summarise the mentioned properties and a few more which follow easily from the definition, in the following proposition:

Proposition 5.1 (Properties of the Wigner function)**.**

1. *The phase point operators are a Hermitian, unit-trace orthonormal basis for* $L\left((\mathbb{C}^q)^{\otimes n}\right)$ *and* $H\left((\mathbb{C}^q)^{\otimes n}\right)$*. Thus:*

$$(X, Y) = \sum_{a \in \mathbb{F}_q^{2n}} \overline{\mathcal{W}_X}(a) \mathcal{W}_Y(b), \quad \textit{and} \quad \operatorname{tr} X = \sum_{a \in \mathbb{F}_q^{2n}} \mathcal{W}_X(a). \tag{5.7}$$

2. *For any Hermitian* X*,* $\mathcal{W}_X$ *is real-valued.*

3. *The Wigner function factors:*

$$\mathcal{W}_{X \otimes Y}(a \oplus b) = \mathcal{W}_X(a) \mathcal{W}_Y(b). \tag{5.8}$$

4. *Superoperators* $\phi : L\left((\mathbb{C}^q)^{\otimes n}\right) \to L\left((\mathbb{C}^q)^{\otimes n}\right)$ *are represented by their matrix representation*

$$\mathcal{W}_\phi(a|b) := \big(A(a), \phi(A(b))\big). \tag{5.9}$$

   Hermiticity-preserving maps have a real matrix representation. ϕ *is trace-preserving if and only if every column sums to 1. Likewise, it is unital if and only if every row sums to 1.*

5. *An effect* $E \geq 0$ *is represented by*

$$\mathcal{W}_E(a) = (E, W(a)). \tag{5.10}$$

6. *The Born rule has the representation*

$$\operatorname{tr}\left(E\phi(\rho)\right) = \sum_{a,b \in \mathbb{F}_q^{2n}} \mathcal{W}_E(a) \mathcal{W}_\phi(a|b) \mathcal{W}_\rho(b). \tag{5.11}$$

Thus, for quantum states the Wigner function gives a *quasi-probability representation* on the phase space $\mathbb{F}_q^{2n}$, i.e. it is real-valued and integrates to 1. Since the Wigner representation $\mathcal{W}_\phi(a|b)$ of a CPTP map preserves these quasi-probability distributions, it has the interpretation of a *transition matrix*. A non-negative Wigner representation would result in a proper probability distribution or stochastic matrix, respectively. Certainly, not all quantum states and operations can have non-negative representations. This would represent a *local hidden variable model* for quantum mechanics, which contradicts Bell's inequalities at the very minimum. Albeit, this will turn out to be true for a subclass of quantum states and operations.

However, the situation is again quite different in even and odd characteristic. First, let us focus on the (simpler) case of odd characteristic.

5.1.1 Non-negative representations

From the discussion in Sec. 4.1.1, we know that Clifford unitaries have the form $U = W(v)\mu(g)$ for $g \in \mathrm{Sp}_{2n}(q)$ and $v \in \mathbb{F}_q^{2n}$. Using their action as centre-fixing automorphisms of the Heisenberg group, we can compute the transformation of phase point operators straightforwardly:

$$\begin{aligned} W(v)\mu(g)A(a)\mu(g)^\dagger W(v)^\dagger &= q^{-n} \sum_{b\in\mathbb{F}_q^{2n}} \overline{\chi}([a,b])\chi([v,gb])W(gb) \\ &= q^{-n} \sum_{b\in\mathbb{F}_q^{2n}} \overline{\chi}([a,g^{-1}b])\chi([v,b])W(b) \\ &= q^{-n} \sum_{b\in\mathbb{F}_q^{2n}} \overline{\chi}([ga-v,b])W(b) \\ &= A(ga-v). \end{aligned} \tag{5.12}$$

Hence, the Wigner function of a state ρ transforms as

$$\mathcal{W}_{U\rho U^\dagger}(a) = \mathcal{W}_\rho(g^{-1}a+v), \qquad U = W(v)\mu(g). \tag{5.13}$$

This is called the *Clifford covariance* of the Wigner function. Put differently, a Clifford unitary corresponds to an affine permutation of the points in phase space without actually changing the values of the Wigner function. The matrix representation of a Clifford unitary is thus a permutation matrix:

$$\mathcal{W}_U(a|b) = \delta_{a,gb-v}. \tag{5.14}$$

This means that the *negativity* of a state ρ,

$$\mathcal{N}(\rho) := \sum_{a\in\mathbb{F}_q^{2n}} |\mathcal{W}_\rho(a)| \equiv \|\mathcal{W}_\rho\|_1 \geq 1, \tag{5.15}$$

is an invariant under Clifford transformations.

We know that every stabiliser state can be written as

$$s = P(L,a) = q^{-n} \sum_{l\in L} \chi([h,l])W(l), \tag{5.16}$$

where $L \subset \mathbb{F}_q^{2n}$ is a Lagrangian subspace and $h \in \mathbb{F}_q^{2n}$ represents an additive character on L This directly gives the characteristic function of s as

$$\Xi_s(a) = q^{-n}\chi([h,a])\mathbf{1}_L(a), \tag{5.17}$$

where $\mathbf{1}_L$ is the indicator function on L. The Wigner function is its symplectic Fourier transform:

$$\begin{aligned} \mathcal{W}_s(a) &= q^{-n} \sum_{b\in\mathbb{F}_q^{2n}} \overline{\chi}([a,b])q^{-n}\chi([h,b])\,\mathbf{1}_L(b) \\ &= q^{-2n} \sum_{b\in L} \overline{\chi}([a,b])\chi([h,b]) \\ &= q^{-n}\,\mathbf{1}_L(a-h) \\ &= q^{-n}\,\mathbf{1}_{L+h}(a) \end{aligned} \tag{5.18}$$

Here, we used that a and h define the same character on L if and only if $a - h \in L^\perp = L$, see also Sec. 3.1.2. Thus, the Wigner function of a stabiliser state is given by the normalised indicator function of affine shifts of the underlying Lagrangian subspace. In particular, it is *non-negative*. In the light of the previous comment, this means that the sub-theory encompassing stabiliser states and Clifford has a *hidden variable model*, given by their phase space representation.

While all states in the convex hull of stabiliser states, the *stabiliser polytope* SP, are non-negatively represented, a natural question to ask is whether these are all. Let us define the *Wigner polytope* WP as the polytope in the $(q^{2n} - 1)$-dimensional space of unit-trace Hermitian operators which is given by the intersection of the q^{2n} half spaces $\mathrm{tr}(OA(a)) \geq 0$. By definition, any point in WP corresponds to a probability distribution on $\mathbb{F}_q^{2n}$ and WP is a q^{2n}-simplex. Since SP is clearly *not* a simplex and we have SP $\subsetneq$ WP by a purely geometric argument. However, the actual question is whether SP $\stackrel{?}{=}$ WP $\cap\, \mathbb{S}_+$ where $\mathbb{S}_+$ is the cone of positive semi-definite matrices. As all stabiliser states have a non-negative representation it is straightforward to show that the facets of WP also define facets of SP [26]. Since these have to be a proper subset of the facets of SP (otherwise it would be a simplex), there are states in WP $\setminus$ SP.

Indeed, Gross [75] showed that the only *pure* states with non-negative Wigner function are stabiliser states. This implies that the states in WP $\setminus$ SP are necessarily *mixed*. An example for such a state was given in Ref. [75]. These mixed states belong to the class of *bound magic states* which will be discussed in the next section.

Finally, we want to remark that the here introduced discrete Wigner function corresponds to a certain choice of representation which is in accordance with the axioms for generalised Wigner functions, introduced in Ref. [65] It is the unique choice which is Clifford-covariant [75].

5.1.2 Classical simulation

An overall non-negative Wigner representation of a quantum state undergoing a quantum channel with eventual measurement represents a stochastic process on the phase space $\mathbb{F}_q^{2n}$. Indeed, consider the expansion of the Born rule:

$$\mathrm{tr}\left(E\phi_d \circ \cdots \circ \phi_1(\rho)\right) = \sum_{a_0,\ldots,a_d \in \mathbb{F}_q^{2n}} \mathcal{W}_E(a_d)\mathcal{W}_{\phi_d}(a_d|a_{d-1}) \cdots \mathcal{W}_{\phi_1}(a_1|a_0)\mathcal{W}_\rho(a_0). \quad (5.19)$$

If any Wigner representation on the right hand side is non-negative, then the sequence of quantum channels $\phi_1, \ldots, \phi_d$ define a Markov chain with random variables $A_0, \ldots, A_d$ on phase space which are distributed according to

$$\Pr[A_0 = a_0, \ldots, A_d = a_d] = \mathcal{W}_{\phi_d}(a_d|a_{d-1}) \cdots \mathcal{W}_{\phi_1}(a_1|a_0)W_\rho(a_0). \quad (5.20)$$

The $\mathcal{W}_{\phi_d}(a_i|a_{i-1})$ represent the transition probabilities $a_{i-1} \to a_i$ for the states of the Markov chain. In particular, it is possible to efficiently sample from this distribution, given that we can efficiently sample from the initial distribution $\mathcal{W}_\rho$. Hence, we can approximate the Born probability in Eq. (5.19) using Monte-Carlo sampling. Since the estimator $X := \mathcal{W}_E(A_d)$ is bounded between 0 and 1, Hoeffding's inequality ensures that after taking N samples we have

$$\Pr\left[|\bar{X} - \mathbb{E}[\bar{X}]| \geq \delta\right] \leq 2e^{-2N\delta^2}, \quad (5.21)$$

where $\bar{X}$ is the mean of N iid copies of X and $\mathbb{E}[\bar{X}] = \mathbb{E}[X] = \mathrm{tr}\,(E\phi_d \circ \cdots \circ \phi_1(\rho))$. Conversely, we need

$$N \geq \frac{1}{2}\delta^{-2}\log\left(\frac{2}{\varepsilon}\right) \tag{5.22}$$

samples to ensure that $\bar{X}$ is in a confidence interval of size δ around μ with probability at least $1-\varepsilon$.

For the simulation of pure state dynamics of stabiliser states with respect to Clifford unitaries and stabiliser measurements, Monte-Carlo simulation based on the Wigner representation is generally not the most efficient method (cp. Sec. 4.4). However, the presence of noise or more general quantum channels leads to mixed-state dynamics which cannot be simulated by other means. Moreover, the non-negatively represented states and operations are strictly larger than the convex hull of stabiliser states and Clifford unitaries. In this sense, Monte-Carlo simulation is the most general efficient simulation method.

This argument shows that *negativity in the Wigner representation is necessary for a quantum speed-up* [26]. In fact, the Wigner negativity of an input state

$$\mathcal{N}(\rho) := \sum_{a\in\mathbb{F}_q^{2n}} |\mathcal{W}_\rho(a)| \equiv \|\mathcal{W}_\rho\|_1, \tag{5.23}$$

can be directly related to the runtime of a classical simulation algorithm simulating non-negatively represented dynamics with ρ as an input [29]. More precisely, we can rewrite the Born rule as follows

$$\begin{aligned}
\mathrm{tr}\,(E\phi(\rho)) &= \sum_{a,b\in\mathbb{F}_q^{2n}} \mathcal{W}_E(a)\mathcal{W}_\phi(a|b)\mathcal{W}_\rho(b) && (5.24)\\
&= \sum_{a,b\in\mathbb{F}_q^{2n}} \mathrm{sgn}(\mathcal{W}_\rho(b))\mathcal{N}(\rho)\mathcal{W}_E(a)\mathcal{W}_\phi(a|b)\frac{|\mathcal{W}_\rho(b)|}{\mathcal{N}(\rho)} && (5.25)\\
&= \sum_{a,b\in\mathbb{F}_q^{2n}} X(a,b)p(a,b). && (5.26)
\end{aligned}$$

Hence, it can be interpreted as the expectation value of $X(a,b) = \mathrm{sgn}(\mathcal{W}_\rho(b))\mathcal{N}(\rho)\mathcal{W}_E(a)$ with respect to the probability distribution $p(a,b) = \mathcal{W}_\phi(a|b)|\mathcal{W}_\rho(b)|/\mathcal{N}(\rho)$. Using Monte-Carlo sampling as before, it is hence possible to approximate $\mathbb{E}[X] = \mathrm{tr}\,(E\phi(\rho))$. In contrast to before, the random variable X is now bounded as $|X| \leq \mathcal{N}(\rho)$. To use Hoeffding's inequality a renormalisation $\delta \mapsto \delta/\mathcal{N}(\rho)$ is necessary which results in the following Hoeffding bound on the number of samples:

$$N \geq \frac{1}{2}\mathcal{N}(\rho)^2\delta^{-2}\log\left(\frac{2}{\varepsilon}\right). \tag{5.27}$$

To illustrate the qualitative change, let us consider the simulation of quantum computation in the magic state model. In this model, any quantum circuit is re-expressed as a stabiliser circuit acting on enough copies of a magic state $|\theta\rangle$ with $\mathcal{N}(\theta) > 1$. Since the Wigner function is multiplicative, the above argument shows that the runtime of a Monte-Carlo simulation scales as $O(\mathcal{N}(\theta)^{2t})$. Thus, this approach scales exponentially with the required number of non-stabiliser resources.

It is straightforward to extend this idea from negatively represented input states to negatively represented operations [29]. Then, the runtime scales quadratically in the overall negativity in the representation which is given as the product of the negativities in the input state and all operations.

5.1.3 The situation in even characteristic

The previous discussions show that the Wigner function is a powerful tool in the analysis of finite-dimensional quantum systems, especially in the context of quantum computing. Hence, a natural question to ask is whether this construction can be generalised to the qubit case. In Sec. 3.3 and 4, we have seen that the case of even characteristic comes with additional obstacles such as phases of higher order and non-linearities in the representations of stabiliser codes and Clifford unitaries. As we will see shortly, these mathematical problems eventually lead to the non-existence of a suitable Wigner function for qubits.

Given the definition of the Wigner function in Eq. (5.4), we can compute the Wigner function of a n-qubit stabiliser state

$$\rho = \frac{1}{2^n} \sum_{v \in L} (-1)^{[h,v]+\alpha(v)} W(v). \tag{5.28}$$

Here, α is a phase function which encodes the non-linear dependence on v (cp. Sec. 4). Due to this non-linear term, the Wigner function on ρ will not be a simple indicator function. Similarly, the non-linearity in the action of Clifford unitaries on Weyl operators result in a *non-covariance* of the Wigner function under the Clifford action. These problems are in fact intertwined. Due to the non-linearity, one can find stabiliser states which are *negatively represented*, although some like the $|0\rangle$ state are still non-negative. Since all stabiliser states form a single Clifford orbit of $|0\rangle$, this negativity can be interpreted as being induced from certain non-negatively represented Clifford unitaries.

One might hope that it is possible to find an alternative definition of the Wigner function for qubits, such that stabiliser states and Clifford unitaries are again non-negatively represented. Thus, the task is to find an operator basis of $L(\mathbb{C}^q)$ such that the Clifford group acts *covariantly* on it, i. e. the Clifford group induces a transitive permutation action on the labels of the basis. Even under these very general assumptions, Zhu [112] showed that when q is an odd prime-power, than any Clifford-covariant operator basis is equivalent to the basis of phase point operators. Moreover, if q is an even prime-power, then such an operator basis does not exist. As it shown in Ref. [112], the latter conclusion follows from an old result in Bolt, Room and Wall [77], namely that the Clifford group does not have a subgroup isomorphic to $\mathrm{Sp}_{2n}(2)$. This is a manifestation of the non-existence of a proper Weil representation in even characteristic.

More generally, Zhu [113] also showed that no operator basis can be covariant with respect to a unitary 3-design. The Clifford group forms such a 3-design in even prime-power dimensions, but only a unitary 2-design in odd prime-power dimensions [113, 114]. Albeit, a recent classification of unitary group designs shows that the multi-qubit Clifford group is basically the only unitary 3-design which forms a group, besides exceptions in special dimensions [115]. For a discussion of this result, see also Ch. 13.

5.2 Mutually unbiased bases

In this section, we make use of the introduced extension field structure to show that stabiliser states define a maximal set of *mutually unbiased bases*. Two orthonormal bases B, B' of $\mathbb{C}^d$ are called *unbiased* if

$$|\langle\psi|\varphi\rangle|^2 = \frac{1}{d} \qquad \forall\psi \in B, \varphi \in B'. \tag{5.29}$$

It is not hard to show that the maximum number of bases which are mutually unbiased is $d+1$ [116]. We call such a complete, i. e. maximal, set of mutually unbiased bases a MUB.

Originally, MUBs have been introduced as on optimal way to perform state reconstruction via measurements of the MUB in the sense that errors are minimised [61, 117]. This is closely related to the fact that a MUB forms a *complex projective 2-design*, i. e. the MUB vectors minimise the *frame potential*

$$\Phi_2[(\psi_i)] := \frac{1}{N^2}\sum_{i,j=1}^{N} \left|\langle\psi_i|\psi_j\rangle\right|^4 \geq \frac{2}{d(d+1)}. \tag{5.30}$$

This is straightforward to check: By pairing all vectors from two different bases we get a contribution of $d^{-2}d^2 = 1$ and there are $d(d+1)$ many basis pairs. Moreover, the sum of the norms of all basis elements yields a total contribution of $d(d+1)$. Thus, the frame potential is

$$\Phi_2[\text{MUB}] = \frac{2d(d+1)}{d^2(d+1)^2} = \frac{2}{d(d+1)}, \tag{5.31}$$

which shows that any MUB is a 2-design.

If the dimension d is a prime-power $d = q = p^m$, then there exists a "canonical" MUB which can be constructed as follows. Consider the phase space $\mathbb{F}_q^2$ associated with $\mathbb{C}^q$. Recall from Sec. 4.2 that any Lagrangian L defines an orthonormal basis $B(L)$ of $\mathbb{C}^q$ via its associated stabiliser states. Furthermore, there are $q+1$ Lagrangians which simply correspond to the one-dimensional subspaces of $\mathbb{F}_q^2$. This implies that any two different Lagrangians $L \neq L'$ can only intersect in 0. Hence, by the overlap formula (4.33), any two stabiliser states corresponding to $L \neq L'$ have overlap

$$|\langle\psi|\varphi\rangle|^2 = \frac{1}{q} \qquad \forall\psi \in B(L), \varphi \in B(L'). \tag{5.32}$$

Therefore, the $q+1$ bases $B(L)$ indexed by Lagrangians $L \subset \mathbb{F}_q^2$ define a complete set of mutually unbiased bases.

The so-constructed MUB is canonical in the sense that it is the unique minimal complex projective 2-design which is covariant with respect to the Clifford group $\mathrm{Cl}_1(q)$ (except for $q = 3$, then it is the second smallest) [71]. Since the Clifford group $\mathrm{Cl}_1(q)$ is a unitary 2-design in any prime-power dimension, any orbit is a Clifford-covariant complex projective 2-design (cp. Part III, Sec. 12.2). The canonical MUB is the smallest among all orbits (respectively second smallest for $q = 3$).

Notably, the existence of MUB in non-prime-power dimensions has not been proven, although this topic has attracted a lot of attentions in the quantum information and mathematical community. This is also due to the fact that MUBs are closely related to symmetric informationally complete positive operator-valued measures (SIC-POVM). There

exist explicit constructions of mutually unbiased bases, but the maximal number of bases in a given dimension is usually unknown, e. g. for the smallest case $d = 6$. Some works even raised doubts on whether a complete set exists in $d = 6$ [84].

5.3 Algorithms

5.3.1 Subgroup algorithm for $\mathrm{Sp}_{2n}(q)$ sampling

Uniform sampling from the symplectic group $\mathrm{Sp}_{2n}(q)$ can be achieved using a variant of the subgroup algorithm [118]. Here, we give a generalisation of the approach by Koenig and Smolin [119] for qubits to fields of any characteristic.

Within this section, we a different coordinate convention than in the rest of this part. The "local" convention used here is given by grouping symplectic pairs, explicitly this is $(z_1, \ldots, z_n, x_1, \ldots, x_n) \mapsto (z_1, x_1, \ldots, z_n, x_n)$. In this way, the phase space factorises as $\mathbb{F}_q^{2n} = \mathbb{F}_q^2 \oplus \cdots \oplus \mathbb{F}_q^2$.

The key observation is the following. Given a nested chain of subgroups of a finite group G,

$$G_1 < G_2 < \cdots < G_{n-1} < G_n = G, \tag{5.33}$$

we have an isomorphism of right cosets

$$\begin{aligned} G_n/G_{n-1} \times G_{n-1}/G_{n-2} \times \cdots \times G_2/G_1 \times G_1 &\xrightarrow{\sim} G, \\ ([g_n], [g_{n-1}], \ldots, [g_2], g_1) &\longmapsto g_n \cdots g_1. \end{aligned} \tag{5.34}$$

In particular, given a transversal (a choice of representatives) for the cosets, any element in G has a unique decomposition as a product. Drawing independently and uniform from every quotient yields therefore a uniform sample of the group G.

For the symplectic group $\mathrm{Sp}_{2n}(q)$, we naturally have such a subgroup chain, given by the embeddings

$$\mathrm{Sp}_{2m-2}(q) \hookrightarrow \mathrm{Sp}_{2m}(q), \quad S \longmapsto \mathbb{1} \oplus S. \tag{5.35}$$

Hence, the right action of $\mathrm{Sp}_{2m-2}(q)$ in $\mathrm{Sp}_{2m}(q)$ will only effect the last $2m-2$ columns while leaving the symplectic product between any two columns invariant. Thus, this action corresponds to a symplectic basis change in the symplectic complement $\langle v_1, v_2 \rangle^\perp$ of the first two columns v_1, v_2. This establishes an isomorphism between the right cosets $\mathrm{Sp}_{2m}(q)/\mathrm{Sp}_{2m-2}(q)$ and the symplectic pairs $\mathcal{S}_m := \left\{ (v_1, v_2) \in \mathbb{F}_q^{2m} \times \mathbb{F}_q^{2m} \mid [v_1, v_2] = 1 \right\}$. Vice versa, given a symplectic pair, one can construct a representative of the corresponding coset by extending the pair to a symplectic basis (e. g. using Gram-Schmidt).

The here described subgroup algorithm basically achieves the task of randomly selecting a symplectic pair for the first two columns and then proceeds by repeating this construction in the symplectic complement.

Given a random vector $v_1 \in \mathbb{F}_q^{2m} \setminus 0$, all symplectic partners lie in the affine plane $u + v_1^\perp$ where u is some vector with $[u, v_1] = 1$. Thus, drawing a partner at random can be achieved by completing v_1 to a symplectic basis $v_1, \ldots, v_{2m}$ and adding a random vector from $v_1^\perp = \langle v_1, v_3, \ldots, v_{2m} \rangle$ to v_2. However, instead of constructing the symplectic extension explicitly, we will construct a symplectic map S mapping the first standard basis vector e_1 to v_1 and e_2 to a random symplectic partner v_2. Such a matrix is automatically a representative of a random coset in $\mathrm{Sp}_{2m}(q)/\mathrm{Sp}_{2m-2}(q)$.

The major tool are so-called *symplectic transvections*. Given a vector $h \in \mathbb{F}_q^{2m}$ and a scalar $\lambda \in \mathbb{F}_q^\times$, a symplectic transvection is a symplectic map $T_{\lambda,h}$ such that $T_{\lambda,h}(x) = x + \lambda[x,h]h$. A basic fact from symplectic geometry is that transvections generate the symplectic group.

We need the following lemma.

Lemma 5.1. *Let $x, y \in \mathbb{F}_q^{2m} \setminus 0$ be two vectors. Then, there are vectors h_1, h_2 and scalars λ_1, λ_2 such that $y = T_{\lambda_1,h_1} T_{\lambda_2,h_2}(x)$.*

We will give a constructive proof.

Proof. If $x = y$, $h_1 = h_2 = 0$ and $\lambda_1 = \lambda_2 = 1$ will do the job. For $x \neq y$, we will consider two cases.

Case 1: $[x,y] = a \neq 0$. Let us define $h = -x + y$ and $\lambda = a^{-1}$. We get

$$T_{\lambda,h}(x) = x + \lambda[x,h]h = x + \lambda[x,y](-x+y) = y. \tag{5.36}$$

Case 2: $[x,y] = 0$. Let us denote by $x^{(j)} = (x_{2j-1}, x_{2j})$ and similar $y^{(j)}$ the components in the $j-th$ subsystem. We will further distinguish the following cases:

a) $\exists j \in \{1,\dots,m\}$ such that $x^{(j)} \neq 0$ and $y^{(j)} \neq 0$. In this case, there is always a vector $v \in \mathbb{F}_q^2 \setminus 0$ such that $[x^{(j)}, v] \neq 0$ and $[v, y^{(j)}] \neq 0$. Padding v with zeros to a vector z in $\mathbb{F}_q^{2m}$, we can apply Case 1 twice to get two transvections mapping $x \mapsto z \mapsto y$.
More precisely, if $[x^{(j)}, y^{(j)}] \neq 0$, then there is a unique vector $v \in \mathbb{F}_q^2 \setminus 0$ such that $[x^{(j)}, v] = [v, y^{(j)}] = 1$ since this is a linear system of equations

$$\begin{pmatrix} x_{2j-1} & -x_{2j} \\ -y_{2j-1} & y_{2j} \end{pmatrix} \begin{pmatrix} v_2 \\ v_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \tag{5.37}$$

and the determinant is exactly $[x^{(j)}, y^{(j)}] \neq 0$.
Otherwise, if $[x^{(j)}, y^{(j)}] = 0$, the two vectors have to be proportional, $x^{(j)} = a y^{(j)}$, since the orthocomplement of a two-dimensional vector is spanned by the vector itself. Then, there is a vector $v \in \mathbb{F}_q^2 \setminus 0$, such that $[x^{(j)}, v] = 1$ and $[v, y^{(j)}] = a$ and we can again apply Case 1.

b) If such an index does not exist, there have to be pairs $j, k \in \{1,\dots,n\}$ such that $x^{(j)} \neq 0$ and $y^{(j)} = 0$ and vice versa (otherwise one of the vectors would be zero). We can find vectors $v, w \in \mathbb{F}_q^2 \setminus 0$ such that $[x^{(j)}, v] = 1$ and $[w, y^{(k)}] = 1$. Setting $z = v_1 e_{2j-1} + v_2 e_{2j} + w_1 e_{2k-1} + w_2 e_{2k}$, we can again apply Case 1 to $x \mapsto z \mapsto y$.

□

Finally, a random symplectic pair can be generated as follows. Select a random vector $v_1 \in \mathbb{F}_q^{2m} \setminus 0$. By the previous lemma, there is a pair of transvections $T = T_{\lambda_1,h_1} T_{\lambda_2,h_2}$ such that $T(e_1) = v_1$. Clearly, the images $v_i = T(e_i)$ of the standard basis form a symplectic basis. Next, let us sample random scalars $c_3, \dots, c_{2n} \in \mathbb{F}_q$ and define the vectors

$$e := e_1 + \sum_{i=3}^{2m} c_i e_i, \qquad h_0 := T(e) = v_1 + \sum_{i=3}^{2m} c_i v_i. \tag{5.38}$$

Note that $[v_1, h_0] = 0$ and $[v_2, h_0] = -1$. Thus, we have

$$\begin{aligned} T_{-1,h_0}T(e_1) &= T_{-1,h_0}(v_1) = v_1 - [v_1, h_0]h_0 = v_1, \\ T_{-1,h_0}T(e_2) &= T_{-1,h_0}(v_2) = v_2 - [v_2, h_0]h_0 = v_1 + v_2 + \sum_{i=3}^{2m} c_i v_i. \end{aligned} \tag{5.39}$$

Next, choose another random scalar $c_1 \in \mathbb{F}_q$ and compute

$$\begin{aligned} T_{(1-c_1),v_1}T_{-1,h_0}T(e_1) &= T_{(1-c_1),v_1}(v_1) = v_1, \\ T_{(1-c_1),v_1}T_{-1,h_0}T(e_2) &= v_1 + v_2 + \sum_{i=3}^{2m} c_i v_i + (1-c_1)[v_2, v_1]v_1 \\ &= c_1 v_1 + v_2 + \sum_{i=3}^{2m} c_i v_i. \end{aligned} \tag{5.40}$$

Hence, the random product of transvections $T' = T_{(1-c_1),f_1}T_{-1,h_0}T_{\lambda_1,h_1}T_{\lambda_2,h_2}$ maps e_1 to v_1 and e_2 to a random symplectic partner of v_1. Thus, T' is a representative of a random right coset in $\mathrm{Sp}_{2m}(q)/\mathrm{Sp}_{2m-2}(q)$.

Note that the image under a transvection $T_{\lambda,h}$ can be computed in time $O(m)$ whereas for an arbitrary matrix $g \in \mathbb{F}_q^{2m\times 2m}$ this is $O(m^2)$. Thus, the product $T_{\lambda,h}\,g$ can be computed in time $O(m^2)$ by applying $T_{\lambda,h}$ row-wise. Hence, it is not only more efficient to store the components of $T' = T_{(1-c_1),f_1}T_{-1,h_0}T_{\lambda_1,h_1}T_{\lambda_2,h_2}$ instead of T', but this storage allows for a faster matrix multiplication with T' from the left.

Let RANDOMCOSET(m) be the routine which outputs a representative of a random coset in $\mathrm{Sp}_{2m}(q)/\mathrm{Sp}_{2m-2}(q)$ as a list of transvections $\{T_1, \ldots, T_4\}$ (given by their parameters). Then, we can sample a random symplectic matrix in $\mathrm{Sp}_{2n}(q)$ by calling RANDOMCOSET recursively as follows:

Algorithm 1 Sampling of random symplectic matrix $g \in \mathrm{Sp}_{2n}(q)$ using subgroup algorithm

```
1: function RandomSymplecticMatrix(n)
2:     T_1, ..., T_4 ← RandomCoset(n)
3:     if n = 1 then
4:         g ← T_1 ··· T_4
5:         return g
6:     else
7:         g ← T_1 ··· T_4 (𝟙 ⊕ RandomSymplecticMatrix(n − 1))
8:         return g
9:     end if
10: end function
```

In Algorithm 1, the product of transvections in line 4 is most efficiently computed by applying the transvections consecutively on the standard basis $\{e_1, e_2\}$. Similarly, in line 7, the matrix product should be performed by applying the transvections row-wise. Thus, any matrix operation can be done in time $O(n^2)$. Moreover, RANDOMCOSET(n) has runtime $O(n)$. Since we have n recursions, the total runtime of RANDOMSYMPLECTICMATRIX(n) is $O(n^3)$.

5.3.2 Synthesis for $\mathrm{Sp}_{2n}(q)$

With this section, we return to the standard convention for symplectic basis of $\mathbb{F}_q^{2n}$, which is $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$.

To goal of this section is to derive a decomposition of symplectic matrices into matrices from the subgroups introduced in Sec. 3.1.4. There, we defined

$$S_n(q) := \left\{ S(R) := \begin{pmatrix} \mathbb{1} & R \\ 0 & \mathbb{1} \end{pmatrix} \mid R \in \mathrm{Sym}_n(q) \right\}, \tag{5.41}$$

$$G_n(q) := \left\{ G(Q) := \begin{pmatrix} Q^{-\top} & 0 \\ 0 & Q \end{pmatrix} \mid Q \in \mathrm{GL}_n(q) \right\}. \tag{5.42}$$

These subgroups, together with the symplectic unit

$$J = \begin{pmatrix} 0 & \mathbb{1}_n \\ -\mathbb{1}_n & 0 \end{pmatrix}, \tag{5.43}$$

generate the symplectic group.

The decomposition is a slightly modified version of the one given by Rengaswamy, Calderbank, Kadhe and Pfister [103]. We show that any element $M \in \mathrm{Sp}_{2n}(q)$ for $q = p^m$ can be written as

$$M = G(Q_1) J S(R_1) J_r^\top S(R_2) G(Q_2), \tag{5.44}$$

where J_r is defined by $U_r := \mathbb{1}_r \oplus 0_{n-r}$, $L_{n-r} := 0_r \oplus \mathbb{1}_{n-r}$ as follows

$$J_r := \begin{pmatrix} L_{n-r} & U_r \\ -U_r & L_{n-r} \end{pmatrix}, \tag{5.45}$$

i. e. J_r is J applied to the first r symplectic pairs.

Proof of decomposition of symplectic matrices

Here is a constructive proof which can be used as an algorithm to compute the decomposition Eq. (5.44). Let us write

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}. \tag{5.46}$$

Using Gauss elimination, we can bring A into reduced row echelon form. If $\mathrm{rk}(A) = r$, we thus find invertible matrices Q_{11} and Q_2 such that

$$Q_{11}^{-\top} A Q_2^{-\top} = \begin{pmatrix} \mathbb{1}_r & 0 \\ 0 & 0 \end{pmatrix}. \tag{5.47}$$

Acting with $G(Q_{11})$ and $G(Q_2)$ on M from the left and right will thus transform the first row of M to

$$Q_{11}^{-\top} \begin{pmatrix} A & B \end{pmatrix} \begin{pmatrix} Q_2^{-\top} & 0_n \\ 0_n & Q_2 \end{pmatrix} = \left(\begin{array}{cc|cc} \mathbb{1}_r & 0 & T_r & E \\ 0 & 0 & E' & F_{n-r} \end{array}\right). \tag{5.48}$$

However, since this is still the first row of a symplectic matrix, we find that $T_r = T_r^\top$ and $E' = 0$, hence F_{n-r} is of full rank. Therefore, setting $Q_{12} := \mathbb{1}_r \oplus F_{n-r}^\top$ and acting with $G(Q_{12}^{-1})$ from the left transforms the first row to

$$Q_{12}^{-\top} Q_{11}^{-\top} \begin{pmatrix} A & B \end{pmatrix} \begin{pmatrix} Q_2^{-\top} & 0_n \\ 0_n & Q_2 \end{pmatrix} = \left(\begin{array}{cc|cc} \mathbb{1}_r & 0 & T_r & E \\ 0 & 0 & 0 & \mathbb{1}_{n-r} \end{array}\right). \tag{5.49}$$

Next, observe that multiplying by $Q_{13}^{-\top} := \begin{pmatrix} \mathbb{1}_r & -E \\ 0 & \mathbb{1}_{n-r} \end{pmatrix}$ from the left sets E to 0:

$$Q_{13}^{-\top} Q_{12}^{-\top} Q_{11}^{-\top} \begin{pmatrix} A & B \end{pmatrix} \begin{pmatrix} Q_2^{-\top} & 0_n \\ 0_n & Q_2 \end{pmatrix} = \left(\begin{array}{cc|cc} \mathbb{1}_r & 0 & T_r & 0 \\ 0 & 0 & 0 & \mathbb{1}_{n-r} \end{array}\right). \tag{5.50}$$

Setting $R_2 := T_r \oplus 0_{n-r}$ and acting with $S(R_2)^{-1}$ from the right yields

$$\left(\begin{array}{cc|cc} \mathbb{1}_r & 0 & T_r & 0 \\ 0 & 0 & 0 & \mathbb{1}_{n-r} \end{array}\right) \left(\begin{array}{cc|cc} \mathbb{1}_r & 0 & -T_r & 0 \\ 0 & \mathbb{1}_{n-r} & 0 & 0 \\ \hline 0 & 0 & \mathbb{1}_r & 0 \\ 0 & 0 & 0 & \mathbb{1}_{n-r} \end{array}\right) = \left(\begin{array}{cc|cc} \mathbb{1}_r & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbb{1}_{n-r} \end{array}\right) \tag{5.51}$$

Finally, we apply the matrix $J_r J^\top$ from the right to get

$$\left(\begin{array}{cc|cc} \mathbb{1}_r & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbb{1}_{n-r} \end{array}\right) \left(\begin{array}{cc|cc} \mathbb{1}_r & 0 & 0 & 0 \\ 0 & 0 & 0 & -\mathbb{1}_{n-r} \\ \hline 0 & 0 & \mathbb{1}_r & 0 \\ 0 & \mathbb{1}_{n-r} & 0 & 0 \end{array}\right) = \begin{pmatrix} \mathbb{1}_n & 0_n \end{pmatrix}. \tag{5.52}$$

Let us define $Q_1 = Q_{13} Q_{12} Q_{11}$. The above reasoning implies that the transformed matrix has the following form

$$G(Q_1)^{-1} M G(Q_2)^{-1} S(R_2)^{-1} J_r J^\top = \begin{pmatrix} \mathbb{1}_n & 0_n \\ R_1 & I \end{pmatrix} = \begin{pmatrix} \mathbb{1}_n & 0_n \\ R_1 & \mathbb{1}_n \end{pmatrix} = J S(-R_1) J^\top. \tag{5.53}$$

Where the second equation follows from the transformed matrix being again symplectic, which implies that R_1 is symmetric and $I = \mathbb{1}_n$. Thus, using $J^{-1} = J^\top$ and $J_r^{-1} = J_r^\top$, we get by rearranging terms:

$$M = G(Q_1) J S(-R_1) J_r^\top S(R_2) G(Q_2). \tag{5.54}$$

Compiling permutations and diagonal gates

The decomposition given in Eq. (5.44) can be used to decompose $M \in \mathrm{Sp}_{2n}(q)$ into generators. More precisely, the individual decomposition of the components in $S_n(q)$ and $G_n(q)$ given in Sec. 3.1.4 can be used to give a decomposition for M. However, this decomposition might not be optimal in the number of generators. This is due to the decomposition of the permutation matrices $G(Q)$ via LU-decomposition which yields generally sub-optimal CX counts.

CHAPTER 6

FURTHER TOPICS

This chapter tries to give more mathematical background for the concepts introduced in this part of the thesis. The previous chapters were written in a way such that an understanding of the following sections is not necessary. Thus, they should be considered *optional*. However, a mathematically inclined reader might be interested in these details.

In Sec. 6.1 we give a construction for *Galois extensions* of the residue ring $\mathbb{Z}_{p^r}$ and discuss its additive and multiplicative structure. For $r = 1$, this is a finite field and the extension yields a finite field of prime-power order. These fields are also called *Galois fields*. For $r > 1$, the extension is a *Galois ring*.

Afterwards, we discuss some peculiarities which occur over finite fields of characteristic 2 in Sec. 6.2. In particular, we discuss the somewhat strange nature of quadratic forms in characteristic 2 which has direct consequences for the symplectic group. Then, we introduce *central extensions* and discuss the Heisenberg group from this point of view. Using this formalism, we try to shed a bit more light on the need for quadratic phases.

6.1 Construction of Galois extensions of fields and rings

6.1.1 Field extensions

A field extension over $\mathbb{F}_p$ can be constructed by taking the polynomial ring $\mathbb{F}_p[x]$ of polynomials in x and choosing a so-called *irreducible polynomial* $f \in \mathbb{F}_p[x]$ of degree m. A polynomial is irreducible if it can not be written as a product of two non-constant polynomials. Equivalently, f does not have roots over the field $\mathbb{F}_p$. The intuitive idea behind the construction is to extend $\mathbb{F}_p$ by a root θ of f to a new field which is given as polynomials of degree m in θ with coefficients in $\mathbb{F}_p$.

Example 6.1. *Arguably, the best known example is the construction of* $\mathbb{C}$ *as an extension of degree 2 over* $\mathbb{R}$. *Take the irreducible polynomial* $f(x) = x^2 + 1$ *and define a root* i *of* f. *Then any element in* $\mathbb{C}$ *can be presented as a polynomial of degree two,* $a + bi$ *with* $a, b \in \mathbb{R}$ *(higher orders are redundant since* $i^2 = -1$*).*

Concretely, we identify the irreducible polynomial f with 0 and consequently any polynomial fg should be identified with 0 as well. The latter polynomials exactly correspond to the ideal[1] generated by f, namely $(f) := f\,\mathbb{F}_p[x]$. Then, we define the Galois extension of $\mathbb{F}_p$ as the quotient ring $\mathbb{F}_{p^m} := \mathbb{F}_p[x]/(f)$ of $\mathbb{F}_p[x]$ by the ideal (f) . The elements in $\mathbb{F}_{p^m}$ can be understood as polynomials over $\mathbb{F}_p$ with degree strictly less than m. Addition is exactly the same as addition of polynomials in $\mathbb{F}_p[x]$. Multiplication is defined as multiplication of polynomials, followed by taking the remainder of the Euklidean (polynomial long) division by f. The subfield $\mathbb{F}_p$ is exactly represented by the

[1] A left/right ideal is an additive subgroup of a ring which is closed under left/right multiplication of elements in the ring. Here, the ring is commutative, thus left and right ideals coincide.

constant polynomials and multiplication is simply multiplication in $\mathbb{F}_p$ since f is irreducible.

By construction, f has a root θ over $\mathbb{F}_{p^m}$. Indeed, consider for example the element θ represented by the monomial x, then $f(x) = 0$. Furthermore, any element in $\mathbb{F}_{p^m}$ can be represented by $\sum_{i=0}^{m-1} c_i x^i$ for $c_i \in \mathbb{F}_p$. This shows that the field has order p^m and that the additive group $\mathbb{F}_{p^m}^+$ is a $\mathbb{F}_p$-vector space.

The multiplicative group $\mathbb{F}_{p^m}^\times$ is Abelian and has $p^m - 1$ elements. By Lagrange's theorem, there is a k such that $x^k = 1$ for all $x \in \mathbb{F}_{p^m}^\times$ and k divides $p^m - 1$. However, since $\mathbb{F}_{p^m}$ is a field, this equation can have at most k solutions and hence $k = p^m - 1$ is the minimal choice. In particular, we have $x^{p^m} = x$ and $\mathbb{F}_{p^m}^\times$ is a cyclic group of order $p^m - 1$.

In general, different choices for f lead to different, however isomorphic, fields. The existence and uniqueness up to isomorphism of a finite field with p^m elements can also be proven abstractly using the notion of splitting fields.

Example 6.2. *Over $\mathbb{F}_2$, there is a unique irreducible polynomial of degree 2, namely $f(x) = x^2 + x + 1$. To construct an extension of degree 2, we take all polynomials of degree 1 with coefficients in $\mathbb{F}_2$, i.e. $\mathbb{F}_4 = \{0, 1, x, 1 + x\}$. The multiplication rules can be deduced from the multiplication of polynomials such as $x^2 = f(x) + (1 + x)$. Hence, after modding out f, we get $x^2 = 1 + x$. From this, we find the remaining rule $x(1 + x) = x + x^2 = 1$.*

6.1.2 Ring extensions

Consider a residue ring $\mathbb{Z}_{p^r} = \mathbb{Z}/p^r\mathbb{Z}$. The maximal ideal of $\mathbb{Z}_{p^r}$ is generated by p and is denoted as $(p) = p\mathbb{Z}_{p^r}$. This implies that any element in $\mathbb{Z}_{p^r}$ as a p-adic expansion

$$\mathbb{Z}_{p^r} \ni a = a_0 + a_1 p^1 + \cdots + a_{r-1} p^{r-1}, \qquad a_i \in \mathbb{F}_p. \tag{6.1}$$

Taking the quotient with respect to (p) yields the *residue field* $\mathbb{Z}_{p^r}/(p) \simeq \mathbb{F}_p$. Explicitly, this isomorphism is $a \mapsto a \mod p = a_0$.

Recall from Sec. 6.1.1 that the Galois extension of a finite field $\mathbb{F}_p$ starts from an irreducible polynomial f of degree m in the polynomial ring $\mathbb{F}_p[x]$. The Galois extension of degree m is then constructed as the quotient of $\mathbb{F}_p[x]$ by the ideal generated by f, which is $(f) = f\mathbb{F}_p[x]$.

The Galois extension of the residue ring $\mathbb{Z}_{p^r}$ can be constructed similarly. Given an irreducible polynomial $\bar{f} \in \mathbb{F}_p[x]$ of degree m, there exists a $f \in \mathbb{Z}_{p^r}[x]$ such that f reduces to $\bar{f}$ modulo p and f divides the polynomial $x^{q-1} - 1$, where $q = p^m$. f is called the *Hensel lift* of $\bar{f}$. Then, define the Galois extension of degree m as

$$\mathrm{GR}(p^r, m) := \mathbb{Z}_{p^r}[x]/(f). \tag{6.2}$$

The maximal ideal (p) of $\mathbb{Z}_{p^r}$ lifts to a maximal ideal of $\mathrm{GR}(p^r, m)$ which is generated by the residue class $p + (f)$. One can check that $(p) \equiv (p + (f))$ contains zero and the zero divisors of $\mathrm{GR}(p^r, m)$ and thus the quotient by (p) is a finite field. More precisely, we have

$$\mathrm{GR}(p^r, m)/(p) \simeq \mathbb{F}_{p^m}. \tag{6.3}$$

As in the case of finite fields, f has a root θ over $\mathrm{GR}(p^r, m)$ by construction. Moreover, since f divides $x^{q-1} - 1$ for $q = p^d$, we can assume that θ has order $q - 1$. Then, any other

element $\mathrm{GR}(p^r, m)$ can represented as polynomial of degree $< m-1$ in θ, i. e. it can be written uniquely as

$$\mathrm{GR}(p^r, m) \ni a = a_0 + a_1\theta^1 + \cdots + a_{m-1}\theta^{m-1}, \qquad a_i \in \mathbb{Z}_{p^r}. \tag{6.4}$$

In particular, the additive group $\mathrm{GR}(p^r, m)^+$ has the structure of a $\mathbb{Z}_{p^r}$-module of rank m. In this representation, $\mathbb{Z}_{p^r}$ is the subring of elements represented by constant polynomials.

Alternatively, there is an analogue of the p-adic expansion of elements in $\mathbb{Z}_{p^r}$, which is

$$\mathrm{GR}(p^r, m) \ni a = t_0 + t_1 p^1 + \cdots + t_{r-1}p^{r-1}. \tag{6.5}$$

Here, the coefficients t_i are either zero or powers of θ. These values define the *Teichmüller set* $\mathcal{T} = \{0\} \cup \mathcal{T}^\times$ where $\mathcal{T}^\times$ is the cyclic group of order $p^m - 1$ generated by θ. As such the Teichmüller set $\mathcal{T}^\times$ can be understood as a lift of the multiplicative group $\mathbb{F}_{p^m}^\times$. The quotient map $t \mapsto \bar{t} = t \mod p$ yields an explicit isomorphism between $\mathcal{T}^\times$ and $\mathbb{F}_{p^m}^\times$. In the p-adic expansion Eq. (6.5), $a \in (p)$ if and only if $t_0 = 0$. Since (p) is exactly the set of zero divisors, a is a unit (i. e. invertible) if and only if $t_0 \neq 0$. Thus, the quotient map w.r.t. to (p) is simply given as

$$\mathrm{GR}(p^r, m) \ni a = t_0 + t_1 p^1 + \cdots + t_{r-1}p^{r-1} \longmapsto \bar{t}_0 \in \mathbb{F}_{p^m}. \tag{6.6}$$

Finally, we construct an analogue to the Frobenius automorphism and the trace map of Galois fields for Galois rings. Recall that over $\mathbb{F}_{p^m}$ the Frobenius automorphism acts as $\phi : x \mapsto x^p$. We define it similarly on the Teichmüller units $\mathcal{T}^\times$, namely as $t \mapsto t^p$ and extend it $\mathbb{Z}_{p^r}$-linearly to $\mathrm{GR}(p^r, m)$. This is simplest in the p-adic expansion Eq. (6.5) where ϕ acts as

$$a = t_0 + t_1 p^1 + \cdots + t_{r-1}p^{r-1} \longmapsto \phi(a) := t_0^p + t_1^p p^1 + \cdots + t_{r-1}^p p^{r-1}. \tag{6.7}$$

Since $\mathcal{T}^\times$ has order $p^m - 1$, we find that $\phi^m = \phi$, thus the *Galois group* generated by ϕ is cyclic of order m. As such, it is isomorphic to the Galois group of $\mathbb{F}_{p^m}$. The trace map is then defined as

$$\operatorname{tr} a := \sum_{k=0}^{m-1} \phi^k(a). \tag{6.8}$$

Since the quotient map on $\mathcal{T}^\times$ is an isomorphism, we have $\overline{\phi(t)} = \overline{t^p} = (\bar{t})^p$. Thus, $\overline{\operatorname{tr} t} = \operatorname{tr} \bar{t} \in \mathbb{F}_p$ which shows, when applied to the p-adic expansion, that $\operatorname{tr} a \in \mathbb{Z}_{p^r}$, analogous to the finite field case.

Example 6.3. *For our case, $p = r = 2$, there is a unique irreducible polynomial of degree 2, $\bar{f} = x^2 + x + 1$. Its Hensel lift is simply $f = x^2 + x + 1$ with coefficients interpreted in $\mathbb{Z}_4$. The elements of $\mathrm{GR}(4, 2)$ can be presented as the 4^2 residue classes of the polynomials $c_0 x + c_1$ for $c_0, c_1 \in \mathbb{Z}_4$. Take θ to be the root corresponding to $c_0 = 1, c_1 = 0$. We find $\alpha^2 = 3\alpha + 3$, $\alpha^3 = 1$, hence the Teichmüller set is $\mathcal{T} = \{0, 1, \alpha, 3\alpha + 3\}$ which reduces to $\{0, 1, \bar{\alpha}, 1 + \bar{\alpha}\} \equiv \mathbb{F}_4$ modulo 2, where $\bar{\alpha}$ is a root of $\bar{f}$. The 2-adic expansion of any element in $\mathrm{GR}(4, 2)$ is $a = t_0 + 2t_1$ for $t_0, t_1 \in \mathcal{T}$.*

6.2 On the problems in even characteristic

Following his original work [83] treating the case of characteristic $\neq 2$, André Weil tried to generalise his construction to the complementary case. However, his approach involves only a subgroup of the symplectic group, namely an orthogonal group $\mathrm{O}_n^+(q)$ associated with a quadratic form Q^+ defined below. While an exact equivalent seems to be impossible due to the exceptional behaviour, the Weil representation can be partially recovered by introducing $\mathbb{Z}_4$ coefficients instead of $\mathbb{F}_2$. From the perspective of the matrix groups generated by those representations, the difference was already observed by Bolt, Room and Wall [77] in 1961 who also introduced the term *Clifford group*. These $\mathbb{Z}_4$-extensions have been studied and used in the quantum information theory community since the early 2000s, sparked by the increasing interest in discrete Wigner functions, MUBs and SIC-POVMs [66–68, 84, 85]. An in-depth mathematical treatise from the perspective of representation theory was given a bit later by Gurevich and Hadani [86]. They constructed a suitable generalisation of the Weil representation in characteristic two which is compatible with the matrix group structures in Ref. [77] that are also used in quantum information theory. Notably, this generalised Weil representation only yields a linear representation of the *fourth cover* of the symplectic group, in contrast to the original Weil representation in odd characteristic.

In this section, we discuss the behaviour of bilinear and quadratic forms in characteristic two and introduce the concept of a central extension to study possible candidates for a Heisenberg group in characteristic two. Finally, we try to give a self-contained construction of the qubit Heisenberg group by combining the approaches used in quantum information theory with the work of Gurevich and Hadani [86].

6.2.1 Quadratic forms in even characteristic

To understand why the case of characteristic two is different, the behaviour of bilinear forms turns out to be important. Recall that any bilinear form b determines a quadratic form by $Q(v) := b(v, v)$ and any quadratic form can be written that way (although this not unique in general). Furthermore, to any quadratic form Q, we associate the following symmetric bilinear form B, called the *polar form* of Q:

$$B(v, w) := Q(v + w) - Q(v) - Q(w). \tag{6.9}$$

Note that for characteristic $\neq 2$ (or generally over a ring where 2 is invertible), the above *polarisation identity* yields a bijection between quadratic forms and symmetric bilinear forms by

$$Q(v) = 2^{-1}B(v, v), \qquad B(v, w) = Q(v + w) - Q(v) - Q(w). \tag{6.10}$$

However, when 2 is not invertible, this is no longer the case. In particular, if the bilinear form b in the definition $Q(v) = b(v, v)$ is symmetric, we have

$$B(v, w) = Q(v + w) - Q(v) - Q(w) = 2b(v, w), \tag{6.11}$$

which means that b determines B *modulo 2*. Over fields with characteristic two, the right hand side even *vanishes* and thus $B = 0$. Thus, Q is actually a linear form instead of a quadratic one. This implies that in characteristic two, only non-symmetric bilinear forms can define non-trivial quadratic forms.

Recall that the symplectic form ω was defined as an alternating, non-degenerate bilinear form on a vector space V. In characteristic $\neq 2$, alternation and anti-symmetry of bilinear forms is equivalent. However, in characteristic two, anti-symmetry and symmetry becomes the same. While alternation still implies anti-symmetry and thus symmetry, the converse direction is not true. Thus, a symplectic form is also a symmetric form which has a direct impact on the symplectic structure in characteristic two. For a classification of sesquilinear and bilinear forms see e. g. Refs. [120, 121].

A quadratic form Q is called *non-degenerate* if the bilinear form B defined in Eq. (6.9) is non-degenerate. In characteristic two, the bilinear form B is actually alternating, $B(v,v) = Q(0) = 0$, and hence a non-degenerate quadratic form Q defines a *symplectic form* B. By construction, the associated orthogonal group

$$\mathrm{O}(V,Q) := \{O \in \mathrm{End}(V) \mid Q \circ O = Q\}\,, \tag{6.12}$$

is a subgroup of the symplectic group $\mathrm{Sp}(V,B)$. Conversely, given a symplectic form ω, what can we see about the possible polarisations Q? Clearly, it is enough to consider the standard form $[\cdot,\cdot]$ on $\mathbb{F}_q^{2n}$.

Generally, we know from the classification of quadratic forms [120, 121] that there are two non-isomorphic orthogonal groups $\mathrm{O}^{\pm}_{2n}(q)$ in even dimensions which can be represented in an arbitrary basis by the quadratic forms

$$Q^+(v) := \sum_{i=1}^{n} v_i v_{n+i}, \qquad\qquad Q^-(v) := Q^+(v) + v_n^2 + v_{2n}^2. \tag{6.13}$$

Note that the polar form of both is the standard symplectic form:

$$Q^{\pm}(v+w) + Q^{\pm}(v) + Q^{\pm}(w) = \sum_{i=1}^{n} v_i w_{n+i} + w_i v_{n+i} = [v,w]. \tag{6.14}$$

Recall that $\mathrm{O}^{\pm}_{2n}(q)$ are then both subgroups of the standard symplectic group $\mathrm{Sp}_{2n}(q)$. It is a simple exercise to show that the subgroup $\mathrm{O}^{+}_{2n}(q)$ corresponds to the group generated by the subgroup $G_n(q)$ together with the symplectic unit J_i applied on every hyperbolic plane $\mathcal{H}_i := \langle e_i, f_i\rangle$, cp. Eq. (3.21). Furthermore, in characteristic two, Q^- acts as Q^+ on $\mathcal{H}_1 \oplus \cdots \oplus \mathcal{H}_{n-1}$ and is zero on $\mathcal{H}_n$. Hence, $\mathrm{O}^{-}_{2n}(q)$ is given as $\mathrm{O}^{+}_{2n-2}(q) \times \mathrm{SL}_2(q) = \mathrm{O}^{+}_{2n-2}(q) \times \mathrm{Sp}_2(q)$. In representation, these subgroups induce the so-called *real and semi-real Clifford groups*, see also Ref. [78]. Any polarisation Q of the symplectic form is thus of the form $Q^{\pm}$, up to a symplectic transformation.

Finally, note that while the groups $\mathrm{O}^{\pm}_{2n}(q)$ also exist in odd characteristic, quadratic forms now polarise *symmetric* instead of symplectic forms. Thus, they do not provide structures which are compatible with the symplectic one.

6.2.2 Central extensions

In the theory of projective representations, the notion of a *central extension* plays an important role. A central extension E of a group $(G,\cdot)$ by an Abelian group $(A,+)$ is a short exact sequence

$$0 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 0, \tag{6.15}$$

i.e. $\operatorname{im}\iota = \ker\pi$, such that A embeds into the centre of E. A trivial example would be $E = G \times A$ with the obvious embedding and projection maps. One says that a central extension *splits* if there is a homomorphism $\varphi : G \to E$ such that $\pi \circ \varphi = \mathrm{id}_G$. In this case, $\Phi : G \times A \to E$, $\Phi(x,t) := \iota(t)\varphi(x)$ defines an isomorphism between E and the trivial extension.

Central extensions are characterised by *2-cocycles*, i. e. functions $\beta : G \times G \to A$, fulfilling $\beta(1,1) = 0$ and the cocycle condition

$$0 = \mathrm{d}\beta(x,y,z) := \beta(y,z) - \beta(xy,z) + \beta(x,yz) - \beta(x,y). \tag{6.16}$$

One can check that the data (G, A, β) defines a central extension $E := G \times_\beta A$ as the set $G \times A$ with group law $(x,t) \bullet (y,s) := (xy, t + s + \beta(x,y))$ and maps $\iota(t) = (1,t)$, $\pi(x,t) = x$. Equation (6.16) guarantees the associativity of E. Note that if β is a *coboundary*, i. e. $\beta(x,y) = \mathrm{d}\alpha(x,y) := \alpha(x) + \alpha(y) - \alpha(xy)$, then $d\beta = 0$ and $\beta(1,1) = 0$ hold trivially. In this case, one can show that $G \times_{\mathrm{d}\alpha} A$ splits and is thus isomorphic to the trivial extension $G \times A$. More generally, two central extensions of G by A given by 2-cocycles β_1 and β_2 are isomorphic if and only if $\beta_1 = \beta_2 + \mathrm{d}\alpha$. It can be checked by a straightforward calculation that the isomorphism is explicitly given by

$$G \times_{\beta_1} A \longrightarrow G \times_{\beta_2} A, \quad (x,t) \longmapsto (x, t + \alpha(x)). \tag{6.17}$$

Thus, the isomorphism classes of central extensions correspond to the *second group cohomology group*

$$H^2(G,A) = \{\text{2-cocycles}\}/\{\text{2-coboundaries}\}. \tag{6.18}$$

Of particular importance to us are the automorphisms of a central extension $E = G \times_\beta A$, in particular the ones which fix its centre. More precisely, we are considering those automorphisms which fix $A \subset Z(E)$ (which could not be the full centre). Let us write an automorphism as $\phi(x,t) = (g(x,t), \alpha(x,t))$. Note that the cocycle condition Eq. (6.16) applied to $y = 1$ implies that $\beta(1,z) = \beta(x,1) = 0$ for all $x, z \in G$. Thus, we have $(x,t) = (1,t) \bullet (x,0)$ where $(1,t)$ is in the centre. Using $\phi(1,t) = (1,t)$, we arrive at

$$\begin{aligned}(g(x,t), \alpha(x,t)) = \phi(x,t) &= \phi(1,t) \bullet \phi(x,0) \\ &= (1,t) \bullet (g(x,0), \alpha(x,0)) = (g(x,0), t + \alpha(x,0)).\end{aligned} \tag{6.19}$$

Hence, ϕ has the form $\phi(x,t) = (g(x), t + \alpha(x))$. Finally, imposing the homomorphism property, we find:

$$\begin{aligned} g(x)g(y) &= g(xy), \\ \beta(x,y) - \beta(g(x),g(y)) &= \mathrm{d}\alpha(x,y). \end{aligned} \tag{6.20}$$

Together with $g(1) = 1$, this implies that $g \in \mathrm{Aut}(G)$.

6.2.3 Revisiting the Heisenberg group as a central extension

Recall that, in odd characteristic, the Heisenberg group $\mathrm{H}_n(q)$ was defined explicitly as the set $\mathbb{F}_q^{2n} \times \mathbb{F}_q$ with composition law $(v,t) \bullet (w,s) := (v + w,\ t + s + 2^{-1}[v,w])$. In the light of the previous section, the Heisenberg group is thus abstractly characterised as a central extension of the group $\mathbb{F}_q^{2n}$ by the additive group of the field $\mathbb{F}_q$ with associated

2-cocycle $\beta = 2^{-1}\omega$ (bilinearity directly implies $d\beta = 0$). We can now characterise the centre-fixing automorphisms $(v,t) \mapsto (g(v), t + \alpha(v))$ of the Heisenberg group using Eq. (6.20). The first equation implies that g is an automorphism of the additive group of $\mathbb{F}_q^{2n}$. The second equation,

$$2^{-1}[g(v), g(w)] - 2^{-1}[v,w] = \alpha(v+w) - \alpha(v) - \alpha(w), \tag{6.21}$$

claims equality between an anti-symmetric expression on the left hand side and a symmetric expression on the right hand side. This implies that twice the LHS vanishes, hence g is additive and preserves the symplectic form. This can only be the case if g is actually linear and thus $g \in \mathrm{Sp}_{2n}(q)$. Since the characteristic is not 2, the RHS can only be anti-symmetric if it vanishes identically. Hence, we can choose α to be a linear form on $\mathbb{F}_q^{2n}$.

In summary, the centre-fixing automorphisms are given by independent pairs (g, α) with $g \in \mathrm{Sp}_{2n}(q)$ and $\alpha \in (\mathbb{F}_q^{2n})^*$. The linear forms can be identified with the inner automorphisms of $\mathrm{H}_n(q)$ which is normalised by $\mathrm{Sp}_{2n}(q)$. Thus, the group of centre-fixing automorphisms has the structure $\mathrm{ASp}_{2n}(q) = \mathrm{Sp}_{2n}(q) \ltimes \mathbb{F}_q^{2n}$.

Clearly, the definition of $\mathrm{H}_n(q)$ is not possible when the characteristic is two due to the lack of inverse of 2=0. Thus, to understand this case, we first have to define a suitable Heisenberg group. One might be tempted to think that if 2^{-1} does not exist in characteristic two, then we could simply leave out this factor and define a central extension with $\beta = [\cdot,\cdot]$ instead. In odd characteristic, however, the associated Heisenberg groups are isomorphic if and only if there is a function α such that

$$2^{-1}[\cdot,\cdot] = [\cdot,\cdot] + \mathrm{d}\alpha \quad \Longleftrightarrow \quad [\cdot,\cdot] = \mathrm{d}\tilde{\alpha}, \qquad \tilde{\alpha} := (2^{-1} - 1)^{-1}\alpha \tag{6.22}$$

In other words, if and only if $[\cdot,\cdot]$ is a coboundary in the first place. Albeit, this is impossible in odd characteristic since $[\cdot,\cdot]$ is anti-symmetric and $\mathrm{d}\tilde{\alpha}$ the right hand side in Eq. (6.22) is always symmetric. Nevertheless, $[\cdot,\cdot]$ *is a coboundary* in even characteristic since the equation $\mathrm{d}\alpha(v,w) = [v,w]$ is exactly the polarisation identity for the symplectic form which we discussed before and has e. g. the solution $\alpha(v) = Q^+(v)$. Thus, taking the central extension associated to $[\cdot,\cdot]$ will make it split $\mathbb{F}_{2^m}^{2n} \times_{[\cdot,\cdot]} \mathbb{F}_{2^m} \simeq \mathbb{F}_{2^m}^{2n} \times \mathbb{F}_{2^m}$, resulting in a too large outer automorphism group containing e. g. $\mathrm{GL}_{2n}(2^m)$.

Interestingly, there is another construction of the Heisenberg group in odd characteristic. Define the bilinear form $\eta(v,w) := \sum_{i=1}^n v_i w_{n+i}$ which obeys $[v,w] = \eta(v,w) - \eta(w,v)$. Consider the central extension $\mathbb{F}_q^{2n} \times_\eta \mathbb{F}_q$ by η. Then, we can immediately compute that it is isomorphic to $\mathrm{H}_n(q)$ since

$$\begin{aligned} \eta - 2^{-1}[\cdot,\cdot] &= -\,\mathrm{d}\alpha \\ \Leftrightarrow \quad 2\eta - [\cdot,\cdot] &= -2\,\mathrm{d}\alpha \\ \Leftrightarrow \quad \eta(v,w) + \eta(w,v) &= 2\left(\alpha(v+w) - \alpha(v) - \alpha(w)\right). \end{aligned} \tag{6.23}$$

Here, the left hand side is a symmetric bilinear form and the right hand side is the polarisation identity. Since the characteristic is odd, this has a unique solution, namely $\alpha(v) = 2^{-1}\eta(v,v)$. The corresponding unitary representation differs exactly by this expression from the representation introduced in Sec. 3.2:

$$D_\chi(z,x,t)f(u) := \chi(t + z\cdot u)f(u+x). \tag{6.24}$$

In general, we can construct a unitary representation for any central extension isomorphic to $\mathrm{H}_n(q)$ by adding the coboundary form to the character part. In the phase space literature, this is sometimes called a *gauge* of the Weyl operators and the above construction is the *displacement operator gauge*.

Building on this observation, we could try to define the Heisenberg group in even characteristic using the central extension by η. However, as André Weil himself already noticed, the group $\mathbb{F}_{2^m}^{2n} \times_\eta \mathbb{F}_{2^m}$ does only allow for outer automorphisms associated with the orthogonal group $\mathrm{O}_{2n}^+(2^m) < \mathrm{Sp}_{2n}(2^m)$ instead of the full symplectic group. To see this, let us again consider the automorphism condition Eq. (6.20) in this context:

$$\eta(g(v), g(w)) - \eta(v, w) = \alpha(v + w) - \alpha(v) - \alpha(w). \tag{6.25}$$

By symmetry, it is again necessary that $g \in \mathrm{Sp}_{2n}(2^m)$. However, taking $v = w$, we also observe that g has to fulfill $Q^+(gv) = Q^+(v)$ for $Q^+(v) := \eta(v, v)$ the quadratic form introduced in Sec. 6.2.1. Thus, g has to be in the orthogonal subgroup $\mathrm{O}_{2n}^+(2^m)$ of the symplectic group. As discussed in Sec. 6.2.1, the quadratic form Q^+ does not determine η in characteristic two and thus the symmetries of Q^+ are not necessarily the symmetries of η. This means that for $g \in \mathrm{O}_{2n}^+(2^m)$, the left hand side $\eta(gv, gw) - \eta(v, w)$ of Eq. (6.25) does not necessarily vanish. Recall that $\mathrm{O}_{2n}^+(2^m)$ is generated by $G_n(2^m)$ and J_i. If $g \in G_n(2^m)$, then the left hand side indeed vanishes and we can choose $\alpha = 0$. This is exactly the reason why we eventually obtain a representation for $G_n(2^m)$, cp. 3.3.2. If $g = J_i$, then the left hand side becomes the symplectic form on the hyperbolic plane $\langle e_i, f_i \rangle$, i. e. $[v_i, w_i]$. In this case, one can choose $\alpha = Q^+$ (up to a linear form).

Along the lines of Secs. 3.2 and 3.3, the centre-fixing automorphisms have a natural projective representation as they normalise the displacement representation defined in Eq. (6.24). Comparing the latter equation with the definition of the even Schrödinger representation in Eq. (3.74), we see that the displacement representation exactly reproduces the Weyl operators with *real matrix entries* in the computational basis. The group which is generated in this way is exactly the one generated by Z and X operators alone – without the Z_4 phases. It is thus often called the *real Pauli group*. The corresponding automorphisms define a proper subgroup of the Clifford group $\mathrm{Cl}_n(2^m)$ given in Eq. (4.11) which are exactly the Clifford matrices with real matrix entries. Consequently, this subgroup associated with orthogonal maps $\mathrm{O}_{2n}^+(2^m)$ is called the *real Clifford group*.

From the given discussion, it might be immanent that a Heisenberg group in even characteristic has to use additional structure. One of the reasons for the failure of the above constructions is that certain polarisations of bilinear forms such as Eq. (6.25), allow for different solutions in even characteristic. This behaviour is known from the study of quadratic forms over finite fields. The difficulties in even characteristic can be partially overcome by letting the quadratic forms take values in the ring Z_4 (respectively $\mathbb{GR}_{4^m}$) which can be seen as a double cover of $\mathbb{F}_2$. Then, there are two qualitative changes. First, proper quadratic forms defined by symmetric forms again exist by Eq. (6.11) and second, the polar form is not alternating anymore. This allows to recover certain properties from the odd characteristic case. In particular, if we allow Eq. (6.25) to take values in $\mathbb{Z}_4$, it is possible to show that it has solutions for any $g \in \mathrm{Sp}_{2n}(2^m)$.

6.2.4 The Heisenberg group over $\mathbb{Z}_4$

We take the discussions in the previous section as a motivation to study Heisenberg groups over $\mathbb{Z}_4$. As it turns out, this provides a suitable covering of the $\mathbb{F}_2$-phase space which allows for a linearised Weil representation of $\mathrm{Sp}_{2n}(2)$. We will also take this analysis as a basis to reflect on the construction of Gurevich and Hadani [86] in Sec. 6.2.5, using a somewhat more accessible language.

For the sake of simplicity, we use the ring $\mathbb{Z}_4$ in the following. However, the reasoning generalises in a straightforward way to the extension case by using the Galois ring $\mathrm{GR}(4, m)$.

As symplectic space, we consider $\tilde{V} = \mathbb{Z}_4^{2n}$, which is now a *module* over $\mathbb{Z}_4$ of rank $2n$, equipped with the standard symplectic form

$$\tilde{\Omega}(\tilde{v}, \tilde{w}) := \sum_{i=1}^{n} \tilde{v}_i \tilde{w}_{n+i} - \tilde{v}_{n+i} \tilde{w}_i. \tag{6.26}$$

Here, we use the convention to decorate $\mathbb{Z}_4$-valued objects with a tilde. Recall that the quotient of $\mathbb{Z}_4$ by its maximal ideal $(2) = 2\mathbb{Z}_4$ is the residue field $\mathbb{F}_2$. As a consequence, the quotient module $V := \tilde{V}/2\tilde{V}$, defined by the usual equivalence relation

$$\tilde{v} \sim \tilde{w} \quad \Longleftrightarrow \quad \tilde{v} - \tilde{w} \in 2\tilde{V}, \tag{6.27}$$

is naturally a $\mathbb{F}_2$-vector space. The projection $\tilde{V} \to V \simeq \mathbb{F}_2^{2n}$ can be explicitly realised in a basis by applying π to every component of a vector $\tilde{v}$. Given a linear form $\tilde{\alpha}$ on $\tilde{V}$, the form $2\tilde{\alpha}$ induces a linear form α on V with values in $2\mathbb{Z}/4\mathbb{Z}$ since

$$2\tilde{\alpha}(v + 2x) = 2\tilde{\alpha}(v) + 4\tilde{\alpha}(x) = 2\tilde{\alpha}(v). \tag{6.28}$$

Thus, $2\tilde{\alpha}$ is constant on equivalence classes and descends to a map α on V. The map α can be explicitly given for $\tilde{\alpha}(\tilde{v}) = \sum_i \tilde{a}_i \tilde{v}_i$ as

$$2\alpha(v) = \sum_{i=1}^{2n} (2\tilde{a}_i) v_i = 2 \left(\sum_{i=1}^{2n} a_i v_i \right) \in 2\mathbb{Z}/4\mathbb{Z}, \tag{6.29}$$

where $v \in \mathbb{F}_2^{2n}$, $a = \tilde{a} \mod 2$. Note that the operations in the first equation are to be performed in $\mathbb{Z}_4$ and the ones in the parentheses of the second equation in $\mathbb{F}_2$. Finally, let us remark that this argument works in the same way for multilinear forms. In the following, we will often omit the tilde if mean the projection modulo 2, e. g. $v \equiv \pi(\tilde{v}) = \tilde{v} \mod 2$.

Finally, we define the Heisenberg group $H_n(\mathbb{Z}_4)$ over $\mathbb{Z}_4$ as the set $\mathbb{Z}_4^{2n} \times \mathbb{Z}_4$ with multiplication law

$$(\tilde{v}, \tilde{t}) \bullet (\tilde{w}, \tilde{s}) := (\tilde{v} + \tilde{w}, \tilde{t} + \tilde{s} + \tilde{\Omega}(\tilde{v}, \tilde{w})). \tag{6.30}$$

As in the odd case, we can compute

$$(\tilde{v}, \tilde{t}) \bullet (\tilde{w}, \tilde{s}) \bullet (\tilde{v}, \tilde{t})^{-1} = (\tilde{w}, \tilde{s} + 2\tilde{\Omega}(\tilde{v}, \tilde{w})). \tag{6.31}$$

By the same argument as before, the form $2\tilde{\Omega}(\tilde{v}, \tilde{w})$ does only depend on its arguments *modulo 2*, since for any $\tilde{u} \in \mathbb{Z}_4^{2n}$

$$2\tilde{\Omega}(\tilde{v} + 2\tilde{u}, \tilde{w}) = 4\tilde{\Omega}(\tilde{u}, \tilde{w}) + 2\tilde{\Omega}(\tilde{v}, \tilde{w}) = 2\tilde{\Omega}(\tilde{v}, \tilde{w}). \tag{6.32}$$

Thus, with $\Omega = [\cdot,\cdot]$ the standard symplectic product on $\mathbb{F}_2^{2n}$, it holds

$$2\tilde{\Omega}(\tilde{v},\tilde{w}) = 2[\pi(\tilde{v}),\pi(\tilde{w})] \equiv 2[v,w], \tag{6.33}$$

where the multiplication on the right hand side is the additive homomorphism $\mathbb{F}_2 \hookrightarrow \mathbb{Z}_4$. Hence, the inner automorphism in Eq. (6.31) does only depend on $\tilde{v} \mod 2$ and the inner automorphism group of $H_n(\mathbb{Z}_4)$ is isomorphic to the additive group of $\mathbb{F}_2^{2n}$. The elements in $2\mathbb{Z}_4^{2n}$ act trivially and thus the centre of $H_n(\mathbb{Z}_4)$ does not only contain $\mathbb{Z}_4$ but is actually given by the direct product $2\mathbb{Z}_4^{2n} \times \mathbb{Z}_4$. Hence, we see that modding out the centre yields $H_n(\mathbb{Z}_4)/Z(H_n(\mathbb{Z}_4)) \simeq \mathbb{F}_2^{2n}$.

Albeit, we only require that the "centre-fixing" automorphisms $(\tilde{v},\tilde{t}) \mapsto (\tilde{g}(\tilde{v}),\tilde{t} + \tilde{\alpha}(\tilde{v}))$ fix the $\mathbb{Z}_4$ part of the centre. By Sec. 6.2.2, this is enough to determine the form of the automorphism. The automorphism condition

$$\tilde{\Omega}(\tilde{g}(\tilde{v}),\tilde{g}(\tilde{w})) - \tilde{\Omega}(\tilde{v},\tilde{w}) = \tilde{\alpha}(\tilde{v}+\tilde{w}) - \tilde{\alpha}(\tilde{v}) - \tilde{\alpha}(\tilde{w}), \tag{6.34}$$

implies that the left hand side of Eq. (6.34) has to be symmetric. This condition becomes

$$0 = 2\tilde{\Omega}(\tilde{g}(\tilde{v}),\tilde{g}(\tilde{w})) - 2\tilde{\Omega}(\tilde{v},\tilde{w}) = 2\left([g(v),g(w)] - [v,w]\right). \tag{6.35}$$

Therefore, the projection of $\tilde{g}$ is symplectic $g \in \mathrm{Sp}_{2n}(2)$. Vice versa, given a $g \in \mathrm{Sp}_{2n}(2)$ we can lift it to a map $\tilde{g}$ on $\mathbb{Z}_4^{2n}$. This lift is not unique, but we can certainly find one for which $\tilde{g} \in \mathrm{Sp}_{2n}(\mathbb{Z}_4)$. Then the left hand side of Eq. (6.34) vanishes, showing that we can choose $\tilde{\alpha} = 0$.

In the following, we restrict our attention to the centre-fixing automorphisms of the Heisenberg group $H_n(\mathbb{Z}_4)$ which are given by $\tilde{g} \in \mathrm{Sp}_{2n}(\mathbb{Z}_4)$ (and $\tilde{\alpha} = 0$) and the inner automorphisms $\varphi \in (\mathbb{F}_2^{2n})^* \simeq \mathbb{F}_2^{2n}$. As in the odd characteristic case, we define the the *affine symplectic group* $\mathrm{ASp}_{2n}(\mathbb{Z}_4) \simeq \mathrm{Sp}_{2n}(\mathbb{Z}_4) \ltimes \mathbb{F}_2^{2n}$ as the group of these "restricted" centre-fixing automorphisms.

Given an additive character χ_4 of $\mathbb{Z}_4$, define the associated additive character of $\mathbb{F}_2$ by $\chi(s) := \chi_4(2s)$. Then, with respect to the standard polarisation, we define the *Schrödinger representation* over $\mathbb{Z}_4$ on the function space $\mathbb{C}[\mathbb{Z}_4^n]$ as

$$W_4(\tilde{z},\tilde{x},\tilde{t})f(\tilde{u}) := \chi_4(\tilde{t} + 2\tilde{z}\cdot\tilde{u} + \tilde{z}\cdot\tilde{x})f(\tilde{u}+\tilde{x}), \quad \tilde{z},\tilde{x},\tilde{u} \in \mathbb{Z}_4^n,\ \tilde{t} \in \mathbb{Z}_4. \tag{6.36}$$

It is straightforward to verify that this indeed defines a unitary representation of $H_n(\mathbb{Z}_4)$. However, since we want the centre of $H_n(\mathbb{Z}_4)$ to act as a multiply of the identity, we restrict the domain of the representation by demanding

$$f(\tilde{u}+2\tilde{x}) = f(\tilde{u}), \quad \forall \tilde{u},\tilde{x} \in \mathbb{Z}_4^n. \tag{6.37}$$

In this way we get an induced representation W on the quotient of $\mathbb{C}[\mathbb{Z}_4^{2n}]$ up to this relation. This quotient is isomorphic to the function space $\mathbb{C}[\mathbb{F}_2^n]$ obtained by taking the projection modulo two of the coordinates. The induced representation reads

$$\tilde{W}(\tilde{z},\tilde{x},\tilde{t})f(u) := \chi_4(\tilde{t} + \tilde{z}\cdot\tilde{x})\chi(z\cdot u)f(u+x), \quad u \in \mathbb{F}_2^n, \tag{6.38}$$

with the centre acting as

$$\tilde{W}(2\tilde{z},2\tilde{x},\tilde{t}) = \chi_4(\tilde{t})\mathbb{1}. \tag{6.39}$$

Note that this representation still depends on $\tilde{z}, \tilde{x} \in \mathbb{Z}_4^n$ since

$$\tilde{W}(\tilde{z} + 2\tilde{z}', \tilde{x} + 2\tilde{x}', \tilde{t}) = \chi([(z, x), (z', x')])\tilde{W}(\tilde{z}, \tilde{x}, \tilde{t}). \tag{6.40}$$

The W representation defines unitary operators of order 2 and 4 which are distinguished by the parameter $t = \tilde{t} \mod 2$:

$$\tilde{W}(\tilde{z}, \tilde{x}, \tilde{t})^2 = \tilde{W}(2\tilde{z}, 2\tilde{x}, 2\tilde{t}) = \chi(t)\mathbb{1}. \tag{6.41}$$

This implies that the operators $W(\tilde{z}, \tilde{x}, \tilde{t})$ are not only unitary but also Hermitian for $\tilde{t} \in \{0, 2\}$ and anti-Hermitian for $\tilde{t} \in \{1, 3\}$. As in the odd case, we call the operators $W(\tilde{v}) := W(\tilde{v}, 0)$ the *Weyl operators*. As W defines a representation of $H_n(\mathbb{Z}_4)$, the Weyl operators fulfill the relations

$$\begin{aligned} \tilde{W}(\tilde{v})\tilde{W}(\tilde{w}) &= \chi_4(\tilde{\Omega}(\tilde{v}, \tilde{w}))\tilde{W}(\tilde{v} + \tilde{w}), \\ \tilde{W}(\tilde{v})\tilde{W}(\tilde{w}) &= \chi([v, w])\tilde{W}(\tilde{w})\tilde{W}(\tilde{v}). \end{aligned} \tag{6.42}$$

This is in analogy to the odd case in Eq. (4.3). The Weyl operators can be written as products of the well-known *Pauli operators*

$$Z(z)\,|u\rangle := \chi(z \cdot u)\,|u\rangle\,, \qquad X(x)\,|u\rangle := |u + x\rangle\,. \tag{6.43}$$

Concretely, we find

$$\tilde{W}(\tilde{z}, \tilde{x}) = \chi_4(\tilde{z} \cdot \tilde{x})Z(z)X(x) = \chi_4(\tilde{z} \cdot \tilde{x})\chi(z \cdot x)X(x)Z(z). \tag{6.44}$$

Thus, the group generated by this representation coincides with the *Heisenberg-Weyl group* introduced in Sec. 3.3.

In contrast to Sec. 3.3 and similar to the odd case in Sec. 3.2, the here introduced Heisenberg group and its representation give rise to a projective representation of $\mathrm{Sp}_{2n}(\mathbb{Z}_4)$ by the *Stone-von Neumann theorem*:

$$\tilde{W}(\tilde{g}(\tilde{v}), \tilde{t}) = \tilde{\mu}(\tilde{g})\tilde{W}(\tilde{v}, \tilde{t})\tilde{\mu}(\tilde{g})^{-1}. \tag{6.45}$$

The projective representation $\tilde{\mu}$ can be lifted to a faithful representation on the *metaplectic group* $\mathrm{Mp}_{2n}(\mathbb{Z}_4)$ which is a central extension of $\mathrm{Sp}_{2n}(\mathbb{Z}_4)$ by the second roots of unity $\{\pm 1\}$, i. e. a double cover [86].

In summary, a formulation over the ring $\mathbb{Z}_4$ allows to recover the (projective) Weil representation for $\mathrm{Sp}_{2n}(\mathbb{Z}_4)$. Since any $g \in \mathrm{Sp}_{2n}(2)$ can be lifted to a $\tilde{g} \in \mathrm{Sp}_{2n}(\mathbb{Z}_4)$, this can be seen as a lifting of the $\mathbb{F}_2$-formulation in Sec. 3.3 which linearises the quadratic dependencies in the projective representation of $\mathrm{ASp}_{2n}(2)$ given there.

6.2.5 The Gurevich-Hadani construction

Gurevich and Hadani [86] gave a similar construction of a Weil representation in characteristic two. Their construction can be seen as a "displacement"-type version of the representation given in the last section. In fact, a presentation along this lines can already be found in the 1961 paper by Bolt, Room and Wall [78].

To this end, consider the bilinear form $\tilde{\eta}$ on $\mathbb{Z}_4^{2n}$ given as

$$\tilde{\eta}(\tilde{v},\tilde{w}) = \sum_{i=1}^{n} \tilde{v}_i \tilde{w}_{n+i}. \tag{6.46}$$

Note that $\tilde{\Omega}(\tilde{v},\tilde{w}) = \tilde{\eta}(\tilde{v},\tilde{w}) - \tilde{\eta}(\tilde{w},\tilde{v})$. In analogy to the odd characteristic case, Eq. (6.23), we can observe that the central extensions $\mathbb{Z}_4^{2n} \times_{\tilde{\Omega}} \mathbb{Z}_4$ and $\mathbb{Z}_4^{2n} \times_{2\tilde{\eta}} \mathbb{Z}_4$ are isomorphic:

$$2\tilde{\eta} - \tilde{\omega} = \tilde{\eta} + \tilde{\eta}^\top = -\,\mathrm{d}\alpha, \quad \text{for } \alpha(\tilde{v}) = \tilde{\eta}(\tilde{v},\tilde{v}). \tag{6.47}$$

The extension by $\tilde{\Omega}$ corresponds to the already mentioned "lift" of the Heisenberg group to $\mathbb{Z}_4$. However, the second extension has the nice property that the form $2\tilde{\eta}$ factors and descends to a form on $\mathbb{F}_2^{2n}$ with values in $2\mathbb{Z}/4\mathbb{Z}$. This form is precisely given by (cp. Eq. (6.29)):

$$2\eta(v,w) = 2\sum_{i=1}^{n} v_i w_{n+i}, \quad v,w \in \mathbb{F}_2^{2n}. \tag{6.48}$$

Therefore, we arrive at the Gurevich-Hadani definition of the Heisenberg group [86]

$$\mathrm{GH}_n(2) := \mathbb{F}_2^{2n} \times_{2\eta} \mathbb{Z}_4. \tag{6.49}$$

The definition of the β function in Sec. 3.3, Eq. (3.70) explicitly states that the group $\mathrm{GH}_n(2)$ is isomorphic to $\mathrm{H}_n(2) = \mathbb{F}_2^{2n} \times_\beta \mathbb{Z}_4$:

$$\beta = 2\eta - \mathrm{d}\gamma. \tag{6.50}$$

The choice made by Gurevich and Hadani simplifies the analysis of centre-fixing automorphisms compared to Sec. 3.3. This is because $\mathrm{GH}_n(2)$ has a direct and natural lift to $\mathbb{Z}_4$. Although the centre-fixing automorphisms have to be isomorphic to the ones constructed before in Sec. 3.3, we give a self-contained analysis for completeness here.

The centre-fixing automorphisms have the form $(v,t) \mapsto (g(v), t + \alpha(v))$ for $g \in \mathrm{GL}_{2n}(2)$ and $\alpha : \mathbb{F}_2^{2n} \to \mathbb{Z}_4$ such that

$$2\eta(gv,gw) - 2\eta(v,w) = \alpha(v+w) - \alpha(v) - \alpha(w), \quad \forall v,w \in \mathbb{F}_2^{2n}. \tag{6.51}$$

If such an automorphism exists, then the left hand side has to be symmetric. Said symmetry $\eta(gv,gw) - \eta(v,w) = \eta(gw,gv) - \eta(w,v)$ is equivalent to $[gv,gw] = [v,w]$ and thus $g \in \mathrm{Sp}_{2n}(2)$. Next, we will show that for any $g \in \mathrm{Sp}_{2n}(2)$, there is a solution α_g of Eq. (6.51). Choose a lift $\tilde{g} \in \mathrm{Sp}_{2n}(\mathbb{Z}_4)$ of g, i.e. $g \circ \pi = \pi \circ \tilde{g}$, and set

$$\tilde{\alpha}_{\tilde{g}}(\tilde{v}) := \tilde{\eta}(\tilde{g}\tilde{v},\tilde{g}\tilde{v}) - \tilde{\eta}(\tilde{v},\tilde{v}). \tag{6.52}$$

Using as above that $\tilde{\eta}(\tilde{g}\tilde{w},\tilde{g}\tilde{w}) - \tilde{\eta}(\tilde{v},\tilde{w})$ is symmetric, we compute

$$\tilde{\alpha}_{\tilde{g}}(\tilde{v}+\tilde{w}) = \tilde{\alpha}_{\tilde{g}}(\tilde{v}) + \tilde{\alpha}_{\tilde{g}}(\tilde{w}) + 2\tilde{\eta}(\tilde{g}\tilde{v},\tilde{g}\tilde{w}) - 2\tilde{\eta}(\tilde{v},\tilde{w}). \tag{6.53}$$

First, this shows that $\tilde{\alpha}_{\tilde{g}}(\tilde{v}+2\tilde{x}) = \tilde{\alpha}_{\tilde{g}}(\tilde{v})$ and thus $\tilde{\alpha}_{\tilde{g}}$ descends to a function $\alpha_{\tilde{g}}$ (which still depends on the chosen lift). Second, Equation (6.53) implies that this function fulfills

$$\alpha_{\tilde{g}}(v+w) = \alpha_{\tilde{g}}(v) + \alpha_{\tilde{g}}(w) + 2\eta(gv,gw) - 2\eta(v,w), \tag{6.54}$$

where we used that the form $2\tilde{\eta}$ descends to the form 2η on $\mathbb{F}_2^{2n}$ and applied the lift property $gv = \pi(\tilde{g}\tilde{v})$. This shows that the pair $(g, \alpha_{\tilde{g}})$ is a valid centre-fixing automorphism for any lift $\tilde{g}$ of g.

To determine how many solutions for α given $g \in \mathrm{Sp}_{2n}(2)$ exist, we first determine the solutions over $\mathbb{Z}_4$. Given a lift $\tilde{g}$ of g we set $\tilde{B}_{\tilde{g}} := \tilde{g}^*\tilde{\eta} - \tilde{\eta}$ and consider the lifted version of Eq. (6.51):

$$2\tilde{B}_{\tilde{g}}(\tilde{v}, \tilde{w}) = 2\tilde{\eta}(\tilde{g}\tilde{v}, \tilde{g}\tilde{w}) - 2\tilde{\eta}(\tilde{v}, \tilde{w}) = \tilde{\alpha}(\tilde{v} + \tilde{w}) - \tilde{\alpha}(\tilde{v}) - \tilde{\alpha}(\tilde{w}). \tag{6.55}$$

Note that the left hand side factors with $2\tilde{B}_{\tilde{g}} = 2\pi^* B_g$, and thus *does not actually depend on the lift*. Thus, any quadratic form $\tilde{\alpha}$ solving this equation has to fulfill $2\tilde{\alpha}(\tilde{v}) = 2\tilde{\alpha}_{\tilde{g}}(\tilde{v}) = 2B_g(v, v)$ and hence its values are determined up to $2\mathbb{Z}/4\mathbb{Z}$. Fixing an arbitrary lift, we can thus write any quadratic solution as $\tilde{\alpha}(\tilde{v}) = \tilde{\alpha}_{\tilde{g}}(\tilde{v}) + 2\tilde{b}(\tilde{v}, \tilde{v})$ where $\tilde{b}$ is a symmetric bilinear form. By construction, $\tilde{\alpha}$ factors to a quadratic form α on $\mathbb{F}_2^{2n}$ with values in $\mathbb{Z}_4$ fulfilling the polarisation identity Eq. (6.51). It can be written as

$$\alpha(v) = \alpha_{\tilde{g}}(v) + 2b(v, v), \tag{6.56}$$

where b is $\mathbb{F}_2$-valued symmetric form on $\mathbb{F}_2^{2n}$ such that $2\tilde{b} = 2\pi^* b$. However, over $\mathbb{F}_2$ we have

$$b(v + w, v + w) = b(v, v) + 2b(v, w) + b(w, w) = b(v, v) + b(w, w), \tag{6.57}$$

and thus $\varphi(v) := b(v, v)$ is actually a linear form. Thus, we have proven that there is essentially a unique quadratic solution $\alpha_g \equiv \alpha_{\tilde{g}}$ to the polarisation identity Eq. (6.51) and that all other solutions differ by a linear form 2φ from this one, i.e. by an inner automorphism. Here, "essentially" means that it still depends on a choice of lift. This shows that the centre-fixing automorphisms (g, α) form a fibre bundle where the fibre at g is isomorphic to $\mathbb{F}_2^{2n}$. As in the odd case, we will call this automorphism group the *affine symplectic group* $\mathrm{ASp}_{2n}(2)$ which is now *not* a simple semidirect product.

The representation of $\mathrm{GH}_n(2)$ again depends on a character χ_4 of $\mathbb{Z}_4$. Let $\chi := \chi_4 \circ \iota$ be the induced character of $\mathbb{F}_2$. Denote by $z = (z_1, \ldots, z_n)$ and $x = (x_1, \ldots, x_n)$ standard symplectic coordinates of $\mathbb{F}_2^{2n}$. Then, a direct computation shows that the following definition is a linear representation of $\mathrm{GH}_n(2)$ on $\mathbb{C}[\mathbb{F}_2^n]$:

$$D_{\chi_4}(z, x, t)f(u) := \chi_4(t + 2z \cdot u)f(u + x) = \chi_4(t)\chi(z \cdot u)f(u + x). \tag{6.58}$$

We call this the *displacement representation* of the Heisenberg group $\mathrm{GH}_n(2)$. Comparing this representation, we see that it differs from the Schrödinger representation in Eq. (3.74) exactly by the coboundary γ as expected. Hence, this representation is another way of constructing the Heisenberg-Weyl group $\mathrm{HW}_n(2)$.

PART II

CLASSICAL SIMULATION AND THE RESOURCE THEORY OF MAGIC

CHAPTER 7

INTRODUCTION

Despite the advancing development of quantum platforms, it remains elusive precisely which quantum phenomena are required for a quantum advantage over classical computers. However, for the eventual design of fault-tolerant quantum computers, the understanding of quantum resources seems to be imperative for an efficient architecture. Here, the *magic state model* of quantum computing offers a particularly fruitful perspective on the resource question. In this model, a quantum computer is only required to perform a limited set of operations, namely the preparation of stabiliser states, Clifford gates and Pauli measurements. These *stabiliser operations* by themselves do not suffice for universal quantum computing and can be efficiently simulated by a classical computer. In addition, the quantum computer needs a supply of *magic states* to promote the model to universality [55].

Therefore, there has been an increasing interest in developing a resource theory of quantum computing where the resource is *magic*. The first resource theory was developed for the somewhat simpler case of odd-dimensional systems. Based on the phase-space representation which we introduced in Part I, the *Wigner function* provides a *quasi-probability representation* of quantum mechanics on a discrete phase space. As discussed in Sec. 5.1, the non-negatively represented sub-theory encompasses stabiliser states, Clifford unitaries and Pauli measurements. However, the Wigner function of an arbitrary state might have negative values. Since the sum of negative entries is preserved under Clifford unitaries due to the Clifford covariance of the Wigner function, this *negativity* defines a *resource monotone* called *mana*. Recall from Sec. 5.1 that a non-negative Wigner representation allows for an efficient simulation of a classical computer. As a consequence, negativity, i.e. non-trivial mana, is a necessary condition for a quantum speed-up [24–28]. Interestingly, the existence of negativity in the Wigner function is also equivalent to contextuality with respect to Pauli measurements [122, 123]. The classical simulation based on the Wigner function can be extended to negatively represented states which, however, increases the computational complexity. Thus, the operational meaning of mana is to quantify the runtime of such an algorithm [29]. In this sense, the more magic a quantum computation requires, the harder it is for a classical computer to simulate it. Beyond the Clifford covariance, the Wigner function has two important properties which make it a useful tool for the resource theory of magic. First, it is a *minimal* representation, meaning that the degrees of freedom in the phase space representation are equal to the dimension of operator space. This is because the Wigner function is given by the coefficients in a suitable operator basis. Second, it is *multiplicative* with respect to tensor products. Although the Wigner function generally has exponentially many non-zero entries and is thus inefficient to compute, such is the mana, the multiplicativity allows us to efficiently compute it for product states.

Unfortunately, in the practically more relevant case of qubits, the phase space approach suffers from mathematical problems which cannot be overcome completely as we saw in Sec. 3.3 and 6.2. Eventually these problems lead to the non-existence of a

suitable Wigner function for qubits [112], a result which is non-trivially implied by older works on the Clifford group [77]. This fact is closely related to the existence of state-independent contextuality for qubits. Henceforth, a number of works tried to recover properties the Wigner function by restricting the set of non-negatively represented states and operations [124–126] or by relaxing the definition of the Wigner function [105, 127]. Although important from a conceptual point of view, these attempts are arguably unsatisfactory from a resource-theoretic perspective: In the first case, the representation is not able to cover all stabiliser states and the full Clifford group efficiently. In the second case, the representation is highly overcomplete and the defined structures are not closed under tensor products. Besides these works, there has been a number of parallel developments of finding alternatives to the Wigner function [30–39]. A common element in these approaches is that the finite set of stabiliser states is taken as the set of free states. Since stabiliser operations (probabilistically) map stabiliser states to stabiliser states, and this can be classically simulated, any *magic monotone* should be non-increasing under those. Two notable examples are the so-called *robustness of magic* [32] and the *stabiliser rank and extent* [34], both of which again quantify the runtime of a suitable classical simulation algorithm. The stabiliser rank and extent are only defined for pure states and could be considered as pure state monotones which are non-increasing under Clifford unitaries. Although hard to compute in general, the stabiliser extent is multiplicative for product states if the individual tensor factors are supported on ≤ 3 qubits [34]. In contrast, the robustness of magic is defined for mixed states and is *faithful* on the convex hull of stabiliser states. Although being a more general monotone in this way, the robustness of magic is strictly *non-multiplicative*, which makes it hard to derive tight asymptotic bounds. However, in certain regimes, exploiting symmetries can help to compute the robustness of magic yielding better bounds on its asymptotic behaviour, as I show in Ref. [33] which is included as Ch. 8.

Albeit, it was recently shown that the stabiliser extent is eventually non-multiplicative, too [38]. In fact, the argument generalises to any monotone based on a ℓ_1-optimal decomposition in a frame of states.

Recently, there as been increased effort in unifying and developing the magic resource theory [36, 39]. Seddon et al. [36] showed that the stabiliser extent can be understood as the pure-state specialisation of three more general mixed-state monotones, the *mixed-state extent*, the *dyadic negativity* and the *generalised robustness*. Interestingly, these three monotones can be bounded by each other and agree on tensor products of single-qubit states. Typically, there is an exponential gap between these monotones and the robustness of magic. The operational meaning of these magic monotones can again be related to the runtime of different classical simulation algorithms [34, 36].

Stabiliser operations do not form the most general set of free operations in the qubit resource theory of magic. Defining *completely stabiliser-preserving* (CSP) channels as those quantum channels which map the polytope spanned by stabiliser states to itself, it was shown that the *robustness of magic*, the *mixed-state extent*, the *dyadic negativity* and the *generalised robustness* are also non-increasing with respect to CSP channels [35, 36]. CSP channels were first studied in Ref. [128] in the context of interconversion between single-qudit states. There, the authors give a single-qutrit CSP channel which introduces negativity in the Wigner function of input states. This shows that CSP channels and stabiliser operations are distinct for a single qutrit. However, due to the lack of a Wigner function, the qubit case is considerably different from the higher-dimensional case. The set of

multi-qubit CSP channels was studied by my collaborators and I in Ref. [129] (included as Ch. 9). There, we give a characterisation and interpretation of CSP channels and show that it is strictly larger than the set of stabiliser operations.

Structure of this part

This part of the thesis contains two publications to which I contributed significantly. These works address two very different questions arising in the resource theory of magic state quantum computing.

Chapter 8 discusses the computability of magic monotones for many-qubit states. In general, this is a very high-dimensional optimisation problem the runtime of which is super-exponential in the number of qubits. However, as we show, the computation can be significantly sped up after a careful study of the geometry, algebraic structure and symmetries of the involved objects, which are *stabiliser states* and *magic states*. Combined with symmetry reduction techniques from convex optimisation, this yields a simplification strategy which is carried out in detail and implemented numerically for the robustness of magic as an example. The results include the exact monotone values of single-qubit magic states for up to 10 copies as well as approximations beyond, indicating the asymptotic behaviour of the underlying monotone. The work also contains the first characterisation of the symmetries of the stabiliser polytope which is the set of free states in the qubit resource theory of magic. It is shown that the symmetries are determined by the design property of stabiliser states, thereby showing a qualitative difference for qubits and higher-dimensional qudits. This chapter has been previously published as Ref. [33].

The emphasis of Chapter 9 is on the characterisation of the natural set of free operations in the resource theory of magic state quantum computing, the *completely-stabiliser preserving* (CSP) channels. These are exactly the quantum channels which preserve the convex hull of stabiliser states. As such, they encompass the well-known stabiliser operations among which are Clifford unitaries, Pauli measurements and preparation of stabiliser states. The structure of CSP channels and their relation to stabiliser operations is studied. We present a canonical form of CSP channels, giving them an interpretation in terms of a set of Clifford unitaries, conditionally applied on the outcome of general stabiliser POVMs. Moreover, we give an explicit example of a CSP channel which is not a stabiliser operation, thereby showing that the set of CSP channels strictly contains the set of stabiliser operations. Our conclusions are based on a canonical form of bipartite stabiliser states and Pauli invariance properties of stabiliser operations, both of which seem to be previously unknown and of independent interest. This chapter has been previously published as Ref. [129] and is presented at the QIP 2021 conference.

CHAPTER 8

ROBUSTNESS OF MAGIC AND SYMMETRIES OF THE STABILISER POLYTOPE

About this chapter

The following text has been previously published as

> Markus Heinrich and David Gross. "Robustness of Magic and Symmetries of the Stabiliser Polytope". In: *Quantum* 3 (2019), p. 132. DOI: 10.22331/q-2019-04-08-132

Deviations from the published version are limited to typesetting and notation. These changes were performed to match the rest of this dissertation. Note that this chapter has its own independent appendix.

The results in this chapter were derived by Markus Heinrich with the exception of Sec. 8.C which is due to David Gross who also supervised this work. The introduction of the paper was laid out by DG, the remaining sections are written by MH.

Abstract

We give a new algorithm for computing the *robustness of magic*—a measure of the utility of quantum states as a computational resource. Our work is motivated by the *magic state model* of fault-tolerant quantum computation. In this model, all unitaries belong to the Clifford group. Non-Clifford operations are effected by injecting non-stabiliser states, which are referred to as *magic states* in this context. The *robustness of magic* measures the complexity of simulating such a circuit using a classical Monte Carlo algorithm. It is closely related to the degree negativity that slows down Monte Carlo simulations through the infamous *sign problem*. Surprisingly, the robustness of magic is *sub*multiplicative. This implies that the classical simulation overhead scales subexponentially with the number of injected magic states—better than a naive analysis would suggest. However, determining the robustness of n copies of a magic state is difficult, as its definition involves a convex optimisation problem in a 4^n-dimensional space. In this paper, we make use of inherent symmetries to reduce the problem to n dimensions. The total run-time of our algorithm, while still exponential in n, is super-polynomially faster than previously published methods. We provide a computer implementation and give the robustness of up to 10 copies of the most commonly used magic states. Guided by the exact results, we find a finite hierarchy of approximate solutions where each level can be evaluated in polynomial time and yields rigorous upper bounds to the robustness. Technically, we use symmetries of the stabiliser polytope to connect the robustness of magic to the geometry of a low-dimensional convex polytope generated by certain *signed quantum weight enumerators*. As a by-product, we characterised the automorphism group of

the stabiliser polytope, and, more generally, of projections onto complex projective 3-designs.

8.1 Introduction

In fault-tolerant quantum computation (for a recent review, see Ref. [130]), each logical qubit is encoded in a non-local subspace of a number of physical qubits. There are several ways of effecting a unitary transformation of logical qubits. In the simplest case, logical unitaries can be implemented *transversally*, i.e. by local gates acting on the physical qubits. Unfortunately, a no-go theorem by Eastin and Knill [131] states that there are no quantum codes that allow for a *universal* set of transversal gates.

In the *magic state model* [55], the logical gate set is chosen to be the Clifford group, which can be implemented transversally in various quantum codes using their physical counterparts. Any logical non-Clifford gate would promote the Clifford group to universality. This remaining problem is solved by providing an auxiliary qubit in a non-stabiliser state. Using a circuit gadget (which only requires Clifford operations), one can turn this auxiliary state into a non-Clifford gate (Fig. 8.1). The auxiliary qubit state is consumed in the process, so that one such input needs to be injected for each non-Clifford gate. These inputs are the *magic states* from which the protocol derives its name.

A common choice for a non-Clifford gate is the T-gate $T = \mathrm{diag}(1, e^{i\pi/4})$, which is realised by the following magic state

$$|H\rangle := T\,|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi/4}\,|1\rangle\right). \tag{8.1}$$

Moreover, there is a second magic state, $|T\rangle$, which realises the non-Clifford gate $\mathrm{diag}(1, e^{i\pi/6})$. Their Bloch representation is shown in Fig. 8.5. Interestingly, it has been found that even certain mixed states can "supply the magic" to promote a Clifford circuit to universality. Indeed, a process called *magic state distillation* (Fig. 8.2) can turn many copies of some mixed state ρ into a pure magic state using Clifford unitaries and computational basis measurements [55, 132].

Magic state distillation motivates the search for quantitative measures of the "computational utility" of auxiliary states. This analysis turns out to be slightly simpler for quantum systems with odd-dimensional Hilbert spaces [26–28], as the theory of stabiliser states is somewhat better-behaved in this case, and there is a better-developed toolbox of "phase space methods" available in this case (see e.g. Refs. [75, 133, 134]). However, as qubits are the paradigmatic systems for quantum computation, quantitative resource theories for multi-qubit magic states have since been developed [30, 32].

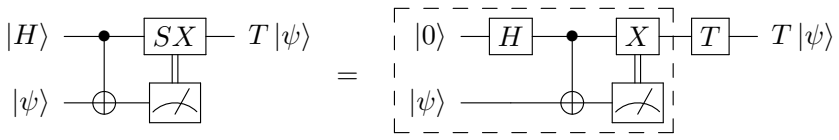


Figure 8.1: Use of magic state injection to perform a T gate on some input state $|\psi\rangle$. The state injection circuit can be rewritten as a swap circuit followed by T gate.

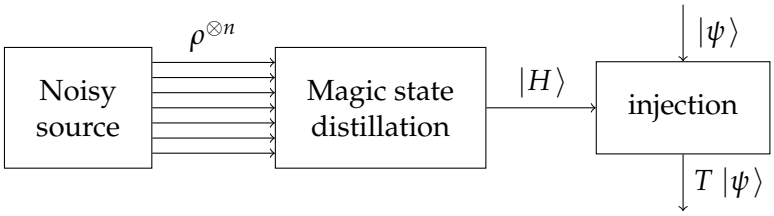


Figure 8.2: Magic state distillation turns a supply of mixed states ρ into a pure magic state, e.g. $|H\rangle$ using only Clifford operations.

The starting point of these theories is the Gottesman-Knill Theorem [135]. It states that quantum circuits consisting only of preparations of stabiliser states, Clifford unitaries, and computational basis measurements can be efficiently simulated on a classical computer. Therefore, if the auxiliary states are stabilisers, there can be no quantum computational advantage. Next, assume that an auxiliary n-qubit state ρ is an element of the *stabiliser polytope* SP_n, i.e.

$$\rho = \sum_i p_i s_i,$$

where $(p_i)_i$ is a probability distribution and the $s_i = |\psi_i\rangle\langle\psi_i|$ are stabiliser states. This readily gives rise to an efficient classical randomised algorithm that will draw outcomes from the same distribution as a quantum computer would [136], provided that one can sample efficiently from the probability distribution $(p_i)_i$: Indeed, draw s_i with probability p_i, and then continue to simulate the further time evolution using Gottesman-Knill. Thus, density matrices contained in the convex hull of stabiliser states are equally useless as computational resource states in the magic state model (Fig. 8.3).

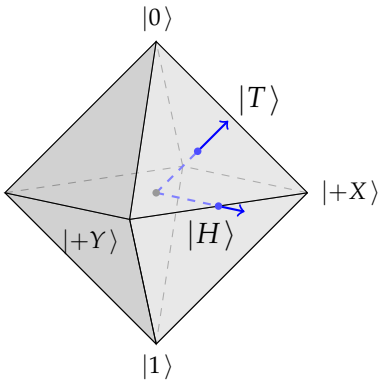


Figure 8.3: Bloch representation of the the two most commonly considered magic states $|H\rangle$ and $|T\rangle$. These states lie outside of the octahedron spanned by 1-qubit stabiliser states having a Bloch vector orthogonal to an edge ($|H\rangle$) or a facet ($|T\rangle$) of the stabiliser octahedron. The intersection of their Bloch vector with the facet or edge is marked with a blue dot. Certain mixed states can be used to distil these pure states using Clifford unitaries and measurements. However, states lying inside the stabiliser polytope are useless as a resource state.

Since the stabiliser states $\{s_i\}_i$ span the space of Hermitian operators, any auxiliary state can be expanded as $\rho = \sum_i x_i s_i$, with coefficients x_i that are not necessarily non-negative. However, taking traces on both sides shows that the expansion is *affine*, i.e. $\sum_i x_i = 1$. It is well-known in the theory of Quantum Monte Carlo methods [137] that the probabilistic algorithm sketched above can be extended to the more general scenario. However, the runtime will increase with the total amount of "negativity" in the expansion coefficients x_i. This is the dreaded *sign problem*. A precise theory of the simulation

runtime in the context of quantum computation has been developed in Ref. [29] and applied to the magic state model in Ref. [32]. More precisely, they define the *robustness of magic* (RoM) as

$$\mathcal{R}(\rho) := \min\left\{ \|x\|_1 \;\middle|\; x \in \mathbb{R}^N :\ \rho = \sum_{i=1}^{N} x_i s_i \right\}, \tag{8.2}$$

where the sum ranges over stabiliser states $\{s_1, \ldots, s_N\}$ and the ℓ_1-norm

$$\|x\|_1 = \sum_{i=1}^{N} |x_i| = 1 + 2 \sum_{i:\, x_i \leq 0} |x_i|$$

measures the "amount of negativity" in the affine combination. Then, the number of samples which have to be taken in the Monte Carlo simulation scales as $O(\mathcal{R}(\rho)^2)$ [29, 32].

In addition to measuring the "computational utility" in the above precise sense, the RoM has further interpretations. For example, it can be used to systematically lower-bound the number of non-Clifford gates required to synthesise certain unitaries, namely those that allow for a magic state realisation [32]. Lastly, the RoM derives its name from the fact that it quantifies the robustness of a state's computational utility against noise processes. A precise account of this point of view is given in Section 8.2.

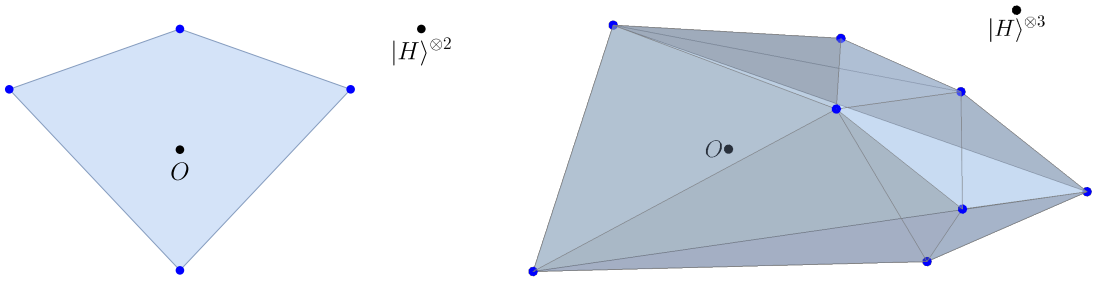
Interestingly, the RoM is *sub*multiplicative, i.e. $\mathcal{R}(\rho^{\otimes 2}) \leq \mathcal{R}(\rho)^2$, where the inequality is usually strict [32]. That means that the simulation effort of a magic state circuit grows subexponentially with the number of injected magic states—an intriguing phenomenon. Therefore, a quantity of interest is the *regularised RoM*:

$$\mathcal{R}_{\mathrm{reg}}(\rho) := \lim_{n\to\infty} \mathcal{R}(\rho^{\otimes n})^{1/n}.$$

Unfortunately, computing $\mathcal{R}(\rho^{\otimes n})$ seems to be a difficult task. For ρ being a single-qubit state, the tensor power $\rho^{\otimes n}$ lives in an 4^n-dimensional space, and the sum over the s_i in the definition (8.2) of the RoM has to range over the $2^{O(n^2)}$ stabiliser states defined for n-qubit systems. Any direct implementation of the optimisation problem (8.2) will thus quickly became computationally intractable—and, indeed, Howard and Campbell [32] could carry it out only up to $n = 5$.

The starting point of this work is the observation that there is a large symmetry group shared by $\rho^{\otimes n}$ and the stabiliser polytope. Thus, we formulate the optimisation in a space where the joint symmetries have been "modded out". The space of operators invariant under the joint symmetry group turns out to have a dimension mildly polynomial in n. For the especially interesting cases where the state is $|H\rangle^{\otimes n}$ or $|T\rangle^{\otimes n}$, the dimension reduces further to exactly n. While the projection of the stabiliser polytope to this invariant space (Fig. 8.4) still has exponentially many vertices, it turns out that formulating the optimisation problem in this symmetry-reduced way leads to a super-polynomially faster algorithm.

Equipped with the knowledge of the exact solution to Eq. (8.2) for the commonly used magic states $|H\rangle^{\otimes n}$ and $|T\rangle^{\otimes n}$ and $n \leq 10$ qubits, we formulate a relaxation of the RoM problem for these states which yields an upper bound for the exact RoM. These approximations are in excellent agreement with the exact data for $n \leq 10$ and can be carried out for up to 26 qubits. What is more, we can not only compute the RoM bounds



(a) $n = 2$ (b) $n = 3$

Figure 8.4: Projected n-qubit stabiliser polytopes with respect to the symmetry group of the magic state $|H\rangle^{\otimes n}$ and $n = 2, 3$. We use a Bloch-like representation in the basis constructed in Sec. 8.3.3. The origin O corresponds to the maximally mixed state $\mathbb{1}/2^n$ and lies inside the polytope. The complexity of the polytopes is significantly reduced compared to the full 15-dimensional (respectively 63-dimensional) stabiliser polytopes. Visual inspection suggests that no joint symmetries of $|H\rangle^{\otimes n}$ and the projected polytope remain.

for these approximations, but also find the corresponding affine decompositions $\rho^{\otimes n} = \sum_i x_i s_i$, which can directly be used in Monte Carlo simulations. Furthermore, we find a hierarchy of such RoM approximations by restricting to k-partite entangled stabiliser states which converges to the exact RoM. Interestingly, every level of the hierarchy can be computed in polynomial time.

Finally, both the exact and approximate results imply a runtime of $O(2^{0.737t})$ for simulating a circuit with t T gates using the RoM algorithm. Moreover, our analysis suggests that this runtime is the optimal one that can be achieved using a RoM algorithm. Our work improves on the previously known runtime of $O(2^{0.753t})$ derived in Ref. [32]. Note that the RoM algorithm is able to simulate noisy circuits and mixed states. This is in contrast to simulation algorithms based on the so-called *stabiliser rank* which can achieve a runtime of $O(2^{0.48t})$ for pure states [30, 31, 138].

This paper is organised as follows. Section 8.2 is devoted to a short discussion of the Robustness of Magic, giving an alternative definition to the one in the previous section and stating the properties of this resource monotone. Next, a series of techniques is presented which use the symmetries in the definition of the monotone to simplify the computation significantly. To this end, the symmetry group of the stabiliser polytope is characterised in Sec. 8.3.2 and certain classes of states are singled out in Sec. 8.3.3 which profit from a high degree of symmetry. For these states, we explicitly derive the symmetry-reduced problem by constructing a suitable basis for the invariant subspace in Sec. 8.3.3, followed by enumerating equivalence classes of stabiliser states up to symmetry in Sec. 8.3.4. The numerical solutions for the constructed problems are presented and discussed in Section 8.4. Based on this, we prove a polytime relaxation of the RoM problem in Sec. 8.4.3. Our results are summarised in Sec. 8.5.

8.2 Robustness of Magic

The resource theory of magic states can be developed in analogy to the more-established resource theory of entanglement and the *robustness of entanglement* [139] studied in this context. There, the robustness of a state can be interpreted as a measure for the worst-case separable noise that renders the state separable. However, its construction can be generalised to any resource theory as follows: Given a convex set S of free resources, the robustness of a relative to $b \in S$ is defined as

$$R(a||b) := \inf\left\{ s \geq 0 \;\middle|\; \frac{1}{1+s}\,(a + sb) \in S \right\}. \tag{8.3}$$

Depending on the choice of b, the robustness might be infinite. If it is finite, we can express a as a pseudo-mixture

$$a = (1+s)b^{+} - sb^{-}, \qquad \text{with } b^{\pm} \in S. \tag{8.4}$$

Following Vidal and Tarrach [139], one can define the so-called *total robustness* by minimising over the set of free resources:

$$R(a) := \inf_{b \in S} R(a||b). \tag{8.5}$$

In the following, we choose $S = \mathrm{SP}_n$ to be the convex polytope spanned by the n-qubit stabiliser states. More precisely, $\mathrm{SP}_n = \operatorname{conv} \mathrm{stab}(n)$, where $\mathrm{stab}(n) = \{s_1, \ldots, s_N\}$ is the set of all n-qubit stabiliser states. Here, and in the following, by a "quantum state", we will always mean the density matrix representing it. In the case of pure states $s_i = |\psi_i\rangle\langle\psi_i|$, the associated vector $|\psi_i\rangle$ will be referred to as a *state vector*. The polytope SP_n is a subset of the real vector space of $(D \times D)$-dimensional Hermitian matrices H_D where $D = 2^n$ is the overall dimension of Hilbert space. More specifically, quantum states lie in the (D^2-1)-dimensional affine subspace given by $\operatorname{tr}\rho = 1$. Within this affine hyperplane, SP_n is full-dimensional and we usually consider it as the the ambient space of SP_n.

Howard and Campbell [32] work with an equivalent robustness measure: the *robustness of magic* (RoM) introduced in Eq. (8.2). A straightforward calculation (c.f. Appendix 8.A) shows that the two measures are related by a simple affine transformation:

$$\mathcal{R}(\rho) = 1 + 2R(\rho). \tag{8.6}$$

The robustness of magic provides a proper resource monotone with the following properties:

Proposition 8.1 (Properties of Robustness of Magic [32])**.** *The* robustness of magic *has the following properties:*

1. Faithfulness*:* $\mathcal{R}(\rho) = 1$ *iff* $\rho \in \mathrm{SP}_n$
2. Monotonicity*:* $\mathcal{R}(\mathcal{X}(\rho)) \leq \mathcal{R}(\rho)$ *for all stabiliser operations* $\mathcal{X}$ *with equality if* $\mathcal{X}$ *is unitary.*
3. Convexity*:* $\mathcal{R}((1-t)\rho + t\sigma) \leq (1-t)\mathcal{R}(\rho) + t\,\mathcal{R}(\sigma)$ *for* $0 \leq t \leq 1$.
4. Submultiplicativity*:* $\mathcal{R}(\rho \otimes \sigma) \leq \mathcal{R}(\rho)\,\mathcal{R}(\sigma)$.

8.3 Exploiting stabiliser symmetries

8.3.1 Definition of the RoM problem.

The Robustness of Magic is defined as the following optimisation problem.

Problem 8.1 (Robustness of Magic)**.** Let $\mathrm{stab}(n) = \{s_1, \ldots, s_N\}$ be the set of stabiliser states. Given a state ρ, solve the following problem:

$$\begin{aligned} \textbf{min} \quad & \|x\|_1 \quad \text{over } x \in \mathbb{R}^N \\ \textbf{s.t.} \quad & \rho = \sum_{i=1}^{N} x_i s_i. \end{aligned}$$

Using standard techniques, this problem can be reformulated as a linear program (LP) with $D^2 + 2N$ constraints and $2N$ variables [140]. Although the time complexity of LPs is linear in the product of number of constraints and variables, these numbers themselves grow super-exponentially with the number of qubits n. Concretely, $N = 2^{O(n^2)}$ and $D^2 = 4^n$. Moreover, the LP needs access to an oracle which provides the N stabiliser states. The implementation of such an oracle would necessarily have super-exponential time complexity itself. However, even if an efficient oracle were provided, the storage of the states would quickly exceed the memory capacity of any computer. In practice, this limits the evaluation of the problem to $n \leq 5$ on normal computers and renders it infeasible, even on supercomputers, for $n \geq 8$.[1]

A standard method in the analysis of optimisation problems is dualising the problem. Clearly, by Slater's condition, strong duality holds and thus the dual problem is an equivalent definition for the Robustness of Magic. In Appendix 8.B, we state the dual problem and derive a lower bound from a feasible solution. However, this bound matches the one that was already found in Ref. [32].

8.3.2 Symmetry reduction

The complexity of the RoM problem can be significantly reduced by exploiting the symmetries of the problem, a procedure that we will call *symmetry reduction* and is well-known in convex optimisation theory, see e. g. [141]. Here, we will explain the basic ideas and refer the interested reader to App. 8.E for a mathematical review.

By *stabiliser symmetries* $\mathrm{Aut}(\mathrm{SP}_n)$, we mean the linear symmetry group of the stabiliser polytope. This is the group of linear maps $H_D \to H_D$ that leave SP_n invariant. These maps necessarily have to preserve the set of vertices, i. e. the set of stabiliser states $\mathrm{stab}(n)$. Clearly, the group of n-qubit Clifford unitaries Cl_n induces such symmetry transformations by conjugation. Another obvious symmetry of the set of stabilisers is the *transposition*:

$$s_i = |\psi_i\rangle\langle\psi_i| \mapsto s_i^T = \mathcal{C}\,|\psi_i\rangle\langle\psi_i|\,\mathcal{C},$$

where $\mathcal{C}$ is the (anti-unitary) operation of complex conjugation in the computational basis. The group of unitary and anti-unitary operations generated by Clifford unitaries and complex conjugation is known as the *extended Clifford group* EC_n [66]. Our first result

[1] Already the storage of stab(7) would require around 77 TiB of memory. For $n = 8$, this number increases to around 76 PiB which exceeds the state-of-the-art by a factor of 7.

states that any stabiliser symmetry is induced by the action of an element of the extended Clifford group on the Hilbert space. This is a corollary of the more general Thm. 8.1 on symmetries of 3-designs and is proven in App. 8.C.

Corollary 8.1. *The group of stabiliser symmetries* $\mathrm{Aut}(\mathrm{SP}_n)$ *is given by the adjoint representation of the extended Clifford group* $\mathrm{E}\mathcal{C}_n$.

We emphasise that this is a non-trivial result which is in general wrong for the case of odd-dimensional qudits where it is possible to construct explicit counter-examples. This turns out to be related to the fact that stabiliser states fail to form 3-designs in odd dimensions [108, 113, 114].

Note that anti-unitary symmetries in $\mathrm{E}\mathcal{C}_n$ act in the adjoint representation as $\mathrm{Ad}(C) \circ T$, where $C \in \mathrm{Cl}_n$ and T is the transposition map. Hence, there are only *global* antiunitary symmetries. Every tensor product of local antiunitary symmetries would involve a partial transposition and such a map could not preserve the set of *entangled* stabiliser states.

Let $G_\rho < \mathrm{E}\mathcal{C}_n$ be a (not necessarily maximal) subgroup fixing ρ. The projection onto the subspace of G_ρ-fixed points $V^{G_\rho} \subset H_D$, see App. 8.E, is given by

$$\Pi_{G_\rho}(\sigma) = \frac{1}{|G_\rho|} \sum_{U \in G_\rho} U\sigma U^\dagger. \tag{8.7}$$

Note that Π_{G_ρ} is trace-preserving, hence the image of quantum states will again lie in the affine subspace $\mathrm{tr}^{-1}(\{1\}) \cap V^{G_\rho}$.

Recall that we can express the robustness of ρ as a minimisation over $t \geq 0$ and (mixed) stabiliser states $\sigma^\pm \in \mathrm{SP}_n$ such that

$$\rho = (1+t)\sigma^+ - t\sigma^-. \tag{8.8}$$

Since Π_{G_ρ} preserves SP_n, every such decomposition yields a decomposition in terms of G_ρ-invariant mixed stabiliser states:

$$\rho = \Pi_{G_\rho}(\rho) = (1+t)\,\Pi_{G_\rho}(\sigma^+) - t\,\Pi_{G_\rho}(\sigma^-), \tag{8.9}$$

In particular, if the decomposition was optimal in the first place, the projected decomposition is also optimal.

This shows that there is always G_ρ-invariant optimal solution for the problem. Hence, instead of optimising over the whole set of stabiliser states, we only have to optimise over G_ρ-invariant mixed stabiliser states $\overline{\mathrm{SP}}_n := \mathrm{SP}_n \cap V^{G_\rho}$. By Lemma 8.3 in App. 8.E, these are exactly given by $\overline{\mathrm{SP}}_n = \Pi_{G_\rho}(\mathrm{SP}_n)$ and can thus be computed by evaluating the projections $\overline{\mathrm{stab}}(n) := \Pi_{G_\rho}(\mathrm{stab}(n))$. Since $\Pi_{G_\rho}(UsU^\dagger) = \Pi_{G_\rho}(s)$ for all $U \in G_\rho$ and $s \in \mathrm{stab}(n)$, it is sufficient to compute the projections on representatives of $\mathrm{stab}(n)/G_\rho$. Finally, we remark that a majority of the projected states $\overline{\mathrm{stab}}(n)$ are not extremal points of the projected polytope $\overline{\mathrm{SP}}_n$. Given an extremal subset $\mathcal{V}_n = \{v_1, \ldots, v_M\} \subset \overline{\mathrm{stab}}(n)$, the symmetry-reduced version of Prob. 8.1 is given by substituting $\mathrm{stab}(n) \mapsto \mathcal{V}_n$ and $N \mapsto M$.

8.3.3 Identification of symmetries

The first step towards the explicit symmetry-reduced problem is to identify the group G_ρ that fixes the state ρ of interest. Motivated by magic state distillation and the submultiplicativity problem, we are especially interested in the case $\rho = |\psi\rangle\langle\psi|^{\otimes n}$ with $|\psi\rangle$ being a m-qubit state. A large part of the analysis does not depend on the choice of $|\psi\rangle$, so we keep the discussion as general as possible and specialise later to $m = 1$ and particular choices of $|\psi\rangle$. The symmetries of $|\psi\rangle^{\otimes n}$ can be classified as follows:

Permutation symmetry Clearly, $|\psi\rangle^{\otimes n}$ is invariant under permutations of the n tensor factors. Such permutations also preserve the stabiliser polytope. Thus, the symmetric group S_n is contained in the symmetry group of the problem.

Local symmetries By local symmetries of $|\psi\rangle^{\otimes n}$ we mean products of m-qubit stabiliser symmetries of $|\psi\rangle$. By Corollary 8.1, this class contains only local Clifford operations. Let $(\mathrm{Cl}_m)_\psi$ be the stabiliser of $|\psi\rangle$ within the m-qubit Clifford group Cl_m, then the local symmetry group is given by $(\mathrm{Cl}_m)_\psi^{\otimes n}$.

Global symmetries We refer to all other symmetries as global. The global symmetry group contains e.g. the transposition $\rho \mapsto \rho^T$.

The maximal symmetry group for $\rho = |\psi\rangle\langle\psi|^{\otimes n}$ is given by the subgroup Cl_ρ that stabilises ρ within $\mathrm{E}\mathcal{C}_n$. Here, we focus on the subgroup of Cl_ρ which is given by local symmetries and permutations:

$$G_\rho := (\mathrm{Cl}_m)_\psi^{\otimes n} \rtimes S_n. \tag{8.10}$$

The following analysis suggests that for our choices of ρ, G_ρ actually coincides with Cl_ρ, meaning that there are no further global symmetries. However, since the study of symmetries in $\mathrm{E}\mathcal{C}_n$ can be quite involved [142], we can not exclude the possibility that we missed some of the symmetries.

For the rest of this paper, we will consider the case $m = 1$. Note that Cl_1 acts by rotating about the symmetry axes of the stabiliser polytope. It is easy to see that states $|\psi\rangle$ with non-trivial stabilisers $(\mathrm{Cl}_1)_\psi$ fall into three classes: Stabiliser states (with trivial robustness), and magic states that lie on the Clifford orbit of $|H\rangle$ or $|T\rangle$. Since the RoM is Clifford-invariant, we can pick the following states for concreteness:

$$|H\rangle\langle H| = \frac{1}{2}\left(\mathbb{1} + \frac{1}{\sqrt{2}}(X+Y)\right), \quad |T\rangle\langle T| = \frac{1}{2}\left(\mathbb{1} + \frac{1}{\sqrt{3}}(X+Y+Z)\right). \tag{8.11}$$

Figure 8.5 shows the two states and their stabiliser symmetries. The respective unitary symmetries correspond to a two-fold rotation symmetry about the $|H\rangle$-axis and three-fold rotation symmetry about the $|T\rangle$-axis. In terms of Clifford operations, these stabiliser groups are represented by

$$(\mathrm{Cl}_1)_H = \langle SX\rangle, \qquad (\mathrm{Cl}_1)_T = \langle SH\rangle. \tag{8.12}$$

Recall that these should be understood in the adjoint representation and thus the order of these groups is indeed $|(\mathrm{Cl}_1)_H| = 2$ and $|(\mathrm{Cl}_1)_T| = 3$.

Furthermore, there are antiunitary stabiliser symmetries

$$\begin{aligned} \mathcal{A}: \quad & X \mapsto X, \\ & Y \mapsto Y, \\ & Z \mapsto -Z, \end{aligned} \qquad \begin{aligned} \mathcal{B}: \quad & X \mapsto Y, \\ & Y \mapsto X, \\ & Z \mapsto Z, \end{aligned} \qquad \begin{aligned} \mathcal{C}: \quad & X \mapsto Z, \\ & Y \mapsto Y, \\ & Z \mapsto X, \end{aligned} \tag{8.13}$$

such that $|H\rangle$ is fixed by $\mathcal{A}$ and $\mathcal{B}$ and $|T\rangle$ is fixed by $\mathcal{B}$ and $\mathcal{C}$. Recall that these can only contribute global symmetries such as $\mathcal{A}^{\otimes n}$. However, the common $+1$ eigenspace of $\mathcal{A}^{\otimes n}$ and $\mathcal{B}^{\otimes n}$ coincides with that of $SX^{\otimes n}$ and thus adding these symmetries to the symmetry group will not further reduce the invariant subspace. A similar argument holds also for the antiunitary symmetries of $|T\rangle$.

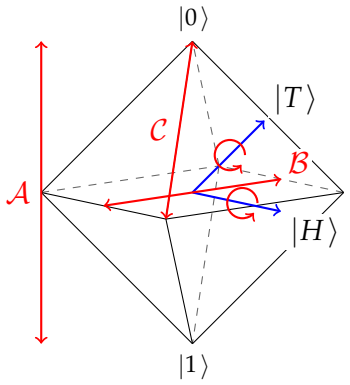


Figure 8.5: Stabiliser symmetries of the magic states $|H\rangle$ and $|T\rangle$ and the octahedron of stabiliser states. $|H\rangle$ is fixed by the antiunitary reflections $\mathcal{A}$, $\mathcal{B}$ and unitary π rotations around its axis. $|T\rangle$ is fixed by the antiunitary reflections $\mathcal{B}$, $\mathcal{C}$ and unitary $\pi/3$ rotations around its axis.

Hence, the considered symmetry groups are as follows:

$$G_H := \langle SX \rangle^{\otimes n} \rtimes S_n, \qquad G_T := \langle SH \rangle^{\otimes n} \rtimes S_n. \tag{8.16}$$

Since the symmetric group S_n is always a subgroup of the symmetry group, the fixed point subspace V^{G_ρ} is always a subspace of the totally symmetric subspace $\mathrm{Sym}(H_D)$. Let us first consider a generic state ρ with no further symmetries. Then, V^{G_ρ} coincides with $\mathrm{Sym}(H_D)$. Thus, the trace 1 subspace has dimension $\frac{1}{6}(n+3)(n+2)(n+1)-1$ and is thus exponentially smaller than the full space. A basis for the symmetric subspace is given by a Fock-style "occupation number basis" constructed from the Pauli basis $\mathbb{1}, X, Y, Z$ as follows

$$N_{i,j,k} = \mathrm{Sym}\left(X^{\otimes i} \otimes Y^{\otimes j} \otimes Z^{\otimes k} \otimes \mathbb{1}^{\otimes(n-i-j-k)}\right), \qquad \text{for } i,j,k \in \{0,\dots,n\} \quad \text{such that} \quad i+j+k \leq n. \tag{8.17}$$

Here, the symmetrisation operator $\mathrm{Sym} \equiv \Pi_{S_n}$ is given by averaging over all permutations of the tensor factors. The trace one subspace can be obtained as the span of all basis elements with the $N_{0,0,0} = \mathbb{1}$ component set to $1/D$.

Due to linearity, the symmetrisation map is completely determined by its action on the Pauli basis. Given a Pauli operator g, there is a permutation $\pi \in S_n$ such that $\pi(g) = X^{\otimes i} \otimes Y^{\otimes j} \otimes Z^{\otimes k} \otimes \mathbb{1}^{\otimes(n-i-j-k)}$. The appearing exponents $i = \mathrm{wt}_X(g)$, $j = \mathrm{wt}_Y(g)$ and $k = \mathrm{wt}_Z(g)$ are exactly the *weights* of g, i. e. the number of X, Y, Z factors, respectively. By

the invariance of Sym under permutations, we thus get $\mathrm{Sym}(g) = \mathrm{Sym}(\pi(g)) = N_{i,j,k}$. We define *weight indicator functions*,

$$A_{i,j,k}(g) := \begin{cases} 1 & \text{if } \mathrm{wt}_X = i,\ \mathrm{wt}_Y = j,\ \mathrm{wt}_Z = k, \\ 0 & \text{else,} \end{cases} \tag{8.18}$$

such that we can write the S_n-projection of a Pauli operator g as

$$\mathrm{Sym}(g) = \sum_{i,j,k} A_{i,j,k}(g) N_{i,j,k}. \tag{8.19}$$

By extending the functions $A_{i,j,k}$ linearly to H_D, we thus get exactly the coefficients of the projection in the number basis.

Let $S < \mathcal{P}_n$ be a stabiliser group stabilising a state s. The projection of this state is

$$\begin{aligned} \mathrm{Sym}(s) &= \frac{1}{2^n} \sum_{g \in S} \mathrm{sgn}(g)\, \mathrm{Sym}(g) \\ &= \frac{1}{2^n} \sum_{i,j,k} \left(\sum_{g \in S} \mathrm{sgn}(g) A_{i,j,k}(g) \right) N_{i,j,k} \\ &= \frac{1}{2^n} \sum_{i,j,k} A^{\pm}_{i,j,k}(S)\, N_{i,j,k}. \end{aligned} \tag{8.20}$$

The $A^{\pm}_{i,j,k}(S)$ are the coefficients of the *complete signed quantum weight enumerators* of the stabiliser code S. Recall that for a classical code $C \subset \mathbb{F}_d^n$, the *complete weight enumerator* is the degree-n polynomial in d variables given by

$$\sum_{c \in C} x_0^{\mathrm{wt}_0(c)} \dots x_{d-1}^{\mathrm{wt}_{d-1}(c)} =: \sum_{i_1,\dots,i_{d-1}} A_{i_1,\dots,i_{d-1}}(C)\, x_0^{n-(i_1+\dots+i_{d-1})} x_1^{i_1} \dots x_{d-1}^{i_{d-1}},$$

where $\mathrm{wt}_i(c)$ gives the number of times $i \in \mathbb{F}_d$ appears in c [143]. The analogy should be clear. *Unsigned* weight enumerators for quantum codes have been studied since the early days of quantum coding theory [144, Ch. 13]. Much less seems to be known about their signed counterparts, with Refs. [145, 146] being the only related references we are aware of. There it is shown that, as their classical analogues, signed quantum weight enumerators are NP-hard to compute.

Finally, we want to return to the cases $|\psi\rangle = |H\rangle$ and $|\psi\rangle = |T\rangle$ and discuss the invariant subspaces $V^{H,T} := V^{G_{H,T}}$ for these states. Let us rotate the Pauli basis such that the first basis vector corresponds to the Bloch representation of $|H\rangle$ and $|T\rangle$, respectively:

$$E_1^H := \frac{1}{\sqrt{2}}(X+Y), \qquad E_1^T := \frac{1}{\sqrt{3}}(X+Y+Z), \tag{8.21}$$

$$E_2^H := \frac{1}{\sqrt{2}}(X-Y), \qquad E_2^T := \frac{1}{\sqrt{6}}(X-2Y+Z) \tag{8.22}$$

$$E_3^H := Z, \qquad E_3^T := \frac{1}{\sqrt{2}}(X-Z). \tag{8.23}$$

Note that this choice of basis is such that the orthogonal decompositions of state space $H_2 = \langle \mathbb{1} \rangle \oplus \langle E_1^H \rangle \oplus \langle E_2^H \rangle \oplus \langle E_3^H \rangle = \langle \mathbb{1} \rangle \oplus \langle E_1^T \rangle \oplus \langle E_2^T, E_3^T \rangle$ correspond to (real) irreps of the respective Clifford stabilisers $(\mathrm{Cl}_1)_{H,T}$, as can be seen from the matrix representation of the generators in the rotated basis:

$$SX \simeq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \qquad SH \simeq \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -1 & \sqrt{3} \\ 0 & 0 & -\sqrt{3} & -1 \end{pmatrix}. \tag{8.24}$$

In general, a basis for the trivial representation of $(\mathrm{Cl}_1)_{H,T}^{\otimes n}$ in the n-qubit state space H_{2^n} is given by $\mathcal{B}^{H,T} := \{\mathbb{1}, E_1^{H,T}\}^{\otimes n}$. To construct a basis for the full invariant subspace, we have to symmetrise $\mathcal{B}^{H,T}$ resulting in $\{N_{i,0,0}^{H,T} =: N_i^{H,T} \mid i = 0, \ldots, n\}$. Here, $N_{i,j,k}^{H,T}$ is the occupation number basis associated to the rotated basis $\{\mathbb{1}, E_1^{H,T}, E_2^{H,T}, E_3^{H,T}\}$ and is constructed analogously to before.

In general, the components of stabiliser states in the rotated bases can be written in terms of weight enumerators by computing the induced basis transformations on $\mathrm{Sym}(H_D)$ from $N_{i,j,k}$ to $N_{i,j,k}^{H,T}$. However, we are only interested in the projection onto $j = k = 0$ which simplifies this computation. First, let us rewrite the n-qubit Pauli operators in the H-basis. Note that every operator with non-vanishing Z-weight is already in the orthocomplement of V^H.

$$\begin{aligned} X^{\otimes i} \otimes Y^{\otimes j} &= \left(\frac{1}{\sqrt{2}}\right)^{i+j} \left(E_1^H + E_2^H\right)^{\otimes i} \otimes \left(E_1^H - E_2^H\right)^{\otimes j} \\ &= \left(\frac{1}{\sqrt{2}}\right)^{i+j} \left(E_1^H\right)^{\otimes (i+j)} + \text{orth. terms} \end{aligned} \tag{8.25}$$

Here, we left out possible identity factors and all orthogonal terms on the RHS, i. e. those containing E_2^H. This result implies that we can write the projection of a stabiliser state s as

$$\Pi_H(s) = \frac{1}{2^n} \sum_{i=0}^{n} \left(\sum_{j=0}^{i} A_{i-j,j,0}^{\pm}(S) \right) \frac{N_i^H}{2^{i/2}} =: \frac{1}{2^n} \sum_{i=0}^{n} B_i^{\pm}(S) \frac{N_i^H}{2^{i/2}}. \tag{8.26}$$

We call the numbers $B_i^{\pm}(S)$ the *partial signed quantum weight enumerators* of S. The analysis works the same way for the T-projection:

$$\begin{aligned} X^{\otimes i} \otimes Y^{\otimes j} \otimes Z^{\otimes k} = &\left(\frac{E_1^T}{\sqrt{3}} + \frac{E_2^T}{\sqrt{6}} + \frac{E_3^T}{\sqrt{2}}\right)^{\otimes i} \otimes \left(\frac{E_1^T}{\sqrt{3}} - \sqrt{\frac{2}{3}} E_2^T\right)^{\otimes j} \otimes \\ &\otimes \left(\frac{E_1^T}{\sqrt{3}} + \frac{E_2^T}{\sqrt{6}} - \frac{E_3^T}{\sqrt{2}}\right)^{\otimes k} \\ = &\left(\frac{1}{\sqrt{3}}\right)^{i+j+k} \left(E_1^T\right)^{\otimes (i+j+k)} + \text{orth. terms} \end{aligned} \tag{8.27}$$

In this case, the T-projection of a stabiliser state s with stabiliser group S involves *total signed quantum weight enumerators* $C_i^{\pm}(S)$ as follows:

$$\Pi_T(s) = \frac{1}{2^n} \sum_{i=0}^{n} \left(\sum_{j=0}^{i} \sum_{k=0}^{i-j} A_{i-j-k,j,k}^{\pm}(S) \right) \frac{N_i^T}{3^{i/2}} =: \frac{1}{2^n} \sum_{i=0}^{n} C_i^{\pm}(S) \frac{N_i^T}{3^{i/2}}. \tag{8.28}$$

Note that all projections $\mathrm{Sym} \equiv \Pi_{S_n}$, Π_H and Π_T can be computed from the complete signed weight enumerators of the stabiliser codes which themselves are functions of the weight distributions. For numerical purposes, it is convenient to absorb all appearing factors in the bases such that the coefficients of stabiliser states are given by the integer weight enumerators.

Finally, we want to give expressions for the states $|H\rangle^{\otimes n}$ and $|T\rangle^{\otimes n}$ in the respective bases:

$$|H\rangle\langle H|^{\otimes n} = \frac{1}{2^n}\left(\mathbb{1} + E_1^H\right)^{\otimes n} = \frac{1}{2^n}\sum_{i=0}^{n}\binom{n}{i}N_i^H, \tag{8.29}$$

$$|T\rangle\langle T|^{\otimes n} = \frac{1}{2^n}\left(\mathbb{1} + E_1^T\right)^{\otimes n} = \frac{1}{2^n}\sum_{i=0}^{n}\binom{n}{i}N_i^T. \tag{8.30}$$

In general, we are not aware of any method which can predict whether the projection of a stabiliser state will be extremal within the projected polytope. However, the following lemma gives a necessary condition on the extremality of products $s \otimes s'$ of stabiliser states which will be useful later.

Lemma 8.1 (Projection of product states)**.** *The following is true for $\Pi = \mathrm{Sym}, \Pi_H, \Pi_T$: If the projection $\Pi(s)$ of an arbitrary stabiliser state s is non-extremal, so is $\Pi(s \otimes s')$ for any other stabiliser state s'.*

Proof. We prove the statement by showing it on the level of the complete signed weight enumerators $A^{\pm}_{i,j,k}$. This proves the claim directly for $\Pi = \mathrm{Sym}$ and the other cases follow since the partial and total signed weight enumerators are linear functions of the complete ones.

Note that the Pauli X, Y, Z weights are additive under tensor products, e. g. $\mathrm{wt}_X(g \otimes g') = \mathrm{wt}_X(g) + \mathrm{wt}_X(g')$. This implies that we can write the indicator function as $A_{i,j,k}(g \otimes g') = A_{i',j',k'}(g)A_{i-i',j-j',k-k'}(g')$ for i', j', k' being the weights of g. However, since $A_{i',j',k'}(g)$ is zero if i', j', k' are *not* the weights of g, we can instead sum over all possible decompositions on the right hand side. Hence, for any two stabiliser codes S, S' we get

$$\begin{aligned} A^{\pm}_{i,j,k}(S \times S') &= \sum_{g\in S, g'\in S'} \mathrm{sgn}(g \otimes g')A_{i,j,k}(g \otimes g') \\ &= \sum_{i'=0}^{i}\sum_{j'=0}^{j}\sum_{k'=0}^{k}\sum_{g\in S}\sum_{g'\in S'} \mathrm{sgn}(g)\,\mathrm{sgn}(g')A_{i',j',k'}(g)A_{i-i',j-j',k-k'}(g') \\ &= \sum_{i'=0}^{i}\sum_{j'=0}^{j}\sum_{k'=0}^{k} A^{\pm}_{i',j',k'}(S)A^{\pm}_{i-i',j-j',k-k'}(S'). \end{aligned} \tag{8.31}$$

Suppose S is the stabiliser of a state s and $\mathrm{Sym}(s)$ can be written as convex combination,

$$\mathrm{Sym}(s) = \sum_{l=1}^{M}\lambda_l\,\mathrm{Sym}(s_l) \quad \Leftrightarrow \quad A^{\pm}_{i,j,k}(S) = \sum_{l=1}^{M}\lambda_l A^{\pm}_{i,j,k}(S_l), \tag{8.32}$$

with stabiliser states s_l, stabilised by the groups S_l. Let s' be stabilised by S', then we find by Eq. (8.31),

$$A^{\pm}_{i,j,k}(S \times S') = \sum_{i',j',k'} \sum_{l=1}^{M} \lambda_l A^{\pm}_{i',j',k'}(S_l) A^{\pm}_{i-i',j-j',k-k'}(S') = \sum_{l=1}^{M} \lambda_l A^{\pm}_{i,j,k}(S_l \times S'), \tag{8.33}$$

and hence the projection of the product state $s \otimes s'$ is non-extremal. □

Note that Eq. (8.31) allows us to compute the projection of products $\Pi(s \otimes s')$ from $\Pi(s)$ and $\Pi(s')$ via the signed quantum weight enumerators using poly(n) operations. This is an important improvement over computing $\Pi(s)$ for a general (fully entangled) stabiliser state s which requires $O(2^n)$ operations.

8.3.4 Representatives of inequivalent stabiliser states

Computing the projected polytope involves the computation of the signed quantum weight enumerators for all stabiliser states. However, from the previous discussions we know that we can restrict the computations to the orbits stab$(n)/G_\rho$ with respect to the symmetry group G_ρ. In this section we will construct representatives for these orbits.

Our approach is based on a subset of the set of stabiliser states, the so-called *graph states* graph(n). For every simple, i. e. self-loop free, graph G of n vertices, there is a state vector $|G\rangle$ that is stabilised by operators of the form

$$K_j = X_j \prod_{k=1}^{n} Z_k^{\theta_{jk}}, \qquad (j = 1, \ldots, n), \tag{8.34}$$

where X_j, Z_j are the Pauli operators on the j-th qubit and θ is the adjacency matrix of the graph G. Graph states play a fundamental role in the studies of stabiliser states since Schlingemann [42] proved that every stabiliser state is equivalent to a graph state under the action of the local Clifford group $L\mathrm{Cl}_n = \mathrm{Cl}_1^{\otimes n}$:

$$\mathrm{stab}(n) = L\mathrm{Cl}_n \cdot \mathrm{graph}(n). \tag{8.35}$$

This result can be used to label every stabiliser state vector $|C, G\rangle$ by a local Clifford unitary $C \in L\mathrm{Cl}_n$ and a graph state $|G\rangle \in \mathrm{graph}(n)$ such that $|C, G\rangle = C\,|G\rangle$. However, $L\mathrm{Cl}_n$-equivalent graph states generate the same $L\mathrm{Cl}_n$-orbit and are equally well suited to represent a stabiliser state. Nest, Dehaene and De Moor [43] and Hein, Eisert and Briegel [45] discovered that that two graph states are $L\mathrm{Cl}_n$-equivalent if and only if the underlying graphs are related by a graph theoretic transformation called *local complementation* (LC). Thus, it is sufficient to consider graphs up to local complementation.

Furthermore, the symmetry group G_ρ induces additional equivalence relations on the graph state representation. Let us again begin the discussion with the case of a generic state with S_n-symmetry. This already allows us to restrict the representation to non-isomorphic graphs, i. e. graphs up to permutation of their vertices, since for any graph state $|G\rangle$ and a permuted version $|\pi G\rangle \equiv \pi\,|G\rangle$ the $L\mathrm{Cl}_n$-orbits are isomorphic: $\pi C\,|G\rangle = C_\pi\,|\pi G\rangle$ with the permuted local Clifford unitary $C_\pi = \pi C \pi^\dagger \in L\mathrm{Cl}_n$. Moreover, it is straightforward to show that the composition of graph isomorphism and local complementation is symmetric and thus a equivalence relation $\sim_{LC,S_n}$ on graphs whose

equivalence classes are isomorphic to $\text{graph}(n)/\sim_{L\text{Cl}_n,S_n}$. These equivalence classes have been studied in the context of graph codes and entanglement in graph states [47, 147] and were enumerated by Danielsen [148]. However, different local Clifford unitaries can still result in equivalent states. To see this, pick some symmetry $\pi \in \text{Aut}(G)$ of the graph, i. e. $\pi G = G$, then the actions of C and C_π yield isomorphic states. Hence, it is enough to act with $L\text{Cl}_n/\text{Aut}(G)$ on the graph state $|G\rangle$.

For the computation of the $L\text{Cl}_n$-orbits it is enough to consider $L\text{Cl}_n/\mathcal{P}_n$, since Pauli operators will only change the possible 2^n signs of the final generators which are better added by hand. It is well known that the quotient $\text{Cl}_n/\mathcal{P}_n$ is isomorphic to the binary symplectic group $\text{Sp}_{2n}(\mathbb{Z}_2)$ which is the foundation of the phase space formalism. We make use of this formalism to compute the $L\text{Cl}_n$-orbits of graph states G by evaluating the orbits of the local symplectic group $\text{Sp}_2(\mathbb{Z}_2)^{\times n}$ up to the stabiliser of G and $\text{Aut}(G)$.

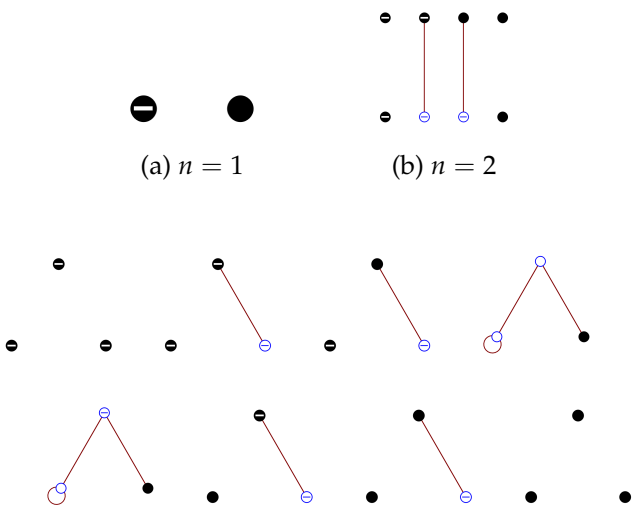
The additional symmetries in the case of the $|H\rangle$ and $|T\rangle$ state can be taken into account by restricting the allowed symplectic transformations using the symplectic maps $\hat{S}$ and $\hat{S}\hat{H}$ induced by the generators SX and SH, respectively. The corresponding cosets are given by the representatives $\text{Sp}_2(\mathbb{Z}_2)/\langle\hat{S}\rangle \simeq \{\mathbb{1}, \hat{H}, \hat{H}\hat{S}\}$ and $\text{Sp}_2(\mathbb{Z}_2)/\langle\hat{S}\hat{H}\rangle \simeq \{\mathbb{1}, \hat{S}\}$, respectively.

However, the described generation procedure will quickly become computationally expensive. Moreover, most of the projected stabiliser states are non-extremal points for the projected polytope and thus redundant. Unfortunately, there is no simple way of deciding whether a state will be extremal after projection or not. However, Lemma 8.1 states at least a criterion for product states which allows us to restrict to projecting only *fully entangled stabiliser states*. To this end, we only have to iterate over *connected* graph representatives with respect to $\sim_{LC,S_n}$ and compute the projections of product states directly from lower-dimensional vertices using the appropriate version of Eq. (8.31).

8.4 Computing the robustness of magic

Using the enumeration procedure of the last section, we generated the set of H- and T-projections of *fully entangled* stabiliser states $\overline{\text{stab}}_c^{H/T}(n) = \Pi_{H/T}(\text{stab}_c(n))$ and the set of projected product states from lower-dimensional vertices. In an additional step, we removed non-extremal points from the set of projected states, resulting in vertex sets $\mathcal{V}_n^{H/T}$ of the projected stabiliser polytopes for $n \leq 9$ and $n \leq 10$, respectively. As described in the last section, we are labelling the vertices by certain stabiliser representatives. To this end, we use a notation in terms of "decorated graph states" compatible with Refs. [42, 44]: A graph is decorated by symbols which indicate the action of local Clifford operations on the respective graph state. Nodes with signs indicate a sign change of the respective stabiliser generator, or alternatively, the action of Z on the respective qubit prior the any other gates. A hollow node in the graph denotes a Hadamard gate acting on the respective qubit and self-loops correspond to the action of phase gates (prior to possible Hadamard gates). Figure 8.6 shows the vertex sets $\mathcal{V}_n^H$ for $n = 1, 2, 3$. Since the dimension of the polytope is exactly n, it can be easily visualised for $n \leq 3$, see also Fig. 8.4 in Sec. 8.2.

The database of vertices and the program code can be found on the arXiv [33]. For a discussion of the algorithmic details see App. 8.D.



(a) $n = 1$ (b) $n = 2$

(c) $n = 3$

Figure 8.6: Vertices of the projected stabiliser polytope for the $|H\rangle$ symmetry group G_H. These states are represented as decorated graph states compatible with Refs. [42, 44], c.f. the description in the text. The convex hull of these vertices is shown in Fig. 8.4.

n	$\lvert\mathrm{stab}(n)\rvert$	$\lvert\overline{\mathrm{stab}}_c^H(n)\rvert$ + prod.	$\lvert\mathcal{V}_n^H\rvert$	$\lvert\overline{\mathrm{stab}}_c^T(n)\rvert$ + prod.	$\lvert\mathcal{V}_n^T\rvert$
1	6	3+0	2	2+0	2
2	60	5+3	4	4+3	4
3	1080	11+8	8	4+8	6
4	36720	48+18	13	18+14	12
5	2423520	252+38	32	61+26	22
6	315057600	1881+86	60	256+57	42
7	81284860800	20378+208	144	2151+116	66
8	41780418451200	331794+510	304	21475+226	131
9	42866709330931200	8410183+1270	804	329712+462	238
10	–	–	–	5964000+991	371

Table 8.1: Number of stabiliser states $|\mathrm{stab}(n)|$ in comparison with the number of projections of fully entangled stabiliser states $|\overline{\mathrm{stab}}_c(n)|$, projected product states and vertices $|\mathcal{V}_n|$ of the projected stabiliser polytope as a function of the number of qubits n.

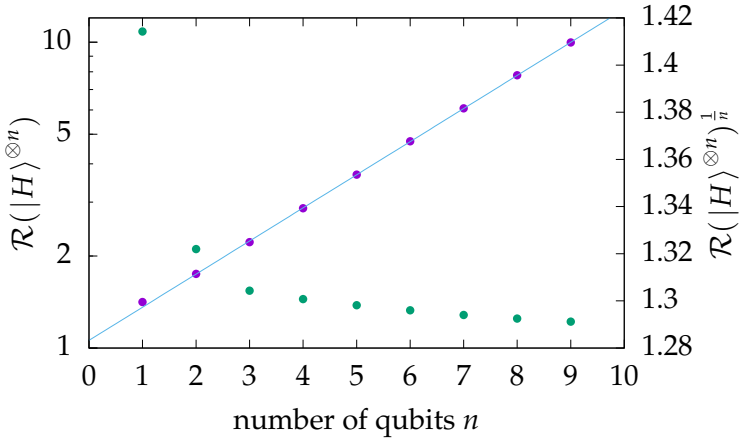
Table 8.1 shows the number of vertices of the projected polytopes in comparison with the original number of stabiliser states. We see that the number of states N that have to be used in the ℓ_1-minimisation is reduced drastically from $2^{O(n^2)}$ to a scaling which is approximately 2^n. Additionally, the dimension d of the ambient space is reduced exponentially from $4^n - 1$ to exactly n. As discussed in Sec. 8.3.2, the required ℓ_1-minimisation for RoM is computed via a linear program with $2N + d$ constraints and $2N$ variables and has a runtime that is linear in its size $(2N + d)(2N) = 4N^2 + 2Nd$. The runtime is thus reduced as

$$2^{O(n^2)} \longrightarrow 2^{O(n)}, \tag{8.36}$$

leading to a super-polynomial speed-up in the ℓ_1-minimisation. Although both time and space complexity of the ℓ_1-minimisation are exponential in n, it is in principle feasible for moderate n. Here, the limiting factor is the implementation of the oracle providing the projected states with runtime which is still super-exponential in n.

8.4.1 Robustness of the $|H\rangle^{\otimes n}$ and $|T\rangle^{\otimes n}$ states

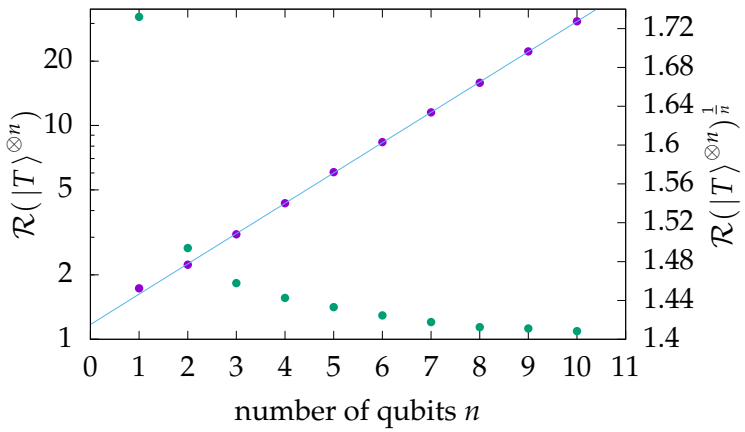
Figure 8.7 shows the Robustness of Magic of $|H\rangle^{\otimes n}$ for $n = 1, \ldots, 9$, computed from the vertices $\mathcal{V}_n^H$ of the projected stabiliser polytope. Note that the data for $n \leq 5$ is in perfect agreement with the so-far computed values in Ref. [32]. We are particularly interested in the submultiplicative behaviour of $\mathcal{R}$. Here, the new data for $n > 5$ turns out to be helpful: We can observe that the data points quickly approach an apparent exponential scaling with n. More precisely, submultiplicativity is clearly observable for $1 \leq n \leq 4$, but the scaling becomes effectively multiplicative for larger n. We quantified this using an exponential fit of the data range $3 \leq n \leq 9$ (shown in blue in Fig. 8.7) resulting in $(1.059 \pm 0.015) \times (1.283 \pm 0.002)^n$. From previous works it is known that the *regularised* robustness $\mathcal{R}_{\text{reg}}(|H\rangle)$ is bounded from below by 1.207. Our work, however, indicates that it converges from above to a constant which is given by the fit as (1.283 ± 0.002).



n	$\mathcal{R}(\lvert H\rangle^{\otimes n})$	$\mathcal{R}(\lvert H\rangle^{\otimes n})^{\frac{1}{n}}$
1	1.41422	1.41422
2	1.74754	1.32195
3	2.21896	1.30432
4	2.86274	1.30076
5	3.68705	1.29818
6	4.73894	1.29603
7	6.07646	1.29405
8	7.78935	1.29252
9	9.97501	1.29119

Figure 8.7: Robustness (blue) and regularised robustness (green) of the magic state $|H\rangle^{\otimes n}$ as a function of the number of qubits n. The blue line is the exponential fit $(1.059 \pm 0.015) \times (1.283 \pm 0.002)^n$ of the data.

The previously known time complexity for simulating a circuit with t T gates using the RoM algorithm is $O(2^{0.753t})$ [32]. Our findings improve this to $O(\mathcal{R}(|H\rangle^{\otimes 9})^{\frac{2t}{9}}) =$



n	$\mathcal{R}(\lvert T\rangle^{\otimes n})$	$\mathcal{R}(\lvert T\rangle^{\otimes n})^{\frac{1}{n}}$
1	1.73206	1.73206
2	2.23206	1.49401
3	3.09808	1.45780
4	4.33100	1.44260
5	6.04494	1.43311
6	8.35898	1.42460
7	11.5114	1.41772
8	15.8436	1.41248
9	22.1823	1.41110
10	30.7056	1.40839

Figure 8.8: Robustness (blue) and regularised robustness (green) of the magic state $|T\rangle^{\otimes n}$ as a function of the number of qubits n. The blue line is the exponential fit $(1.169 \pm 0.011) \times (1.386 \pm 0.0014)^n$ of the data.

$O(1.667^t) = O(2^{0.737t})$. Moreover, since we already explored an effectively multiplicative regime of the RoM, solving the problem for higher $n > 9$ will not much reduce the runtime. From our estimate for the asymptotic regularised robustness, we can estimate the best possible scaling to be $2^{0.719t}$.

Furthermore, we applied the same procedure to compute the robustness of the magic state $|T\rangle^{\otimes n}$. Since the T-symmetry group is larger than in the previous case, we were able to compute $\mathcal{R}(|T\rangle^{\otimes n})$ for up to 10 qubits, see Fig. 8.8. Qualitatively, the results agree very well with those of the last section. Quantitatively, the robustness of the T state is considerably higher than the one of the H state. Using again an exponential fit, we find the scaling $(1.169 \pm 0.011) \times (1.3865 \pm 0.0014)^n$ which predicts a regularised robustness of $(1.3865 \pm 0.0014)^n$. By the RoM construction, the 10-qubit solution gives rise to a simulation algorithm with runtime $O(1.984^m) = O(2^{0.988m})$ where m is the total number of $|T\rangle$ magic states used, or equivalently, the number of $\pi/12$ Z-rotation gates.

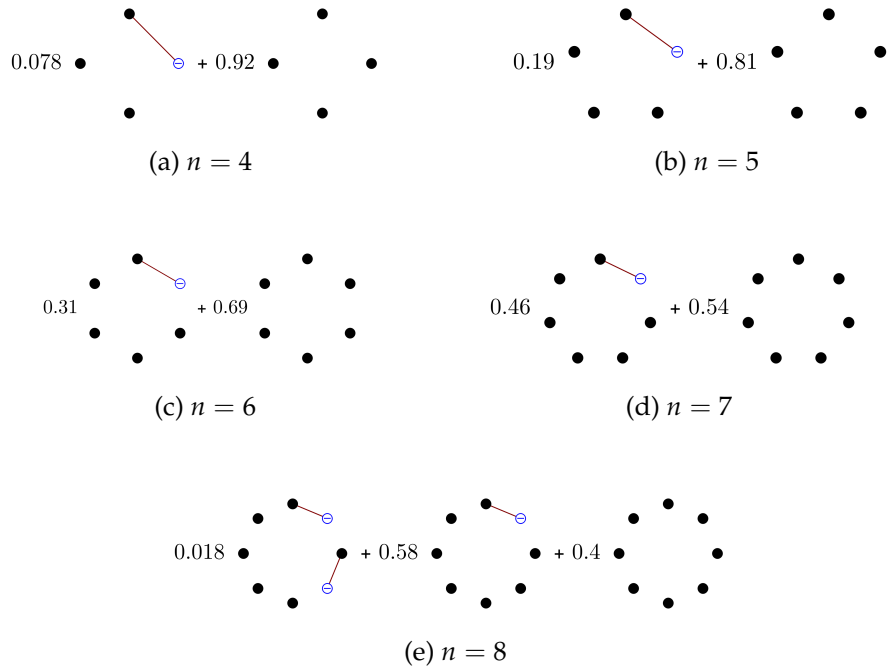
8.4.2 Analysis of the optimal solutions

Additionally, we studied the optimal solutions of the ℓ_1-minimisation for the previously discussed cases of $|H\rangle^{\otimes n}$ and $|T\rangle^{\otimes n}$. For this purpose, it is instructive to use the original formulation of the robustness of a state ρ in terms of an optimal affine combination of two (mixed) stabiliser states $\sigma^{\pm} \in \overline{\mathrm{SP}}_n^{H,T}$, cp. Eq. (8.5):

$$\rho = \frac{1}{2}\left[(\mathcal{R}(\rho)+1)\sigma^{+} - (\mathcal{R}(\rho)-1)\sigma^{-}\right]. \tag{8.37}$$

The states $\sigma^{\pm}$ can be obtained from the optimal solution of the ℓ_1-minimisation $\rho = \sum_i x_i^* v_i$ as follows:

$$\sigma^{+} = \frac{2}{\mathcal{R}(\rho)+1} \sum_{i:\, x_i^*>0} x_i^* v_i, \qquad \sigma^{-} = -\frac{2}{\mathcal{R}(\rho)-1} \sum_{i:\, x_i^*<0} x_i^* v_i. \tag{8.38}$$



(a) $n = 4$ (b) $n = 5$

(c) $n = 6$ (d) $n = 7$

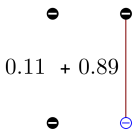
(e) $n = 8$

Figure 8.9: Positive contributions to the optimal affine combination for $|H\rangle^{\otimes n}$, written as convex combinations of stabiliser states. These states are represented as decorated graph states where hollow nodes indicate Hadamard action on the respective nodes and signs represent the respective sign of the stabiliser generator. Note that these states have only $\lfloor \log_2 n \rfloor$ contributions which themselves are products of $|+\rangle$ and Bell states.

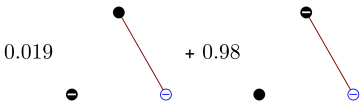
Recall from the discussion in Sec. 8.3.2 that replacing every vertex v_i in the optimal solution by a stabiliser representative in its preimage $\Pi_{H,T}^{-1}(v_i)$ yields an optimal solution for the original problem. Hence, we simply identify the vertices of the projected polytope by their stabiliser representatives constructed in Sec. 8.3.3. Surprisingly, these states seem to have a rather simple structure, especially the positive contributions σ^+. We will discuss the solutions in the following for the H and T case separately.

Optimal solutions for the $|H\rangle^{\otimes n}$ state The positive contributions σ^+ to the $|H\rangle^{\otimes n}$ state for $n = 1, 2, 3$ are simply given by the graph state $|+\rangle^{\otimes n}$. Figure 8.9 shows the remaining states for $n = 4, \ldots, 8$. Note that these states have to lie on a facet of the polytope to minimise the robustness. But instead of the generic n contributions, they can be written using only $\lfloor \log_2 n \rfloor$ terms. The vertices themselves are products of $|+\rangle$ and the Bell state $|\Psi^+\rangle$.

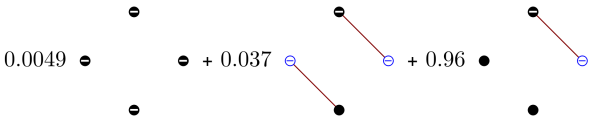
In contrast, the negative contributions σ^-, shown in Fig. 8.10, have less structure and seem to be partially irregular. Of course, σ^- has a non-unique convex combination and thus part of structure could be shadowed by the non-uniqueness. Nevertheless, since the dominant part of the contributions consists of products of $|\pm\rangle$ and the Bell states $|\Psi^\pm\rangle$, it is reasonable to assume that the σ^- can be approximated by Bell states. We suspect that this approximation is quite good, at least for a moderate number of qubits, due to the apparent suppression of vertices with more complex structure.



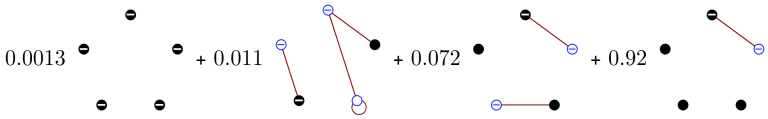
(a) $n = 2$



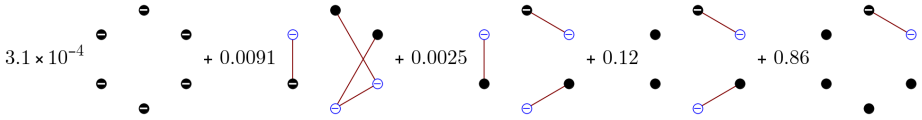
(b) $n = 3$



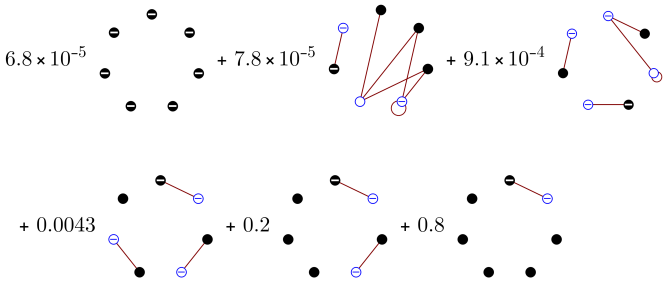
(c) $n = 4$



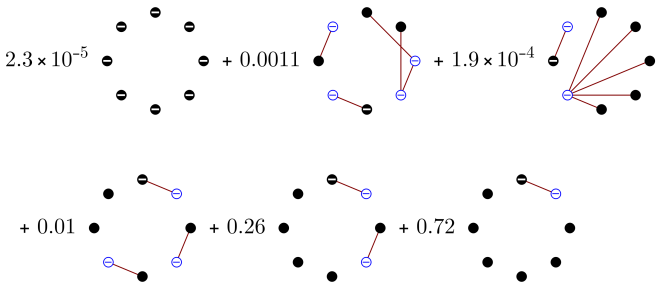
(d) $n = 5$



(e) $n = 6$



(f) $n = 7$



(g) $n = 8$

Figure 8.10: Negative contributions to the optimal affine combination for $|H\rangle^{\otimes n}$, written as convex combinations of stabiliser states. Note that these states have more contributions compared to the positive terms and seem partially irregular.

Motivated by these observations, we define the following polytope:

$$\mathrm{Q}_n^H = \operatorname{conv} \Pi_H \left(\{ \text{all } n \text{ qubits states that are products of } |\pm\rangle \text{ and } |\Psi^\pm\rangle \} \right). \tag{8.39}$$

By Eq. (8.31), we can compute these states efficiently from the signed weight enumerators of $|\pm\rangle$ and $|\Psi^\pm\rangle$. Note that the projection of $|+\rangle \otimes |-\rangle$ is a convex combination of the projected Bell states and thus only states with "all plus" or "all minus" contributions are extremal in Q_n^H. Let $\mathcal{W}_n^H$ be the set of vertices of Q_n^H and $m = \lfloor n/2 \rfloor$. We can explicitly enumerate its elements by tuples $(i,j,k) \in \{0,\ldots,m\}^3$ such that $i+j+k = m$. Every such tuple corresponds to a product of i $|\Psi\rangle^+$, j $|\Psi\rangle^-$ and $(2k+n-2m)$ $|\pm\rangle$ states. Hence, the number of vertices is

$$K := |\mathcal{W}_n^H| = 2\sum_{i=0}^{m}(m+1-i) = (m+1)(m+2). \tag{8.40}$$

We define the approximate robustness of $|H\rangle^{\otimes n}$ as the robustness with respect to the polytope Q_n^H:

$$r_n^H := \min \left\{ \|x\|_1 \;\middle|\; x \in \mathbb{R}^K : \; \rho = \sum_{i=1}^{K} x_i w_i \text{ with } w_i \in \mathcal{W}_n^H \right\}. \tag{8.41}$$

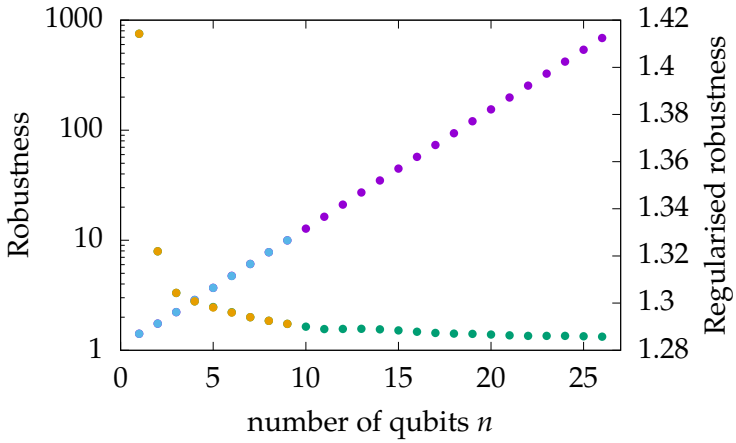
Since the optimisation is over a subset of all projected stabiliser states, r_n^H is an upper bound for $\mathcal{R}(|H\rangle^{\otimes n})$. Moreover, it can be efficiently evaluated since both the complexity of computing $\mathcal{W}_n^H$ and of the ℓ_1-minimisation is $O(n^4)$. Figure 8.11 shows a comparison of r_n^H with the exact robustness. From the previous analysis it is clear that the approximation is exact for $n \leq 4$. The deviation from the exact data for $4 < n \leq 9$ is at most 0.06% and thus negligible. However, we expect that the deviation becomes larger the higher n is, since it is likely that the importance of multipartite entangled contributions increases. Nevertheless, the approximation seems to be surprisingly good. The approximate data again follows an exponential increase with n, predicting an asymptotic regularised robustness of about (1.2829 ± 0.0017) which is compatible with the prediction (1.283 ± 0.002) from the exact data.

However, this approach is limited to $n \leq 26$. For larger n, the ℓ_1-minimisation lacks a feasible solution, which can only be the case if $|H\rangle^{\otimes n}$ is not in the affine span of the product states $\mathcal{W}_n^H$. This indicates that the dimension of the subpolytope Q_n^H becomes too small. A solution to these infeasibility problems will be discussed in Sec. 8.4.3.

Optimal solutions for the $|T\rangle^{\otimes n}$ state As in the previous case, the two connected vertices of the projected 2-qubit polytope constitute a dominant part in the optimal solutions. They are not projections of Bell states, so we will denote their representatives by $|\gamma^\pm\rangle$ and define them to be the states stabilised by $\{X_1Z_2, Z_1X_2\}$ and $\{-X_1Z_2, -Z_1Y_2\}$, respectively. The analysis of the optimal solutions shows that the σ^+ states are convex combinations of products of $|+\rangle$ and the maximally entangled state $|\gamma^+\rangle$. Moreover, they seem to be even more sparse than for the previous case, see Fig. 8.12. As in the case of $|H\rangle$, the σ^- state shows only partial structure, see Fig. 8.14 .

The similarities suggest that the robustness for $|T\rangle^{\otimes n}$ can be well approximated using a similar procedure as in the last section. To this end, we define the polytope

$$\mathrm{Q}_n^T = \operatorname{conv} \Pi_T \left(\{ \text{all } n \text{ qubits states that are products of } |\pm\rangle \text{ and } |\gamma^\pm\rangle \} \right). \tag{8.42}$$



n	$\mathcal{R}(\|H\rangle^{\otimes n})$	r_n^H
1	1.41422	1.41422
2	1.74754	1.74754
3	2.21896	2.21896
4	2.86274	2.86274
5	3.68705	3.68930
6	4.73894	4.74071
7	6.07646	6.07650
8	7.78935	7.78942
9	9.97501	9.97510

Figure 8.11: Exact (blue, orange) and approximate (purple, green) robustness and regularised robustness of the magic state $|H\rangle^{\otimes n}$ as a function of the number of qubits n.

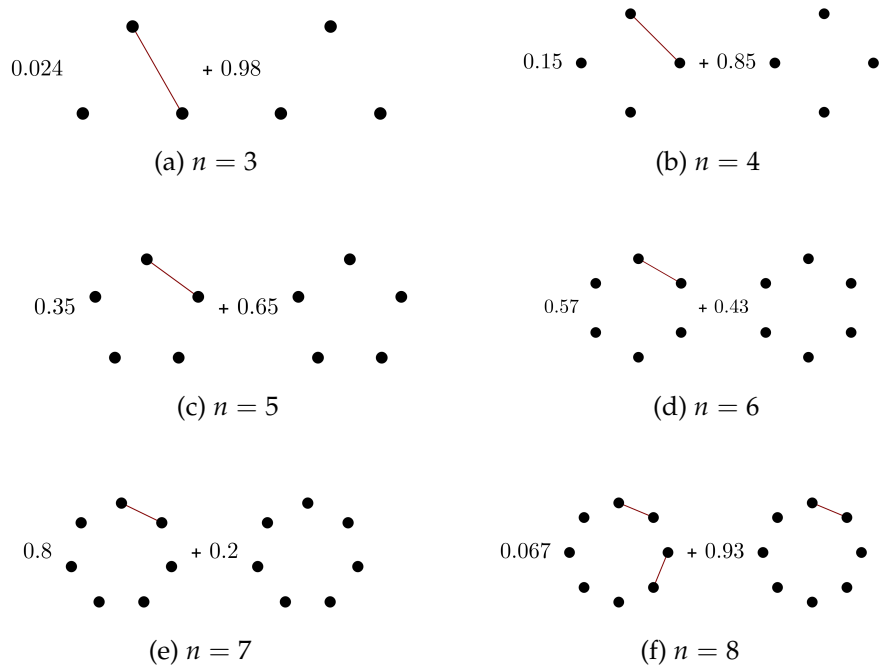
The approximate robustness r_n^T is again defined with respect to this polytope. The vertices $\mathcal{W}_n^T$ can be efficiently computed using the same procedure as in the $|H\rangle$ case and the approximation is exact for $n \leq 3$. Figure 8.13 shows the approximate robustness compared to the exact results. The approximation is again surprisingly good with a maximum deviation from the exact data of around 0.8%. Although this error is still small, it is an order of magnitude larger than for the $|H\rangle$ state. The approximation yields an asymptotic regularised robustness of (1.3916 ± 0.0014) which is slightly larger than the result from the exact data. Similar to the last section, the applicability of this approximation is limited to $n \leq 24$ due to the infeasibility of the optimisation problem for larger n. In the next section, we will show how to generalise this approximation to overcome the feasibility problems.

8.4.3 Finite hierarchy of RoM approximations

In general, the idea of restricting to at most k-partite entangled stabiliser states leads to a hierarchy of approximations with levels $1 \leq k \leq n$. Clearly, for $k = n$ the exact problem is recovered. The set of at most k-partite entangled n-qubit stabiliser states can be constructed by taking all possible tensor products of states in $\mathrm{stab}(i)$ for $1 \leq i \leq k$ which result in n-qubit states. However, without the presence of additional symmetries, this will still result in an exponentially large set since already the set of fully separable stabiliser states ($k = 1$) has size 6^n.

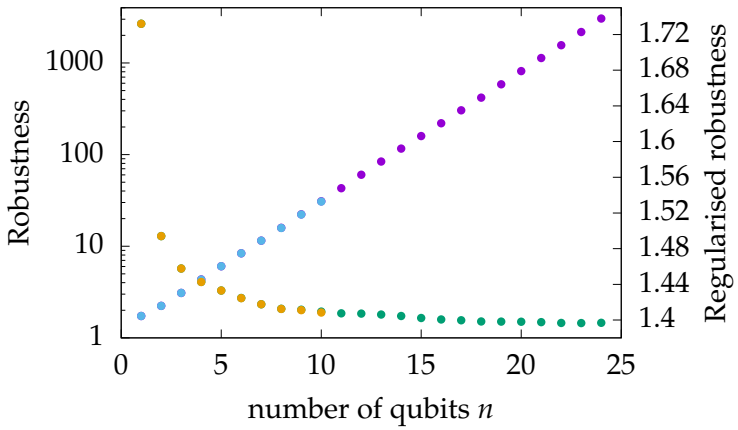
Hence, we assume that we want to compute approximations to $\mathcal{R}(\rho)$ where ρ is a symmetric n-qubit state (not necessarily pure) such that the stabiliser symmetry group contains at least the symmetric group S_n. In particular, this applies to the magic states $|H\rangle^{\otimes n}$ and $|T\rangle^{\otimes n}$. In this case, we are able to give $\mathrm{poly}(n)$ upper bounds on the runtime for every fixed level $k < n$.

Following Lemma 8.1 and Section 8.3.3, the set of S_n-projections of k-partite entangled n-qubit stabiliser states can be constructed from the vertices of the projected polytopes $\overline{\mathrm{SP}_i} = \mathrm{Sym}(\mathrm{SP}_i)$ for $1 \leq i \leq k$ which have *fully entangled* representatives. Let us denote the sets of representatives by $V_i \subset \mathrm{stab}(i)$. Since the order does not matter, the possible



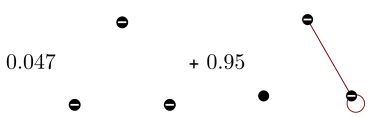
(a) $n = 3$ (b) $n = 4$ (c) $n = 5$ (d) $n = 6$ (e) $n = 7$ (f) $n = 8$

Figure 8.12: Positive contributions to the optimal affine combination for $|T\rangle^{\otimes n}$ and $3 \leq n \leq 8$, written as convex combinations of stabiliser states. These states are again represented as decorated graph states, see Sec. 8.4. Note that these states have less than $\lfloor \log_2 n \rfloor$ contributions which themselves are product states made from $|+\rangle$ and Bell states.

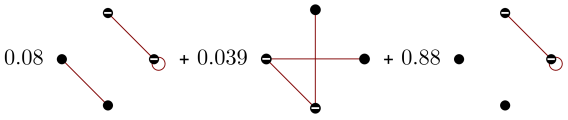


n	$\mathcal{R}(\|T\rangle^{\otimes n})$	r_n^T
1	1.73206	1.73206
2	2.23206	2.23206
3	3.09808	3.09808
4	4.33100	4.33316
5	6.04494	6.04494
6	8.35898	8.36006
7	11.5114	11.5117
8	15.8436	15.8492
9	22.1823	22.2499
10	30.7056	30.9411

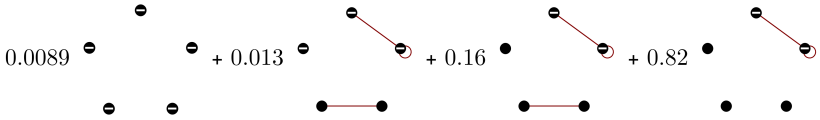
Figure 8.13: Exact (blue, orange) and approximate (purple, green) robustness and regularised robustness of the magic state $|T\rangle^{\otimes n}$ as a function of the number of qubits n.



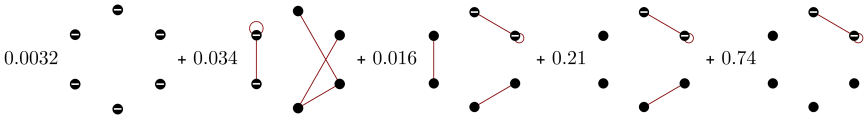
(a) $n = 3$



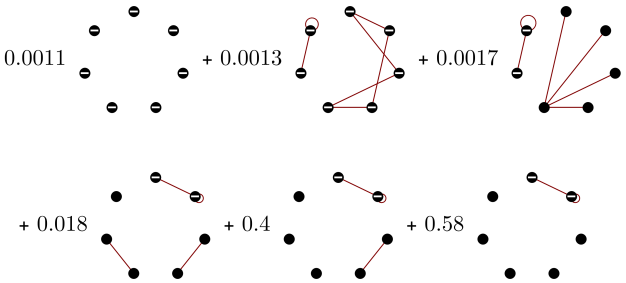
(b) $n = 4$



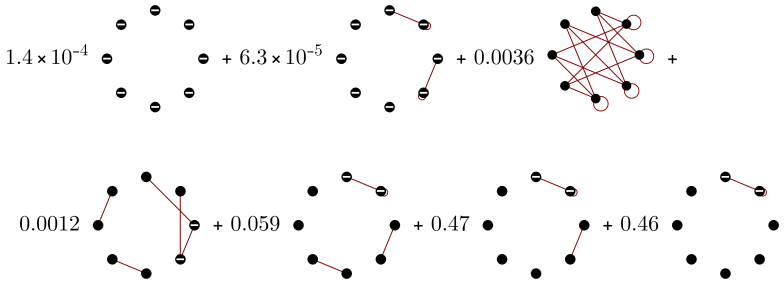
(c) $n = 5$



(d) $n = 6$



(e) $n = 7$



(f) $n = 8$

Figure 8.14: Negative contributions to the optimal affine combination for $|T\rangle^{\otimes n}$ and $3 \leq n \leq 8$, written as convex combinations of stabiliser states. These states are again represented as decorated graph states, see Sec. 8.4.

ways to take tensor products of these sets are exactly captured by (descending) partitions of n into parts with size at most k. We will denote such a partition by $\lambda \vdash_k n$. Then, we define the subpolytope of projected k-partite entangled states as

$$Q_{n,k} := \operatorname{conv} \operatorname{Sym} \left(\bigcup_{\lambda \vdash_k n} \bigotimes_{i \in \lambda} V_i \right), \tag{8.43}$$

and the *k-th level of the RoM hierarchy* by the relaxation of Prob. 8.1 to the subpolytope $Q_{n,k}$. Clearly, this defines an upper bound $r_{n,k}(\rho)$ to the exact RoM $\mathcal{R}(\rho)$.

To bound the runtime of the k-th level of the hierarchy, we have to count the vertices $\mathcal{W}_{n,k}$ of $Q_{n,k}$. An upper bound to this number is given by the number of tensor products appearing in Eq. (8.43) up to permutations. Thus, let λ be a (descending) partition of n into r parts, with no part larger than k:

$$n = \lambda_1 + \cdots + \lambda_r, \qquad k \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r > 0. \tag{8.44}$$

This can be rewritten as

$$n = \sum_{i=1}^{k} m_i \, i, \tag{8.45}$$

where $0 \leq m_i \leq n$ is the *multiplicity* of i in the partition λ. Since the permutations of the partition itself were already considered, the number of product states corresponding to the partition λ is given, up to permutations, by

$$\prod_{i=1}^{k} |V_i^{m_i} / S_{m_i}| = \prod_{i=1}^{k} \binom{m_i + L_i - 1}{L_i - 1}, \qquad L_i := |V_i|. \tag{8.46}$$

Using that the number of fully entangled vertices is increasing with i, we can bound this number by

$$\prod_{i=1}^{k} \binom{m_i + L_i - 1}{L_i - 1} \leq \prod_{i=1}^{k} m_i^{L_i} \leq n^{k L_k}. \tag{8.47}$$

Finally, the number of partitions of n with parts no greater than k coincides with the number of partitions of n into at most k parts and is denoted by $p_k(n)$. A standard result in number theory is that

$$p_k(n) = \frac{n^{k-1}}{k!(k-1)!} + O(n^{k-2}). \tag{8.48}$$

Thus, we can bound the number of vertices $\mathcal{W}_{n,k}$ to be

$$|\mathcal{W}_{n,k}| \leq p_k(n) \, n^{k L_k} = \frac{n^{k(L_k+1)-1}}{k!(k-1)!} + O(n^{k(L_k+1)-2}). \tag{8.49}$$

Since the dimension is $O(n^3)$, this implies that the runtime of the relaxation of Problem 8.1 is polynomial in n for a fixed k.

Finally, we remark that one has to know the vertex sets V_i up to k to run the k-th level of the hierarchy. Moreover, the bounds are very loose due to the fact we have not strictly bound the number of fully entangled vertices L_i which is beyond the scope of this paper. However, by using the actual numbers for L_i, one can obtain much better bounds on

$|\mathcal{W}_{n,k}|$ by evaluating the binomial coefficients. Let us illustrate this for the case of $|H\rangle^{\otimes n}$ and $k = 2, 3$: Using that $p_2(n) = \lfloor \frac{n}{2} \rfloor + 1$, $p_3(n) = \lfloor \frac{(n+3)^3}{12} + \frac{1}{2} \rfloor$ and $L_1 = L_2 = L_3 = 2$, we find

$$|\mathcal{W}_{n,2}| \leq \left(\left\lfloor \frac{n}{2} \right\rfloor + 1 \right) \binom{n+2-1}{2-1}^2 = O(n^3), \tag{8.50}$$

$$|\mathcal{W}_{n,3}| \leq \left\lfloor \frac{(n+3)^3}{12} + \frac{1}{2} \right\rfloor n^3 = O(n^6). \tag{8.51}$$

Note that we derived $|\mathcal{W}_{n,2}| = O(n^2)$ in the previous section using further information about the extremality of products.

8.5 Conclusion & Outlook

In this work, we have studied the symmetries of the n-qubit stabiliser polytope and showed how to use these to greatly reduce the combinatorical complexity of computing the robustness of single-qubit magic states and to gain insight into the structure of the problem.

We have determined the symmetry groups for the two types of single-qubit magic states and have constructed explicit stabiliser state representatives of the symmetry orbits. This has allowed us to evaluate the robustness of $|H\rangle^{\otimes n}$ for $n \leq 9$ and $|T\rangle^{\otimes n}$ for $n \leq 10$ qubits. Using the structure of the solutions, we have proposed an approximation based on at most bipartite entangled states which is efficient in n and gives an upper bound on the exact robustness. Furthermore, the agreement with the exact data for $n \leq 10$ qubits is excellent. Since the RoM becomes effectively multiplicative for larger n, we expect that the approximation is still very good in the regime $n > 10$. Moreover, by restricting to k-partite entangled stabiliser states, we obtained a finite hierarchy of approximations which recovers the exact RoM for $k = n$. We showed that a fixed level $k < n$ of the hierarchy can be computed in $\mathrm{poly}(n)$ time.

We feel that the most interesting task left open in this work is to explain why even two-body entangled states are sufficient to produce excellent bounds on the RoM. This may be insightful in a wider context. Indeed, sub-additivity of resource costs occurs in several areas of quantum information theory, most famously for the entanglement of formation [149]. The violations to additivity in [149] can be proven to exist for randomised constructions in high dimensions. This makes it hard to study the structure of the optimal solutions, or their behavior in a limit of many copies. The combinatorial nature of the stabiliser polytope, and the observation that only few-body entanglement is enough to find almost-optimal solutions, suggest that RoM may provide an instance where understanding submultiplicativity is feasible.

8.A Equivalence of the two robustness measures

The equivalence given in Eq. (8.6) is stated implicitly in [32]. Here, we give an explicit proof.

Vidal and Tarrach [139] defined the so-called *total robustness* which is given by

$$R(a) := \inf_{b \in S} R(a||b). \tag{8.52}$$

For S being a (compact) polytope, this can be rewritten as follows. Since S is compact, the minimum b^* is attained. Hence, $R(a) = R(a||b^*) =: s^*$ and

$$b^+ := \frac{1}{1+s^*}\left(b^* + s^* a\right) \in S. \tag{8.53}$$

Let $\{v_1, \ldots, v_N\}$ be the vertices of S and write $b^+, b^* \in S$ as convex combinations with coefficients λ_i and μ_i. It follows:

$$a = (1+s^*)b^+ - s^* b^* = \sum_{i=1}^{N} \underbrace{\left((1+s^*)\lambda_i - s^*\mu_i\right)}_{=:x(s^*)_i} v_i. \tag{8.54}$$

The last sum is an affine combination of the vertices since $\sum_i x(s^*)_i = 1$. In other words, $x(s^*)$ is a feasible solution for the following minimisation problem:

$$\mathcal{R}(a) := \min \left\{ \|x\|_1 \;\middle|\; x \in \mathbb{R}^N \,:\, a = \sum_{i=1}^{N} x_i v_i \text{ and } 1 = \sum_{i=1}^{N} x_i \right\}. \tag{8.55}$$

Moreover, the optimal value can be bounded as follows:

$$\mathcal{R}(a) \leq \sum_{i=1}^{N} |x(s^*)_i| \leq (1+s^*) \sum_{i=1}^{N} \lambda_i + s^* \sum_{i=1}^{N} \mu_i = 1 + 2s^* = 1 + 2R(a). \tag{8.56}$$

Assume x^* is the optimal solution for $\mathcal{R}(a)$. Then, we can rewrite $\mathcal{R}(a)$, using $\sum_i x_i = 1$, as follows:

$$\mathcal{R}(a) = \|x^*\|_1 = \sum_{i:\, x_i^* \geq 0} x_i^* - \sum_{i:\, x_i^* < 0} x_i^* = 1 + 2s(x^*), \quad \text{with } s(x^*) := -\sum_{i:\, x_i^* < 0} x_i^*. \tag{8.57}$$

Hence, the optimal affine combination for a becomes

$$a = \sum_{i:\, x_i^* \geq 0} x_i^* v_i - \sum_{i:\, x_i^* < 0} |x_i^*| v_i \tag{8.58}$$

$$= (1 + s(x^*)) \underbrace{\sum_{i:\, x_i^* \geq 0} \frac{x_i^*}{1+s(x^*)} v_i}_{=:\beta^+} - s(x^*) \underbrace{\sum_{i:\, x_i^* < 0} \frac{|x_i^*|}{s(x^*)} v_i}_{=:\beta^-}. \tag{8.59}$$

Here, the renormalised modulus of the affine coefficients form a convex combination and hence $\beta^\pm \in S$. Thus, we found a pseudo-mixture for a and the parameter $s(x^*)$ can not be smaller than the total robustness of a:

$$R(a) \leq s(x^*) \quad \Leftrightarrow \quad \mathcal{R}(a) \geq 1 + 2R(a). \tag{8.60}$$

Combined with Eq. (8.56), this shows that the two measures are equivalent:

$$\mathcal{R}(a) = 1 + 2R(a). \tag{8.61}$$

Finally, let us remark that β^- constructed from the optimal affine combination for a is such that

$$R(a) = R(a||\beta^-). \tag{8.62}$$

8.B On the dual RoM problem

At this point, any analytical insight could be helpful in simplifying the problem. A standard method is dualising the problem. Clearly, by Slater's condition, strong duality holds and thus the dual problem is an equivalent definition for the Robustness of Magic. The dual problem is straightforwardly obtained as follows:

Problem 8.2 (Dualised Robustness of Magic)**.** Let $\mathrm{stab}(n) = \{s_1, \ldots, s_N\}$ be the set of stabiliser states. Given a state ρ, solve the following problem:

$$\begin{aligned} \textbf{max} \quad & \mathrm{tr}(\rho Y) \quad \text{over } Y \in H_D, \\ \textbf{s.t.} \quad & |\,\mathrm{tr}(Y s_i)| \leq 1. \end{aligned}$$

This formulation of the RoM has a particularly nice form. Thus, it seems at first that the dual problem might be easier to solve. Indeed, one can guess the following feasible solution:

$$Y = \frac{1}{2^n} \sum_{i=1}^{4^n} \mathrm{sgn}\left(\mathrm{tr}(\rho w_i)\right) w_i. \tag{8.63}$$

Here, $\{w_1, \ldots, w_{4^n}\}$ denote the n-qubit Pauli operators which generate the n-qubit Pauli group $\mathcal{P}_n$. Feasibility follows from the following calculation for a stabiliser state s with stabiliser group $S < \mathcal{P}_n$:

$$\begin{aligned} |\,\mathrm{tr}(Y s)| &= \left| \frac{1}{2^n} \sum_{i=1}^{4^n} \mathrm{sgn}\left(\mathrm{tr}(\rho w_i)\right) \mathrm{tr}(w_i s) \right| \\ &\leq \frac{1}{4^n} \sum_{i=1}^{4^n} \left|\, \mathrm{sgn}\left(\mathrm{tr}(\rho w_i)\right) \right| \sum_{g \in S} \left|\, \mathrm{tr}(w_i g) \right| \\ &= \frac{1}{2^n} \sum_{i=1}^{4^n} (\delta(w_i \in S) + \delta(-w_i \in S)) \\ &\leq \frac{1}{2^n} |S| = 1. \end{aligned} \tag{8.64}$$

The corresponding objective value is

$$\mathrm{tr}(\rho Y) = \frac{1}{2^n} \sum_{i=1}^{4^n} \mathrm{sgn}\left(\mathrm{tr}(\rho w_i)\right) \mathrm{tr}(\rho w_i) = \sum_{i=1}^{4^n} \left| \frac{\mathrm{tr}(\rho w_i)}{2^n} \right| = \|p(\rho)\|_1, \tag{8.65}$$

where $p(\rho) \in \mathbb{R}^{D^2}$ is the coefficient vector of ρ in the Pauli basis, i.e. $p(\rho)_i = 2^{-n} \mathrm{tr}(\rho w_i)$. The objective value yields a lower bound to the RoM of ρ. Note that this bound, also called *st-norm* $\|\rho\|_{\mathrm{st}}$, was already found in [32] with different techniques and gives the following lower bound on the RoM of $|H\rangle^{\otimes n}$ and $|T\rangle^{\otimes n}$:

$$1.207^n \leq \mathcal{R}(|H\rangle^{\otimes n}), \qquad 1.366^n \leq \mathcal{R}(|T\rangle^{\otimes n}). \tag{8.66}$$

8.C Symmetries of 3-designs

In this section, we characterise the symmery group associated with the projectors of certain *t-designs*.

A *complex projective t-design* is a finite family $(\psi_i)_{i=1}^N$ of unit vectors in $\mathbb{C}^d$ such that

$$\frac{1}{N}\sum_{i=1}^{N} |\psi_i\rangle\langle\psi_i|^{\otimes t} = \frac{\mathrm{Sym}_{[t]}}{D_{[t]}}, \tag{8.67}$$

where

$$\mathrm{Sym}_{[t]} : (\mathbb{C}^d)^{\otimes t} \longrightarrow (\mathbb{C}^d)^{\otimes t}, \qquad \mathrm{Sym}_{[t]} := \frac{1}{t!}\sum_{\pi\in S_t} \pi \tag{8.68}$$

is the orthogonal projection onto the totally symmetric subspace $\mathrm{Sym}((\mathbb{C}^d)^{\otimes t})$. Furthermore, $D_{[t]} = \binom{d+t-1}{t}$ is its dimension and $\pi \in S_t$ acts by permuting the factors of the tensor product $(\mathbb{C}^d)^{\otimes t}$. Taking a partical trace of Eq. (8.67) shows that a t-design is also a $t-1$ design.

As in the main part of this paper, we denote by H_d the real vector space of Hermitian $d \times d$ matrices with the induced Hilbert-Schmidt inner product $(A, B) := \mathrm{tr}(AB)$. With respect to this inner product, we denote by $L^\dagger$ the adjoint of a linear map $L : H_d \to H_d$ and call L orthogonal if it preserves the inner product, or equivalently, if $L^\dagger = L^{-1}$.

Theorem 8.1. *Let $(\psi_i)_{i=1}^N \subset \mathbb{C}^d$ be a set of unit vectors. Let $L \in \mathrm{End}(H_d)$ be a linear map on Hermitian operators that permutes the projectors $(|\psi_i\rangle\langle\psi_i|)_{i=1}^N$.*

1. *If $(\psi_i)_{i=1}^N$ is a 1-design, then L is unital (i.e. $L(\mathbb{1}) = \mathbb{1}$).*

2. *If $(\psi_i)_{i=1}^N$ is a 2-design, then L is orthogonal and trace-preserving.*

3. *If $(\psi_i)_{i=1}^N$ is a 3-design, then L is of the form $L = U \cdot U^\dagger$, where U is either a unitary or an antiunitary operator on $\mathbb{C}^d$.*

Proof. Define $\rho_i := |\psi_i\rangle\langle\psi_i|$.

1.—Using $\mathrm{Sym}_{[1]} = \mathbb{1}$, we get

$$L(\mathbb{1}) = \frac{d}{N}\sum_{i=1}^{N} L(\rho_i) = \frac{d}{N}\sum_{i=1}^{N}\rho_i = \mathbb{1}, \tag{8.69}$$

hence L is unital.

2.—Let us define the traceless operators operators $f_i := \rho_i - \mathbb{1}/d$. Using the fact that $\{\psi_i\}_i$ forms a 2-design, Eq. (8.68), and the "swap trick"

$$\mathrm{tr}(AB) = \mathrm{tr}(A \otimes B\,\pi) \tag{8.70}$$

valid for the non-trivial element π of S_2, one verifies the following for any traceless Hermitian operator $A \in H_d^0$:

$$\begin{aligned}\frac{1}{N}\sum_{i=1}^{N}(f_i, A)^2 &= \frac{1}{N}\sum_{i=1}^{N}\left[\operatorname{tr}(\rho_i A) - \frac{1}{d}\operatorname{tr}(A)\right]^2 \\ &= \frac{1}{N}\sum_{i=1}^{N}\operatorname{tr}(\rho_i^{\otimes 2}A^{\otimes 2}) \\ &= \frac{1}{D_{[2]}}\operatorname{tr}(\operatorname{Sym}_{[2]} A^{\otimes 2}) \\ &= \frac{1}{2D_{[2]}}\left(\operatorname{tr}(A)^2 + \operatorname{tr}(A^2)\right) \\ &= \frac{\|A\|_2^2}{2D_{[2]}}.\end{aligned} \tag{8.71}$$

In other words, the operators (f_i) form a tight frame for the subspace $H_d^0 \subset H_d$ of traceless Hermitian matrices. Moreover, setting $f_0 = c\mathbb{1}$ with $c^2 = \frac{N(1-d)}{d^2+d^3}$, a similar calculation shows that the set $\{f_0, \ldots, f_N\}$ forms a tight frame for all of H_d.

By *1.*, L is unital and thus permutes the tight frame $\{f_0, \ldots, f_N\}$. However, any map permuting the elements of a tight frame is orthogonal. Finally, orthogonal and unital maps preserve the trace:

$$\operatorname{tr} L(A) = \operatorname{tr} \mathbb{1}L(A) = \operatorname{tr} L^\dagger(\mathbb{1})A = \operatorname{tr} L^{-1}(\mathbb{1})A = \operatorname{tr} \mathbb{1}A = \operatorname{tr} A. \tag{8.72}$$

3.—Consider the following trilinear function on H_d:

$$F(A, B, C) := \frac{1}{N}\sum_{i=1}^{N}\operatorname{tr}(A \otimes B \otimes C\, \rho_i^{\otimes 3}). \tag{8.73}$$

F is invariant under L since $L^\dagger = L^{-1}$ is also a symmetry of the projectors ρ_i:

$$\begin{aligned}F(L(A), L(B), L(C)) &= \frac{1}{N}\sum_{i=1}^{N}\operatorname{tr}\left(L(A) \otimes L(B) \otimes L(C)\, \rho_i^{\otimes 3}\right) \\ &= \frac{1}{N}\sum_{i=1}^{N}\operatorname{tr} A \otimes B \otimes C\, \left(L^\dagger(\rho_i)\right)^{\otimes 3} \\ &= \frac{1}{N}\sum_{i=1}^{N}\operatorname{tr} A \otimes B \otimes C\, \rho_i^{\otimes 3} \\ &= F(A, B, C).\end{aligned} \tag{8.74}$$

We can explicitely evaluate F by expanding $\operatorname{Sym}_{[3]}$ in terms of permutations and arguing

as in Eq. (8.70). This yields

$$\begin{aligned} F(A,B,C) &= \operatorname{tr}\left(A\otimes B\otimes C\,\frac{1}{N}\sum_{i=1}^{N}\rho_i^{\otimes 3}\right) \\ &= \frac{1}{D_{[3]}}\operatorname{tr}\left(A\otimes B\otimes C\,\operatorname{Sym}_{[3]}\right) \\ &= \frac{1}{6D_{[3]}}\Big(\operatorname{tr}(A)\operatorname{tr}(B)\operatorname{tr}(C)+\operatorname{tr}(A)\operatorname{tr}(BC)+ \\ &\qquad +\operatorname{tr}(AB)\operatorname{tr}(C)+\operatorname{tr}(AC)\operatorname{tr}(B)+\operatorname{tr}(ABC)+\operatorname{tr}(BAC)\Big). \end{aligned} \tag{8.75}$$

The first four terms are individually L-invariant since L preserves the trace and is orthogonal. Hence, the L-invariance of F implies

$$\begin{aligned} \operatorname{tr}(ABC)+\operatorname{tr}(BAC) &= \operatorname{tr} L(A)L(B)L(C)+\operatorname{tr} L(B)L(A)L(C) \\ &= \operatorname{tr} L^\dagger\big(L(A)L(B)\big)C+\operatorname{tr} L^\dagger\big(L(B)L(A)\big)C. \end{aligned} \tag{8.76}$$

Since this holds $\forall C\in H_d$, we get

$$\begin{aligned} AB+BA &= L^\dagger\big(L(A)L(B)\big)+L^\dagger\big(L(B)L(A)\big) \\ \Leftrightarrow L(AB+BA) &= L(A)L(B)+L(B)L(A) \\ \Leftrightarrow L(\{A,B\}) &= \{L(A),L(B)\}. \end{aligned} \tag{8.77}$$

A linear automorphism on a matrix algebra fulfilling (8.77) is called a *Jordan automorphism*. Our goal is to apply a known structure theorem that restricts that form of such maps [150]. For the theorem to be applicable, we have to extend L from a map on the real vector space of Hermitian matrices, to a map on the algebra $M_d(\mathbb{C})$ of all matrices. To this end, we use that every $A\in M_d(\mathbb{C})$ can be written uniquely as $A=A_1+iA_2$ where $A_{1,2}\in H_d$, and set

$$\hat{L}(A) := L(A_1)+iL(A_2)\in M_d(\mathbb{C}). \tag{8.78}$$

Clearly, this continuation yields a linear automorphism on $M_d(\mathbb{C})$. Morover, since the anticommutator $\{\cdot,\cdot\}$ is bilinear, we get $\forall A,B\in M_d(\mathbb{C})$:

$$\hat{L}(\{A,B\}) = \{\hat{L}(A),\hat{L}(B)\}, \tag{8.79}$$

i. e. the continuation $\hat{L}$ to $M_d(\mathbb{C})$ is a Jordan automorphism. It is also straightforward to check that orthogonality of L implies that $\hat{L}$ is unitary with respect to the trace inner product.

It is known that every Jordan automorphism is either an algebra automorphism or algebra anti-automorphism [150]. Since every algebra automorphism is inner and $\hat{L}$ is unitary, $\hat{L}$ (and thus also $L\equiv\hat{L}|_{H_d}$) can in the first case be written as $\hat{L}=U\cdot U^\dagger$ for some $U\in U(d)$. In the second case, we can write $\hat{L}$ as a composition $\hat{L}=\hat{L}'\circ T$, where $\hat{L}'=U\cdot U^\dagger$ is an algebra automorphism and T is the transposition map. For every Hermitian matrix, transposition coincides with complex conjugation as $A^T=(A^\dagger)^*=A^*$. Hence, we can write $L=U\mathcal{C}\cdot\mathcal{C}U^\dagger$, where $U\in U(d)$ and $\mathcal{C}$ is complex conjugation on $\mathbb{C}^d$. Hence, L is in this case given by conjugation with the anti-unitary operator $U\mathcal{C}$. □

Since the qubit stabiliser state vectors in Hilbert space form a complex projective 3-design [108, 113, 114], we get the following corollary:

Corollary 8.1. *The group of stabiliser symmetries* $\mathrm{Aut}(\mathrm{SP}_n)$ *is given by the adjoint representation of the extended Clifford group* $\mathrm{E}\mathcal{C}_n$.

Proof. Theorem 8.1 implies that every qubit stabiliser symmetry is given by conjugation with either an unitary or anti-unitary operator on the Hilbert space $\mathbb{C}^{2^n}$.

Theorem 2 in [76] implies that every unitary operator that preserves the set of stabiliser states is an element of the Clifford group, up to a global phase.

Furthermore, note that complex conjugation $\mathcal{C}$ preserves the set of stabiliser states. Thus, if A is an anti-unitary operator preserving this set, $\mathcal{C}A$ is a perserving unitary operator. Hence, up to a phase, $\mathcal{C}A$ is Clifford and thus A is anti-Clifford. Finally, this implies our claim that $\mathrm{Aut}(\mathrm{SP}_n) = \mathrm{Ad}(\mathrm{E}\mathcal{C}_n)$ □

We note that the result is in general wrong for stabiliser states on odd-dimensional qudits. This also means that the third conclusion of Thm. 8.1 is not in general true for 2-designs. Concretely, take $(\psi_i)_i$ to be the set of stabiliser state vectors for $\mathbb{C}^d$, with d a prime number larger than or equal to 5. Then $(\psi_i)_{i=1}^N$ is a 2-design, but the group of linear symmetries of $\{|\psi_i\rangle\langle\psi_i|\}_i$ contains maps that cannot be represented by a linear or anti-linear operator on $\mathbb{C}^d$.

Sketch of proof. We sketch the proof of this claim in the language of [75]. With each $a \in \mathbb{Z}_d^2$, one can associate a *phase space point operator* $A(a)$. The $\{A(a)\}_a$ form a basis for H_d. The finite general linear group $GL(\mathbb{Z}_d^2)$ acts on this basis by permuting the indices $g\,A(a) = A(g\,a)$. The expansion coefficients $W_\rho(a)$ of an operator ρ with respect to the phase space point basis are the *Wigner function* of the operator. The stabiliser state $\rho_i = |\psi_i\rangle\langle\psi_i|$ are exactly the set of Hermitian operators whose Wigner function is the indicator function of an affine line in $\mathbb{Z}_d^2$ [75]. Clearly, the $GL(\mathbb{Z}_d^2)$-action introduced above preserves the set of affine lines and thus permutes the ρ_i. As argued in the proof of Corollary 8.1, the group of (anti-)linear operators acting on the state vectors ψ_i is the extended Clifford group $\mathrm{E}\mathcal{C}_n$. To each U in $\mathrm{E}\mathcal{C}_n$, one can associate a $g \in \mathbb{Z}_d^2$ such that $UA(a)U^{-1} = A(g\,a)$. But g's that arise this way have determinant $\det g = 1 \mod d$ (if U is unitary) or $\det g = -1 \mod d$ (if U is anti-unitary) [66]. The claim follows, as for $d \geq 5$, there are elements $g \in \mathrm{GL}(\mathbb{Z}_d^2)$ with determinant different from ± 1. □

8.D Numerical implementation

Based on the discussion in Sec. 8.3.3, we can construct a generic algorithm for generating projected stabiliser states by calling various oracles. GRAPHREPRESENTATIVES(n) generates suitable representatives of graph states. Here, these are given by *connected* representatives of $\mathrm{graph}(n)/\sim_{LC,S_n}$ which were classified by Danielsen and Parker [147] up to 12 qubits and can by found in Ref. [148]. GENERATORMATRIX(G) computes the binary generator matrix of the graph state $|G\rangle$. Furthermore, LOCALSYMPLECTIC(n, G) returns the set of local symplectic matrices, ideally up to the considered symmetry group. For the discussed cases in Sec. 8.3.3, this is either the set of direct sums of $\{\mathbb{1}, \hat{H}, \hat{H}\hat{S}\}$ or $\{\mathbb{1}, \hat{S}\}$ up to the symmetry of the graph G. Finally, PROJECTSTATE(M', s) and PRODUCTSTATE$(v_1, \ldots, v_k)$ basically evaluate the weight enumerator formulas (8.18) and (8.31).

Algorithm 2 Algorithm for generating vertices of the projected stabiliser polytope

Require: Maximum number of qubits $n_{\max} \geq 1$, set of vertices $\mathcal{V}_n$
  for $n = 1, \ldots, n_{\max}$ **do**
    for $G \in$ GRAPHREPRESENTATIVES(n) **do**
      $M \leftarrow$ GENERATORMATRIX(G)
      for $S \in$ LOCALSYMPLECTIC(n, G) **do**
        $M' \leftarrow S \cdot M$
        for $s \in \{-1, 1\}^{\times n}$ **do**
          Add PROJECTSTATE(M', s) to $\mathcal{V}_n$
        end for
      end for
    end for
    for $(i_1, \ldots, i_k) \in$ PARTITIONS(n) **do**
      for $v_1 \in \mathcal{V}_{i_1}, \ldots, v_k \in \mathcal{V}_{i_k}$ **do**
        Add PRODUCTSTATE$(v_1, \ldots, v_k)$ to $\mathcal{V}_n$.
      end for
    end for
  end for

Furthermore, we use a output-sensitive algorithm by Dulá and Helgason [151] to compute the extremal points of the projected stabiliser polytope. This algorithm has time complexity $O(dNm)$ where d is the dimension, N the input size and m the output size, i. e. the number of extremal points. It performs way better than a naive approach since the input size $N = O(2^{n^2})$ is much larger than the number of extremal points $m = O(2^n)$.

8.E Symmetry reduction of convex optimisation problems

8.E.1 Group projections

The central tool for performing a symmetry reduction with respect to some (finite) group G is the so-called *G-projection*. Suppose g is represented by $\rho : G \to \mathrm{GL}(V)$ on a (real or complex) vector space V, we define a linear map $\Pi_G : V \to V$, the *G-projection*, by

$$\Pi_G := \frac{1}{|G|} \sum_{g \in G} \rho(g). \tag{8.80}$$

The G-projection is well known in the representation theory of finite groups. In the physics literature, it is often called a *twirl* or *twirling operation*. Thus, we will also sometimes refer to it as G-twirl. For reference, we state some elementary properties of these maps without proof.

Proposition 8.2 (Properties of G-projections)**.** *Let $\Pi_G : V \to V$ be a G-projection. Then the following holds:*

1. *Π_G is a projection operator. Its image is the subspace V^G of fixed points of G.*
2. *If V is an inner product space and ρ is an orthogonal/unitary representation, then the projection is orthogonal/unitary.*

3. *For all $x \in V$, it holds that*
$$\Pi_G(x) = \frac{1}{|G \cdot x|} \sum_{y \in G \cdot x} y. \tag{8.81}$$

4. *Π_G is constant on every orbit in V/G*

5. *If $G = N \rtimes H$, then $\Pi_G = \Pi_N \circ \Pi_H = \Pi_H \circ \Pi_N$.*

8.E.2 Symmetries in convex optimisation

A convex optimisation is the problem of minimising a convex function F over a convex set $\mathcal{X}$. It can always be rewritten in standard form as follows: Let $F : \mathbb{R}^N \to \mathbb{R}$ be a convex function and $C : \mathbb{R}^N \to \mathbb{R}^K$ be a (generalised) convex function with respect to the component-wise partial order $\preceq$ on $\mathbb{R}^K$, i. e. every component of C is convex. Furthermore, let $A : \mathbb{R}^N \to \mathbb{R}^M$ be an affine function. The problem is defined as [140]

$$\begin{aligned} &\textbf{Minimise} && F(x), \quad \text{for } x \in \mathbb{R}^N \\ &\textbf{subject to} && A(x) = 0, \\ & && C(x) \preceq 0. \end{aligned} \tag{8.82}$$

Here, the function F is called the *objective function* and the functions C and A are the (in-)equality *constraints*. Depending on the convex set that is modelled, one distinguishes between many subclasses such as linear, conic or semi-definite programming.

We call G a symmetry of the problem (8.82), if it acts on $\mathbb{R}^N$ such that the feasible set

$$\mathcal{X} = \{x \in \mathbb{R}^N \mid A(x) = 0,\ C(x) \preceq 0\}, \tag{8.83}$$

and the objective function F are left invariant. In particular, this will be the case if G acts linearly on all vector spaces such that the objective function is G-invariant and the constraints are G-equivariant, i. e. for all $x \in \mathbb{R}^N$ and $g \in G$ it holds

$$\begin{aligned} F(g \cdot x) &= F(x), \\ A(g \cdot x) &= g \cdot A(x), \\ C(g \cdot x) &= g \cdot C(x). \end{aligned} \tag{8.84}$$

Again, note that the G-action is different on the left and right hand side. Additionally, for G to be a proper symmetry, we require that its representation on $\mathbb{R}^K$ is given by *order automorphisms*, i. e.

$$p \preceq q \quad \Longleftrightarrow \quad g \cdot p \preceq g \cdot q \quad \forall p, q \in \mathbb{R}^K,\ g \in G \tag{8.85}$$

Consequently, both the inequality $C(g \cdot x) \preceq 0$ and the equality constraint $A(g \cdot x) = 0$ are fulfilled if and only if they hold for x. Hence, $x \in \mathbb{R}^N$ is a feasible solution of Eq. (8.82) iff its orbit is feasible. Moreover, the objective function is constant on every orbit and thus any optimal solution x^* will have an orbit of optimal solutions.

The key point for the simplification of the problem is that all functions are *convex* (A is even affine). Let us again slightly abuse notation and denote with

$$\Pi_G = \frac{1}{|G|} \sum_{g \in G} g, \tag{8.86}$$

all G-projections on the respective spaces. Using this, we will derive two important consequences of G-equivariance of A and C. First, we evaluate the affine function A:

$$A \circ \Pi_G(x) = \frac{1}{|G|} \sum_{g \in G} A \circ g(x) = \frac{1}{|G|} \sum_{g \in G} g \circ A(x) = \Pi_G \circ A(x). \tag{8.87}$$

Recall that C is convex w.r.t. to the component-wise order $\preceq$ and that every $g \in G$ preserves this order. Thus, Π_G preserves order, too, and it follows:

$$C \circ \Pi_G(x) \preceq \frac{1}{|G|} \sum_{g \in G} C \circ g(x) = \frac{1}{|G|} \sum_{g \in G} g \circ C(x) \preceq \Pi_G \circ C(x). \tag{8.88}$$

Suppose x is a feasible solution, then by these relations, its G-projection $x^G = \Pi_G(x)$ is feasible, too. Following the same argument as above, we get $F(x^G) \leq F(x)$. Finally, we find the following results:

Lemma 8.2. *Every G-symmetric convex optimisation problem has a G-invariant optimal solution.*

Proof. Be x^* a optimal solution, then $\Pi_G(x^*)$ is G-invariant, feasible and $F(\Pi_G(x^*)) \leq F(x^*)$. Hence, $\Pi_G(x^*)$ is optimal, too. □

Theorem 8.2 (Symmetry reduction of convex optimisation problems)**.** *The convex optimisation problem* (8.82) *with symmetry group G is equivalent to the following,* symmetry-reduced *convex optimisation problem:*

$$\begin{aligned} &\textbf{\textit{Minimise}} && F^G(x), \quad \textit{for } x \in X^G \\ &\textbf{\textit{subject to}} && A^G(x) = 0, \\ & && C^G(x) \preceq 0. \end{aligned} \tag{8.89}$$

With $F^G : X^G \to \mathbb{R}$, $A^G : X^G \to Y^G$ and $C^G : X^G \to Z^G$ being functions such that

$$F^G \circ \Pi_G = F, \qquad A^G \circ \Pi_G = \Pi_G \circ A, \qquad C^G \circ \Pi_G = \Pi_G \circ C, \tag{8.90}$$

and X^G, Y^G, Z^G being the G-invariant subspace of $X = \mathbb{R}^N$, $Y = \mathbb{R}^M$ and $Z = \mathbb{R}^K$.

Proof. First, it should be clear that the functions F^G, A^G and C^G exist and are well-defined by Eq. (8.90). Moreover, we compute for $x, y \in X^G$ and $t \in [0,1], s \in \mathbb{R}$:

$$\begin{aligned} F^G(tx + (1-t)y) &= F(tx + (1-t)y) \\ &\leq tF(x) + (1-t)F(y) \\ &= tF^G(x) + (1-t)F^G(y), \\ A^G(sx + (1-s)y) &= \Pi_G \circ A(sx + (1-s)y) \\ &= s\Pi_G \circ A(x) + (1-s)\Pi_G \circ A(y) \\ &= sA^G(x) + (1-s)A^G(y), \\ C^G(tx + (1-t)y) &= \Pi_G \circ C(tx + (1-t)y) \\ &\preceq t\Pi_G \circ C(x) + (1-t)\Pi_G \circ C(y) \\ &= tC^G(x) + (1-t)C^G(y). \end{aligned} \tag{8.91}$$

Hence, F^G and C^G are convex and A^G as an affine function.

Suppose $x \in \mathbb{R}^N$ is a feasible solution of the original problem (8.82) which can be assumed to be G-invariant, i. e. $x \in X^G$. It will be feasible for the reduced problem since

$$\begin{aligned} A^G(x) &= A^G \circ \Pi_G(x) = \Pi_G \circ A(x) = 0, \\ C^G(x) &= C^G \circ \Pi_G(x) = \Pi_G \circ C(x) \preceq 0, \end{aligned} \tag{8.92}$$

and $F^G(x) = F(x)$.

Next, suppose x^G is feasible for the reduced problem. By the same line of argumentation we get due to Eq. (8.87):

$$0 = A^G(x^G) = A^G \circ \Pi_G(x) = \Pi_G \circ A(x) = A \circ \Pi_G(x) = A(x). \tag{8.93}$$

In the same fashion, we compute using Eq. (8.88):

$$0 \succeq C^G(x^G) = C^G \circ \Pi_G(x) = \Pi_G \circ C(x) \succeq C \circ \Pi_G(x) = C(x). \tag{8.94}$$

Hence, x^G is feasible for the original problem and $F^G(x^G) = F^G \circ \Pi_G(x^G) = F(x^G)$.

Finally, this implies that the optimal objective values have to agree: Suppose x^* and x_*^G are (G-invariant) optimal solutions for the original and the reduced problem, respectively. Then, $F^G(x^*) = F(x^*)$ and $F(x_*^G) = F^G(x_*^G)$. But since both x^* and x_*^G are feasible for both problems, $F(x_*^G) \neq F(x^*)$ would be a contradiction to the optimality of the solutions.

□

8.E.3 Affine constraints and symmetries

In the remainder of this work, both A and C will be affine maps and originate from a set of points $\mathcal{V}$ that span a polytope $\mathcal{P}$. The symmetry group G leaves $\mathcal{P}$ invariant and hence introduces permutations on $\mathcal{V}$. This will lead naturally lead to G-equivariance of these functions, as we will see in the following.

To simplify the discussion, we will focus on the function A. We can write the affine function A as

$$A(x) = \sum_{i=1}^{N} x_i v_i + v_0 \tag{8.95}$$

Here, $\mathcal{V} := \{v_1, \ldots, v_N\} \subset Y$ are the column vectors of the matrix representing the linear part of A and v_0 is its affine part. Suppose G is represented on Y such that it leaves the set $\mathcal{V}$ invariant and fixes v_0[2]. Hence, it can by identified with the left action of some subgroup of the symmetric group S_N on the index set $[N] = \{1, \ldots, N\}$ via $g \cdot y_i =: y_{\pi_g(i)}$ for some $\pi_g \in S_N$. We can associate a right action on X with this left action by $(x \cdot g)_i := x_{\pi_g^{-1}(i)}$. This action is clearly linear and such that for all $g \in G$:

$$\sum_{i=1}^{N} x_i \, (g \cdot v_i) = \sum_{i=1}^{N} x_i \, v_{\pi_g(i)} = \sum_{i=1}^{N} x_{\pi_g^{-1}(i)} \, v_i = \sum_{i=1}^{N} (x \cdot g)_i \, v_i. \tag{8.96}$$

[2]In general, G-equivariance requires that the action preserves the range of A which is a weaker condition.

In particular, the function A is G-equivariant:

$$g \cdot A(x) = \sum_{i=1}^{N} x_i \, (g \cdot v_i) + g \cdot v_0 = \sum_{i=1}^{N} (x \cdot g)_i \, v_i + v_0 = A(x \cdot g). \tag{8.97}$$

To make use of Thm. 8.2, we have to compute the function A^G. Note that Π_G is constant on the every orbit $O \in [N]/G$ and hence $\Pi_G(v_j) =: w_O$ for all $j \in O$:

$$\begin{aligned} \Pi_G \circ A(x) &= \sum_{i=1}^{N} x_i \, \Pi_G(v_i) + v_0 \\ &= \sum_{O \in [N]/G} \sum_{j \in O} x_j \, \Pi_G(v_j) + v_0 \\ &= \sum_{O \in [N]/G} \left(\sum_{j \in O} x_j \right) w_O + v_0 \\ &= \sum_{O \in [N]/G} y_O \, w_O + v_0, \end{aligned} \tag{8.98}$$

where in the last step we set $y_O = \sum_{j \in O} x_j$. Finally, we have to turn this into a map on X^G. Note that the right permutation action of G on $X = \mathbb{R}^N$ partitions the standard basis $\{e_1, \ldots, e_N\}$ into L orbits $O_1, \ldots, O_L$ corresponding to $[N]/G$. Next, the linear spans $X_j = \langle O_j \rangle$ of these orbits provide a decomposition of $X = \bigoplus_j X_j$ and G acts transitively on every orbit. Hence, $\Pi_G(X_j)$ is one-dimensional and $\Pi_G(X) = \bigoplus_j \Pi_G(X_j)$ due to linearity. This implies that $\dim X^G = L = |[N]/G|$. Hence, the y_O are the components of a vector $y \in X^G$ w.r.t. the basis $\tilde{e}_O = \sum_{j \in O} e_j$. Note that if we normalise that basis as $e_O = \frac{1}{|O|} \tilde{e}_O$, then the new components are $\bar{x}_O = \frac{1}{|O|} \, y_O$, which are exactly the components of $\Pi_G(x)$. Hence, the induced map on X^G is

$$A^G(x) = \sum_{j=1}^{L} x_j w_j + v_0. \tag{8.99}$$

As stated in the beginning of this subsection, the points $\mathcal{V}$ are the extremal points of a polytope $\mathcal{P}$ and G is as subgroup of the polytope symmetries $\mathrm{Aut}(\mathcal{P})$. We saw that the symmetry reduction corresponds to projecting the vertices of the polytope, and hence the polytope itself, onto the G-invariant subspace. This is equivalent to taking its intersection with this subspace as the following lemma states:

Lemma 8.3 (Projection with Polytope Symmetries)**.** *Be $G < \mathrm{Aut}(\mathcal{P})$ a subgroup. Then, the G-projection of $\mathcal{P}$ is contained in $\mathcal{P}$, $\Pi_G(\mathcal{P}) \subset \mathcal{P}$. More precisely, $\Pi_G(\mathcal{P}) = \mathcal{P} \cap X^G$.*

Proof. For all $x \in \mathcal{P}$, we have $G \cdot x \subset \mathcal{P}$ and $\Pi_G(x)$ is a convex combination of points in $\mathcal{P}$, hence in $\mathcal{P}$ itself. Moreover, it holds $\mathcal{P} \cap X^G = \Pi_G(\mathcal{P} \cap X^G) \subset \Pi_G(\mathcal{P})$. The converse direction follows since $\Pi_G(\mathcal{P}) \subset X^G$ and $\Pi_G(\mathcal{P}) \subset \mathcal{P}$, thus $\Pi_G(\mathcal{P}) \subset \mathcal{P} \cap X^G$, which shows $\Pi_G(\mathcal{P}) = \mathcal{P} \cap X^G$. □

Finally, we want to remark that for computing the projection of the vertices $\{v_1, \ldots, v_M\}$, it is sufficient to compute $\Pi_G(w_O)$ for some representatives w_O of the orbits $O \in \mathcal{V}/G$ since the projection only depends on the orbit.

CHAPTER 9

THE AXIOMATIC AND THE OPERATIONAL APPROACHES TO RESOURCE THEORIES OF MAGIC DO NOT COINCIDE

About this chapter

The following text has been previously published as a preprint:

> Arne Heimendahl*, Markus Heinrich* and David Gross. *The axiomatic and the operational approaches to resource theories of magic do not coincide*. 2020. arXiv: 2011.11651
>
> * Authors contributed equally

Deviations from the preprint version are limited to typesetting and notation. These changes were performed to match the rest of this dissertation. Note that this chapter has its own independent appendix.

Arne Heimendahl and Markus Heinrich are the main contributors to this paper and contributed equally. MH had the idea for the paper and derived the characterisation of CSP maps. MH wrote the main text as well as App. 9.A, 9.C, and 9.F. MH contributed significantly to the formulation of Thm. 9.3, the proof of which was worked out in equal parts by all authors (App. 9.B). MH helped finalising AH's proof of Thm. 9.4.

Abstract

Stabiliser operations occupy a prominent role in the theory of fault-tolerant quantum computing. They are defined *operationally*: by the use of Clifford gates, Pauli measurements and classical control. Within the stabiliser formalism, these operations can be efficiently simulated on a classical computer, a result which is known as the *Gottesman-Knill* theorem. However, an additional supply of *magic states* is enough to promote them to a universal, fault-tolerant model for quantum computing. To quantify the needed *resources* in terms of magic states, a *resource theory of magic* has been developed during the last years. Stabiliser operations (SO) are considered free within this theory, however they are not the most general class of free operations. From an axiomatic point of view, these are the *completely stabiliser-preserving* (CSP) channels, defined as those that preserve the convex hull of stabiliser states. It has been an open problem to decide whether these two definitions lead to the same class of operations. In this work, we answer this question in the negative, by constructing an explicit counter-example. This indicates that recently proposed stabiliser-based simulation techniques of CSP maps are strictly more powerful than Gottesman-Knill-like methods. The result is analogous to a well-known fact in entanglement theory, namely that there is a gap between the class of local operations and classical communication (LOCC) and the class of separable channels. Along the way, we develop a number of auxiliary techniques which allow us to better characterise the set of CSP channels.

9.1 Introduction

Despite the advances in the development of quantum platforms, the precise quantum phenomena required for a quantum advantage over classical computers remain elusive. However, for the design of fault-tolerant quantum computers, it seems imperative to understand these necessary resources. Here, the *magic state model* of quantum computing offers a particularly fruitful perspective. In this model, all operations performed by the quantum computer are divided into two classes. The first class consists of the preparation of stabiliser states, the implementation of Cifford gates, and Pauli measurements. These *stabiliser operations* by themselves can be efficiently simulated classically by the Gottesman-Knill Theorem [51, 88]. Secondly, the quantum computer needs to be able to prepare *magic states*, defined as states that allow for the implementation of any quantum algorithm when acted on by stabiliser operations [55]. In this sense, the magic states provide the "non-classicality" required for a quantum advantage.

During recent years, there has been an increasing interest in developing a resource theory of quantum computing that allows for a precise quantification of *magic*. First resource theories were developed for the somewhat simpler case of odd-dimensional systems, based on a phase-space representation via Wigner functions. There, the total negativity in the Wigner function of a state is a *resource monotone* called *mana*, and non-zero mana is a necessary condition for a quantum speed-up [24–28, 122, 123]. In the more relevant case of qubits, this theory breaks down, which has led to a number of parallel developments [32, 33, 35–39, 152]. A common element is that the finite set of stabiliser states, or more generally their convex hull, is taken as the set of free states. Since stabiliser operations preserve this *stabiliser polytope*, they are considered free operations in this theory and any monotones should be non-increasing under those. A number of such *magic monotones* have been studied and their values linked to the runtime of classical simulation algorithms [29, 31, 34, 36]. In this sense, the degree of magic present in a quantum circuit does seem to correlate with the quantum advantages it confers – thus validating the premise of the approach.

The set of stabiliser operations (SO) are defined in terms of concrete actions ("prepare a stabiliser state, perform a Clifford unitary, make a measurement") and thus represent an *operational* approach to defining free transformations in a resource theory of magic. It is often fruitful to start from an *axiomatic* point of view, by defining the set of free transformations as those physical maps that preserve the set of free states. This approach has been introduced recently by Seddon and Campbell [35]. They suggest to refer to a linear map as *completely stabiliser-preserving* (CSP) if it preserves the stabiliser polytope, even when acting on parts of an entangled system. It has been shown that the magic monotones mentioned above are also non-increasing under CSP maps [36].

A natural and pressing question is therefore whether the two approaches coincide – i.e. whether SO = CSP, or whether there are CSP maps that cannot be realised as stabiliser operations [35].

To build an intuition for the question, consider the analogous problem in entanglement theory, where the free resources are the separable states. The axiomatically defined free transformations are the *separable maps* – completely positive maps that preserve the set of separable states. The operationally defined free transformations are those that can be realised by local operations and classical communication (LOCC). It is known that the set of separable maps is strictly larger than the set of LOCC [153, 154] – a fact that leads

e.g. to a notable gap in the success probability of quantum state discrimination [155, 156] and entanglement conversion [157] between the two classes.

In this work, we show that – also in resource theories of magic – the axiomatic and the operational approaches lead to different classes, this is SO $\neq$ CSP. The result builds on a characterisation of CSP maps in terms of their Choi states, which might be of independent interest.

Outline

In Section 9.2, we give an introduction to the relevant concepts used throughout the main part of this work. Afterwards, we present our results in Sec. 9.3, including examples and a high-level discussion. We conclude the main part by commenting on potential implications and future work in Sec. 9.4. Since the proofs turn out to be rather technical, we have moved them to the appendix. Further introduction to the necessary techniques can be found in App. 9.A and App. 9.C such that this work can be considered self-contained.

9.2 Preliminaries

9.2.1 Stabiliser formalism

Throughout this paper, we adapt the *phase space* or *symplectic formalism* for stabiliser quantum mechanics [65, 66, 72, 75, 85]. The basic notation is introduced here, with more details given in App. 9.A.

We define the n-qubit Pauli Z and X operator as usual by their action on the computational basis:

$$Z(z)\,|u\rangle := (-1)^{z\cdot u}\,|u\rangle\,, \quad X(x)\,|u\rangle := |u+x\rangle\,, \quad z,x,u \in \mathbb{F}_2^n. \tag{9.1}$$

Here, we label the computational basis by elements in the discrete vector space $\mathbb{F}_2^n$ and all operations take place in the finite field $\mathbb{F}_2$ (i.e. modulo 2), if not stated otherwise. We group the Z and X operators and their coordinates to define an arbitrary Pauli operator indexed by $a = (a_z, a_x) \in \mathbb{F}_2^{2n}$:

$$w(a) := i^{-\gamma(a)} Z(a_z) X(a_x), \qquad \gamma(a) := a_z \cdot a_x \mod 4. \tag{9.2}$$

One can easily verify that the multiplication of Pauli operators yields another Pauli operator up to a power of i:

$$w(a)w(b) = i^{\beta(a,b)} w(a+b), \qquad \beta(a,b) := \gamma(a+b) - \gamma(a) - \gamma(b) + 2(a_x \cdot b_z). \tag{9.3}$$

In other words, w defines a projective representation of the additive group of $\mathbb{F}_2^{2n}$. The commutation relations can be expressed using the standard *symplectic form* $[\cdot,\cdot]$ on $\mathbb{F}_2^{2n}$:

$$w(a)w(b) = (-1)^{[a,b]} w(b)w(a), \qquad [a,b] := a_z \cdot b_x + a_x \cdot b_z. \tag{9.4}$$

For this reason, the discrete symplectic vector space $\mathbb{F}_2^{2n}$ is called *phase space* in this context.

Finally, the *Pauli group* is the group generated by Pauli operators and can be written as:

$$\mathcal{P}_n := \langle \{ w(a) \mid a \in \mathbb{F}_2^{2n} \} \rangle = \{ i^k w(a) \mid k \in \mathbb{Z}_4, a \in \mathbb{F}_2^{2n} \}. \tag{9.5}$$

The *Clifford group* is defined as the group of unitary symmetries of the Pauli group:

$$\mathrm{Cl}_n := \left\{ U \in U(2^n) \mid U\mathcal{P}_n U^\dagger = \mathcal{P}_n \right\} / U(1). \tag{9.6}$$

Note that we take the quotient with respect to irrelevant global phases in order to render the Clifford group a finite group.

Let $S \subset \mathcal{P}_n$ be an Abelian subgroup of the n-qubit Pauli group that does not contain $-\mathrm{id}$. The subspace $C(S) \subset (\mathbb{C}^2)^{\otimes n}$ of common fixed points of S is called the *stabiliser code* associated with S. One verifies easily that te the orthogonal projection onto $C(S)$ is given by $P_S = |S|^{-1} \sum_{g \in S} g$. Taking traces, it follows that the dimension $\dim C(S)$ equals $2^n/|S| = 2^{n-k}$, where $k = \mathrm{rk}(S)$ is the rank of S. Hence, S defines a $[[n, n-k]]$ quantum code and we denote by $\mathrm{stab}_{n,k}$ the set of these stabiliser codes. Of particular interest is the case $k = n$, for which P_S is rank 1 and thus defines a pure quantum state, called *stabiliser state*. The set of pure stabiliser states $\mathrm{stab}_n \equiv \mathrm{stab}_{n,n}$ spans a convex polytope that is full-dimensional in state space, the *stabiliser polytope* $\mathrm{SP}_n := \mathrm{conv}\,\mathrm{stab}_n$. For a single qubit, this is the well-known octahedron spanned by the Pauli X, Y, Z eigenstates, see Fig. 9.1. Elements of SP_n will be referred to as *mixed stabiliser states*.

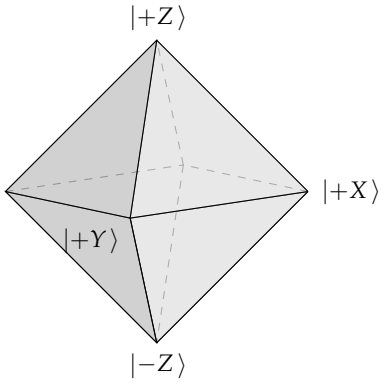


Figure 9.1: Bloch representation of the single-qubit *stabiliser polytope*, which is the octahedron spanned by the six ± 1 eigenstates of the Pauli X,Y, and Z operators. The simple geometry is not representative for the general situation in high dimensions.

9.2.2 Stabiliser operations and completely stabiliser-preserving maps

The Gottesman-Knill theorem states that *stabiliser operations* can be simulated in a time which is polynomial in the system size [51, 88]. These operations are defined as follows.

Definition 9.1 (Stabiliser operation)**.** A quantum channel taking n input qubits to m output qubits is a *stabiliser operation*, if it is composed of the following fundamental operations

- application of Clifford unitaries,
- preparation of (ancilla) qubits in stabiliser states,
- Pauli measurements, and
- tracing out of qubits.

We allow for an efficient classical algorithm to control which fundamental operation to apply based on previous measurement outcomes and independently distributed random bits. The set of all stabiliser operations is denoted by $\mathrm{SO}_{n,m}$, with $\mathrm{SO}_n := \mathrm{SO}_{n,n}$.

Due to the possibility to make use of randomness, the set of stabiliser operations $\mathrm{SO}_{n,m}$ is convex. Its extreme points will turn out to play an important role in our construction.

From a resource-theoretic perspective, all maps which preserve the set of free states should be considered as free operations. Following this idea, Seddon and Campbell [35] defined the so-called *completely stabiliser-preserving maps* as the free operations in a resource theory of magic state quantum computing. Originally, they defined these maps with the same input and output space which, however, can be generalised in a straightforward way.

Definition 9.2. A superoperator $\mathcal{E} : L((\mathbb{C}^2)^{\otimes n}) \to L((\mathbb{C}^2)^{\otimes m})$ is called *completely stabiliser-preserving* (CSP) if and only if $\mathcal{E} \otimes \mathrm{id}_k(\mathrm{SP}_{n+k}) \subset \mathrm{SP}_{m+k}$ for all $k \in \mathbb{N}$. The set of CSP maps is denoted by $\mathrm{CSP}_{n,m}$ and $\mathrm{CSP}_n := \mathrm{CSP}_{n,n}$.

As for completely positive maps, one can show that it is indeed enough to check the condition for $k = n$ [35, Lem. 4.1].

It will be helpful to characterise CSP maps via their *Choi-Jamiołkowski representation*. Recall that in this representation, a linear map $\mathcal{E} : L((\mathbb{C}^2)^{\otimes n}) \to L((\mathbb{C}^2)^{\otimes m})$ is associated with an operator

$$\mathcal{J}(\mathcal{E}) := \mathcal{E} \otimes \mathrm{id}_n(|\phi^+\rangle\langle\phi^+|) \in L((\mathbb{C}^2)^{\otimes m}) \otimes L((\mathbb{C}^2)^{\otimes n}), \tag{9.7}$$

where $|\phi^+\rangle = 2^{-n} \sum_{x \in \mathbb{F}_2^n} |xx\rangle$ is the standard maximally entangled state with respect to the computational basis. The *Choi-Jamiołkowski Theorem* states that $\mathcal{E}$ is completely positive if and only if its Choi representation lies in the positive semi-definite cone

$$\mathrm{PSD}_{n,m} \subset L((\mathbb{C}^2)^{\otimes m}) \otimes L((\mathbb{C}^2)^{\otimes n}). \tag{9.8}$$

What is more, the map $\mathcal{E}$ is trace-preserving if and only if its Choi representation lies in the affine space

$$\mathrm{TP}_{n,m} = \left\{\rho \in L((\mathbb{C}^2)^{\otimes m}) \otimes L((\mathbb{C}^2)^{\otimes n}) \mid \mathrm{tr}_1 \rho = \mathbb{1}/2^m\right\}. \tag{9.9}$$

In particular, for the set $\mathrm{CPTP}_{n,m}$ of completely positive and trace-preserving maps, we have the characterization

$$\mathcal{J}(\mathrm{CPTP}_{n,m}) = \mathrm{PSD}_{n,m} \cap \mathrm{TP}_{n,m}. \tag{9.10}$$

We now turn to the CSP version of this theory. It turns out that the CSP property has strong implications:

Lemma 9.1. *Any CSP map is completely positive and trace-preserving.*

Proof. The first claim follows from the Choi-Jamiołkowski Theorem, because $|\phi^+\rangle$ is a stabiliser state. As for the second claim: Because the set of stabiliser states (as projections) spans $L((\mathbb{C}^2)^{\otimes n})$, every Hermitian trace-one operator can be written as an affine combination of stabiliser states. By definition, any CSP map maps this to an affine combination of stabiliser states in the output space $L((\mathbb{C}^2)^{\otimes m})$. In particular, it is trace-preserving. □

The CSP-analogue of Eq. (9.10) was proven in Ref. [35].

Lemma 9.2 (Lem. 4.2 in [35]). *A linear map $\mathcal{E} : L((\mathbb{C}^2)^{\otimes n}) \to L((\mathbb{C}^2)^{\otimes m})$ is CSP if and only if its Choi representation lies in the intersection of the stabiliser polytope with the affine space* $\mathrm{TP}_{n,m}$*:*

$$\mathcal{J}(\mathrm{CSP}_{n,m}) = \mathrm{SP}_{n,m} \cap \mathrm{TP}_{n,m}. \tag{9.11}$$

Lemma 9.2 implies directly that $\mathrm{CSP}_{n,m}$ is a convex polytope.

CSP maps can be considered as the most general set of free operations in resource theories of magic state quantum computing. Most magic monotones, such as the *robustness of magic* and mixed-state extensions of the *stabiliser extent*, are non-increasing with respect to CSP maps [35, 36]. As these monotones are connected to various classical simulation schemes, CSP operations are also classically efficiently simulable [36]. While any stabiliser operation is certainly a CSP map, we will show in the next section that the converse is not true.

9.3 Results

9.3.1 A separating property for extremal stabiliser operations

In this section, we derive a property of *extremal* stabiliser operations. This result will play a key role in the proof that there are CSP maps which are not stabiliser operations, given in the next section. To this end, let us define a *Clifford dilation* as a stabiliser operation $\mathcal{O} \in \mathrm{SO}_{n,m}$ which acts as $\mathcal{O}(\rho) = \mathrm{tr}_{m+1,\dots,n+k}\left[U(\rho \otimes |0^k\rangle\langle 0^k|)U^\dagger\right]$ for a suitable Clifford unitary U.

Corollary 9.1. *Let $\mathcal{O} \in \mathrm{SO}_{n,m}$ be an extremal stabiliser operation that does not have a Clifford dilation. Then the kernel of $\mathcal{O}$ contains a Pauli operator.*

Corollary 9.1 follows directly from the more general Thm. 9.3 which is stated and proved in App. 9.B. The basic idea of the proof is that it is sufficient to focus on the first elementary operation in a circuit representation of $\mathcal{O}$, which we can assume to be a (possibly trivial) measurement of a Pauli operator $w(a) \otimes w(b)$ supported on the input and an ancilla register. This simplifies to proof considerably, since it removes the need to consider adaptive operations. As we show, the extremality of $\mathcal{O}$ implies that $w(b)$ has to stabilise the ancilla state. Moreover, as $\mathcal{O}$ is not a Clifford dilation, we can choose $a \neq 0$ since otherwise the measurement would act trivial. Then, any Pauli operator which anti-commutes with $w(a)$ lies in the kernel of $\mathcal{O}$.

9.3.2 Characterisation of completely stabiliser-preserving maps and channels

For this work, the focus lies on the case $m = n$, i. e. on channels which map the input space to itself. However, the following results should be possible to generalise.

As we saw in Sec. 9.2.2, completely stabiliser-preserving maps are in bijection with the subset of the bipartite $2n$-qubit stabiliser polytope fulfilling the TP condition. Notably, bipartite stabiliser states have a special structure that can be exploited to bring them into a standard form which we call the *polar form*. It is given by $|s\rangle = 2^{k/2} UP \otimes \mathbb{1} |\phi^+\rangle$ for a Clifford unitary $U \in \mathrm{Cl}_n$ and a stabiliser code projector P of rank 2^{n-k}. While this seems to be folk knowledge in the relevant community, we have been unable to find an explicit

formulation in the literature. Note that from this form, one can immediately derive the Schmidt rank of $|s\rangle$ as $\log_2 \mathrm{rk}(P) = n - k$.

For the sake of readibility, the proof of this fact can be found in App. 9.C.

Theorem 9.1. *Let* $\mathrm{stab}_{n,k}$ *be the set of* $[[n, n-k]]$ *stabiliser code projectors with* $\mathrm{stab}_n \equiv \mathrm{stab}_{n,n}$. *Then the following holds:*

(i) For $U \in \mathrm{Cl}_n$ *and* $P \in \mathrm{stab}_{n,k}$, *the Choi state* $\mathcal{J}(2^k \mathrm{Ad}(UP))$ *is a stabiliser state.*

(ii) For all $s \in \mathrm{stab}(2n)$, *there is a* $U \in \mathrm{Cl}_n$ *and* $P \in \mathrm{stab}_{n,k}$ *such that* $2^k \mathrm{Ad}(UP) = \mathcal{J}^{-1}(s)$.

Note that while the projective part in the polar form of a stabiliser state is unique, the unitary part is not. This is because replacing the Clifford unitary by $U \mapsto UV$ where V acts trivially on the code space gives an equivalent presentation of the state. Technically, this means that the unitary part is unique *up to the left Clifford stabiliser* of the stabiliser code.

Using the polar form, the polytope of CSP maps can be characterised as follows: The SP_{2n} polytope corresponds under the inverse Choi-Jamiołkowski isomorphism to the polytope which is spanned by channels with a single stabiliser Kraus operator $2^{k/2}UP$. Hence, any CSP map is of the form

$$\mathcal{E} = \sum_{i=1}^{r} \lambda_i \frac{2^n}{\mathrm{rk}\, P_i} U_i P_i \cdot P_i U_i^\dagger, \tag{9.12}$$

where λ_i are convex coefficients. However, Eq. (9.12) only defines a valid CSP map $\mathcal{E}$ if it is trace-preserving. Using the above form, we can cast the TP condition into an appealing form: $\mathcal{E}$ is a CSP map if and only if

$$\mathbb{1} = \mathcal{E}^\dagger(\mathbb{1}) = \sum_{i=1}^{r} \frac{2^n \lambda_i}{\mathrm{rk}\, P_i} P_i. \tag{9.13}$$

Thus, a sufficient and necessary condition for a convex combination of stabiliser Kraus operators to define a CSP map is that the rescaled projective parts $\tilde{P}_i := (2^n \lambda_i / \mathrm{rk}\, P_i) P_i$ form a POVM. In this context, the CSP channel $\mathcal{E}$ in Eq. (9.12) can be seen as the instrument associated with the stabiliser POVM $\{\tilde{P}_i\}$ combined with the application of Clifford unitaries U_i conditioned on outcome i. A priori, this allows for more general quantum channels than in the case of stabiliser operations where the POVM has to come from Pauli measurements, and thus the $\tilde{P}_i$ are mutually orthogonal. Albeit, it is not clear how strongly Eq. (9.13) restricts the admissible stabiliser codes P_i and coefficients λ_i. In particular, one could think of arranging overlapping codes with the right weights in non-trivial ways such that they yield the identity on Hilbert space. Indeed, an example of a CSP channel defined via overlapping stabiliser codes is given in Sec. 9.3.3. Finally, note that given a set of stabiliser codes, it is in principle possible to decide whether there exist coefficients such that Eq. (9.13) holds by solving a linear system of equations which depends on the structure of code overlaps.

Let us give some examples of CSP maps:

1. *Mixed Clifford channels.* Take $P_i \equiv \mathbb{1}$, then $2^n / \mathrm{rk}\, P_i = 1$ and Eq. (9.13) is trivially fulfilled for any convex combination.

2. *Dephasing in a stabiliser basis.* Take a basis of stabiliser states, and let P_i be the rank-one projectors onto the basis. A uniform convex combination $\lambda_i = 2^{-n}$ of these fulfills the TP condition Eq. (9.13). Such a channel corresponds to a dephasing in the chosen basis, followed by the potential application of conditional Clifford unitaries U_i depending on the basis measurement outcome i.

3. *Dephasing in stabiliser codes.* More generally, take an arbitrary stabiliser group $S = \langle g_1, \ldots, g_k \rangle$ and let P_i be all 2^k orthogonal stabiliser codes corresponding to different sign choices of the generators and $\lambda_i = 2^{-k}$. This defines a POVM ("syndrome measurement").

4. *Reset channels.* Let $s \in \mathrm{stab}_n$ be an arbitrary stabiliser state and consider the channel which replaces every input by s, i.e. $\mathcal{R}_s : X \mapsto \mathrm{tr}(X)s$. It is clearly CSP and is a special cases of the second example where $|s\rangle$ is completed to a stabiliser basis and the Clifford unitaries are chosen such that all basis elements are mapped to $|s\rangle$.

An important open question in this context is what the vertices, i.e. the extremal channels, of the CSP polytope are. Clearly, Clifford unitaries, corresponding to maximally entangled stabiliser states, are extremal and trace-preserving and thus vertices of the CSP polytope. However, new vertices emerge by intersecting the stabiliser polytope with the affine TP subspace and a full characterisation of those seems to be difficult. Albeit, it is possible to state some necessary conditions for the new vertices using geometrical arguments. Clearly, any vertex has to lie on the boundary of the stabiliser polytope, i.e. on one of its faces. Note that the TP condition defines $4^n - 1$ independent affine constraints. Thus, any vertex of the CSP polytope has to lie on a sufficiently low-dimensional face of SP_{2n}, namely one with dimension $< 4^n$ (compared to $\dim \mathrm{SP}_{2n} = 4^{2n} - 1$). An example of this is the following: Consider a non-trivial convex combination of two stabiliser states. Their polar forms can only fulfill the TP condition Eq. (9.13), if the projective parts are orthogonal and have rank 2^{n-1} and the convex coefficients are $\frac{1}{2}$ each. Thus, we can write them as

$$P_\pm = \frac{1}{2}\left(\mathbb{1} \pm w(a)\right), \quad a \in \mathbb{F}_2^{2n} \setminus 0. \tag{9.14}$$

Moreover, it is known that any two stabiliser states are connected by an edge of the stabiliser polytope if and only if their support on the Pauli basis is not identical [158, 159]. To achieve non-identical support of two stabiliser states with projective parts $P_\pm$, it is enough to add a Clifford unitary that acts non-trivially on $P_\pm$. Thus, the following map

$$\mathcal{E}_a := UP_+ \cdot P_+U^\dagger + P_- \cdot P_-, \tag{9.15}$$

lies on an edge of the stabiliser polytope and is the only point on the edge which is TP. Therefore, it is extremal within the CSP polytope by the previous dimension argument. Note that the channel $\mathcal{E}_a$ represents a stabiliser operation since it corresponds to measuring the Pauli operator $w(a)$ and applying the Clifford unitary U conditioned on the "+1" outcome.

9.3.3 Construction of a CSP map which is not a stabiliser operation

Notably, all of the examples given in the last section are stabiliser operations. The goal of this section is to show that the class of CSP maps is generally larger than the class of

stabiliser operations by constructing an explicit example of a CSP map which is not SO for $n \geq 2$.

Theorem 9.2 ($\mathrm{SO}_n \subsetneq \mathrm{CSP}_n$)**.** *It holds* $\mathrm{CSP}_n = \mathrm{SO}_n$ *if and only if* $n = 1$*. In particular, the set of CSP maps is strictly larger than the set of stabiliser operations for* $n \geq 2$*.*

The proof strategy is as follows: In App. 9.E, we show that any single-qubit CSP map is a stabiliser operation. Furthermore, we define a CSP map Λ and prove that it is extremal within the CSP polytope. We show that for $n \geq 2$ the kernel of Λ does not contain a Pauli operator and Λ does not have a Clifford dilation. Consequently, Λ is not a stabiliser operation by Corollary 9.1.

Lemma 9.3 (Extremality of Λ)**.** *Define the following CSP channel:*

$$\Lambda := \mathrm{Ad}(H^{\otimes n} P) + \frac{1}{2^{n-1}} \sum_{a \in \mathsf{Z}_n} \mathrm{Ad}(P_a), \tag{9.16}$$

where $P := |0^n\rangle\langle 0^n|$*, and* $P_a := \frac{1}{2}(\mathbb{1} - w(a))$*. Then,* Λ *is extremal within the CSP polytope for all* n*.*

Due to its length and technicality, we defer the proof to App. 9.D, preceded by an introduction into the required techniques. There, we prove a stronger version of Lemma 9.3 which is given as Theorem 9.4.

Note that Eq. (9.16) is in standard form (9.12) with uniform weights $\lambda_a = 2^{-n}$. It is straightforward to verify that Λ is TP since

$$\Lambda^\dagger(\mathbb{1}) = P + 2^{1-n} \sum_{a \in \mathsf{Z}_n} P_a = P + \mathbb{1} - 2^{-n} \sum_{a \in \mathsf{Z}_n} w(a) = \mathbb{1}. \tag{9.17}$$

Here, we used that $P = |0^n\rangle\langle 0^n| = 2^{-n} \sum_{a \in \mathsf{Z}_n} w(a)$.

The channel Λ can be understood as the geometrical generalisation of the "edge construction" of a CSP map given in Eq. (9.15). Indeed, for $n = 1$, there is only one $P_a = |1\rangle\langle 1|$ and the channel is a stabiliser operation of the form

$$\Lambda = H\,|0\rangle\langle 0| \cdot |0\rangle\langle 0|\,H + |1\rangle\langle 1| \cdot |1\rangle\langle 1|\,. \tag{9.18}$$

The idea is that generalising this from edges to higher-dimensional *faces* naturally requires *non-orthogonal* codes and should thus give us the required example of a non-SO map.

A natural question to ask is whether Λ can be expressed in terms of more elementary quantum channels. Indeed, it is straightforward to compute its action in the computational basis, see App. 9.F. Write an arbitrary density matrix as $\rho = \sum_{x,y} \rho_{xy}\,|x\rangle\langle y|$, then the channel acts as

$$\Lambda(\rho) = \rho_{00}\,|+\rangle\langle +| + \sum_{x \neq 0} \rho_{xx}\,|x\rangle\langle x| + \frac{1}{2} \sum_{x \neq y \neq 0} \rho_{xy}\,|x\rangle\langle y|\,. \tag{9.19}$$

It can be written as a composition of the following three operations:

1. Perform a projective measurement with projectors $\{|0^n\rangle\langle 0^n|, \mathbb{1} - |0^n\rangle\langle 0^n|\}$. This channel sets all off-diagonal terms in the first row and column of ρ to zero, i.e. it block-diagonalises ρ with respect to the entry at position $(0, 0)$.

2. Partial dephasing in the computational basis with probability 1/2. This channel reduces the amplitude of the off-diagonal terms by 1/2.
3. Apply a global Hadamard gate on all qubits conditioned on the "0" outcome of the measurement.

Interestingly, all three components are necessary for Λ to have the desired properties. If we leave out the second channel, it is possible to show that the composition of 1 and 3 is not stabiliser-preserving for $n \geq 2$ (see App. 9.F), while for $n = 1$ it is simply a stabiliser operation. Moreover, if we leave out channel 2 and 3, then we can rewrite the block-diagonalisation as a uniform convex combination of the identity and the diagonal n-qubit gate $V_n := \mathrm{diag}(-1, 1, \ldots, 1)$. Note that $V_n = X^{\otimes n}(C^{n-1}Z)X^{\otimes n}$, thus it is in the same level of the Clifford hierarchy as the multiply-controlled Z gate, namely in the n-th level. Hence, for $n \leq 2$, this is a mixed Clifford channel and in particular a stabiliser operation. For $n > 2$, the same technique as before can be used to show that this channel is not CSP and is thus a "magic" channel. The effect of the dephasing channel is to sufficiently reduce the "magic" of the overall channel. With increasing dephasing strength, it approaches the CSP polytope from the outside and eventually becomes CSP. Figuratively speaking, the Hadamard gate in the last step fine-tunes the direction from which the CSP polytope is being approached, resulting in a channel which is able to separate the CSP from the SO polytope.

Lemma 9.4. *Let Λ be as in Eq. (9.16) and $n \geq 2$. Then, there is no $u \in \mathbb{F}_2^{2n}$ such that $w(u) \in \ker \Lambda$.*

Proof. Note that we have for any $u \in \mathbb{F}_2^{2n}$:

$$Pw(u)P = \mathbf{1}_{\mathsf{Z}_n}(u)P, \qquad P_a w(u) P_a = \mathbf{1}_{a^\perp}(u) w(u) P_a, \tag{9.20}$$

where $\mathbf{1}_M$ is the indicator function on a set M. Thus, we find

$$\Lambda(w(u)) = \mathbf{1}_{\mathsf{Z}_n}(u)|+^n\rangle\langle+^n| + \frac{1}{2^{n-1}} w(u) \sum_{a \in \mathsf{Z}_n \cap u^\perp} P_a. \tag{9.21}$$

First, assume that $u \in \mathsf{Z}_n$. Then we get

$$\Lambda(w(u)) = |+^n\rangle\langle+^n| + 2^{-n} w(u) \left(2^n \mathbb{1} - \sum_{a \in \mathsf{Z}_n} w(a) \right) = |+^n\rangle\langle+^n| + w(u) - |0^n\rangle\langle 0^n|. \tag{9.22}$$

However, this is not zero since e.g. $\langle 0^n| \Lambda(w(u)) |0^n\rangle = 2^{-n}$. Next, assume $u \notin \mathsf{Z}_n$. Write $u = (u_z, u_x)$ with $u_x \neq 0$. Then, $u^\perp \cap \mathsf{Z}_n = \{(z, 0) \mid z \cdot u_x = 0\}$ which has dimension $n - 1$ by assumption. Compute:

$$\Lambda(w(u)) = 2^{-n} w(u) \left(2^{n-1} \mathbb{1} - \sum_{z \in u_x^\perp} Z(z) \right) = i^{-u_z \cdot u_x} \left(\frac{1}{2} Z(u_z) - 2^{-n} \sum_{z \in u_x^\perp} Z(z + u_z) \right) X(u_x). \tag{9.23}$$

Since $n \geq 2$, we can find a $y \in \mathbb{F}_2^n \setminus \{0\}$ such that $y \neq u_x$. Then, we find

$$\begin{aligned} \langle y| \Lambda(w(u)) |y + u_x\rangle &= \frac{1}{2} i^{-u_z \cdot u_x} (-1)^{u_z \cdot y} \left(1 - \frac{1}{|u_x^\perp|} \sum_{z \in u_x^\perp} (-1)^{z \cdot y} \right) \\ &= \frac{1}{2} i^{-u_z \cdot u_x} (-1)^{u_z \cdot y} \neq 0. \end{aligned} \tag{9.24}$$

Here, we used that the sum has the form of an inner product of characters and is thus zero, since by assumption $y \notin (u_x^\perp)^\perp = \langle u_x \rangle$. □

As discussed before, Λ is an extremal stabiliser operation for $n = 1$. It is straightforward to check that in this case we have $\Lambda(X) = 0$ for the Pauli X matrix.

Lemma 9.5. *Λ does not have a Clifford dilation.*

Proof. If it had a Clifford dilation, then $\Lambda^\dagger$ would map Pauli operators to Pauli operators, up to a phase. Along the line of the proof of Lem. 9.4 we find for any $u \in \mathbb{F}_2^{2n}$:

$$PH^{\otimes n} w(u) H^{\otimes n} P = \mathbf{1}_{\mathsf{X}_n}(u) P \quad \Rightarrow \quad \Lambda^\dagger(w(u)) = \mathbf{1}_{\mathsf{X}_n}(u)\, |0^n\rangle\langle 0^n| + \frac{1}{2^{n-1}} w(u) \sum_{a \in \mathsf{Z}_n \cap u^\perp} P_a. \tag{9.25}$$

For e.g. $u = e_1 \in \mathsf{Z}_n$, we thus get

$$\Lambda^\dagger(Z_1) = 2^{-n} Z_1 \left(2^n \mathbb{1} - \sum_{a \in \mathsf{Z}_n} w(a) \right) = Z_1 - |0^n\rangle\langle 0^n|, \tag{9.26}$$

which is certainly not proportional to a Pauli operator. □

9.4 Summary and open questions

In this work, we have characterised CSP maps by suitable stabiliser POVMs with conditional application of Clifford unitaries. Based on these insights, we have constructed a CSP map which is extremal in the CSP polytope. By deriving a special property of extremal stabiliser operations, we have been able to prove that our example is not a stabiliser operation, except for $n = 1$ in which case the classes coincide. Finally, this shows that the class of CSP maps is strictly more general than the class of stabiliser operations for $n \geq 2$, reflecting the well-known result from entanglement theory that LOCC operations are contained but not equal to the set of separable quantum channels.

This finding indicates that recently proposed stabiliser-based simulation techniques of CSP maps are strictly more powerful than Gottesman-Knill-like methods [36].

Furthermore, our result has direct applications to the problem of quantifying resources required in the magic state model for quantum computing. The axiomatic approach to free operations has the advantage that it is possible to directly apply results from general resource theory and obtain explicit bounds on e.g. state conversion and distillation rates [27, 36, 160–162]. For this case, it is also known that the theory is asymptotically reversible [39]. Here, it would be interesting to study whether tasks like magic state distillation can show a gap in the achievable rates between CSP channels and stabiliser operations. Again, this question is motivated from entanglement theory, where a significant separation between separable channels and LOCC operations for e.g. entanglement conversion is known [157].

Finally, we expect that our results also hold for qudit systems of odd prime-power dimension. Arguably, this is the mathematically simpler case and our proof strategy should still be applicable after replacing the representation of stabiliser states via the characteristic function with the Wigner function.

9.A Phase space formalism in a nutshell

9.A.1 Discrete phase space

The central insight of the phase space formalism is that the n-qubit stabiliser formalism can be formulated using discrete symplectic geometry on the $2n$-dimensional vector space $\mathbb{F}_2^{2n}$ over the finite field $\mathbb{F}_2$, equipped with the standard symplectic form

$$[a, b] := a_z \cdot b_x + a_z \cdot b_x \tag{9.27}$$

for $a = (a_z, a_x)$, $b = (b_z, b_x) \in \mathbb{F}_2^{2n}$. Before we will make this connection precise, let us introduce some definitions. Given a subspace $M \subset \mathbb{F}_2^{2n}$, its *symplectic complement* is defined as $M^\perp := \{a \in \mathbb{F}_2^{2n} \mid [a, b] = 0 \ \forall b \in M\}$. We call M *isotropic* if $M \subset M^\perp$, i.e. if all elements of M are orthogonal to each other. The dimension of an isotropic subspace M is upper bounded by n since $\dim M^\perp + \dim M = 2n$. A maximally isotropic subspace $M = M^\perp$ is also called a *Lagrangian*. Finally, it is always possible to write the symplectic space as $\mathbb{F}_2^{2n} = L \oplus L'$ for L and L' disjoint Lagrangian subspaces. This is called a *polarisation* of the underlying space. An example of such a polarisation is given by the standard basis $e_1, \ldots, e_n, f_1, \ldots, f_n$ of $\mathbb{F}_2^{2n}$ as $\mathsf{Z}_n \oplus \mathsf{X}_n$ where $\mathsf{Z}_n := \langle e_1, \ldots, e_n \rangle$ and $\mathsf{X}_n := \langle f_1, \ldots, f_n \rangle$. Linear maps $g \in \mathrm{GL}_(\mathbb{F})_2^{2n})$ which preserve the symplectic form, $[g(a), g(b)] = [a, b]$ are called *symplectic* and form the *symplectic group* $\mathrm{Sp}(\mathbb{F}_2^{2n})$ which we will often denote Sp_{2n} for brevity.

The Pauli or *Weyl* operators defined before in Eq. (9.2) as

$$w(a) := i^{-\gamma(a)} Z(a_z) X(a_x), \qquad \gamma(a) := a_z \cdot a_x \mod 4, \tag{9.28}$$

form a projective representation of the discrete phase space $\mathbb{F}_2^{2n}$ as an additive group:

$$w(a)w(b) = i^{\beta(a,b)} w(a + b), \qquad \beta(a, b) := \gamma(a + b) - \gamma(a) - \gamma(b) + 2(a_x \cdot b_z). \tag{9.29}$$

Here, β is a function $\mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} \to \mathbb{Z}_4$. By definition, it has the following properties:

$$\beta(a, a) = \beta(a, 0) = \beta(0, a) = 0, \tag{9.30}$$

We have $\beta(a, b) - \beta(b, a) = 2[a, b] \in 2\mathbb{Z}_4$, and thus the symplectic structure of the phase space is encoded in the commutation relations as

$$w(a)w(b) = (-1)^{[a,b]} w(b)w(a). \tag{9.31}$$

Moreover, it holds that $2\beta(a, b) = 2[a, b] \in 2\mathbb{Z}_4$.

Note that if we take $e \in \mathsf{Z}_n$ and $f \in \mathsf{X}_n$, then β takes the form

$$\beta(e, f) = \gamma(e + f) = \Omega(e, f) \quad \text{with} \quad \Omega(a, b) = a_z \cdot a_x - a_x \cdot b_z \mod 4. \tag{9.32}$$

Moreover, on the Lagrangian subspaces X_n and Z_n, the function β is identically zero by the definition of the Weyl operators in Eq. (9.28):

$$\beta(e, e') = 0 = \beta(f, f'), \qquad \forall e, e' \in \mathsf{X}_n, \ f, f' \in \mathsf{Z}_n. \tag{9.33}$$

On more general isotropic subspaces, this is not the case, but β takes only values in $2\mathbb{Z}_4$, which can be seen by squaring Eq. (9.29). Furthermore, it is also symmetric. Thus, we can

define a $\mathbb{F}_2$-valued symmetric function $\bar{\beta}$ on all isotropic subspaces via $2\bar{\beta}(a,b) = \beta(a,b)$ where $[a,b] = 0$.

Finally, let us note that if we consider a composite system of n and m qubits, its phase space is $\mathbb{F}_2^{2n} \oplus \mathbb{F}_2^{2m}$. The β function then splits as

$$\beta(a \oplus b, c \oplus d) = \beta(a,c) + \beta(b,d). \tag{9.34}$$

The $\bar{\beta}$ function however does not necessarily split since

$$0 = [a \oplus b, c \oplus d] = [a,c] + [b,d], \tag{9.35}$$

does not necessarily imply that $[a,c] = 0 = [b,d]$.

9.A.2 Clifford group

Since Clifford unitaries preserve the Pauli group and the commutation relations, they can be uniquely represented by a *symplectic map* $g \in \mathrm{Sp}_{2n}$ and a phase function $\alpha : \mathbb{F}_2^{2n} \to \mathbb{F}_2$ as follows:

$$Uw(a)U^\dagger = (-1)^{\alpha(a)} w(g(a)). \tag{9.36}$$

It is not very instructive to write down the explicit form of the phase function α. However, by the composition law Eq. (9.29) it has to fulfill the polarisation equation:

$$2\big(\alpha(a+b) - \alpha(a) - \alpha(b)\big) = \beta(g(a), g(b)) - \beta(a,b). \tag{9.37}$$

This implies that α is completely determined on a basis of $\mathbb{F}_2^{2n}$. Moreover, any linear form $a \mapsto [h,a]$ gives rise to another phase function $\alpha' = \alpha + [h,\cdot]$ compatible with $g \in \mathrm{Sp}_{2n}$ and it is possible to show that any phase function can be obtained this way. By Eq. (9.29), these linear forms change the Clifford unitary as $U' = Uw(h)$. This shows that the quotient of the Clifford group Cl_n by the Pauli group $\mathcal{P}_n$ is isomorphic to the symplectic group Sp_{2n}, in formula $\mathrm{Cl}_n / \mathcal{P}_n \simeq \mathrm{Sp}_{2n}$.

9.A.3 Stabiliser codes

Recall that a $[[n, n-k]]$ stabiliser code is defined by an Abelian subgroup $-\mathbb{1} \notin S \subset \mathcal{P}_n$ of order 2^k, i.e. with k independent generators. Using the above notation, we can write

$$S = \{(-1)^{\varphi(a)} w(a) \mid a \in M\}, \tag{9.38}$$

for $M \subset \mathbb{F}_2^{2n}$ and a phase function $\varphi : M \to \mathbb{F}_2$. The properties of S imply that M is a k-dimensional isotropic subspace. The orthogonal projector on the code space stabilised by S can be written as

$$P_S = \frac{1}{|S|} \sum_{g \in S} g = \frac{1}{2^k} \sum_{a \in M} (-1)^{\varphi(a)} w(a). \tag{9.39}$$

As before, by Eq. (9.29), we find that the phase function has to fulfill

$$\varphi(a+b) - \varphi(a) - \varphi(b) = \bar{\beta}(a,b). \tag{9.40}$$

Thus, it is completely determined on a basis of M and any two phase functions compatible with M differ by a linear form. Hence, the number of stabiliser codes associated to M is exactly $|M^*| = |M| = 2^k$. These are all orthogonal since for any two codes, there is at least one $a \in M$ such that the phase function differs and thus $w(a)$ takes different eigenvalues on the two codes.

In particular, stabiliser states are $[[n, 0]]$ stabiliser codes. They are exactly represented by maximally isotropic, i.e. Lagrangian subspaces. The above argument shows that there are 2^n orthogonal stabiliser states associated to any Lagrangian L, which form an orthonormal basis of $(\mathbb{C}^2)^{\otimes n}$. Conversely, one can show that any orthonormal basis of stabiliser states has to correspond to a single Lagrangian.

Since the Pauli operators form a basis for the space of linear operators on $(\mathbb{C}^2)^{\otimes n}$, we can expand any state as

$$\rho = \frac{1}{2^n} \sum_{a \in \mathbb{F}_2^{2n}} \chi_\rho(a) w(a), \qquad \chi_\rho(a) = \mathrm{tr}(w(a)\rho). \tag{9.41}$$

We call χ_ρ the *characteristic function* of the state ρ. Since ρ is Hermitian, χ_ρ is a real-valued function and its values are in $[-1, 1]$. Sometimes, it is also called the *Bloch representation* of ρ.

Of course, we can expand any operator in the Pauli basis such as stabiliser code projectors. It will be convenient to choose a different normalisation for those such that Eq. (9.39) becomes

$$P = \frac{1}{2^k} \sum_{a \in M} \chi(a) w(a). \tag{9.42}$$

Let us now state the properties of stabiliser codes in terms of their characteristic function. A real-valued function χ is the characteristic function of a stabiliser code if and only if its *support* is given by an isotropic subspace $\mathrm{supp}(\chi) = M \subset \mathbb{F}_2^{2n}$ and it obeys the following rules:

$$\chi(0) = 1, \qquad \chi(a+b) = (-1)^{\bar{\beta}(a,b)} \chi(a)\chi(b) \quad \forall a, b \in M. \tag{9.43}$$

The first one is coming from the trace condition, the second one from Eq. (9.40). Note that the second relation is reminiscent of the definition of an additive character on the subspace M, except for the additional "twist" by the function β.

9.B Proof of Corollary 9.1

Theorem 9.3 (Pauli invariance of extremal stabiliser operations)**.** *Let $\mathcal{O} \in \mathrm{SO}_{n,m}$ be an extremal stabiliser operation. Then, at least one of the following is true:*

(i) *There is a $x \in \mathbb{F}_2^{2n} \setminus 0$ such that $\mathcal{O} = \mathcal{O} \circ \mathrm{Ad}(w(x))$.*

(ii) *$\mathcal{O}$ has a Clifford dilation.*

Here, we use $\mathrm{Ad}(A)$ to denote the superoperator which is given by the adjoint action of A, i. e. $\mathrm{Ad}(A)(X) := AXA^\dagger$.

Proof of Corollary 9.1. Let $\mathcal{O} \in \mathrm{SO}_{n,m}$ be an extremal stabiliser operation which does not have a Clifford dilation. By Thm. 9.3, there is a $x \neq 0$ such that $\mathcal{O} = \mathcal{O} \circ \mathrm{Ad}(w(x))$. Then, for all $y \notin x^{\perp}$:

$$\mathcal{O}(w(y)) = \mathcal{O}(w(x)w(y)w(x)) = -\mathcal{O}(w(y)) \quad \Rightarrow \quad w(y) \in \ker \mathcal{O}. \tag{9.44}$$

□

In fact, it is possible to state Thm. 9.3 more precisely. However, this is not needed for the purpose of this work and thus the additional steps in the proof have been omitted. Nevertheless, it is straightforward to prove the following statements along the lines of this appendix. For $m \leq n$, an extremal Clifford dilation can always be written without the use of ancillas, in particular, for $m = n$, this is simply a Clifford unitary. Moreover, for $m < n$, the existence of Pauli invariances is a generic feature of stabiliser operations and thus the importance of Thm. 9.3 lies in the existence of invariances in the regime $m \geq n$. To make this plausible, consider an n-qubit Clifford unitary U, followed by tracing out the last $n - m$ qubits. Under such a stabiliser operation, any Pauli operator which is mapped under U to a Pauli operator having support only on the last $n - m$ qubits yields an invariance. This example shows that both statements in Thm. 9.3 can be simultaneously true. However, in the regime $m \geq n$, they are mutually exclusive since then any Clifford dilation is a partial isometry, in particular it has a trivial kernel.

For the proof, we make use of the symplectic language introduced in App. 9.A. Moreover, it will turn out to be beneficial to prove to following lemma first:

Lemma 9.6. *Suppose that $\mathcal{O}$ is an extremal stabiliser operation which starts by preparing an ancilla state $|0^k\rangle$, followed by the measurement of a Pauli operator $w(a) \otimes w(b)$ where the ancilla state is not an eigenvector of $w(b)$. Then this measurement can be replaced by a Clifford unitary.*

Proof. Let us denote the stabiliser operation which prepares $|0^k\rangle$ and measures $w(a) \otimes w(b)$ by $\tilde{\mathcal{O}}$. Because $w(b)|0^k\rangle$ is an element of the computational basis, there is a Clifford unitary V which maps $|0^k\rangle \mapsto |0^k\rangle$ and $(w(b)|0^k\rangle) \mapsto |1\rangle|0^{k-1}\rangle$. There is also a Clifford U such that $Uw(a)U^{\dagger} = Z_1$. Thus, up to acting with U on the input register before, and with V on the ancilla register after the measurement, we may assume that $w(a) = Z_1$ and $w(b)|0^k\rangle = |1\rangle|0^{k-1}\rangle$.

Assume the inputs are in the state $|\psi\rangle$ before the measurement. In terms of a controlled Z-gate (first ancilla qubit controlling the first input qubit), the projections onto the $\pm$-eigenspaces of $w(a) \otimes w(b)$ are given by

$$\frac{1}{2}\Big[\, |\psi\rangle \otimes |0\rangle \pm (Z_1\,|\psi\rangle) \otimes |1\rangle \,\Big] \otimes |0^{k-1}\rangle = \frac{1}{\sqrt{2}}\Big[CZ\,|\psi\rangle\,|\pm\rangle\,\Big] \otimes |0^{k-1}\rangle. \tag{9.45}$$

Since the norm-squared is $1/2$ in either case, the channel $\tilde{\mathcal{O}}$ can be written as

$$\tilde{\mathcal{O}}(\rho) = \frac{1}{2}\,\mathrm{Ad}(CZ)\big(\rho \otimes |+\rangle\langle+| \otimes |0^{k-1}\rangle\langle 0^{k-1}|\big) + \frac{1}{2}\,\mathrm{Ad}(CZ)\big(\rho \otimes |-\rangle\langle-| \otimes |0^{k-1}\rangle\langle 0^{k-1}|\big). \tag{9.46}$$

By extremality, both summands must realise the same channel, so we may replace the measurement by a Hadamard on the first ancilla, followed by the controlled-Z. □

Proof of Theorem 9.3. We can assume that an extremal stabiliser operation $\mathcal{O}$ has a circuit representation with k ancilla qubits in the state $|0^k\rangle$. Without loss of generality, we can furthermore assume that it starts with the measurement of a $(n+k)$-qubit Pauli operator $w(a,b) = w(a) \otimes w(b)$ with $a \in \mathbb{F}_2^{2n}$ and $b \in \mathbb{F}_2^{2k}$ by propagating the first Pauli measurement through the preceding Clifford unitaries. Moreover, by Lemma 9.6, we can assume that $b \in \mathsf{Z}_k$. Note that $\mathcal{O}$ is a Clifford dilation if and only if we can find no or only a trivial Pauli measurement, which is $a = 0$. Let us thus assume that $a \neq 0$ and show that $x = a$ is the claimed invariance.

Let us denote the stabiliser operation which prepares $|0^k\rangle$ and measures $w(a) \otimes w(b)$ by $\tilde{\mathcal{O}}$. Clearly, it its enough to argue that $\tilde{\mathcal{O}}$ has the desired property. Let $\mathcal{M}$ be the instrument associated to the projectors $P_\pm = \frac{1}{2}(\mathbb{1} \pm w(a,b))$ onto the eigenspaces of the Pauli operator $w(a,b)$. Then, for any $u \in \mathbb{F}_2^{2n}$ and $v \in \mathsf{Z}_k$, we have

$$\mathcal{M}\big(w(u,v)\big) = P_+ w(u,v) P_+ + P_- w(u,v) P_- = \begin{cases} w(u,v) & \text{if } u \in a^\perp, \\ 0 & \text{else.} \end{cases} \tag{9.47}$$

In particular, for any state ρ, we find $\mathcal{M}\big(\rho \otimes |0^k\rangle\langle 0^k|\big) = \rho' \otimes |0^k\rangle\langle 0^k|$, where ρ' is a potentially sub-normalised state which commutes with $w(a)$. Hence:

$$\begin{aligned} \tilde{\mathcal{O}}(\rho) &= \mathcal{M}\big(\rho \otimes |0^k\rangle\langle 0^k|\big) \\ &= (w(a) \otimes \mathbb{1})\mathcal{M}\big(\rho \otimes |0^k\rangle\langle 0^k|\big)(w(a)^\dagger \otimes \mathbb{1}) \\ &= \mathcal{M}\big(w(a)\rho\, w(a)^\dagger \otimes |0^k\rangle\langle 0^k|\big) \\ &= \tilde{\mathcal{O}}(w(a)\rho\, w(a)^\dagger). \end{aligned} \tag{9.48}$$

□

9.C Polar form of bipartite stabiliser states

9.C.1 Double Lagrangians

Let us consider stabiliser states in the bipartite setting where every subsystem is composed of n qubits. Define $V := \mathbb{F}_2^{2n}$, then the corresponding $2n$-qubit phase space is $2V := V \oplus V$. The goal of this section is to derive a standard form for the bipartite Lagrangians $\mathrm{Lag}(2V)$. Note that this characterisation is possible in full generality for local prime-power dimensions and also plays an important role in the representation theory of the Clifford group. A more detailed treatise will be given in Ref. [129]

Note that the graph $\Gamma(g)$ of a symplectic map $g \in \mathrm{Sp}(V)$ is a Lagrangian subspace since

$$[g(a) \oplus a, g(b) \oplus b] = [g(a), g(b)] + [a,b] = 0. \tag{9.49}$$

Moreover, note that $\Gamma(g)$ is *transverse* to the left and right embedding of V, i. e. $\Gamma(g) \cap (0 \oplus V) = \Gamma(g) \cap (V \oplus 0) = 0$. Conversely, it is straightforward to show that any transverse Lagrangian is the graph of symplectic map.

In general, a Lagrangian subspace $L \subset 2V$ will have non-trivial overlap with the left/right embeddings. As as starting point, we thus define the *left and right defect spaces* of a "double" Lagrangian $L \subset 2V$ as

$$L_{LD} \oplus 0 := L \cap (V \oplus 0), \qquad 0 \oplus L_{RD} := L \cap (0 \oplus V). \tag{9.50}$$

By definition, L_{LD} and L_{RD} are isotropic subspaces of V. Denoting by pr_L and pr_R the projections onto the left and right factor of L, we see that $\ker \mathrm{pr}_L = L \cap (0 \oplus V) \simeq L_{RD}$ and $\ker \mathrm{pr}_R = L \cap (V \oplus 0) \simeq L_{LD}$. Setting $L_L := \mathrm{im}\, \mathrm{pr}_L$ and $L_R := \mathrm{im}\, \mathrm{pr}_R$, we find that $L_L \subset L_{LD}^\perp$ and $L_R \subset L_{RD}^\perp$. Moreover, it holds:

$$\begin{aligned} \dim L_{LD}^\perp &= \dim V - \dim L_{LD} = \dim L - \dim \ker \mathrm{pr}_R = \dim L_R \leq \dim L_{RD}^\perp, \\ \dim L_{RD}^\perp &= \dim V - \dim L_{RD} = \dim L - \dim \ker \mathrm{pr}_L = \dim L_L \leq \dim L_{LD}^\perp. \end{aligned} \tag{9.51}$$

Hence, we have $L_{LD}^\perp = L_R$, $L_{RD}^\perp = L_L$ and $\dim L_{LD} = \dim L_{RD}$. Recall that the quotients $L_{LD}^\perp / L_{LD}$ and $L_{RD}^\perp / L_{RD}$ inherit a (non-degenerate) symplectic form from the one on V. Then, the Lagrangian L uniquely determines a symplectic map $\varphi : L_{RD}^\perp / L_{RD} \to L_{LD}^\perp / L_{LD}$ as follows: For any $w \in L_{RD}^\perp$ pick a $v = v(w) \in L_{LD}^\perp$ such that $v(w) \oplus w \in L$ and set $\varphi([w]) := [v(w)]$. This map is well-defined since for any $w' \in [w]$ and v' such that $v' \oplus w' \in L$ we find that

$$(v - v') \oplus 0 = v \oplus w - 0 \oplus (w - w') - v' \oplus w' \in L, \tag{9.52}$$

thus $v' \in [v(w)]$. Hence, L uniquely determines $(L_{LD}, L_{RD}, \varphi)$ and vice versa, we can recover L by

$$L = \{ v \oplus w \mid w \in L_{RD}^\perp,\ v \in \varphi([w]) \}. \tag{9.53}$$

This is indeed the complete Lagrangian subspace since its dimension is $\dim L_{RD}^\perp + \dim L_{LD} = \dim V$.

Let us add some remarks. The symplectomorphism $\varphi : L_{RD}^\perp / L_{RD} \to L_{LD}^\perp / L_{LD}$ can be seen as being induced from a (non-unique) symplectic map $g \in \mathrm{Sp}(V)$ as follows: Lift φ to an isometry $\tilde{\varphi} : L_{RD}^\perp \to L_{LD}^\perp$ mapping L_{RD} to L_{LD} and use Witt's theorem to extend it to a symplectic map $g \in \mathrm{Sp}(V)$ which yields $\varphi([v]) = [g(v)]$. Moreover, it should be clear that given two isotropic subspaces $M, N \subset V$ of the same dimension, any bijective linear map $h : M \to N$ is an isometry and thus extends to a symplectic map $g \in \mathrm{Sp}(V)$ which automatically maps $M^\perp$ to $N^\perp$. Then, Eq. (9.53) yields a valid double Lagrangian L with left and right defect subspaces $L_{LD} = N$, $L_{RD} = M$ and isometry induced by g. Alternatively, we can write it as follows:

$$L = L(M, g) := \{ g(w + v) \oplus w \mid w \in M^\perp,\ v \in M \}. \tag{9.54}$$

Remark 9.1. The given decomposition of "double Lagrangians" was introduced in representation theory and harmonic analysis by Howe [163, 164] together with the closely connected oscillator semigroup (in odd characteristic).

9.C.2 Bipartite stabiliser states

The standard form of double Lagrangians, Eq. (9.54), already implies that any bipartite stabiliser state is of the form

$$|s\rangle = 2^{k/2} UP \otimes \mathbb{1} |\phi^+\rangle, \tag{9.55}$$

which we call the *polar form*. To show this implication explicitly, note that the Lagrangian and characteristic function of $|\phi^+\rangle$ is given by

$$L^+ = \{(v, v) \mid v \in V\}, \qquad \chi^+(v, v) = (-1)^{v_z \cdot v_x}. \tag{9.56}$$

Note that on L^+, we have (cp. App. 9.A):

$$\beta((v,v),(w,w)) = \beta(v,w) + \beta(v,w) = 2\beta(v,w) = 2[v,w] \in 2\mathbb{Z}_4. \tag{9.57}$$

Thus, χ^+ indeed fulfills the composition law, Eq. (9.43):

$$\chi^+(v+w,v+w) = (-1)^{[v,w]}\chi^+(v,v)\chi^+(w,w) = (-1)^{\tilde{\beta}((v,v),(w,w))}\chi^+(v,v)\chi^+(w,w). \tag{9.58}$$

Assume that P has an associated isotropic subspace $M \subset V$ with characteristic function χ_P and $U = \mathbb{1}$ (for now). First, note that by definition $\chi_P(b)w(b)P = P$ for all $b \in M$ and thus the state $|s\rangle$ in Eq. (9.55) is stabilised by all Pauli operators of the form $\chi(b)w(b,0)$ where $b \in M$. Moreover, it is also stabilised by those of the form $w(a) \otimes \overline{w(a)} = (-1)^{a_z \cdot a_x} w(a,a)$ where $a \in M^\perp$, since we have

$$w(a,a)(P \otimes \mathbb{1})\big|\phi^+\big\rangle = (w(a)P\overline{w(a)}) \otimes \mathbb{1}\big|\phi^+\big\rangle = (-1)^{a_z \cdot a_x}(P \otimes \mathbb{1})\big|\phi^+\big\rangle. \tag{9.59}$$

Here, we used that $A \otimes \mathbb{1}\big|\phi^+\big\rangle = \mathbb{1} \otimes A^\top\big|\phi^+\big\rangle$ for any matrix A. Note that these two sets of stabilisers are independent and commute, and are hence described by the isotropic subspace

$$L = \{(a+b,a) \,|\, a \in M^\perp,\, b \in M\} \subset 2V, \tag{9.60}$$

of dimension $\dim M + \dim M^\perp = 2n$, i.e. a Lagrangian. This shows that $2^{k/2}(P \otimes \mathbb{1})\big|\phi^+\big\rangle$ is a stabiliser state with characteristic function defined on the generating sets by

$$\chi(a,a) = (-1)^{a_z \cdot a_x} = \chi^+(a,a), \quad \chi(b,0) = \chi_P(b), \quad a \in M^\perp,\, b \in M. \tag{9.61}$$

Observe that acting with $w(v,0)$ for any $v \in V$ on $2^{k/2}(P \otimes \mathbb{1})\big|\phi^+\big\rangle$ changes the characteristic function as $\chi(a+b,a) \mapsto (-1)^{[v,a+b]}\chi(a+b,a)$. This action is trivial if and only if $v \in M$ and thus we get $|V \setminus M|$ orthogonal stabiliser states in this way. However, there are also $|M|$ different characteristic functions χ_P for a given $M \subset V$. Thus, we get in this way all $|V| = |L|$ characteristic functions. In other words, any stabiliser state with a Lagrangian of the form in Eq. (9.60) can be written as $2^{k/2}(w(v)P) \otimes \mathbb{1}\big|\phi^+\big\rangle$.

Finally, if we allow any Clifford unitary U in Eq. (9.55), this simply maps the orthogonal stabiliser basis supported on L to another orthogonal stabiliser basis with support

$$L' = \{(g(a+b),a) \,|\, a \in M^\perp,\, b \in M\} \subset 2V, \tag{9.62}$$

where g is the symplectic matrix associated to U. Since any Lagrangian in $2V$ is of this form, this shows that all bipartite stabiliser states have the claimed form (9.55).

Finally, we remark that is straightforward to classify bipartite stabiliser states by their entanglement using the above language. Since the polar form Eq. (9.55) is precisely the polar decomposition of the matrix representing $|s\rangle$, we can see that the Schmidt rank of $|s\rangle$ is $\log_2 \operatorname{rk} P = n - k$. As it is well known, the maximally entangled stabiliser states are thus exactly those with $P = \mathbb{1}$, resulting in a trivial defect subspace $M = \{0\}$. Moreover, the product states are those for which P is a stabiliser state itself, i.e. the subspace M associated to P is a Lagrangian subspace.

9.D Proof that Λ is extremal

This section is formulated using the representation of stabiliser states in terms of their characteristic functions introduced in App. 9.A.3. Since the n-qubit CSP_n polytope is isomorphic to a sub-polytope of the $2n$-qubit stabiliser polytope SP_{2n}, it is possible to embed it in this way into the Euclidean space of real functions on the double phase space $2V = V \oplus V$, $f : 2V \to \mathbb{R}$ with the inner product

$$f^\top g := \sum_{v,w \in V} f(v,w) g(v,w). \tag{9.63}$$

Note that here and in the following, $V = \mathbb{F}_2^{2n}$ is the n-qubit phase space. The characteristic functions of stabiliser states are special among all functions since they have support on a Lagrangian subspace $L \subset 2V$, are ± 1-valued on L, and obey the composition law (9.43). In this representation, a CP map with Choi state ρ is trace-preserving if and only if its characteristic function $\chi_\rho : 2V \to \mathbb{R}$ fulfills the condition $\chi_\rho(0,a) = \delta_{a,0}$ for all $a \in V$. We will sometimes abuse notation and write SP_{2n} for the convex hull of characteristic functions of stabiliser states, respectively CSP_n for its subpolytope that satisfies the trace-preserving condition $\chi_\rho(0,a) = \delta_{a,0}$ for all $a \in V$.

Let $P = |0\rangle\langle 0|$. Set $\mathsf{Z}_n := \langle e_1, ..., e_n \rangle$ and $\mathsf{Z}_n^* = \mathsf{Z}_n \setminus \{0\}$. For $a \in \mathsf{Z}_n^*$ let $P_a = \frac{1}{2}(\mathbb{1} - w(a))$, where $w(a)$ is a Pauli-Z operator. We consider the channel defined in Eq. (9.16)

$$\Lambda = H^{\otimes n} P \cdot P H^{\otimes n} + \frac{1}{2^{n-1}} \sum_{a \in \mathsf{Z}_n^*} P_a \cdot P_a, \tag{9.64}$$

where H is the Hadamard-gate, acting on one qubit. The goal is to prove that this channel is extremal, in the sense that it cannot be written as a convex combination of other CSP channels. The channel Λ is an equal-weight convex combination of the maps given by $2^{n/2} H^{\otimes n} P$ and $2^{1/2} P_a$ for $a \in \mathsf{Z}_n^*$. The Choi state associated with $H^{\otimes n} P$ is simply:

$$\begin{aligned} 2^n (H^{\otimes n} P \otimes \mathbb{1}) |\phi^+\rangle\langle\phi^+| (P H^{\otimes n} \otimes \mathbb{1}) &= H^{\otimes n} \otimes \mathbb{1} |0^{2n}\rangle\langle 0^{2n}| H^{\otimes n} \otimes \mathbb{1} \\ &= |+^n\rangle\langle +^n| \otimes |0^n\rangle\langle 0^n|, \end{aligned} \tag{9.65}$$

Thus, the associated Lagrangian is $L_\xi = \mathsf{X}_n \oplus \mathsf{Z}_n$, where $\mathsf{X}_n = \langle f_1, \ldots, f_n \rangle$. Note that the corresponding characteristic function ξ is identically 1 on its support, i.e. $\xi(e,f) = 1$ for all $e \in \mathsf{Z}_n$ and $f \in \mathsf{X}_n$. Using the results from Sec. 9.C.2, we obtain the following Lagrangian for P_a:

$$L_{\xi_a} := L_a := \{(u + b, u) \mid u \in a^\perp, b \in \langle a \rangle\}. \tag{9.66}$$

For all $u \in a^\perp$, the associated characteristic function ξ_a can be computed using Eq. (9.61) and the composition law (9.29):

$$\begin{aligned} \xi_a(a,0) &= -1 \\ \xi_a(u,u) &= (-1)^{u_z \cdot u_x}, \\ \xi_a(u+a,u) &= \xi_a(a,0)\xi_a(u,u)(-1)^{\bar{\beta}(a,u)} = (-1)^{u_z \cdot u_x + \bar{\beta}(u,a) + 1}. \end{aligned} \tag{9.67}$$

At this point, let us outline our proof strategy, which relies on elementary properties of polytopes (see e. g. Ref. [165]). For an illustration, see Fig. 9.2.

(I) We construct a face F of $\mathrm{SP}_{2n} \supset \mathrm{CSP}_n$ such that $\xi_a \in F$ and every other (pure) stabiliser state $\chi \in F$ is maximally entangled. This is made precise in Lemma 9.7.

(II) We show that by adding ξ to F, we get another face $F' = \mathrm{conv}(F \cup \{\xi\})$ of SP_{2n} in the form of a pyramid. This is Lemma 9.8.

(III) By intersecting F' with the TP condition, we get a face F'_{TP} of CSP_n. This is still a pyramid with apex $\lambda := \frac{1}{2^n}(\xi + \sum_{a \in \mathbb{Z}_n^*} \xi_a)$, ensuring that the corresponding channel Λ is a vertex of the polytope CSP_n, as shown in Theorem 9.4.

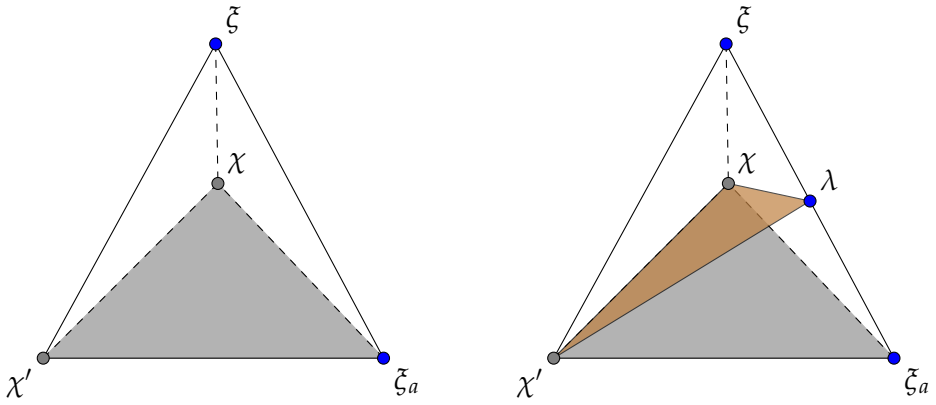


Figure 9.2: Geometrical construction for $n = 1$. The characteristic function λ is a uniform convex combination of ξ_a and ξ. The face F' is a 3-dimensional pyramid with base F (in gray) and apex ξ. F is spanned by ξ_a and additional characteristic functions χ, χ' corresponding to maximally entangled stabiliser states (in gray). After intersecting SP_2 with the TP-condition, we obtain the pyramidal face F'_{TP} (in brown) with apex λ within the polytope CSP_2. In fact, for $n = 1$, one can show the extremality of λ, using that $\mathrm{conv}(\xi, \xi_a)$ is even an edge of SP_2, without requiring an extra base face F, cp. Eqs. (9.15) and (9.18).

Remark 9.2. Note that stabiliser states with trivial right defect subspace, i.e. their characteristic function obeys $\mathrm{supp}(\chi) \cap (0 \oplus V) = \{0\}$, are exactly the maximally entangled ones. Under the Choi-Jamiołkowski isomorphism, these are in bijection with the set of Clifford unitaries.

In order to characterise the face F we define a function $\ell : V \oplus V \to \mathbb{R}$ such that

$$F = \{\chi \in \mathrm{SP}_{2n} : \ell^\top \chi = \max_{\chi' \in \mathrm{SP}_{2n}} \ell^\top \chi'\}, \tag{9.68}$$

i. e. ℓ is the normal vector of F. A crucial observation is that the characteristic functions ξ_a coincide on the intersection of their support. This can be deduced from Eq. (9.67):

$$\xi_a(u,u) = \xi_{a'}(u,u) \quad \text{for all} \quad (u,u) \in L_a \cap L_{a'} = \{(u,u) : u \in a^\perp \cap a'^\perp\}. \tag{9.69}$$

This motivates to choose ℓ in a such a way that is locally looks like the ξ_a's, more precisely, we define ℓ implicitly as follows:

(i) $\mathrm{supp}(\ell) = \cup_{a\in \mathsf{Z}_n^*} L_a$

(ii) $\ell_{|L_a} = (\xi_a)_{|L_a}$ for all $a \in \mathsf{Z}_n^*$.

The function ℓ is well-defined, because, as we have already seen, it holds $(\xi_a)_{|L_a\cap L_{a'}} = (\xi_{a'})_{|L_a\cap L_{a'}}$.

For completeness, we will explicitly state the values of ℓ, which follow from Eq. (9.67). Let $a \in \mathsf{Z}_n^*$, $e \in \mathsf{Z}_n$, $f \in \mathsf{X}_n$, and $v \in a^\perp$. Then:

$$\ell(0,a) = -1 = \ell(a,0), \tag{9.70}$$
$$\ell(e,e) = 1 = \ell(f,f), \tag{9.71}$$
$$\ell(v,v) = \xi_a(v,v) = (-1)^{v_z\cdot v_x}, \tag{9.72}$$
$$\ell(v,v+a) = \xi_a(v,v)\xi_a(0,a)(-1)^{\bar\beta(v\oplus v,0\oplus a)} = -\ell(v,v)\,(-1)^{\bar\beta(v,a)}, \tag{9.73}$$

We can reformulate Eq. (9.73) as follows: For all $a \in \mathsf{Z}_n^*$ and $v \in a^\perp$, it holds

$$\ell(v,v+a) = \ell(v,v)\ell(0,a)(-1)^{\bar\beta(v,a)}. \tag{9.74}$$

Computing the inner product of ℓ and ξ_a, we obtain $\ell^\top\xi_a = |L_a| = 2^{2n}$. Moreover, for any other stabiliser state with characteristic function χ and underlying Lagrangian subspace L_χ we have $\ell^\top\chi \le |L_\chi|$ with equality if and only if

$$L_\chi \subset \mathrm{supp}(\ell) = \cup_{a\in\mathsf{Z}_n^*} L_a \quad \text{and} \quad \ell_{|L_\chi} = \chi_{|L_\chi}. \tag{9.75}$$

Here, a crucial observation is that $\chi_{|L_\chi\cap(0\oplus\mathsf{Z}_n)}$ always induces a character on $L_\chi \cap (0\oplus \mathsf{Z}_n)$, cp. App. 9.A. However, if we look at the particular values of ℓ on $L_\chi \cap (0\oplus\mathsf{Z}_n)$, this is not the case (we have $\ell_{|L_\chi\cap(0\oplus\mathsf{Z}_n)} = 2\mathbf{1}_{(0,0)} - \mathbf{1}_{L_\chi\cap(0\oplus\mathsf{Z}_n)}$, which is certainly not a character). Based on this idea, we obtain the following lemma:

Lemma 9.7. *Let $n \ge 2$. If the characteristic function χ of a $(2n)$-qubit stabiliser state is contained in F, then $\chi = \xi_a$ for some $a \in \mathsf{Z}_n^*$, or the right defect subspace of L_χ is trivial, i.e. $L_\chi \cap (0\oplus V) = \{0\}$.*

Proof. As pointed out in (9.75), a necessary condition for χ to be in F is that $L_\chi \subset \cup_{b\in\mathsf{Z}_n^*} L_b$, so we assume that this holds for χ. Hence,

$$L_\chi \cap (0\oplus V) \subset \big(\cup_{b\in\mathsf{Z}_n^*} L_b\big) \cap (0\oplus V) = \cup_{b\in\mathsf{Z}_n^*}(0\oplus\langle b\rangle) = 0\oplus\mathsf{Z}_n. \tag{9.76}$$

First, assume that $\dim(L_\chi\cap(0\oplus V)) \ge 2$, so there is $(0,a),(0,\hat a) \in L_\chi\cap(0\oplus V)$ for $a \ne \hat a \in \mathsf{Z}_n^*$. Let $M = \langle(0,a),(0,\hat a)\rangle$. We will prove that $\chi_{|M} \ne \ell_{|M}$. Therefore, consider the values of ℓ on M:

$$\ell(0,0) = 1, \quad \ell(0,a) = -1, \quad \ell(0,\hat a) = -1, \quad \ell(0,a+\hat a) = -1. \tag{9.77}$$

This shows that ℓ does not induce a character on the additive group M. However, since $M \subset \mathsf{Z}_{2n}$ and β vanishes on Z_{2n}, χ induces a character on M, cp. App. 9.A. This proves that $\chi_{|M} \ne \ell_{|M}$.

Next, we assume that $\dim(L_\chi \cap (0 \oplus V)) = 1$, so $L_\chi \cap (0 \oplus V) = \{(0,0),(0,a)\} \subset L_a$ for some $a \in \mathsf{Z}_n^*$. Using the canonical form of Lagrangian subspaces in $V \oplus V$, derived in App. 9.C, L_χ is of the form

$$L_\chi = \{(g(u), u+b) : u \in a^\perp,\, b \in \{0,a\}\} \tag{9.78}$$

for some symplectic matrix g acting on V. In the sequel, we prove that demanding $\chi_{|L_\chi} = \ell_{|L_\chi}$ requires

$$\begin{aligned} L_\chi &= \{(g(u), u+b) : u \in a^\perp,\, b \in \{0,a\}\} \\ &= \{(u, u+b) : u \in a^\perp,\, b \in \{0,a\}\} \\ &= L_a, \end{aligned} \tag{9.79}$$

which means that the action of g leaves L_a invariant. In order to do so, we will assume $L_\chi \neq L_a$ and we will argue as in the case before, so we will construct a 2-dimensional subspace $M \subset \mathrm{supp}(\chi)$, containing the point $(0,a)$ and then prove $\chi_{|M} \neq \ell_{|M}$.

Define $s_u := g(u) + u$. If we set $b = 0$ in (9.78) and use that $L_\chi \subset \cup_{x \in \mathsf{Z}_n^*} L_x$, we see that it must hold

$$(g(u), u) = (g(u),\, g(u) + s_u) \in \cup_{x \in \mathsf{Z}_n^*} L_x \tag{9.80}$$

for all $(g(u), u) \in L_\chi$ and therefore for all u with $g(u) \neq u$

$$s_u \in \mathsf{Z}_n, \qquad g(u) \in s_u^\perp \quad \text{and} \quad (g(u), u) \in L_{s_u} \tag{9.81}$$

The idea is to show that demanding $\ell_{|L_\chi} = \chi_{|L_\chi}$ forces the generating system

$$\{(g(e), e) : e \in \mathsf{Z}_n\} \cup \{(g(f), f) : f \in \mathsf{X}_n \cap a^\perp\} \cup \{(0,a)\} \tag{9.82}$$

of L_χ to be contained in L_a. We split the argument into two parts:

(a) Assume that $(g(e), e) \in L_\chi \setminus L_a$ for some $e \in \mathsf{Z}_n$. Note that by Eq. (9.81), we have $(g(e), e) \in L_{s_e}$ and by assumption $s_e \notin \{0, a\}$.

Let $M = \langle (g(e), e), (0, a) \rangle$. The goal is to prove that $\ell_{|M} \neq \chi_{|M}$. Therefore, consider the values of ℓ on M:

1. $\ell(0,0) = 1$
2. $\ell(0,a) = -1$
3. To evaluate ℓ at $(g(e), e)$, note that $g(e) = e + s_e$, hence $g(e) \in \mathsf{Z}_n$. We obtain from Eq. (9.74):

$$\ell(g(e), e) = \ell(g(e),\, g(e) + s_e) = \ell(g(e),\, g(e)) \cdot \ell(0, s_e) = -1. \tag{9.83}$$

4. For $(g(e), e+a)$ we obtain, using $s_e + a \in \mathsf{Z}_n$:

$$\ell(g(e),\, e+a) = \ell(g(e),\, g(e) + s_e + a) = -1. \tag{9.84}$$

The assigned values show that ℓ does not induce a character for the additive group $M \subset \mathsf{Z}_{2n}$. However, as argued before, β vanishes on Z_{2n} and thus $\chi_{|M}$ is a character for M, proving that $\ell_{|M} \neq \chi_{|M}$.

(b) Next, assume that $(g(f), f) \in L_\chi \setminus L_a$ for some $f \in \mathsf{X}_n$. We define $e := s_f = g(f) + f \in \mathsf{Z}_n$, hence

$$(g(f), f) = (f + e, f) \tag{9.85}$$

with $f \in e^\perp$. As $(g(f), f) \notin L_a$, it follows that $e \notin \{0, a\}$.

Analogously to case (a), let $M = \langle (g(f), f), (0, a) \rangle$.

We will show that, again, $\chi_{|M} \neq \ell_{|M}$. The values of ℓ on M are given by

1. $\ell(0, 0) = 1$
2. $\ell(0, a) = -1$
3. Consider $(g(f), f)$. By first applying Eq. (9.73) and using that $f + e \in e^\perp$, we obtain

$$\begin{aligned} \ell(g(f), f) &= \ell(f + e,\, (f + e) + e) \\ &= \ell(f + e,\, f + e) \cdot \ell(0, e) \cdot (-1)^{\bar{\beta}(f,e)} \\ &= -(-1)^{f_x \cdot e_z} \cdot (-1)^{\bar{\beta}(f,e)} \\ &= -(-1)^{\bar{\beta}(f,e)}, \end{aligned} \tag{9.86}$$

   where we used in the fourth equation that $f \in e^\perp$, so $0 = [f, e] = f_x \cdot e_z$.
4. For $(g(f), f + a)$ we obtain analogously, since $f + e \in (e + a)^\perp = e^\perp \cap a^\perp$

$$\begin{aligned} \ell(g(f), f + a) &= \ell(f + e, (f + e) + (e + a)) \\ &= -(-1)^{\bar{\beta}(f, e+a)}. \end{aligned} \tag{9.87}$$

Note that the above properties hold for any pair $(g(f), f) \notin L_a$. As we will show in a moment, the existence of such a pair implies the existence of another pair $(g(\hat{f}), \hat{f}) = (\hat{f} + \hat{e}, \hat{f}) \notin L_a$ such that

$$\beta(\hat{f}, \hat{e}) + \beta(\hat{f}, a) = \beta(\hat{f}, \hat{e} + a). \tag{9.88}$$

Applying the previous results to this pair with $\hat{M} = \langle (0, a), (g(\hat{f}), \hat{f}) \rangle$, demanding $\chi_{|\hat{M}} = \ell_{|\hat{M}}$ would imply $\chi(0, a) = -1$ and $\chi(g(\hat{f}), \hat{f}) = -(-1)^{\bar{\beta}(\hat{f}, \hat{e})}$. However, by the the composition law (9.29) that needs to hold for χ:

$$\chi((g(\hat{f}), \hat{f}) + (0, a)) = (-1)^{\bar{\beta}(\hat{f}, a)} \cdot \chi(g(\hat{f}), \hat{f}) \cdot \chi(0, a) \tag{9.89}$$

$$= (-1)^{\bar{\beta}(\hat{f}, a)} \cdot (-1)^{\bar{\beta}(\hat{f}, \hat{e})} = (-1)^{\bar{\beta}(\hat{f}, \hat{e} + a)}, \tag{9.90}$$

which does not coincide with $\ell((g(\hat{f}), \hat{f}) + (0, a)) = -(-1)^{\bar{\beta}(\hat{f}, \hat{e}+a)}$, so $\chi_{|\hat{M}} \neq \ell_{|\hat{M}}$. As a consequence, $\chi_{|L_\chi} = \ell_{|L_\chi}$ requires that any pair $(g(f), f) \in L_\chi$ is contained in L_a and thus of the form (f, f) or $(f + a, f)$.

Finally, we show that a pair $(g(\hat{f}), \hat{f})$ satisfying the bilinearity condition (9.88) exists. Since $f \in \mathsf{X}_n$, $e, a \in \mathsf{Z}_n$, we have by Eq. (9.32),

$$\begin{aligned} \beta(f, e) &= \Omega(f, e) = f_x \cdot e_z \pmod 4 \\ \beta(f, a) &= \Omega(f, a) = f_x \cdot a_z \pmod 4 \\ \beta(f, e + a) &= \Omega(f, e + a) = f_x \cdot (e + a)_z \pmod 4. \end{aligned} \tag{9.91}$$

We define the sets

$$M_e = \{i : f_x(i) = e_z(i) = 1\}, \qquad M_a = \{i : f_x(i) = a_z(i) = 1\}. \tag{9.92}$$

Considered as integer vectors, the (Euclidean) inner products are $f_x \cdot e_z = |M_e|$ and $f_x \cdot a_z = |M_a|$. If we consider the inner product of f_z and $(e+a)_x$, we obtain

$$f_x \cdot (e+a)_z = |M_e| + |M_a| - 2|M_e \cap M_a|. \tag{9.93}$$

Therefore, $\beta(f,e) + \beta(f,a) = \beta(f,e+a)$ if $|M_e \cap M_a|$ is even. So we have to prove that there exists an e, where this is indeed the case. In order to show this property we will derive some restrictions on the symplectic map g.

First, suppose that $|M_e \cap M_a|$ is odd. Let $\hat{f} \in (a^\perp \setminus e^\perp) \cap \mathsf{X}_n$, which is not empty by assumption. Then, $g(\hat{f}) \neq \hat{f}$, because otherwise we would have $g(\hat{f}+f) = \hat{f} + f + e$, which cannot be the case, as $\hat{f} + f \notin e^\perp$, contradicting Eq. (9.81). Hence, we can assume that $g(\hat{f}) = \hat{f} + \hat{e}$ for some $\hat{e} \neq 0$ and $\hat{f} \in \hat{e}^\perp$. Note that by assumption $\hat{f} \notin e^\perp$, thus $\hat{e} \neq e$. Moreover, since g is a symplectic map, we have

$$0 = [\hat{f}, f] = [g(\hat{f}), g(f)] = [\hat{f} + \hat{e},\, f + e] = [\hat{f}, e] + [\hat{e}, f], \tag{9.94}$$

forcing $1 = [\hat{f}, e] = [\hat{e}, f]$. Since $[f, a] = 0$, we have $\hat{e} \neq a$ and hence, we have found another pair $(g(\hat{f}), \hat{f}) \notin L_a$.

Now, if $|M_{\hat{e}} \cap M_a|$ is even, we are done. If not, choose the pair $(g(f+\hat{f}), f+\hat{f})$ with $g(f+\hat{f}) = f + \hat{f} + e + \hat{e}$. Note that we have $e + \hat{e} \neq 0$ and $e + \hat{e} \neq a$ since the converse would imply that $1 = [\hat{e}, f] = [e, f] + [a, f] = 0$. Again, this implies that we have found a pair $(g(f+\hat{f}), f+\hat{f}) \notin L_a$. Finally, $|M_a \cap M_{e+\hat{e}}|$ is even since

$$|M_a \cap M_{e+\hat{e}}| = |M_e \cap M_a| + |M_{\hat{e}} \cap M_a| - 2|M_e \cap M_{\hat{e}}| \tag{9.95}$$

is even when the first two summands on the right hand side are odd.

In summary, we have shown that $\chi_{|L_\chi} = \ell_{|L_\chi}$ requires that $L_\chi = L_a$ for some $a \in \mathsf{Z}_n^*$ when $\dim(L_\chi \cap (0 \oplus V)) \geq 1$. This finishes the proof. □

We proceed now with step (II) of our proof strategy. Recall that ξ is the characteristic function of the Choi state $|+^n\rangle \otimes |0^n\rangle$ of the first Kraus operator $H^{\otimes n}\, |0^n\rangle\langle 0^n|$ appearing in our channel, Eq. (9.64), and $L_\xi = \mathrm{supp}(\xi) = \mathsf{X}_n \oplus \mathsf{Z}_n$ is the associated Lagrangian.

In the next step, we prove that the set

$$F' := \mathrm{conv}(F \cup \{\xi\}) \tag{9.96}$$

is a face of SP_{2n} in the form of a *pyramid* with base F and apex ξ (the "tip" of the pyramid). The latter statement can be readily verified by evaluating ℓ on ξ:

$$\begin{aligned} \ell^\top \xi = \sum_{(u,v) \in L_\xi \cap \mathrm{supp}(\ell)} \ell(u,v) \cdot \xi(u,v) &= \sum_{a \in \mathsf{Z}_n} \ell(0,a) \cdot \xi(0,a) \\ &= 1 - \sum_{a \in \mathsf{Z}_n^*} 1 \\ &= -2^n + 2 \\ &< 2^{2n}. \end{aligned} \tag{9.97}$$

Thus, ξ does not lie in the hyperplane defined by $\{\chi : \ell^\top \chi = 2^{2n}\}$ which contains the face F and the polytope F' has the form of a pyramid.

In the following, we again construct a linear function ℓ' that is constant on the pyramid F'. To this end, we modify the old function ℓ on

$$L_\xi \setminus \operatorname{supp}(\ell) = (\mathsf{X}_n \oplus \mathsf{Z}_n) \setminus (0 \oplus \mathsf{Z}_n) = \mathsf{X}_n^* \oplus \mathsf{Z}_n. \tag{9.98}$$

We define ℓ' via

(i) $\operatorname{supp}(\ell') = L_\xi \cup \operatorname{supp}(\ell) = L_\xi \cup \big(\cup_{a \in \mathsf{Z}_n^*} L_a\big)$,

(ii) $\ell'_{|\operatorname{supp}(\ell)} := \ell_{|\operatorname{supp}(\ell)}$,

(iii) $\ell'(u,v) := C := \frac{2^{2n}+2^n-2}{2^{2n}-2^n} = 1 + 2^{1-n} \quad \forall (u,v) \in L_\xi \setminus \operatorname{supp}(\ell) = \mathsf{X}_n^* \oplus \mathsf{Z}_n$.

Then, $\ell'^\top \chi = 2^{2n}$ for all stabiliser states χ that are vertices of F and $\ell'^\top \xi = 2^{2n}$, hence ℓ' is constant on F'.

Lemma 9.8. *For $n \geq 2$, it holds that $F' = \{\chi \in \mathrm{SP}_{2n} : \ell'^\top \chi = \max_{\chi' \in \mathrm{SP}_{2n}} \ell'^\top \chi'\}$. Consequently, F' is a face of SP_{2n}.*

Intuitively speaking, a Lagrangian subspace L_ξ and $\operatorname{supp}(\ell) = \cup_{b \in \mathsf{Z}_n^*} L_b$ intersect in a relatively small subspace of size 2^n, whereas $|\operatorname{supp}(\ell)| \geq |L_\xi| \geq 4^n$.

To achieve a large inner product of a characteristic function χ with associated Lagrangian L and the linear function ℓ', it is necessary that L has a large overlap with $\operatorname{supp}(\ell')$. However, if we take some Lagrangian L, its intersection with $\operatorname{supp}(\ell')$ splits roughly into two almost disjoint parts, $L \cap L_\xi$ and $L \cap \operatorname{supp}(\ell)$.

Hence, if we demand that L and $\operatorname{supp}(\ell')$ have a large overlap, we require that either the intersection with L_ξ or with $\operatorname{supp}(\ell')$ is large. In fact, we will prove that L needs to be even contained in one of these two sets for a sufficiently large overlap (and $n \geq 3$) . Then, given a characteristic function χ on $L = L_\xi$, the inner product $\ell'^\top \chi$ cannot be too large, since ξ and χ must be orthogonal and ℓ' differs from ξ only on a small fraction of L_ξ. If instead $L \subset \operatorname{supp}(\ell)$, then Lemma 9.7 implies that χ is already a vertex of F.

Proof. Let χ be the characteristic function of a $(2n)$-qubit stabiliser state. To prove that F' is indeed a face of SP_{2n}, we must show that $\ell'^\top \chi < 2^{2n}$ if $\chi \notin F'$.

First, assume that $\operatorname{supp}(\chi) = L_\chi = L_\xi$ and $\chi \neq \xi$. To compute the inner product $\ell'^\top \chi$, we divide it into a sum over $L_\xi \setminus \operatorname{supp}(\ell) = \mathsf{X}_n^* \oplus \mathsf{Z}_n$ and one over $L_\xi \cap \operatorname{supp}(\ell) = 0 \oplus \mathsf{Z}_n$. On the former set, $\ell'(u,v) = C$, on the latter one $\ell'(0,z) = \ell(0,z) = -1$ for $z \neq 0$ and $\ell'(0,0) = 1$. Therefore, we find

$$\begin{aligned} \ell'^\top \chi &= C \sum_{x \in \mathsf{X}_n^*, z \in \mathsf{Z}_n} \chi(x,z) - \sum_{z \in \mathsf{Z}_n^*} \chi(0,z) + 1 \\ &= C\big|\{x \in \mathsf{X}_n^*, z \in \mathsf{Z}_n : \chi(x,z) = 1\}\big| \\ &\quad - C\big|\{x \in \mathsf{X}_n^*, z \in \mathsf{Z}_n : \chi(x,z) = -1\}\big| - \sum_{z \in \mathsf{Z}_n^*} \chi(0,z) + 1. \end{aligned} \tag{9.99}$$

Since different stabiliser states associated to the same Lagrangian are orthogonal, we have $\chi^\top \xi = 0$. Thus, there are 2^{2n-1} coordinates in L_χ where χ and ξ coincide, i.e. $\chi = 1$,

and 2^{2n-1} where they have opposite signs, $\chi = -1$. Thus, we can upper bound $\ell'^{\top}\chi$ by noting that in the worst case all $\chi(0,z) = -1$. Then, the first set contains all positive points (except the origin) and thus has cardinality $2^{2n-1}-1$. The one of the second set is therefore $2^{2n-1}-2^n+1$:

$$\begin{aligned}\ell'^{\top}\chi &\leq C\left(2^{2n-1}-1-(2^{2n-1}-2^n+1)\right)+2^n \\ &= 2^n(C+1)-2C \\ &= 2^{1-n}(4^n-2) < 2^{2n},\end{aligned} \tag{9.100}$$

for all $n \in \mathbb{N}$. Hence, $\chi \notin F'$.

Next, assume that χ is a $(2n)$-qubit stabiliser state such that $L_\chi \nsubseteq L_\xi$ and $L_\chi \nsubseteq \mathrm{supp}(\ell) = \cup_{b\in \mathsf{Z}_n^*} L_b$ (the cases, where L_χ is contained in one of these two sets were treated above, respectively in Lemma 9.7). We claim that the intersection

$$I := L_\chi \cap (\cup_{b\in \mathsf{Z}_n^*} L_b) \tag{9.101}$$

is closed under addition, i.e. a subspace. In order to see this, assume that there are $(u, u+a), (u', u'+a') \in I$ with $u \in a^\perp$, $u' \in a'^\perp$ and $a, a' \in \mathsf{Z}_n$. We have to show that $(u+u',\ u+u+(a+a'))$ is contained in $\cup_{b\in \mathsf{Z}_n^*} L_b$. It suffices to prove that $u+u' \in (a+a')^\perp$. Since L_χ is isotropic, we have

$$0 = [(u, u+a),\ (u', u'+a')] = [u,u'] + [u+a,\ u'+a'] = [u,a'] + [u',a] = [u+u',\ a+a'], \tag{9.102}$$

where we used in the last equation that $u \in a^\perp$ and $u' \in a'^\perp$.

Write the intersection of L_χ with $\mathrm{supp}(\ell') = L_\xi \cup (\cup_{b\in \mathsf{Z}_n^*} L_b)$ as $L_\chi \cap \mathrm{supp}(\ell') = I \cup J$, using (by assumption nontrivial) subspaces I and

$$J := L_\chi \cap L_\xi. \tag{9.103}$$

Set $k_I = \dim I$ and $k_J = \dim J$. Since $L_\chi \nsubseteq L_\xi$ and $L_\chi \nsubseteq \mathrm{supp}(\ell) = \cup_{b\in \mathsf{Z}_n^*} L_b$, it holds $k_I, k_J \leq 2n-1$.

The intersection of $I \cap J$ is contained in $(\cup_{b\in \mathsf{Z}_n^*} L_b) \cap L_\xi = 0 \oplus \mathsf{Z}_n$, hence $\dim(I\cap J) \leq n$. Furthermore, $I, J \subset L_\chi$, so $\dim(\langle I, J\rangle) \leq 2n$. Combining these upper bounds on the dimension, we obtain

$$k_I + k_J = \dim I + \dim J = \dim(\langle I, J\rangle) + \dim(I\cap J) \leq 2n + n = 3n. \tag{9.104}$$

Note that $\ell'_{|J\setminus \mathrm{supp}(\ell)} \equiv C$ and $|\ell'_{|I}| \equiv 1$. Thus, we can bound the evaluation of ℓ' on χ by

$$\ell'^{\top}\chi \leq |I| + C|J| \leq |I| + C|J| - |I\cap J| \leq 2^{k_I} + 2^{k_J}C. \tag{9.105}$$

For the case $n \geq 2$ we distinguish two cases:

1. Let $k_J \leq n+1$. Due to $k_I \leq 2n-1$, we can upper bound $\ell'^{\top}\chi$ in (9.105) (using $C = 1+2^{1-n}$) by

$$2^{k_I} + 2^{k_J}C \leq 2^{2n-1} + 2^{n+1}(1+2^{1-n}) < 2^{2n-1} + 2^{2n-1} = 2^{2n} \tag{9.106}$$

for $n \geq 3$.

2. Let $n+2 \leq k_J \leq 2n-1$. In this case, due to $k_I \leq 3n - k_J$, we can upper bound $\ell'^{\top}\chi$ in (9.105) by

$$\begin{aligned} 2^{k_I} + 2^{k_J}C \leq 2^{3n-k_J} + 2^{k_J}C \leq 2^{3n-(n+2)} + 2^{2n-1}C &= 2^{2n-2}(1+2C) \\ &= 2^{2n-2}(3+2^{2-n}) \\ &< 2^{2n} \end{aligned} \tag{9.107}$$

for $n \geq 3$.

The case $n = 2$ requires a slightly more careful analysis. If $k_I, k_J \leq 2$, then Eq. (9.105) yields directly that $\ell'^{\top}\chi < 2^{2\cdot 2}$. If $k_J = 3$ and $k_I = 2$, then $\dim(I \cap J) \geq 1$, due to $\dim(\langle I, J\rangle) \leq 4$. By Inequality (9.105), it follows

$$\ell'^{\top}\chi \leq |I| + C|J| - |I \cap J| = 2^2 + C2^3 - 2 = 4 + \frac{3}{2}8 - 2 = 14 < 2^4, \tag{9.108}$$

where we used that $C = \frac{3}{2}$. Analogously, we find that $\ell'^{\top}\chi < 2^4$ if $k_J = 2$ and $k_I = 3$.

It remains the case $k_I = k_J = 3$. Here, we have $\dim(I \cap J) \geq 2$, but as $I \cap J \subset 0 \oplus \mathsf{Z}_2$, it follows that $I \cap J = 0 \oplus \mathsf{Z}_2$. We upper bound $\ell'^{\top}\chi$ via

$$\begin{aligned} \ell'^{\top}\chi &= (\ell'_{|(I\cap J)})^{\top}\chi_{|(I\cap J)} + (\ell'_{|(J\setminus I)})^{\top}\chi_{|(J\setminus I)} + (\ell'_{|(I\setminus J)})^{\top}\chi_{|(I\setminus J)} \\ &\leq (\ell'_{|(I\cap J)})^{\top}\chi_{|(I\cap J)} + C(2^3 - 2^2) + (2^3 - 2^2) \\ &= (\ell'_{|(I\cap J)})^{\top}\chi_{|(I\cap J)} + 10. \end{aligned} \tag{9.109}$$

However, this is strictly smaller than 2^4 because the first summand in the last line is smaller than 2. To this end, note that $\ell'_{|(I\cap J)} = 2\mathbf{1}_{(0,0)} - \mathbf{1}_{0\oplus\mathsf{Z}_2}$ and since $\chi_{|(I\cap J)}$ induces a character on $0 \oplus \mathsf{Z}_2$, it follows that

$$(\ell'_{|(I\cap J)})^{\top}\chi_{|(I\cap J)} = (2\mathbf{1}_{(0,0)} - \mathbf{1}_{0\oplus\mathsf{Z}_2})^{\top}\chi_{|I\cap J} \leq 2. \tag{9.110}$$

In summary, for $\ell'^{\top}\chi = 2^{2n}$ it is required that $\chi = \xi$ or $\chi \in F$, which finishes the proof. □

Finally, we turn to the last step (III) of our proof. Starting with the face F' of SP_{2n}, we can construct a face F'_{TP} of the CSP_n polytope by intersecting F' with the affine subspaces given by the TP condition. Recall that in terms of characteristic functions, this condition is $x(0,a) = \delta_{a,0}$ for all $a \in V$. Then, the following theorem states that the channel Λ is a vertex of CSP_n.

Theorem 9.4. *The point*

$$\lambda := \frac{1}{2^n}\Big(\xi + \sum_{a\in\mathsf{Z}_n^*} \xi_a\Big) \tag{9.111}$$

is a vertex of the n-qubit CSP polytope. More precisely, for $n \geq 2$, the face $F'_{TP} := \mathrm{CSP}_n \cap F'$ of CSP_n is a pyramid with apex λ and base $\mathrm{CSP}_n \cap F$.

The theorem immediately implies that the quantum channel Λ, defined in Eq. (9.16), is an extremal CSP map. This holds since λ is simply the characteristic function of the Choi state associated with Λ.

Proof. The case $n = 1$ was already discussed in Sec. 9.3.2 of the main body of this work. Thus, let us assume that $n \geq 2$. By construction, we have $\lambda(0,a) = \xi(0,a) - \xi_a(0,a) = 1 - 1 = 0$ for all $a \in V$, hence, $\lambda \in \mathrm{CSP}_n$. Let $\chi \in F'$. By applying Lemmata 9.7 and 9.8, we can write χ as a convex combination of vertices of F', i.e.,

$$\chi = c\xi + \sum_{a \in \mathsf{Z}_n^*} c_a \xi_a + \sum_b \tilde{c}_b \eta_b, \qquad c + \sum_{a \in \mathsf{Z}_n^*} c_a + \sum_b \tilde{c}_b = 1, \tag{9.112}$$

where the second summand ranges over all stabiliser states $\eta_b \in F$ such that $\mathrm{supp}(\eta_b) \cap (0 \oplus V) = \{0\}$ (cp. Lem. 9.7). Evaluating χ at a coordinate $(0,a) \in 0 \oplus V$, we obtain

$$\chi(0,a) = \begin{cases} c - c_a, & \text{if } a \in \mathsf{Z}_n^* \\ 1, & \text{if } a = 0 \\ 0, & \text{otherwise.} \end{cases} \tag{9.113}$$

So, $\chi(0,a) = 0$ for all $a \in \mathsf{Z}_n^*$ requires that $c_a = c$ for all $a \in \mathsf{Z}_n^*$, i.e. $c\xi + \sum_{a \in \mathsf{Z}_n^*} c_a \xi_a = \alpha\lambda$ for some $0 \leq \alpha \leq 1$. In summary, any $\chi \in F'_{TP}$ is of the form

$$\chi = \alpha\lambda + \sum_b \tilde{c}_b \eta_b, \tag{9.114}$$

where $\alpha, \tilde{c}_b \geq 0$ and $\alpha + \sum_b \tilde{c}_b = 1$. Note that $\lambda \notin \mathrm{conv}\{\xi_b\}$, as λ can be separated from $\mathrm{conv}\{\eta_b\}$ by the hyperplane that defines the face F, i.e. $\{\chi : \ell^\top \chi = 2^{2n}\}$. We conclude that the face F'_{TP} is a pyramid with apex λ and base $\mathrm{conv}\{\eta_b\} = \mathrm{CSP}_n \cap F$, which holds, since no convex combination of the $\xi_a \in F$ ($a \in \mathsf{Z}_n^*$) fulfills the TP condition.

Finally, since F'_{TP} is a face of CSP_n, the point λ is a vertex of CSP_n. □

9.E Proof that $\mathrm{SO}_1 = \mathrm{CSP}_1$

Theorem 9.5. *Let $\mathcal{E} \in \mathrm{CSP}_1$ be an extremal CSP map. Then either $\mathcal{E} = U \cdot U^\dagger$ for some Clifford unitary U or $\mathcal{E}$ is of the form*

$$\mathcal{E} = U_1 P^+ \cdot P^+ U_1^\dagger + U_2 P^- \cdot P^- U_2^\dagger, \tag{9.115}$$

where $\{P^+, P^-\}$ are projectors on the eigenspaces of a Pauli matrix and U_1, U_2 are Clifford unitaries. Since such a channel $\mathcal{E}$ can be realised via stabiliser operations, it follows $\mathrm{SO}_1 = \mathrm{CSP}_1$.

Proof. Let χ be the characteristic function of the Choi state of a CSP map $\mathcal{E}$. If χ is the characteristic function of a maximally entangled 2-qubit stabiliser state, it follows immediately that $\mathcal{E} = U \cdot U^\dagger$ for some Clifford unitary U. If this is not the case, χ can be decomposed in a convex combination of characteristic functions of stabiliser states,

$$\chi = \sum_b \hat{c}_b \eta_b + \sum_a c_a \xi_a, \tag{9.116}$$

where the Lagrangian subspaces $L_b = \mathrm{supp}\,(\eta_b)$ have trivial right defect subspaces and the Lagrangian subspaces $L_a = \mathrm{supp}\,(\xi_a)$ have 1-dimensional right defect subspaces

(note that the corresponding stabiliser states are separable for $n = 1$). Since χ can be written as a convex combination

$$\chi = \left(\sum_b \hat{c}_b\right) \underbrace{\frac{1}{\sum_b \hat{c}_b} \sum_b \hat{c}_b \eta_b}_{\in \mathrm{CSP}_1} + \left(\sum_a c_a\right) \underbrace{\frac{1}{\sum_a c_a} \sum_a c_a \xi_a}_{\in \mathrm{CSP}_1}, \tag{9.117}$$

it follows that χ can only be extremal when the first sum is empty. Hence, we can assume $\chi = \sum_a c_a \eta_a$. Let $M \subset \mathbb{F}_2^2$ be the set of points such that for all $u \in M$, there is a with $L_a \cap (0 \oplus \mathbb{F}_2^2) = \{(0,0),(0,u)\}$. Now we can decompose ξ further as

$$\chi = \sum_{u \in M} \sum_{a:(0,u)\in L_a} c_a \xi_a. \tag{9.118}$$

We can argue as before and χ is a convex combination of $|M|$ points

$$\frac{1}{\sum_{a:(0,u)\in L_a} c_a} \sum_{a:(0,u)\in L_a} c_a \xi_a \in \mathrm{CSP}_1 \tag{9.119}$$

and χ can only be extremal if $M = \{u\}$ for some $u \in \mathbb{F}_2^2 \setminus 0$. Define

$$A^+ = \{a : \xi_a(0,u) = 1\}, \quad A^- = \{a : \xi_a(0,u) = -1\} \tag{9.120}$$

and write χ as a convex combination

$$\chi = \sum_{a \in A^+} c_a \xi_a + \sum_{a \in A^-} c_a \xi_a. \tag{9.121}$$

Since $\chi \in \mathrm{CSP}_1$, we have

$$\sum_{a \in A^+} c_a = \sum_{a \in A^-} c_a, \quad \text{and} \quad 1 = \sum_{a \in A^+} c_a + \sum_{a \in A^-} c_a. \tag{9.122}$$

Next, we consider the smallest coefficient in the decomposition of χ which we can assume to be c_{a^+} for some $a^+ \in A^+$. Choose any $a^- \in A^-$. Then, χ can be written as a convex combination

$$\chi = (2c_{a^+}) \underbrace{\frac{1}{2}(\xi_{a^+} + \xi_{a^-})}_{\in \mathrm{CSP}_1} + (1 - 2c_a^+) \underbrace{\frac{1}{1-2c_a^+}\Big((c_{a^-} - c_{a^+})\xi_{a^-} + \sum_{a \in A^+ \setminus a^+} c_a \xi_a + \sum_{a \in A^- \setminus a^-} c_a \xi_a\Big)}_{=:\tilde{\chi} \in \mathrm{CSP}_1}. \tag{9.123}$$

The second term $\tilde{\chi}$ has the form

$$\tilde{\chi} = \sum_{a \in \tilde{A}^+} \tilde{c}_a \xi_a + \sum_{a \in \tilde{A}^-} \tilde{c}_a \xi_a, \tag{9.124}$$

for $\tilde{A}^+ := A^+ \setminus a^+$, $\tilde{A}^- := A^-$ and $\tilde{c}_a \geq 0$. In particular,

$$\sum_{a \in \tilde{A}^+} \tilde{c}_a + \sum_{a \in \tilde{A}^-} \tilde{c}_a = \frac{1}{1-2c_{a^+}} \left(\sum_{a \in A^+ \setminus a^+} c_a + c_{a^-} - c_{a^+} + \sum_{a \in A^- \setminus a^-} c_a \right) \tag{9.125}$$

$$= \frac{1}{1-2c_{a^+}} (1 - 2c_{a^+}) = 1, \tag{9.126}$$

$$\sum_{a \in \tilde{A}^+} \tilde{c}_a - \sum_{a \in \tilde{A}^-} \tilde{c}_a = \frac{1}{1-2c_{a^+}} \left(\sum_{a \in A^+ \setminus a^+} c_a + c_{a^+} - \sum_{a \in A^- \setminus a^-} c_a - c_{a^-} \right) = 0. \tag{9.127}$$

Thus, $\tilde{\chi} \in \mathrm{CSP}_1$ as claimed. We can now iterate this scheme and further decompose $\tilde{\chi}$ in the same fashion by taking the smallest coefficient from $\tilde{A}^+ \cup \tilde{A}^-$. The iteration stops when $|A^+| = |A^-| = 1$.

It follows that χ can only be extremal if

$$\chi = \frac{1}{2}(\xi^+ + \xi^-), \qquad \xi^\pm(0,u) = \pm 1. \tag{9.128}$$

Here, $\mathrm{supp}(\xi^+)$ and $\mathrm{supp}(\xi^-)$ have both right defect subspace $\langle u \rangle$, and hence the corresponding stabiliser states are of the form

$$U_1(\mathbb{1} + w(u)) \otimes \mathbb{1} \big| \phi^+ \big\rangle, \quad U_2(\mathbb{1} - w(u)) \otimes \mathbb{1} \big| \phi^+ \big\rangle \tag{9.129}$$

for Clifford unitaries U_1, U_2 and the corresponding channel $\mathcal{E}$ is of the form (9.115). □

9.F Analysis of the channel decomposition of Λ

First, let us compute the representation of

$$\Lambda := \mathrm{Ad}(H^{\otimes n} P) + \frac{1}{2^{n-1}} \sum_{a \in \mathsf{Z}_n} \mathrm{Ad}(P_a) \tag{9.130}$$

in the computational basis. Write $a = (z, 0) \in \mathsf{Z}_n^*$ and note that $P_a = (\mathbb{1} - Z(z))/2$ projects onto the span of computational basis states $|x\rangle$ with $x \cdot z \neq 0$. Thus, $P_a \, |x\rangle\langle y| \, P_a$ is zero if x or y is orthogonal to z and $|x\rangle\langle y|$ otherwise. For any $x \neq 0$, the linear equation $x \cdot z = 1$ has exactly 2^{n-1} solutions $z \in \mathbb{F}_2^n$. Since the first term in Eq. (9.16) yields 0, we get $\Lambda(|x\rangle\langle x|) = |x\rangle\langle x|$ for any $x \neq 0$. Furthermore, adding the condition $y \cdot z = 1$ for any $y \notin \{0, x\}$ will further half the solution space, yielding 2^{n-2} vectors which are not orthogonal to both x and y. Thus, given two non-zero vectors $x \neq y$, we get $\Lambda(|x\rangle\langle y|) = \frac{1}{2} |x\rangle\langle y|$. In summary, the action on an arbitrary density matrix $\rho = \sum_{x,y} \rho_{xy} \, |x\rangle\langle y|$ is

$$\Lambda(\rho) = \rho_{00} \, |+\rangle\langle +| + \sum_{x \neq 0} \rho_{xx} \, |x\rangle\langle x| + \frac{1}{2} \sum_{x \neq y \neq 0} \rho_{xy} \, |x\rangle\langle y| \, . \tag{9.131}$$

Now consider the channel $\tilde{\Lambda}$, that realises block diagonalisation followed by a global Hadamard conditioned on '0" (cp. Sec. 9.3.3). The channel $\tilde{\Lambda}$ can be expressed by removing the $\frac{1}{2}$ from the last summand of Eq. (9.131), so

$$\tilde{\Lambda}(\rho) = \rho_{00} \, |+\rangle\langle +| + 2 \left[\sum_{x \neq 0} \rho_{xx} \, |x\rangle\langle x| + \frac{1}{2} \sum_{x \neq y \neq 0} \rho_{xy} \, |x\rangle\langle y| \right] - \sum_{x \neq 0} \rho_{xx} \, |x\rangle\langle x| \, . \tag{9.132}$$

In terms of the original stabiliser codes, we can write this as

$$\tilde{\Lambda} = \mathrm{Ad}(H^{\otimes n} P) + 2 \frac{1}{2^{n-1}} \sum_{a \in \mathsf{Z}_n} \mathrm{Ad}(P_a) - \sum_{x \neq 0} \mathrm{Ad}(|x\rangle\langle x|). \tag{9.133}$$

Using the representation of $\tilde{\Lambda}$ in (9.133), we are able to derive the characteristic function of the Choi state of $\tilde{\Lambda}$ by using the results from the last section. Note that the Choi state

of $|x\rangle\langle x|$ is simply $2^{-n/2}\,|xx\rangle$ with characteristic function given by $2^{-n}(-1)^{x\cdot e+x\cdot e'}$ for a point (e,e') on its support $\mathsf{Z}_n\oplus\mathsf{Z}_n$. Hence, the overall characteristic function of the last term in (9.133) is

$$\nu(e,e')=2^{-n}\sum_{x\neq 0}(-1)^{x\cdot e+x\cdot e'}=2^{-n}\sum_{x\in\mathbb{F}_2^n}(-1)^{x\cdot(e+e')}-2^{-n}=\delta_{e,e'}-2^{-n}. \tag{9.134}$$

Here, we used that the sum in the second step is only non-zero if $e=e'$ and equals 2^n in this case. Finally, we find that the characteristic function of $\tilde{\Lambda}$ is

$$\tilde{\lambda}=\frac{1}{2^n}\left(\xi+2\sum_{a\neq 0}\xi_a\right)-\nu. \tag{9.135}$$

Let us evaluate ℓ' from the last section on this. Since we already know that $\ell'^{\top}\chi\leq\ell'^{\top}\xi=\ell'^{\top}\xi_a=2^{2n}$ for all $\chi\in\mathrm{SP}_{2n}$, we only have to compute the action on ν.

$$\begin{aligned}\ell'^{\top}\nu&=\sum_{e\in\mathsf{Z}_n}\ell(e,e)\nu(e,e)+\sum_{e\neq e'\in\mathsf{Z}_n}\ell(e,e')\nu(e,e')\\&=(2^n-1)+2^{-n}(2^{2n}-2^n)\\&=2\,(2^n-1)\,.\end{aligned} \tag{9.136}$$

Hence, we get

$$\ell'^{\top}\tilde{\lambda}=2^n+2\cdot 2^n(2^n-1)-2(2^n-1)=2^{2n}\left(2-3\cdot 2^{-n}+2^{-2n}\right). \tag{9.137}$$

It is straightforward to check that the expression in the parenthesis is exactly 1 for $n=1$ and >1 for $n\geq 2$, so $\ell'^{\top}\nu>2^{2n}$ for $n\geq 2$. Since $\{\chi:\ell'^{\top}\chi\leq 2^{2n}\}$ defines a face for the CSP polytope, $\tilde{\Lambda}$ is not CSP for $n\geq 2$.

Next, we show that the channel $\bar{\Lambda}$, that only realises block-diagonalisation is generally non-stabiliser preserving, too. By leaving out the Hadamard gate in Eq. (9.133) we get

$$\bar{\Lambda}=\mathrm{Ad}(P)+2\frac{1}{2^{n-1}}\sum_{a\in\mathsf{Z}_n}\mathrm{Ad}(P_a)-\sum_{x\neq 0}\mathrm{Ad}(\,|x\rangle\langle x|\,). \tag{9.138}$$

Similarly to before, the characteristic function becomes

$$\bar{\lambda}=\frac{1}{2^n}\left(\mathbf{1}_{\mathsf{Z}_{2n}}+2\sum_{a\neq 0}\xi_a\right)-\nu, \tag{9.139}$$

where the indicator function $\mathbf{1}_{\mathsf{Z}_{2n}}$ on the Z Lagrangian $\mathsf{Z}_{2n}=\mathsf{Z}_n\oplus\mathsf{Z}_n$ is the characteristic function of the Choi state of $P=|0^n\rangle\langle 0^n|$, i.e. of $\left|0^{2n}\right\rangle\!\left\langle 0^{2n}\right|$. We have

$$\ell'^{\top}\mathbf{1}_{\mathsf{Z}_{2n}}=\sum_{e\in\mathsf{Z}_n}\ell(e,e)+\sum_{e\neq e'\in\mathsf{Z}_n}\ell(e,e')=2^n(2-2^n), \tag{9.140}$$

thus, we readily compute the evaluation of ℓ' on $\bar{\lambda}$ as

$$\ell'^{\top}\bar{\lambda}=(2-2^n)+2\cdot 2^n(2^n-1)-2(2^n-1)=2^{2n+1}-5\cdot 2^n+4\begin{cases}\leq 2^{2n} & \text{for } n\leq 2,\\ >2^{2n} & \text{for } n>2.\end{cases} \tag{9.141}$$

Hence, we see that the block-diagonalisation $\bar{\Lambda}$ is not CSP for $n > 2$. This is to be expected, since it involves measuring the non-stabiliser projector $\mathbb{1} - |0\rangle\langle 0|$. However, the non-vialotion of a CSP inequality does not imply that the channel is CSP. Rewriting $\bar{\Lambda} = \frac{1}{2}(\mathrm{id} + \mathrm{Ad}(V_n))$ with $V_n := \mathrm{diag}(-1, 1, \ldots, 1) = X^{\otimes n}(C^{n-1}Z)X^{\otimes n}$, we see that this is a mixed Clifford channel for $n \leq 2$, i.e. a stabiliser operation.

CHAPTER 10

OPEN QUESTIONS

Following the results given in Ch. 9, a number of open questions have been raised both by myself and others. In this chapter, I would like to take the opportunity to formulate these questions and discuss them briefly.

The nature of CSP channels

In Ch. 9, CSP channels were characterised by a Kraus decomposition of the form

$$\mathcal{E} = \sum_{i=1}^{r} \lambda_i \frac{2^n}{\operatorname{rk} P_i} U_i P_i \cdot P_i U_i^\dagger, \tag{10.1}$$

where $U_i \in \mathrm{Cl}_n$ and the stabiliser codes P_i fulfill the POVM condition

$$\mathbb{1} = \sum_{i=1}^{r} \frac{2^n \lambda_i}{\operatorname{rk} P_i} P_i. \tag{10.2}$$

Beyond the case of orthogonal codes, it is not obvious what kind of stabiliser code families can fulfill Eq. (10.2). However, it seems imperative to understand this matter in order to obtain an intuition on whether CSP channels have a "simple" implementation. This is in turn related to an operational interpretation of CSP channels.

Open problem 1 (Stabiliser POVMs)**.** What are necessary and sufficient conditions on stabiliser codes P_i and convex coefficients λ_i such that Eq. (10.2) holds? Can these measurements be implemented efficiently?

As a first step, it is straightforward to generalise the construction of the Λ channel in Ch. 9 to obtain stabiliser POVMs associated with a given stabiliser state $|s\rangle$ and generators $g_1, \ldots, g_n$ of its stabiliser group. However, my collaborators and I have not been able to find similar examples of stabiliser POVMs involving codes of different dimension.

Furthermore, it seems that the understanding of stabiliser POVMs is also key to finding extremal CSP channels.

Open problem 2 (Extremal CSP channels)**.** Find more extremal CSP channels. Can they be classified and enumerated?

Classical simulation of CSP channels

First results on the classical simulation of CSP channels have been derived in Ref. [36]. However, the authors need an assumption on the number of non-unitary Kraus operators in the decomposition (10.1). This is unsatisfactory, since it even excludes orthogonal stabiliser POVMs which can be simulated through syndrome measurements. The reason for this assumption is that individual Kraus operators are sampled and then simulated.

However, the simulation of a projector can have an exponentially small success probability, which leads to an increased sampling complexity and even a non-zero failure probability of the algorithm.

A solid understanding of Problem 1, at least for extremal CSP channels, could enable a different simulation algorithm. Assuming that extremal stabiliser POVMs allow for an efficient description and simulation, a Monte-Carlo algorithm combined with this simulation could simulate CSP efficiently.

Open problem 3 (Classical simulation of CSP channels)**.** Is there an efficient classical simulation algorithm for CSP?

Gaps in magic state distillation rates

Finally, the strict inclusion SO $\subsetneq$ CSP makes it conceivable that certain resource tasks can only be optimally performed with CSP channels and not with stabiliser operations. For concreteness, let us consider the task of converting resource states $\rho \to \sigma$ with free operations. The asymptotic rate of conversion $R(\rho \to \sigma)$ is then defined to be the asymptotically optimal rate of converting k copies of ρ into $kR(\rho \to \sigma)$ copies of σ using resource non-generating channels [166]. For the resource theory of magic, the latter class is exactly CSP. It is known that $R(\rho \to \sigma)$ can be upper bounded by resource monotones. In particular, defining the *relative entropy of magic*,

$$E(\rho) := \inf_{\sigma \in \mathrm{SP}_n} S(\rho||\sigma), \qquad S(\rho||\sigma) := \mathrm{tr}\left[\rho(\log\rho - \log\sigma)\right], \tag{10.3}$$

and its regularised version $E^\infty(\rho) := \lim_{t\to\infty} E(\rho^{\otimes t})^{1/t}$, we have for any σ such that $E^\infty(\sigma) > 0$ [166]:

$$R(\rho \to \sigma) \leq \frac{E^\infty(\rho)}{E^\infty(\sigma)}. \tag{10.4}$$

If the class of free operations is slightly enlarged, it is known that any "reasonable" resource theory is asymptotically reversible and equality holds in the above equation [167]. However, recent results indicate that the resource theory of magic is already asymptotically reversible with CSP [39]. This implies that equality holds in Eq. (10.4), even for conversion under CSP channels. In this context, it might be the case that the optimal rate $R(\rho \to \sigma)$ cannot be achieved through stabiliser operations and the gap is significant.

Open problem 4 (Gaps in magic state distillation)**.** Is there a (significant) gap in the performance of resource conversion tasks between SO and CSP?

PART III

EXACT AND APPROXIMATE UNITARY DESIGNS FROM THE CLIFFORD GROUP

CHAPTER 11

INTRODUCTION

Arguably, the Clifford group is one of the most prominent objects in quantum information theory. In quantum computing, the main motivation comes from the idea of *fault-tolerance* [52]. Since stabiliser codes are the best-studied quantum codes, encoding, decoding, and error correction naturally involves Clifford unitaries. Moreover, the set of fault-tolerantly implementable gates is limited to Clifford gates, or more generally, to the Clifford hierarchy [168–175]. Thus, the natural gate set of fault-tolerant quantum computes is often based on Clifford unitaries. Furthermore, Clifford gates are also conceptionally simple and thus provide reasonable logical gates just as NOT, AND, or XOR in classical computing do. Finally, the Clifford group is also in some sense the biggest finite subgroup of the unitary group with those features – as soon as it is extended by a non-trivial gate, it becomes dense in the unitary group [60].

However, there is an additional exceptional detail about the Clifford group – it is a *unitary design*. In fact, this property somewhat singles out the Clifford group among all unitary subgroups [115] (see also Ch. 13). In this sense, the Clifford group combines many desirable properties, making it the prime choice in many applications.

Generally speaking, a *design* is a (usually finite) subset of a statistical ensemble which is able to reproduce the moments of the ensemble up to a certain order t. To illustrate this, consider the example of a *spherical design*. Here, the ensemble is the (real or complex) sphere $\mathbb{S}^d$ equipped with the Haar measure. A finite subset of points $\mathcal{D} \subset \mathbb{S}^d$ is called a *spherical t-design* if the average of any polynomial up to order t in the coordinates is the same over $\mathcal{D}$ as over $\mathbb{S}^d$. A related, but more important, instance for quantum information theory is the *complex projective design*. Instead of the sphere $\mathbb{S}^d$, we take the set of *pure states* given by the complex projective space $\mathbb{CP}^d$. Finally, these ideas initialised the study of *unitary designs* which allow to approximate the Haar measure on the unitary group $\mathrm{U}(d)$ [111, 176, 177].

Many successful protocols in quantum information theory are based on *randomness* in the form of *Haar-random* states or unitaries. In practice, implementing such a protocol can turn out to be difficult due to finite precision errors or limitations of the underlying hardware. Here, the concept of *designs* has proven to be very useful. In particular, designs have been successfully used to partially *derandomise* quantum protocols involving Haar-random states by realising that their function only depends on lower moments of the distribution. Unitary designs are central for many quantum information protocols such as quantum cryptography [10, 56, 57], state estimation and characterisation [7–16], and randomised benchmarking [17–23].

From the general theory of designs, we know that unitary t-designs exist for all t and in all dimensions d. However, little is known about general methods of constructing designs with given parameters. To the best of my knowledge, there had not been any general scheme until an iterative method was recently proposed by Bannai, Nakata, Okuda and Zhao [178]. In principle, this allows to explicitly construct unitary designs for all t and d.

Albeit, it is often of practical importance that a unitary design has both an efficient description and an efficient implementation. Moreover, it should be *scalable* to an arbitrary number of qudits. Groups have the advantage that any element can be written in terms of a small number of generators and thus potentially offer an efficient description of its elements. As discussed in Sec. 5.3.2, this is the case for the Clifford group. For practical purposes, unitary t-designs which form groups, so-called *unitary t-groups*, are thus of special interest. As we will discuss in Ch. 12, the combination of group and design structure requires that the commutant of the representation $U \mapsto U^{\otimes t}$ of a unitary t-group agrees with the one of the unitary group. Here, commutant means the algebra of operators which commute with $U \mapsto U^{\otimes t}$. Remarkably, a complete classification of unitary t-groups has been recently achieved by Bannai, Navarro, Rizo and Tiep [115]. In particular, they have proven the non-existence of unitary t-groups for $t \geq 4$ (in dimension > 2). Moreover, the multi-qubit Clifford group is singled out among all finite, locally generated unitary subgroups by being a unitary 3-design – thus making it the somewhat unique choice in quantum information applications.

Although the Clifford group only forms a unitary 3-design, it is close to a 4-design. Indeed, Zhu, Kueng, Grassl and Gross [87] and Helsen, Wallman and Wehner [179] have proven that the commutant of its fourth tensor power representation has only one dimension more than the one of the unitary group. As they show, the Clifford group is thus close to an exact 4-design for many applications in quantum information theory in the sense that the error is sufficiently small. This analysis has been subsequently used to give strict success guarantees for Clifford-based random protocols which rely on a control of the fourth moments [14–16, 179, 180]. Later, Gross, Nezami and Walter [181] have characterised the commutant of the t-th tensor power representation of the Clifford group for arbitrary t. Crucially, the dimension of the commutant does only depend on t but not on the number of qubits n.

Hence, the Clifford group is the optimal starting point for the construction of higher-order *approximate designs*. Indeed, my collaborators and I have recently shown that it is enough to inject $\tilde{O}(t^4)$ many non-Clifford gates into a random Clifford circuit to elevate the Clifford group to an approximate unitary t-design [58]. The effect of these non-Clifford gates is to sufficiently scramble the circuit which closes the gap between the Clifford and unitary commutant. The fact that the dimension of the Clifford commutant is independent of n allows the number of non-Clifford gates to be *system-size independent*. Thus, in the limit of $n \to \infty$, the proportion of non-Clifford gates becomes negligible. In this sense, a *homeopathic dose* of *magic* is enough to have a measurable effect on a Clifford circuit – in contrast to usual homeopathy.

Our construction of approximate unitary t-designs is efficient in the number of qubits and the design order in the sense that the total number of local gates is $\tilde{O}(n^2t^4)$. This is a considerable improvement over the construction of Brandao, Harrow and Horodecki [182] which uses $\tilde{O}(n^2t^{10})$ random two-qubit unitaries.

Although most known protocols do not require designs beyond the third order, it can be advantageous when control over higher moments of the estimator or tail bounds are needed. For instance, the use of 4-designs can be beneficial for RB and shadow tomography [12, 13, 15, 16, 183, 184]. Furthermore, the availability of unitary t-designs has already triggered the search for applications. A recent work shows that unitary t-designs can be used to construct efficient *quantum physical uncloneable functions* which provide provable cryptographic security against quantum adversaries [185].

Structure of this part

This part of the thesis is organised as follows.

In Chapter 12, we introduce the concept of unitary t-designs and discuss the relation to representation theory. Following the references [111, 113], it is shown that the Clifford groups always form unitary 2-designs, but only the multi-qubit Clifford group forms a unitary 3-design. We then proceed by discussing the general tensor power representations of the Clifford group and the related characterisation of the Clifford commutant by Gross, Nezami and Walter [181]. This result is needed in Ch. 14. Moreover, I give a description of the orthogonal commutant which, to the best of my knowledge, has not been explicitly described in the literature before. We adapt the formalism of Howe [163, 164] (see also Ref. [110]), developed for the symplectic group, to the Clifford group case in arbitrary characteristic, and borrow a result from Gross, Nezami and Walter [181].

In Chapter 13, we give a characterisation of unitary t-designs which form groups. This follows from the recent results by Bannai, Navarro, Rizo and Tiep [115] and Sawicki and Karnas [186]. This chapter is based on a section which I have written for Ref. [58].

Chapter 14 then gives a summary of Ref. [58]. This work is a result of a larger collaboration including myself and was presented at the TQC 2020 and QIP 2021 conferences. Its goal is to answer different questions centered around the design properties of the Clifford group and is important to the context of this thesis. Although I have contributed in various ways to Ref. [58], the precise contribution is difficult to isolate due to the collaborative nature of the work. This prevents the paper to appear in its original form in this thesis. Because of the highly technical nature of the work, only a summary is given with a focus on selected aspects.

This part is closed by Chapter 15 which reports on ongoing efforts in approximating Clifford averages. This work is partially inspired from the construction of approximate designs from the Clifford group. A progress in approximating Clifford averages would considerably simplify the proof in Ref. [58] and potentially improve the overall scaling. Moreover, it is also interesting on its own and shows tight connections to the representation theory of the Clifford group. The performed studies suggest that the limited state-of-the-art understanding of the latter subject is the reason why this remains an open research question.

CHAPTER 12

UNITARY DESIGNS AND THE CLIFFORD GROUP

In this chapter, we introduce the necessary preliminaries needed for the later chapters. We start by defining *unitary designs* and discuss their mathematical background. Then, we review the design properties of the Clifford group and give self-contained proofs. Finally, we summarise literature results on the representation theory of the Clifford group and introduce the Clifford and orthogonal commutant.

12.1 Definitions

A *unitary t-design* is a probability measure ν on the unitary group $U(d)$ which reproduces expectation values of the (normalised) Haar measure μ_{H} for polynomial functions up to degree t (see Refs. [111, 176, 177]). More precisely, let $\mathrm{Hom}_{(t,t)}(U(d))$ be the vector space of homogeneous polynomials of degree t in both the matrix elements of U and $\overline{U}$. Then, ν is a unitary t-design if and only if

$$\int_{U(d)} p(U)\,\mu_{\mathrm{H}}(U) = \int_{U(d)} p(U)\,\nu(U), \qquad \forall p \in \mathrm{Hom}_{(t,t)}(U(d)). \tag{12.1}$$

In most applications, ν has support on a finite set $\mathcal{D} = \{U_1, \ldots, U_N\}$ and coincides with the counting measure thereon. In this case, the integral on the right hand side of Eq. (12.1) is simply the uniform average over $\mathcal{D}$.

A very useful tool in the study of unitary designs is the *frame potential*. It is defined as

$$\Phi_t(\nu) := \int_{U(d)} \int_{U(d)} |\operatorname{tr}(U^\dagger V)|^{2t}\,\nu(U)\,\nu(V). \tag{12.2}$$

The name originates from *frame theory*: A *frame* is a spanning set of a vector space. The frame potential is the sum of squared overlaps between the vectors of a frame and this potential is naturally minimised by a so-called *tight frame*. In some sense, designs are special tight frames in the space of symmetric tensors of rank t.

As it is shown below, the frame potential is bounded from below by [9, 111]

$$\Phi_t(\nu) \geq \gamma(t,d) := \int_{U(d)} |\operatorname{tr}(U)|^2\,\mu_{\mathrm{H}}(U) = \begin{cases} \frac{(2t)!}{t!(t+1)!}, & d = 2, \\ t!, & d \geq t. \end{cases} \tag{12.3}$$

Here, $\gamma(t,d)$ is explicitly given as the number of permutations in S_t with no increasing subsequence of length $> d$. For the given regimes of interest, this takes a particularly simple form.

There are several equivalent definition of a unitary t-design which we summarise in the following proposition (cp. Ref.[87, Prop. 2]).

Proposition 12.1. *Let ν be a probability measure on $U(d)$. Then, the following are equivalent:*

(i) ν is a unitary t-design

(ii) *For all* $A, B \in \mathbb{C}^{d\times d}$, $\int \mathrm{tr}\left(AU^{\otimes t}B(U^{\otimes t})^\dagger\right)\mu_{\mathrm{H}}(U) = \int \mathrm{tr}\left(AU^{\otimes t}B(U^{\otimes t})^\dagger\right)\nu(U)$.

(iii) $\int \mathrm{Ad}(U)^{\otimes t}\,\mu_{\mathrm{H}}(U) = \int \mathrm{Ad}(U)^{\otimes t}\,\nu(U)$.

(iv) $\int U^{\otimes t}\otimes \overline{U}^{\otimes t}\mu_{\mathrm{H}}(U) = \int U^{\otimes t}\otimes \overline{U}^{\otimes t}\nu(U)$.

(v) $\Phi_t(\nu) = \gamma(t,d)$.

Proof. For any $A, B \in \mathbb{C}^{d\times d}$, $p(U) = \mathrm{tr}\left(AU^{\otimes t}B(U^{\otimes t})^\dagger\right)$ is a homogeneous polynomial in $\mathrm{Hom}_{(t,t)}(U(d))$. In fact, these polynomials span $\mathrm{Hom}_{(t,t)}(U(d))$ and thus (i) is equivalent to (ii). The equivalence of (ii) and (iii) is obvious. For statements (iii) and (iv) consider the isomorphism $L(\mathbb{C}^d) \simeq \mathbb{C}^d \otimes (\mathbb{C}^d)^* \simeq \mathbb{C}^d \otimes \mathbb{C}^d$ induced by the Riesz isomorphism of the Hilbert space $\mathbb{C}^d$. Concretely, this is the map which acts on the computational basis as $|x\rangle\langle y| \mapsto |x\rangle \otimes |x\rangle$. In turn, this induces an isomorphism on superoperators $L(L(\mathbb{C}^d)) \simeq L(\mathbb{C}^d \otimes \mathbb{C}^d)$ which maps $\mathrm{Ad}(U) = U \cdot U^\dagger \mapsto U \otimes \overline{U}$. Hence, statements (iii) and (iv) are equivalent under this isomorphism. Finally, the 2-norm distance between the left and right hand side in statement (iv) is given by

$$\left\| \int U^{\otimes t}\otimes \overline{U}^{\otimes t}\mu_{\mathrm{H}}(U) - \int U^{\otimes t}\otimes \overline{U}^{\otimes t}\nu(U) \right\|_2 = \Phi_t(\nu) - \gamma(t,d), \tag{12.4}$$

which shows the equivalence between (iv) and (v). □

From Prop. 12.1 (ii) it is clear that if ν is a t-design, then it is also a $(t-1)$-design. The expression in statement (iv) is sometimes called the t-th *moment operator* of the probability measure ν. In this sense, a unitary t-design exactly reproduces all moments of the Haar measure up to order t.

As for every definition, the first natural question to ask is whether t-designs exist for all t and d. This was already answered affirmatively by Seymour and Zaslavsky [187]. Although the existence has been known for quite some time, methods for constructing a unitary design with given parameters (t,d) are rare. Recently, Bannai, Nakata, Okuda and Zhao [178] have proposed an iterative procedure allowing the explicit construction of unitary designs for all (t,d). To the best of my knowledge, this is the only known general method of constructing unitary designs.

The theory of unitary designs is strongly linked to the representation theory of the unitary group. More precisely, consider the representation $\tau^t : U \mapsto U^{\otimes t}$ of $U(d)$ which we call the *t-th tensor power representation*. Then, ν is a unitary design if and only if the following equality holds for all irreducible representation ρ contained in $\tau^t \otimes \overline{\tau}^t$ [188]:

$$\int_{U(d)} \rho(U)\,\mu_{\mathrm{H}}(U) = \int_{U(d)} \rho(U)\,\nu(U). \tag{12.5}$$

In other words, it is necessary that the averages agree on every irrep of $\tau^t \otimes \overline{\tau}^t$.

In the following, the isotype of the trivial irrep of $\tau^t \otimes \overline{\tau}^t$ is of special importance. Since $\tau^t \otimes \overline{\tau}^t \simeq \mathrm{Ad}(\tau^t)$ where $\mathrm{Ad}(A)(B) := ABA^\dagger$ denotes the adjoint action, the trivial isotype is isomorphic to the subspace of operators which are fixed by the adjoint action, i. e. which commute with τ^t. We call this subspace the *commutant* of τ^t.

Definition 12.1 (Commutant)**.** The *commutant* $\mathcal{A}'$ of a subalgebra $\mathcal{A} \subset L(\mathbb{C}^d)$ is the subalgebra

$$\mathcal{A}' := \left\{ A \in L(\mathbb{C}^d) \mid AB = BA \quad \forall B \in \mathcal{A} \right\}. \tag{12.6}$$

If $\mathcal{A}$ is the algebra spanned by a representation ρ of a group G, then we use the notation $\mathcal{A}' = \rho(G)'$ or simply G' if the representation is clear from the context.

Let us now consider the case that $G < U(d)$ is a finite subgroup and ν is the counting measure on G. If (G, ν) defines a unitary t-design, we call G a *unitary t-group* or a *group design*. Note that G is a group design if and only the projective group $\overline{G} = G/Z(G)$ is, as can be seen explicitly from Prop. 12.1. In this case, Prop. 12.1 (iii) states

$$\int_{U(d)} \tau^t(U) \cdot \tau^t(U)^\dagger \, \mu_{\mathrm{H}}(U) = \frac{1}{|G|} \sum_{U \in G} \tau^t(U) \cdot \tau^t(U)^\dagger. \tag{12.7}$$

These are exactly the projections onto the commutant of τ^t and $\tau^t|_G$, respectively, and thus the commutants have to be identical. Hence, Schur-Weyl duality implies that the commutant of $\tau^t|_G$ has to be spanned by the permutations S_t. Since the commutant of τ^t is isomorphic to the trivial isotype of $\tau^t \otimes \overline{\tau}^t$, this also imposes restrictions on the representation $\tau^t|_G$ of G as follows [111]. Define the character inner product,

$$(\chi|\xi) = \int_{U(d)} \chi(U) \overline{\xi}(U) \, \mathrm{d}\mu_{\mathrm{H}}(U), \tag{12.8}$$

and let $\xi_t := \operatorname{tr} \tau^t$ be the character of the representation τ^t. We have a decomposition into irreps ρ_λ with multiplicities m_λ:

$$\tau^t = \bigoplus_\lambda \rho_\lambda \otimes \mathbb{1}_{m_\lambda}. \tag{12.9}$$

Next, the dimension of the commutant is equal to dimension of the trivial isotype in $\tau^t \otimes \overline{\tau}^t$, which is given by the character inner product with the character 1 of the trivial representation. Let $\chi_\lambda := \operatorname{tr} \rho_\lambda$, then we find

$$\dim \tau^t(U(d))' = (\xi_t \otimes \overline{\xi}_t | 1) = (\xi_t | \xi_t) = \sum_{\lambda, \lambda'} m_\lambda m'_\lambda (\chi_\lambda | \chi_{\lambda'}) = \sum_\lambda m_\lambda^2, \tag{12.10}$$

using that characters of irreps are orthonormal w.r.t. the character inner product. Note that this is exactly the frame potential $\Phi_t(U(d)) = \gamma(t, d)$.

Finally, note that any irrep of $U(d)$ in τ^t is an invariant subspace for G which, however, might not be irreducible anymore. Since we have the identity

$$\Phi_t(G) = \frac{1}{|G|} \sum_{U \in G} |\operatorname{tr}(U)|^{2t} = \dim \tau^t(G)', \tag{12.11}$$

we have $\Phi_t(G) \geq \Phi_t(U(d))$ with equality if and only if any irrep ρ_λ of τ^t is also irreducible under the restricted representation $\tau^t|_G$.

12.2 The Clifford group as a design

Besides its importance for the stabiliser formalism and quantum error correction, the Clifford group is an important example of a *unitary design*. In fact, as explained later in Ch. 13, the Clifford group is in some sense a natural and essentially unique choice of a group design in quantum information theory.

12.2.1 The Clifford group is a unitary 2-design

The aim of this section is to prove that certain subgroups of the Clifford group $\mathrm{Cl}_n(q)$ form unitary 2-designs, following the presentation in Ref. [111]. From the general discussion in the last section, we know that the irreps of any such subgroup have to agree with those of the representation $U \mapsto U^{\otimes 2}$ of the unitary group $U(d)$. This is a particularly simple case, as there are only two irreps, namely the symmetric subspace $\mathrm{Sym}^2(\mathbb{C}^d)$ and the antisymmetric subspace $\bigwedge^2(\mathbb{C}^d)$ with according projectors $P_{\mathrm{Sym}} = (\mathbb{1} + F)/2$ and $P_\wedge = (\mathbb{1} - F)/2$ where F is the *flip* or *swap operator* corresponding to the transposition $\pi = (21)$. Then, we can write the unitary twirl as follows

$$P_{\mathrm{H}} := \int_{U(d)} (U \otimes U) \cdot (U \otimes U)^\dagger \, \mu_{\mathrm{H}} = \frac{2}{d(d+1)} \, |P_{\mathrm{Sym}})(P_{\mathrm{Sym}}| + \frac{2}{d(d-1)} \, |P_\wedge)(P_\wedge| \,. \tag{12.12}$$

Here, $|A)(B|$ is the rank-one superoperator which acts as $C \mapsto \mathrm{tr}(B^\dagger C)A$.

Next, consider the case $d = q^n$ and evaluate P_{H} on the Weyl basis. We find

$$\begin{aligned} P_{\mathrm{H}}(W(a) \otimes W(b)) &= \frac{1}{d+1} \left(d\delta_{a,0}\delta_{b,0} + \delta_{a+b,0}\right) P_{\mathrm{Sym}} + \frac{1}{d-1} \left(d\delta_{a,0}\delta_{b,0} - \delta_{a+b,0}\right) P_\wedge \\ &= \begin{cases} \mathbb{1} & \text{if } a = b = 0, \\ \frac{1}{d^2-1} \left(dF - \mathbb{1}\right) & \text{if } a = -b \neq 0, \\ 0 & \text{else.} \end{cases} \end{aligned} \tag{12.13}$$

Given a subgroup $G < \mathrm{Cl}_n(q)$, we denote by $\pi(G) < \mathrm{Sp}_{2n}(q)$ the induced subgroup of the symplectic group. Concretely, the action of any $U \in G$ on Weyl operators is described by an automorphism $(g, \alpha) \in \mathrm{ASp}_{2n}(q)$ as $UW(v)U^\dagger = \chi(\alpha(v))W(g(v))$. Then, we set $\pi(U) := \mathrm{pr}_1(g, \alpha) = g$.

Proposition 12.2. *Let $q = p^m$ for p prime and $n \in \mathbb{N}$. Let $G < \mathrm{Cl}_n(q)$ be a subgroup such that $\mathrm{HW}_n(q) \lhd G$ and $\pi(G) < \mathrm{Sp}_{2n}(q)$ acts transitively on $\mathbb{F}_q^{2n} \setminus 0$. Then, G is a unitary 2-design.*

Proof. Let $\mathcal{G} := \pi(G) < \mathrm{Sp}_{2n}(q)$ be the induced subgroup. The assumption $\mathrm{HW}_n(q) \lhd G$ then implies that $\mathcal{G} \simeq G/\mathrm{HW}_n(q)$. Hence, the projective group $\overline{G} := G/Z(G)$ is isomorphic to the subgroup of $\mathrm{ASp}_{2n}(q)$ given by pairs (g, α) with $g \in \mathcal{G}$. Recall from Sec. 3.3, that for any g we can write $\alpha = \alpha_g + [v, \cdot]$ for $v \in \mathbb{F}_q^{2n}$ and some fixed $\alpha_g : \mathbb{F}_q^{2n} \to \mathbb{F}_q$ which can be chosen to be zero if $p \neq 2$. For $p = 2$, we will use that $\alpha_g(a) + \alpha_g(-a) =$

$2\alpha_g(a) = 0$. Then, we verify Eq. (12.13) on the Weyl basis. For $a, b \in \mathbb{F}_q^{2n}$ we obtain:

$$\begin{aligned}
&\frac{1}{|G|}\sum_{U\in G}(U\otimes U)\,W(a)\otimes W(b)\,(U\otimes U)^\dagger \\
&\quad= \frac{1}{|\overline{G}|}\sum_{U\in \overline{G}}(U\otimes U)\,W(a)\otimes W(b)\,(U\otimes U)^\dagger \\
&\quad= \frac{1}{q^{2n}}\sum_{v\in\mathbb{F}_q^{2n}}\chi([v,a+b])\frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}}\chi(\alpha_g(a)+\alpha_g(b))W(g(a))\otimes W(g(b)) \\
&\quad= \frac{\delta_{a,-b}}{|\mathcal{G}|}\sum_{g\in\mathcal{G}}W(g(a))\otimes W(-g(a)) \qquad (12.14)\\
&\quad= \frac{\delta_{a,-b}}{|\mathcal{G}\cdot a|}\sum_{v\in(\mathcal{G}\cdot a)}W(v)\otimes W(-v) \qquad (12.15)
\end{aligned}$$

In Eq. (12.14), we have used that $|\overline{G}| = |\mathcal{G}||\mathbb{F}_q^{2n}|$ and that the character sum is only non-zero if $a + b = 0$. In Eq. (12.15), we rewrote the sum as an average over the orbit of a under $\mathcal{G}$. Next, if $a \neq 0$, the orbit is simply $\mathbb{F}_q^{2n} \setminus 0$ since $\mathcal{G}$ acts transitively on $\mathbb{F}_q^{2n} \setminus 0$. Using the expansion of the swap operator in the Weyl basis,

$$F = q^{-n}\sum_{v\in\mathbb{F}_q^{2n}}W(v)\otimes W(-v), \qquad (12.16)$$

we find

$$\begin{aligned}
\frac{1}{|G|}\sum_{U\in G}(U\otimes U)\,W(a)\otimes W(b)\,(U\otimes U)^\dagger &= \frac{\delta_{a,-b}}{q^{2n}-1}\sum_{v\in\mathbb{F}_q^{2n}\setminus 0}W(v)\otimes W(-v) \\
&= \frac{\delta_{a,-b}}{q^{2n}-1}\left(q^n F - \mathbb{1}\right).
\end{aligned} \qquad (12.17)$$

If $a = 0$, then the orbit is simply $\{0\}$ and we get $\delta_{b,0}\mathbb{1}$ as the result. This concludes the proof. □

Proposition 12.2 shows that the Clifford group in any prime-power dimension is a unitary 2-design. It might be surprising that Clifford subgroups can also form unitary 2-designs. A straightforward example is given by the embedding of "restricted" Clifford groups $\mathrm{Cl}_n(p^m)$ into $\mathrm{Cl}_{nm}(p)$. Since $\mathrm{Cl}_n(p^m)$ projects onto $\mathrm{Sp}_n(p^m)$, it acts transitively on $\mathbb{F}_q^{2n} \setminus 0 \simeq \mathbb{F}_p^{2nm}$. Hence, *any* embedding of $\mathrm{Cl}_n(p^m)$ into $\mathrm{Cl}_{nm}(p)$ yields a 2-design. More generally, if n is not prime and $n = mk = m'k'$ for $m < m'$, we have nested subgroups $\mathrm{Cl}_k(p^m) < \mathrm{Cl}_{k'}(p^{m'}) < \mathrm{Cl}_n(p)$ which all form 2-designs. Depending on the application, it can be advantageous to use the Clifford group over the maximal extension field since it can be much smaller:

$$\frac{|\mathrm{Cl}_2(p^n)|}{|\mathrm{Cl}_n(p)|} = \frac{p^n\left(p^{2n}-1\right)}{p^{n^2}\prod_{i=1}^n\left(p^{2i}-1\right)} = \frac{1}{p^{n(n-1)}\prod_{i=1}^{n-1}\left(p^{2i}-1\right)}. \qquad (12.18)$$

I am not aware of a general family of transitively-acting subgroups of $\mathrm{Sp}_{2n}(p)$ which is beyond the above example. The order of any such subgroup $\mathcal{G}$ has to be a multiple of

$|\mathbb{F}_p^{2n} \setminus 0| = p^{2n} - 1$. Thus, the associated subgroup G of $\mathrm{Cl}_n(p)$ has at least $p^{2n}(p^{2n}-1)$ elements (modulo its center). Using Dickson's theorem on the classification of subgroups of $\mathrm{SL}_2(p^n) = \mathrm{Sp}_2(p^n)$ [189], Chau [190] concludes that transitive subgroups $\mathcal{G} < \mathrm{Sp}_2(p^n)$ only exist in prime dimensions $d = p^n = 2, 3, 5, 7, 11$. However, Gross, Audenaert and Eisert [111] found an example of a transitive subgroup $\mathcal{G} < \mathrm{Sp}_4(3)$ of order $2(d^2-1)$ in dimension $d = 3^2 = 9$. This is strictly smaller than the order of $\mathrm{Sp}_2(9)$, which is $d(d^2-1)$.

12.2.2 The qubit Clifford group is a 3-design

Given that the Clifford group forms a unitary 2-design, it is natural to ask whether it also forms a higher-order design, and if so, what the highest order is. This was answered in detail by Zhu [113]:

Theorem 12.1 ([113, Thm. 1])**.** *The Clifford group* $\mathrm{Cl}_n(q)$ *is a unitary 3-design if and only if* $q = p = 2$*. The multi-qubit Clifford group* $\mathrm{Cl}_n(2)$ *is not a unitary 4-design.*

The prime case was also independently proven by Webb [114]. With the last section in mind, one might wonder if there are any subgroups of $\mathrm{Cl}_n(2)$ which form 3-designs. This was answered in Ref. [113] to the negative, except in the case $n = 2$ where there is a proper subgroup which projects onto a subgroup of $\mathrm{Sp}_4(2)$ isomorphic to the alternating group A_6.

We refrain from giving a detailed proof of Thm. 12.1 since it is quite technical and will not be needed in this thesis. Nevertheless, we give a sketch of the techniques used by Zhu [113]. It is based on the following characterisation of the frame potential of a Clifford subgroup.

Lemma 12.1 ([113, Lem. 2])**.** *Given a subgroup* $\mathrm{HW}_n(q) \lhd G < \mathrm{Cl}_n(q)$ *and let* $\mathcal{G} := \pi(G) < \mathrm{Sp}_{2n}(q)$ *be the induced subgroup on the phase space* $V := \mathbb{F}_q^{2n}$*. Then,*

$$\Phi_t(G) = \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} |V^g|^{t-1} = \left|V^{t-1}/\mathcal{G}\right|. \tag{12.19}$$

Here, V^g *is the set of fixed points of* g *and* $V^{t-1}/\mathcal{G}$ *is the set of orbits under the diagonal action of* $\mathcal{G}$ *on* V^{t-1}*.*

Note that the last equation follows from Burnside's lemma, which states that the number of orbits is equal to the average number of fixed points of a group action.

Using Lem. 12.1, we can give a one-line proof of Prop. 12.2: Since for $t \leq d$, $\gamma(t, d) = t!$, G is a 2-design if and only if $\Phi_2(G) = 2$ which is the case if and only if $\mathcal{G}$ acts transitively on $V = \mathbb{F}_q^{2n}$.

Likewise, G is a 3-design if and only if $\mathcal{G}$ has the following number of orbits on $\mathbb{F}_q^{2n} \oplus \mathbb{F}_q^{2n}$:

$$\gamma(3, q^n) = \begin{cases} 5, & \text{if } q = p = 2, n = 1, \\ 6, & \text{else.} \end{cases} \tag{12.20}$$

To show Thm. 12.1, we thus have to compute the number of orbits of $\mathrm{Sp}_{2n}(q)$ on $(\mathbb{F}_q^{2n})^{t-1}$ for $t = 3, 4$. Let us demonstrate the argumentation for the case $t = 3$. Transitivity implies

that we have at least the following distinct orbits under the diagonal action of $\mathrm{Sp}_{2n}(q)$:

$$\mathrm{Sp}_{2n}(q)\cdot(0,0)=\{0\}, \qquad \mathrm{Sp}_{2n}(q)\cdot(e_1,0)=\mathbb{F}_q^{2n}\oplus 0, \tag{12.21}$$

$$\mathrm{Sp}_{2n}(q)\cdot(0,e_1)=0\oplus\mathbb{F}_q^{2n}, \qquad \mathrm{Sp}_{2n}(q)\cdot(e_1,e_1)=\big\{(v,v)\,|\,v\in\mathbb{F}_q^{2n}\big\}. \tag{12.22}$$

Moreover, we can assume that any other orbit is generated by a pair (e_1,u). If $u\in\langle e_1\rangle$, we get $q-2$ additional orbits in this way since $u\in\{0,e_1\}$ is already listed above. By Witt's theorem, (e_1,u) and (e_1,v) for $u,v\notin\langle e_1\rangle$ generate the same orbit if and only if $[e_1,u]=[e_1,v]$ If $n=1$, then $u,v\in\langle e_2\rangle$ and thus the symplectic product can not be zero. Hence, in this case we get $4+(q-2)+(q-1)=2q+1$ orbits. For $n>1$, the symplectic product can take any value and thus we have $2q+2$ orbits. In summary:

$$\Phi_3(\mathrm{Cl}_n(q))=\begin{cases}2q+1, & \text{if } n=1,\\ 2q+2, & \text{if } n>1.\end{cases} \tag{12.23}$$

A comparison with Eq. (12.20) shows that $\mathrm{Cl}_n(q)$ is a unitary 3-design if and only if $q=2$.

In the same way, one can count the orbits on $(\mathbb{F}_q^{2n})^3$. Again, Witt's theorem implies that the orbit is characterised by the mutual symplectic products between any two vectors in a triple. The result is [113]:

$$\Phi_4(\mathrm{Cl}_n(q))=\begin{cases}q^3+q^2+q+1, & \text{if } n=1,\\ 2q^3+2q^2+2q+1, & \text{if } n=2,\\ 2q^3+2q^2+2q+2, & \text{if } n\geq 3.\end{cases} \tag{12.24}$$

In particular, no Clifford group is a unitary 4-design.

12.3 Tensor power representations of the Clifford group

As discussed in Sec. 12.1, the design properties of a subgroup $G<U(d)$ are determined by the irreducible representations of the t-th tensor power representation $\tau^t|_G : U\mapsto U^{\otimes t}$. For the qubit Clifford group, we know that its irreps coincide with the unitary irreps for $t\leq 3$. However, even for $t=4$, the representation of the Clifford group is not too different from the one of the unitary group, since only one additional irrep is appearing [87, 179]. As it is easy to check, the Weyl operators $W(a)^{\otimes 4}$ form an Abelian group $\mathcal{S}_{n,4}$ which is invariant under the Clifford representation:

$$U^{\otimes 4}W(a)^{\otimes 4}(U^{\otimes 4})^\dagger=W(g(a))^{\otimes 4}, \qquad \text{for some } g\in\mathrm{Sp}_{2n}(2). \tag{12.25}$$

In fact, the stabiliser code $\mathcal{C}_{n,4}$ defined by $\mathcal{S}_{n,4}$ is an invariant subspace. Moreover, the Clifford representation induces a unitary representation of $\mathrm{Sp}_{2n}(2)$ on $\mathcal{C}_{n,4}$ in this way.

This stabiliser code is factorising, $\mathcal{C}_{n,4}=\mathcal{C}_{1,4}^{\otimes n}$, which can be deduced in a simple way from the orthogonal projection onto $\mathcal{C}_{n,4}$:

$$P_{n,4}:=\frac{1}{2^{2n}}\sum_{a\in\mathbb{F}_2^{2n}}W(a)^{\otimes 4}=P_{1,4}^{\otimes n}. \tag{12.26}$$

Note that $\mathcal{C}_{1,4}\subset(\mathbb{C}^2)^{\otimes 4}$ is the CSS code given by $\mathcal{S}_{1,4}=\{\mathbb{1},Z^{\otimes 4},X^{\otimes 4},(ZX)^{\otimes 4}\}$.

Zhu, Kueng, Grassl and Gross [87] and Helsen, Wallman and Wehner [179] showed that that $C_{n,4}$ is the only additional irrep in the fourth tensor power representation of the Clifford group $\mathrm{Cl}_n(2)$. Equivalently, the commutant of the Clifford group is spanned by the unitary commutant and $P_{n,4}$.

For arbitrary t, the t-th tensor power representation is not yet completely understood. A first result was given by Gross, Nezami and Walter [181] who showed that the the t-th tensor power representation commutes with the n-th tensor power representation of another group, the so-called *stochastic orthogonal group*. This is a form of *duality* which is reminiscent of the famous *Schur-Weyl duality* for the unitary group and the symmetric group. However, for the Clifford group, this duality is somewhat inexact in the sense that the Clifford commutant is strictly larger than the algebra generated by the stochastic orthogonal group. In odd characteristic, the representation theory of the Clifford group is connected via the Weil representation to the one of the symplectic group. The mentioned duality is then directly related to the *Howe duality* of the symplectic group. Consequently, the representation theory of tensor power representations of the Clifford group in odd characteristic is better understood and the irreps have been recently related to CSS codes [191, 192].

12.3.1 The Clifford commutant

In the context of unitary designs, the knowledge about the Clifford commutant is often sufficient. As we need this result in Ch. 14, we now proceed by constructing an operator basis of the commutant of the t-th tensor power representation of the Clifford group which generalises the above described idea for $t = 4$ to arbitrary t. We follow the presentation in Ref. [181].

Before we present the results, let us review the setting of *Schur-Weyl duality*. We consider a Hilbert space $\mathcal{H} = ((\mathbb{C}^p)^{\otimes n})^{\otimes t}$ of local *prime* dimension p which we depict as a $t \times n$ grid of Hilbert spaces $\mathbb{C}^p$, see Fig. 12.1. The unitary group $\mathrm{U}(p^n)$ acts in parallel on the rows of $\mathcal{H}$ by the diagonal representation $\tau^t : U \mapsto U^{\otimes t}$. Furthermore, let $\pi \mapsto r(\pi)$ be the representation of the symmetric group S_t on $(\mathbb{C}^p)^{\otimes t}$ which acts by permutation of tensor factors. We can extend this to a parallel action of S_t on the columns of $\mathcal{H}$ by $\pi \mapsto r(\pi)^{\otimes n}$.

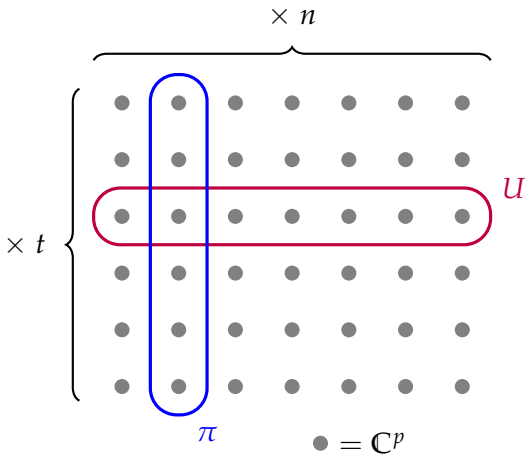


Figure 12.1: The Hilbert space $((\mathbb{C}^p)^{\otimes n})^{\otimes t}$ depicted as a $t \times n$ grid where every point corresponds to a copy of $\mathbb{C}^p$. Unitaries $U \in \mathrm{U}(p^n)$ act row-wise on the grid, while permutations $\pi \in S_t$ act column-wise.

Schur-Weyl duality states that the two actions of $U(p^n)$ and S_t commute and, moreover, the two groups span each others commutant. Since $\mathrm{Cl}_n(p)$ is a subgroup of $U(p^n)$, it certainly commutes with the symmetric group S_t. However, by the result of Sec. 12.2.2, the symmetric group fails to span the commutant of the Clifford group for $t > 2$ ($p > 2$) and $t > 3$ ($p = 2$), respectively. In fact, one can show that the group which is *dual* to the Clifford group in the Schur-Weyl sense is strictly larger than the symmetric group S_t. As we see in a moment, this is the so-called *stochastic orthogonal group* $\mathrm{O}_t^{\mathrm{st}}(p)$. To define this group, let us agree on the following convention:

$$D := \begin{cases} 2p, & \text{if } p = 2, \\ p, & \text{else.} \end{cases} \qquad \Rightarrow \qquad \mathbb{Z}_D := \begin{cases} \mathbb{Z}_4, & \text{if } p = 2, \\ \mathbb{F}_p, & \text{else.} \end{cases} \tag{12.27}$$

Then, we define the following $\mathbb{Z}_D$-valued quadratic form on $\mathbb{F}_p^t$:

$$q : \mathbb{F}_p^t \to \mathbb{Z}_D, \qquad q(x) := x \cdot x \mod D \tag{12.28}$$

The reason for this definition is related to the introduction of $\mathbb{Z}_4$-valued functions in Sec. 3.3. Indeed, the quadratic form q is a quadratic refinement of the Euklidean inner product on $\mathbb{F}_p^t$ over $\mathbb{Z}_D$:

$$q(x + y) - q(x) - q(y) = 2x \cdot y. \tag{12.29}$$

Finally, we define the stochastic orthogonal group as

$$\mathrm{O}_t^{\mathrm{st}}(p) := \left\{ O \in \mathbb{F}_p^{t \times t} \;\middle|\; q(Ox) = x, \quad O \cdot \mathbf{1} = \mathbf{1} \right\} \supset S_t, \tag{12.30}$$

where $\mathbf{1} = (1, \ldots, 1) \in \mathbb{F}_p^t$. Due to Eq. (12.29), any $O \in \mathrm{O}_t^{\mathrm{st}}(p)$ preserves the dot product and hence O is orthogonal in the "usual" sense, i. e. $O^\top O = \mathbb{1}$. The "stochastic" in the name originates from the condition $O \cdot \mathbf{1} = \mathbf{1}$. The symmetric group S_t forms a subgroup given by permutation matrices.

We have a representation of $\mathrm{O}_t^{\mathrm{st}}(p)$ on $\mathbb{C}[\mathbb{F}_p^t] \simeq (\mathbb{C}^p)^{\otimes t}$ which naturally extends the representation of S_t:

$$r(O) = \sum_{x \in \mathbb{F}_p^t} |Ox\rangle\langle x| \,. \tag{12.31}$$

As for the symmetric group, the representation $O \mapsto r(O)^{\otimes n}$ acts in parallel on the columns of the Hilbert space $\mathcal{H}$, see Fig. 12.1. Moreover, this representation still commutes with the Clifford group representation $U \mapsto U^{\otimes t}$, as one can check in a straightforward fashion on the generators of $\mathrm{Cl}_n(p)$ [181]. As in Schur-Weyl duality, this implies that we can decompose the Hilbert space in terms of irreps of $\mathrm{O}_n^{\mathrm{st}}(p)$:

$$\mathcal{H} \simeq \bigoplus_\lambda V_\lambda \otimes M_\lambda, \tag{12.32}$$

where V_λ is an irrep of $\mathrm{O}_n^{\mathrm{st}}(p)$ and M_λ is the multiplicity space on which the Clifford group acts. However, M_λ is in general not irreducible. This also implies that the commutant of the Clifford group is not spanned by operators of the form $r(O)^{\otimes n}$ alone.

In fact, additional operators $r(T)^{\otimes n}$ are needed which will be defined in a moment. Then, the following theorem was proven in Ref. [181]:

Theorem 12.2 (Clifford commutant [181, Thm. 4.3]). *Let $n \geq t-1$ and let Σ_t be the set of* stochastic Lagrangians *in $\mathbb{F}_p^t$. The operators $r(T)^{\otimes n}$ for $T \in \Sigma_t$ are linearly independent and span the commutant of the t-th diagonal action τ^t of the Clifford group. In particular, we have* $\dim \tau^t(\mathrm{Cl}_n(p))' = |\Sigma_t| = \prod_{k=0}^{t-2}(p^k+1)$.

To see how these additional operators $r(T)$ emerge, the following perspective is particularly fruitful. Any orthogonal matrix O is uniquely characterised by its graph

$$\Gamma_O := \left\{(Ox, x) \mid x \in \mathbb{F}_p^t\right\} \subset \mathbb{F}_p^t \oplus \mathbb{F}_p^t. \tag{12.33}$$

Let us endow the vector space $\mathbb{F}_p^t \oplus \mathbb{F}_p^t$ with the quadratic form $\mathfrak{q} := q \oplus (-q)$. We call the quadratic space $(\mathbb{F}_p^{2t}, \mathfrak{q})$ the *signed double* of $\mathbb{F}_p^t$. Then, Γ_O has the following properties:

(i) Γ_O is $\mathfrak{q}$-isotropic: $\mathfrak{q}(Ox, x) = q(Ox) - q(x) = 0$.

(ii) Γ_O has (maximal) dimension t.

(iii) $\mathbf{1} \in \Gamma_O$.

However, not all subspaces $T \subset \mathbb{F}_p^{2t}$ obeying properties (i)–(iii) are graphs. Indeed, it is straightforward to prove that such a T is the graph of some $O \in \mathrm{O}_n^{\mathrm{st}}(p)$ if $T \cap (0 \oplus \mathbb{F}_p^t) = \{0\}$. In general, this intersection can be a non-trivial subspace and thus allows for subspaces T which are not graphs. We call a subspace $T \subset \mathbb{F}_p^{2t}$ a *stochastic Lagrangian subspace* if it fulfils properties (i)–(iii) and define Σ_t to be the set of all stochastic Lagrangians.

This observation is crucial and gives rise to the additional operators $r(T)$ in the characterisation of the Clifford commutant 12.2. For every stochastic Lagrangian $T \in \Sigma_t$, we define an operator on $\mathbb{C}[\mathbb{F}_p^t]$ by

$$r(T) := \sum_{(x,y)\in T} |x\rangle\langle y| \,. \tag{12.34}$$

Note that this is consistent with the representation of $\mathrm{O}_t^{\mathrm{st}}(p)$ introduced before as $r(\Gamma_O) \equiv r(O)$.

Finally, let us elaborate a bit on the structure of the stochastic Lagrangians and the associated operators. The term "Lagrangian" is justified as follows. Define the bilinear form $\mathfrak{b}((x,y),(x',y')) := x \cdot x' - y \cdot y'$ on $\mathbb{F}_p^{2t}$ which is the signed version of the dot product. Then, in analogy to Eq. (12.29), we have the quadratic refinement

$$\mathfrak{q}(v+w) - \mathfrak{q}(v) - \mathfrak{q}(w) = 2\mathfrak{b}(v,w). \tag{12.35}$$

In particular, any stochastic Lagrangian is *self-orthogonal* with respect to the induced form $\mathfrak{b}$:

$$\forall T \in \Sigma_t : \quad T^\perp := \left\{v \in \mathbb{F}_p^{2t} \mid \mathfrak{b}(v,w) = 0 \ \forall w \in T\right\} = T. \tag{12.36}$$

From this it is evident, that the maximal dimension of a self-orthogonal subspace is t and hence a stochastic Lagrangian is indeed maximally isotropic.

Characteristic for a stochastic Lagrangian $T \in \Sigma_t$ are its *left and right defect subspaces*

$$T_{\mathrm{LD}} \oplus 0 := T \cap (\mathbb{F}_p^t \oplus 0), \qquad 0 \oplus T_{\mathrm{RD}} := T \cap (0 \oplus \mathbb{F}_p^t). \tag{12.37}$$

The defining properties (i)–(iii) imply that the left and right defect subspaces are q-isotropic and $\mathbf{1} \in T_{\mathrm{LD}}, T_{\mathrm{RD}}$. As we show in the following, the stochastic Lagrangian T is completely determined by its defect subspaces and an isometry between them.

Denote by pr_L and pr_R the projection onto the left and right component of T. Then, it is clear that we have $T_{\mathrm{LD}} \simeq \ker(\mathrm{pr}_R)$ and $T_{\mathrm{RD}} \simeq \ker(\mathrm{pr}_L)$ as well as $T_L := \operatorname{im} \mathrm{pr}_L \subset T_{\mathrm{LD}}^{\perp}$ and $T_R := \operatorname{im} \mathrm{pr}_R \subset T_{\mathrm{RD}}^{\perp}$. Hence, we find

$$\dim T_{\mathrm{LD}}^{\perp} = \dim \mathbb{F}_p^t - \dim T_{\mathrm{LD}} = \dim T - \dim \ker \mathrm{pr}_R = \dim T_R \leq \dim T_{\mathrm{RD}}^{\perp}, \tag{12.38}$$

$$\dim T_{\mathrm{RD}}^{\perp} = \dim \mathbb{F}_p^t - \dim T_{\mathrm{RD}} = \dim T - \dim \ker \mathrm{pr}_L = \dim T_L \leq \dim T_{\mathrm{LD}}^{\perp}. \tag{12.39}$$

Thus, we find $T_{\mathrm{LD}}^{\perp} = T_R$, $T_{\mathrm{RD}}^{\perp} - T_L$, and $\dim T_{\mathrm{LD}} = \dim T_{\mathrm{RD}}$. In addition, the stochastic Lagrangian T determines a unique map $\varphi : T_{\mathrm{RD}}^{\perp}/T_{\mathrm{RD}} \to T_{\mathrm{LD}}^{\perp}/T_{\mathrm{LD}}$ as follows. For any $w \in T_{\mathrm{RD}}^{\perp}$ select a $v = v(w) \in T_{\mathrm{LD}}^{\perp}$ such that $(v(w), w) \in T$ and set $\varphi([w]) := [v(w)]$. It is straightforward to check that this is well-defined. Then, T is uniquely determined by the triple $(T_{\mathrm{LD}}, T_{\mathrm{RD}}, \varphi)$ since

$$T = \left\{ (v, w) \;\middle|\; w \in T_{\mathrm{RD}}^{\perp},\, v \in \varphi([w]) \right\}. \tag{12.40}$$

Vice versa, one could ask whether there exists a stochastic Lagrangian for a given combination of defect subspaces. To this end, we call a q-isotropic subspace $N \subset \mathbb{F}_p^t$ a *defect subspace* if $\mathbf{1} \in N^{\perp}$. Then, given two defect subspaces $N, M \subset \mathbb{F}_p^t$ of the same dimension, one can show that there exists a $T \in \Sigma_t$ with $T_{\mathrm{LD}} = M$ and $T_{\mathrm{RD}} = N$. The proof uses the fact that any linear map from N to M is an isometry since the subspaces are isotropic. Then, using Witt's theorem for quadratic spaces, one can extend this map to a stochastic orthogonal map $O \in \mathrm{O}_t^{\mathrm{st}}(p)$ on $\mathbb{F}_p^t$ such that $O(N) = M$ (see Ref. [181] for more details). The stochastic Lagrangian is then given as

$$T = \left\{ (O(v + w), w) \;\middle|\; w \in n^{\perp},\, v \in N \right\}. \tag{12.41}$$

This observation can be turned into operator form. Recall that the q-isotropicity of a defect subspace $N \subset \mathbb{F}_p^t$ implies that it is self-orthogonal with respect to the usual Euklidean inner product. Thus, N has the interpretation of a classical self-orthogonal linear code. By the *Calderbank-Shor-Sloane* (CSS) construction this defines a stabiliser code with projector

$$P_N := \frac{1}{|N|^2} \sum_{z,x \in N} Z(z) X(x). \tag{12.42}$$

The above discussion implies that any operator $r(T)$ has the form

$$r(T) = p^{\dim N} r(O) P_N = p^{\dim M} P_M r(O'), \tag{12.43}$$

where N and M are the right and left defect subspaces of T and $O \in \mathrm{O}_t^{\mathrm{st}}(p)$ induces the isometry between them.

For later reference, we state the following lemma at this point.

Lemma 12.2 (Schatten norms of $r(T)$)**.** *For any Schatten b-norm, we have* $\|r(T)\|_b = \|P_N\|_b$. *In particular, we find the following expressions for the* trace, Hilbert-Schmidt *and* spectral norm*:*

$$\|r(T)\|_1 = p^{t - \dim N}, \qquad \|r(T)\|_2 = p^{t/2}, \qquad \|r(T)\|_\infty = p^{\dim N}. \tag{12.44}$$

12.3.2 The orthogonal commutant

The basis of the Clifford commutant introduced in the last section 12.3.1 is based on maximally isotropic subspaces T in the quadratic space $(\mathbb{F}_p^{2t}, \mathfrak{q})$ which has the form of a *signed double* of $\mathbb{F}_p^t$ with its standard Euklidean quadratic form. As we show in this section, a similar construction over a symplectic geometry naturally leads to a spanning set of the *orthogonal commutant* $\mathrm{O}_p^{\mathrm{st}}(t)'$.

To this end, we study Lagrangians in the "signed double" of the phase space $\mathbb{F}_p^{2n}$ and show that they naturally induce operators on Hilbert space. As in the orthogonal case, we give explicit formulas for these operators and show that they can be written as $Q = UP$ for a Clifford unitary U and stabiliser code projector P. These operators form the *Clifford semigroup* which spans the orthogonal commutant. Interestingly, we have already encountered these operators as Kraus operators of CSP channels in Ch. 9. Moreover, they are also related to the study of Clifford projector approximations in Ch. 15.

This construction was introduced for so-called *dual pairs* in the context of Howe duality in representation theory and harmonic analysis by Howe [163, 164] (see also Ref. [110]) together with the closely connected oscillator semigroup (in odd characteristic). However, for the Clifford group there are some notable differences to the construction by Howe. To the best of my knowledge, the orthogonal commutant has not been explicitly described in the literature before.

The Lagrangians in the signed double

We define the *signed double* $(2V, \Omega)$ of a $2n$-dimensional symplectic vector space (V, ω) as the vector space $2V := V \oplus V$ with symplectic form

$$\Omega((v, v'), (w, w')) := \omega(v, w) - \omega(v', w'). \tag{12.45}$$

Its definition is such that the graph of $g \in \mathrm{Sp}(V, \omega)$,

$$\Gamma(g) := \{(g(v), v) \mid v \in V\}, \tag{12.46}$$

forms a $2n$-dimensional isotropic subspace in $2V = V \oplus V$, i. e. a Lagrangian. Vice versa, a subspace $L \subset V \oplus V$ is the graph of a symplectic map if and only if it is Lagrangian and *transverse* with respect to V in the sense that $L \cap (0 \oplus V) = L \cap (V \oplus 0) = \{0\}$. Thus, symplectic maps $g \in \mathrm{Sp}(V, \omega)$ are in bijection with transverse Lagrangians of $2V$ by construction. However, not all Lagrangians subspaces in $2V$ are of this form. In general, a Lagrangian subspace $L \subset 2V$ will have non-trivial overlap with the left/right embeddings.

The following derivation is analogous to App. 9.C. We define the *left and right defect spaces* of a double Lagrangian $L \subset 2V$ as

$$L_{LD} \oplus 0 := L \cap (V \oplus 0), \qquad 0 \oplus L_{RD} := L \cap (0 \oplus V). \tag{12.47}$$

By definition, L_{LD} and L_{RD} are isotropic subspaces of V. Let pr_L and pr_R be the projections onto the left and right factor of L with $\ker \mathrm{pr}_L = L \cap (0 \oplus V) \simeq L_{RD}$ and $\ker \mathrm{pr}_R = L \cap (V \oplus 0) \simeq L_{LD}$. As in App. 9.C, we find $L_L := \mathrm{im}\, \mathrm{pr}_L = L_{RD}^\perp$ and $L_R := \mathrm{im}\, \mathrm{pr}_R = L_{LD}^\perp$. Recall that the quotients $L_{LD}^\perp / L_{LD}$ and $L_{RD}^\perp / L_{RD}$ inherit a symplectic form from ω and

the Lagrangian L uniquely determines a symplectic map $\varphi : L_{RD}^{\perp}/L_{RD} \to L_{LD}^{\perp}/L_{LD}$. Hence, L is uniquely determined by the data $(L_{LD}, L_{RD}, \varphi)$ as

$$L = \{(v,w) \mid w \in L_{RD}^{\perp},\ v \in \varphi([w])\}. \tag{12.48}$$

The symplectomorphism $\varphi : L_{RD}^{\perp}/L_{RD} \to L_{LD}^{\perp}/L_{LD}$ can be seen as being induced from a (non-unique) symplectic map $g \in \mathrm{Sp}(V)$ as follows: Lift φ to an isometry $\tilde{\varphi} : L_{RD}^{\perp} \to L_{LD}^{\perp}$ mapping L_{RD} to L_{LD} and use Witt's theorem 3.1 to extend it to a symplectic map $g \in \mathrm{Sp}(V)$ which yields $\varphi([v]) = [g(v)]$. Vice versa, given two equal-dimensional isotropic subspaces $M, N \subset V$, any bijective linear map $h : M \to N$ is an isometry and thus extends to a symplectic map $g \in \mathrm{Sp}(V)$ which maps $M^{\perp}$ to $N^{\perp}$. Then, Eq. (12.48) yields a valid double Lagrangian L with left and right defect subspaces $L_{LD} = N$, $L_{RD} = M$ and isometry induced by g. Alternatively, we can write it as follows:

$$L = L(M,g) := \{\ (g(w+v), w)\ \mid w \in M^{\perp},\ v \in M\}. \tag{12.49}$$

The set of Lagrangian subspaces is called the *Lagrangian Grassmannian* $\mathrm{Lag}(2V)$. It comes with a semigroup structure via the composition law

$$L \circ L' := \{(v,w) \mid \exists u \in V :\ (v,u) \in L,\ (u,w) \in L'\}. \tag{12.50}$$

The semigroup $\mathrm{Lag}(2V)$ is even a monoid, i. e. it has an additional identity element

$$\Delta = \{(v,v) \mid v \in V\}. \tag{12.51}$$

The Clifford semigroup

As for the stochastic Lagrangian subspaces discussed in Sec. 12.3.1, we want to associate operators to the double Lagrangians $L \in \mathrm{Lag}(2V)$. Here, we describe how such a construction can be achieved on an abstract level and relate it to the well-known Choi-Jamiołkowski isomorphism. In the following, we assume for simplicity that $p > 2$, although all derivations can be done analogously for $p = 2$ as in Sec. 4.2 and were mostly already done in App. 9.C.

Let W be the Schrödinger representation of the Heisenberg group $H(V)$ on a Hilbert space $\mathcal{H} \simeq (\mathbb{C}^p)^{\otimes n}$ with central character χ. The space of linear operators $L(\mathcal{H})$ has a natural irreducible representation of $H(V) \times H(V)$ acting as $A \mapsto W(v,t)AW(w,s)^{\dagger}$. Furthermore, there is a surjective homomorphism $H(V) \times H(V) \to H(2V)$ to the Heisenberg group $H(2V)$ of to signed double $2V$, given by $(v,t) \times (w,s) \mapsto (v,w,t-s)$. Thus, we have an irreducible representation of $H(2V)$ on the Hilbert space $L(\mathcal{H})$ with central character χ given by

$$\tilde{W}(v,w,t)(A) := \chi(t)W(v,0)AW(-w,0). \tag{12.52}$$

With respect to $\tilde{W}$, any double Lagrangian $L \in \mathrm{Lag}(2V)$ can be mapped to a "stabiliser state vector" as described in Sec. 4.2.3. Here, the Hilbert space is $L(\mathcal{H})$ and thus a stabiliser state vector is a linear operator on $\mathcal{H}$. These are exactly the operators we want to construct. Using Eq. (4.49), we can give an explicit formula. Given a Lagrangian $L \in \mathrm{Lag}(2V)$, the "stabiliser operator" w.r.t. $\tilde{W}$ is given by

$$\langle x|\, Q(L)\, |y\rangle = \chi(-q_L(x,y))\mathbf{1}_{\mathsf{X}_L}(x,y). \tag{12.53}$$

Here, X_L is the projection of L onto the x-coordinates and q_L is the quadratic form defined in Eq. (4.52). As in Sec. 4.2.3, stabiliser operators $Q(L,a)$ with non-trivial character $a = (v,w)$ can be obtained by acting with $\tilde{W}(v,w) \equiv W(v)\cdot W(w)^\dagger$ on $Q(L)$.

Note that when the Lagrangian is a graph, $L = \Gamma(g)$, then the defining eigenvalue equation becomes

$$Q(\Gamma(g)) = W(g(v))Q(\Gamma(g))W(v)^\dagger \quad \Leftrightarrow \quad Q(\Gamma(g))W(v)Q(\Gamma(g))^{-1} = W(g(v)). \tag{12.54}$$

Hence, $Q(\Gamma(g))$ has to be proportional to $\mu(g)$. As the normalisation is chosen such that $\|Q(\Gamma(g))\|_2^2 = p^{2n}$, they can only differ by a phase. In fact, one can check that the phase convention agrees with the one in Thm. 3.2, and thus $Q(\Gamma(g)) = \mu(g)$.

Using the above derived normal form (12.49) of Lagrangians $L \in \mathrm{Lag}(2V)$, we can generalise this to arbitrary stabiliser operators $Q(L)$, where

$$L = L(M,g) = \big\{\, (g(w+v), w) \;\big|\; w \in M^\perp,\, v \in M \big\}. \tag{12.55}$$

Indeed, for $w \in M^\perp$ and $v \in M$, we compute

$$\begin{aligned} W(g(v+w))\mu(g)P(M)W(w)^\dagger &= W(g(v+w))\mu(g)W(-w)P(M) \\ &= W(g(v+w))W(-g(w))\mu(g)P(M) \\ &= \mu(g)W(v)P(M) \\ &= \mu(g)P(M). \end{aligned} \tag{12.56}$$

Here, we used that $W(-w)$ commutes with $P(M)$ as $w \in M^\perp$ and that $W(v)P(M) = P(M)$ for $v \in M$. Moreover, one can verify that $\dim \mathsf{X}_L = n - \dim M$ and thus $Q(L) = \mu(g)P(M)$. Finally, general stabiliser operators are obtained as a Weyl orbit $Q(L,(v,w)) = W(v)Q(L)W(w)^\dagger = W(v - g(w))\mu(g)P(M,w)$, and are thus given by all possible Clifford unitaries and stabiliser codes. We refer to the form $Q = UP$ as the "polar form" of the stabiliser operators.

As we have seen, the stabiliser states associated to the above introduced signed double $2V$ have a natural interpretation in terms of operators on the Hilbert space $\mathcal{H} = (\mathbb{C}^p)^{\otimes n}$. This can be seen as a consequence of using the signed symplectic form defined in Eq. (12.45). If we instead use the standard symplectic form on $V \oplus V$, we obtain a set of stabiliser states on the doubled Hilbert space $\mathcal{H}\otimes\mathcal{H} = (\mathbb{C}^p)^{\otimes 2n}$. As we show in the following, the two constructions are related through the *vectorisation* map:

$$\mathrm{vec}: \quad L(\mathcal{H}) \simeq \mathcal{H}\otimes\mathcal{H}^* \longrightarrow \mathcal{H}\otimes\mathcal{H}, \qquad |x\rangle\langle y| \longmapsto |x\rangle\,|y\rangle\,. \tag{12.57}$$

To this end recall that the symplectic structure on a vector space is unique and hence there is an isomorphism mapping $2V$ to $V\oplus V$ with its standard symplectic form. Let us assume for concreteness that $V = \mathbb{F}_p^{2n}$, and write as before any point in the standard polarisation as $v = (z,x)$. Then, consider the isomorphism $*$ which acts on V as $v = (z,x) \mapsto v^* = (-z,x)$. Clearly, the pullback of the standard symplectic form under this map is its negative, i. e. $[v^*,w^*] = -[v,w]$. Thus, letting the map act on the second half of $V\oplus V$, we obtain the desired isomorphism.

Under the vectorisation map, the representation $\tilde{W}(v,w) = W(v)\cdot W(w)^\dagger$ of $H(2V)$ on $L(\mathcal{H})$ corresponds to the representation $W(v)\otimes\overline{W(w)}$ on $\mathcal{H}\otimes\mathcal{H}$. Furthermore, it is

straightforward to check that the isomorphism $*$ acts as complex conjugation on Weyl operators, $W(w^*) = \overline{W(w)}$. Thus, we have the following commutative diagram:

$$\begin{array}{ccc} H(2V) & \xrightarrow{\tilde{W}} & L(\mathcal{H}) \\ \downarrow{\scriptstyle *} & & \downarrow{\scriptstyle \mathrm{vec}} \\ H(V \oplus V) & \xrightarrow{W \otimes W} & \mathcal{H} \otimes \mathcal{H} \end{array} \tag{12.58}$$

This observation gives us an alternative way of constructing the operators. Given a Lagrangian subspace $L \in \mathrm{Lag}(V \oplus V)$ there are p^{2n} associated $2n$-qudit stabiliser states with vectors $|L, a\rangle$ labelled by $a \in V \oplus V/L$ (cp. Secs. 3.1.2 and 4.2.3). Then, we define operators by $Q(L, a) := N \,\mathrm{vec}^{-1}(|L, a\rangle)$. Setting the normalisation to $N = |\mathsf{X}_L|^{1/2}$, it is straightforward to confirm that the so-defined operators $Q(L, a)$ are the same as those in the last section, using the definition of the vectorisation map and the defining Eqs. (12.53) and (4.49) for $Q(L, a)$ and $|L, a\rangle$.

From the perspective of the Choi-Jamiołkowski isomorphism, the stabiliser state vectors $|L, a\rangle$ are the *Choi states* of the operators $Q(L, a)$, up to a constant. Taking care of the correct normalisations, we have the following relation:

$$|L, a\rangle = |\mathsf{X}_L|^{-\frac{1}{2}} Q(L, a) \otimes \mathbb{1}(\mathrm{vec}\,\mathbb{1}) = p^{\frac{n}{2}} \|Q(L, a)\|_2^{-1}\, Q(L, a) \otimes \mathbb{1}\, |\phi^+\rangle\,, \tag{12.59}$$

where $|\phi^+\rangle = p^{-n/2}\,\mathrm{vec}(\mathbb{1})$ is the default maximally entangled state. Based on this observation, it is possible to give an alternative proof of the polar form $Q = UP$ (cp. App. 9.C).

Finally, we can use the eigenvalue equation

$$W(v)Q(L, a)W(w)^\dagger = \chi([a, (v, w^*)])Q(L, a), \quad \forall (v, w^*) \in L, \tag{12.60}$$

to compute the product of stabiliser operators $Q(L, a)Q(L', a')$. As it turns out, this product is proportional to $Q(L \circ L', b)$ for a suitable b. Here, the composition $L \circ L'$ of Lagrangians in $\mathrm{Lag}(V \oplus V)$ is induced from the one in $\mathrm{Lag}(2V)$ defined in Eq. (12.50). Hence, for any $(v, w^*) \in L \circ L'$ there is a $u \in V$ such that $(v, u^*) \in L$ and $(u, w^*) \in L'$. Then, we find

$$\begin{aligned} Q(L, a)Q(L', a')W(w)^\dagger &= \chi([a', (u, w^*)])Q(L, a)W(u)^\dagger Q(L', a') \\ &= \chi([a, (v, u^*)] + [a', (u, w^*)])W(v)^\dagger Q(L, a)Q(L', a'). \end{aligned} \tag{12.61}$$

This equation still depends on the intermediate point $u \in V$. However, the set of admissible points given $(v, w^*) \in L \circ L'$ forms a subspace $U_{v,w} \subset V$. Hence, write $a = (a_L, a_R)$ and $a' = (a'_L, a'_R)$ and average Eq. (12.61) over $u \in U_{v,w}$ to obtain

$$\begin{aligned} W(v)Q(L, a)Q(L', a')W(w)^\dagger &= \chi([(a_L, a'_R), (v, w^*)])Q(L, a)Q(L', a') \times \\ &\qquad \times \frac{1}{|U_{v,w}|} \sum_{u \in U_{v,w}} \chi([a'_L - a_R, u]) \\ &= \chi([(a_L, a'_R), (v, w^*)])Q(L, a)Q(L', a')\mathbf{1}_{U_{v,w}^\perp}(a'_L - a_R). \end{aligned} \tag{12.62}$$

Thus, if $a'_L - a_R$ commutes with all of $U_{v,w}$, then $Q(L, a)Q(L', a')$ has to be proportional to $Q(L \circ L', (a_L, a'_R))$. If it does not, the right hand side of Eq. (12.62) vanishes. Since the superoperator $\tilde{W}(v, w)$ is invertible, this is the case if and only if $Q(L, a)Q(L', a') = 0$.

This shows that the set of operators $Q(L,a)$, obtained as "matrixification" of $2n$-qudit stabiliser states,

$$\begin{aligned}\mathrm{CS}_n(p) &:= \left\{ Q(L,a) \mid L \in \mathrm{Lag}(\mathbb{F}_p^{4n})\ a \in \mathbb{F}_p^{4n}/L \right\} \\ &= \{UP \mid r \in \{0,\dots,n\},\ U \in \mathrm{Cl}_n(p),\ P \in \mathrm{stab}_{n,r}(p)\}\,.\end{aligned} \tag{12.63}$$

can be identified with a semigroup (even monoid) in the projective space $\mathbb{P}(L(\mathcal{H}))$ when the zero matrix is added. By abuse of notation, we call $\mathrm{CS}_n(p)$ the *Clifford semigroup*.

In particular, if we restrict to the operators $Q(L) \equiv Q(L,0)$ (for $p > 2$), this forms a projective representation of the semigroup $\mathrm{Lag}(V \oplus V)$. This is what Howe calls the *oscillator semigroup* [110, 163, 164].

Finally, we will argue that tensor powers of the elements of the Clifford semigroup $\mathrm{CS}_n(p)$ form a generating set for the stochastic orthogonal commutant $\mathrm{O}_t^{\mathrm{st}}(p)'$.

Theorem 12.3 (Thm. 5.6 in Ref. [181])**.** *Let p be any prime and $n, t \in \mathbb{N}$. Then, the trivial isotype of the representation $\mathrm{O}_t^{\mathrm{st}}(p) \ni O \mapsto r(O)^{\otimes n}$ is* $\mathrm{span}\{\,|s\rangle^{\otimes t} \mid s \in \mathrm{stab}_n(p)\}$.

Corollary 12.1. *The t-fold tensor powers of $\mathrm{CS}_n(p)$ span the commutant $\mathrm{O}_t^{\mathrm{st}}(p)'$ of the representation $\mathrm{O}_t^{\mathrm{st}}(p) \ni O \mapsto r(O)^{\otimes n}$.*

Proof. The commutant $\mathrm{O}_t^{\mathrm{st}}(p)'$ is the trivial isotype of the representation $O \mapsto \mathrm{Ad}(r(O)^{\otimes t})$ which in turn is isomorphic to $O \mapsto r(O)^{\otimes n}\overline{r(O)^{\otimes n}} = r(O)^{\otimes 2n}$ via the vectorisation isomorphism. By Thm. 12.3 its trivial isotype is spanned by tensor powers of $2n$-qubit stabiliser states, thus $\mathrm{O}_t^{\mathrm{st}}(p)'$ is spanned by the their pre-image under vec which is exactly $\mathrm{CS}_n(p)^{\otimes n}$. □

However, it is not clear whether the tensor powers of $\mathrm{CS}_n(p)$ are actually *linearly independent*, at least in a certain parameter regime. Contrary to the orthogonal case, where a similar statement for the operators $r(T)^{\otimes n}$ can be readily proven for $n \geq t-1$ [181], this question seems harder to answer. This is also left open in the works by Gurevich and Howe [110] and Howe [163, 164].

Open problem 5 (Basis of the orthogonal commutant)**.** Is the set $\mathrm{CS}_n(p)^{\otimes t}$ linearly independent in some regime of the parameters (t,n)?

CHAPTER 13

GROUP DESIGNS ARE RARE AND ESSENTIALLY CLIFFORD

About this chapter

The following text is based on section V of the following, previously published preprint:

> Jonas Haferkamp, Felipe Montealegre-Mora, Markus Heinrich, Jens Eisert, David Gross and Ingo Roth. *Quantum homeopathy works: Efficient unitary designs with a system-size independent number of non-Clifford gates*. Submitted to Communications in Mathematical Physics. 2020. arXiv: 2002.09524

This section originated from my interest in the special role of the Clifford group in quantum information theory and was conceived by MH and FMM, and eventually formulated by MH.

The following chapter is a slight reformulation of the section in the above paper, adapted to the style and notation of this thesis. In addition, more details and references to other chapters have been included.

There are a number of ways to motivate the prominent use of Clifford unitaries in quantum information theory. For instance, from a physical point of view, Clifford gates are often comparatively easy to implement, in particular in fault-tolerant architectures. As stabiliser codes are treated as the most promising quantum codes for future platforms, fault-tolerantly implementable gates come mostly from the Clifford group.

In this chapter, we point out that Refs. [115, 186] together imply that the Clifford groups are also mathematically distinguished. More precisely, we argue that the Clifford groups are essentially the unique finitely generated family of subgroups which are unitary designs. Proposition 13.1 is a Corollary of the recently published classification of finite unitary subgroups which form t-designs, so-called *unitary t-groups*, by Bannai, Navarro, Rizo and Tiep [115] and a theorem about universality of finitely generated subgroups by Sawicki and Karnas [186].

For any subgroup $G \subseteq \mathrm{U}(d)$, we denote by $\overline{G} := G/Z(G)$ the projective group obtained by modding out the centre. As mentioned in Ch. 12, $\overline{G}$ is a unitary t-design if and only if G is. Hence, any classification of unitary t-groups can only be made up to the centre of a group.

Proposition 13.1 refers to t-designs generated by *finite gate sets*, which we define now. The starting point is a Hilbert space $(\mathbb{C}^q)^{\otimes r}$ for some r. Without loss of generality, we might assume that all gates are special unitaries. Then, a finite gate set is a finite subset

$$\mathcal{G} \subset \mathrm{SU}\big((\mathbb{C}^q)^{\otimes r}\big).$$

We denote by $\mathcal{G}_n$ the subgroup of $\mathrm{SU}\big((\mathbb{C}^q)^{\otimes n}\big)$ generated by elements of $\mathcal{G}$ acting on any r tensor factors (here $r \leq n$). The number q is called the *local dimension* of $\mathcal{G}$.

Proposition 13.1 (Singling out the Clifford group [115, 186]). *Let $t \geq 2$, and let $\mathcal{G}$ be a finite gate set with local dimension $q \geq 2$. Assume that (1) either all $\mathcal{G}_n$ are finite or they are all infinite, and (2) there is an n_0 such that for all $n \geq n_0$, $\mathcal{G}_n$ is a unitary t-design.*

Then, one of the following cases apply:

(i) If $t = 2$, we have either that q is the power of a prime and $\overline{\mathcal{G}}_n$ is isomorphic to a subgroup of the Clifford group $\overline{\mathrm{Cl}}_n(q)$, or *$\mathcal{G}_n$ is dense in $\mathrm{SU}(q^n)$,*

(ii) If $t = 3$, we have either *$q = 2$ and $\overline{\mathcal{G}}_n$ is isomorphic to the full Clifford group $\overline{\mathrm{Cl}}_n(2)$* or *$\mathcal{G}_n$ is dense in $\mathrm{SU}(q^n)$,*

(iii) If $t \geq 4$ then $\mathcal{G}_n$ is dense in $\mathrm{SU}(q^n)$.

Note that a finitely generated infinite subgroup of $\mathrm{SU}(d)$ is always dense in some compact Lie subgroup (cp. [186, Fact 2.6]). In particular, it inherits a Haar measure from this Lie subgroup which allows for a definition of unitary t-design.

Finite case. In the classification in Ref. [115], the non-existence of finite unitary t-groups was shown for $t \geq 4$ (and dimension $d > 2$). Already the case $t = 3$ is very restrictive, since the authors arrive at the following result:

Lemma 13.1 (Ref. [115, Thm. 4]). *Suppose $d \geq 5$ and $H < \mathrm{U}(d)$ is a finite unitary 3-group. Then, $\overline{H}$ is either one of finitely many exceptional cases or $d = 2^n$ and $\overline{H}$ is isomorphic to the Clifford group $\overline{\mathrm{Cl}}_n(2)$.*

Since neither of the exceptions is a finitely generated family of subgroups, this establishes the finite version of (ii), the $t = 3$ case.

The classification of unitary 2-designs is however more involved, it includes certain irreducible representations of finite unitary and symplectic groups (compare [115, Thm. 3, Lie-type case]), and a finite set of exceptions. We give a shortened version of the result as follows.

Lemma 13.2 (Ref. [115, Thm. 5]). *Suppose $d \geq 5$ and $H < \mathrm{U}(d)$ is a finite unitary 2-group. Then, one of the following cases applies*

(i) (Lie-type case) [...]

(ii) (Extraspecial case) $d = p^k$ for a prime p and $\overline{\mathrm{HW}}_k(p) \lhd \overline{H}$. Moreover, $\overline{H}/\overline{\mathrm{HW}}_k(p)$ is isomorphic to a subgroup of $\mathrm{Sp}_k(p)$ which acts transitively on $\mathbb{F}_p^{2k} \setminus 0$.

(iii) (Exceptional case) [...]

The exceptional case (iii) can be ruled out in the same way as above. The Lie-type cases (i) happen in dimensions $(3^n \pm 1)/2$ and $(2^n + (-1)^n)/3$. There is no q for which there exists an n_0 such that for all $n \geq n_0$ there exists an $m \in \mathbb{N}$ satisfying either

$$q^n = (3^m \pm 1)/2 \qquad \text{or} \qquad q^n = (2^m + (-1)^m)/3.$$

Thus, the assumptions of Prop. 13.1 rule these out. Then, case (ii) of Lemma 13.2 establishes the finite version of Prop. 13.1 (i), cp. also Sec. 12.2.

Infinite case. Define the commutant for a set $S \subset \mathrm{SU}(d)$ of the adjoint action as

$$\mathrm{Comm}(\mathrm{Ad}_S) := \left\{ L \in \mathrm{End}\left(\mathbb{C}^{d\times d}\right) \,\middle|\, [\mathrm{Ad}_g, L] = 0 \;\; \forall g \in S \right\}.$$

We show that the second case can be reduced to Cor. 3.5 from Ref. [186] applied to the simple Lie group $\mathrm{SU}(d)$.

Lemma 13.3 ([186, Cor. 3.5])**.** *Given a finite set $G \subset \mathrm{SU}(d)$ such that $\mathcal{G} = \langle G \rangle$ is infinite. Then, the group $\mathcal{G}$ is dense in* $\mathrm{SU}(d)$ *if and only if*

$$\mathrm{Comm}(\mathrm{Ad}_{\mathcal{G}}) \cap \mathrm{End}(\mathfrak{su}(d)) = \{\lambda\, \mathrm{id}_{\mathfrak{su}(d)} \,|\, \lambda \in \mathbb{R}\}. \tag{13.1}$$

Recall that a subgroup $\mathcal{G} \subseteq U(d)$ is a unitary 2-group if and only if $\mathrm{Comm}(U \otimes U | U \in \mathcal{G}) = \mathrm{Comm}(U \otimes U | U \in \mathrm{U}(d)) = \mathrm{span}\{\mathbb{1}, \mathbb{F}\}$, where $\mathbb{F}$ denotes the flip of two tensor copies.Let us denote the partial transpose on the second system of a linear operator $A \in L(\mathbb{C}^d \otimes \mathbb{C}^d)$ by A^Γ. Then, one can easily verify that Γ induces a vector space isomorphism between $\mathrm{Comm}(U \otimes U | U \in \mathcal{G})$ and $\mathrm{Comm}(U \otimes \overline{U} | U \in \mathcal{G})$. The image of the basis $\{\mathbb{1}, \mathbb{F}\}$ is readily computed as

$$\mathbb{1}^\Gamma = \mathbb{1}, \qquad \mathbb{F}^\Gamma = d\, |\Omega\rangle\langle\Omega|\,, \tag{13.2}$$

where $|\Omega\rangle = d^{-1/2} \sum_{i=1}^d |ii\rangle$ is the maximally entangled state vector. Next, we use that $U \otimes \overline{U} = \mathrm{mat}(\mathrm{Ad}_U)$ is the matrix representation of $\mathrm{Ad}_U = U \cdot U^\dagger$ with respect to the basis $E_{i,j} = |i\rangle\langle j|$ of $L(\mathbb{C}^d)$. Thus, we have $\mathrm{Comm}(\mathrm{Ad}_{\mathcal{G}}) \simeq \mathrm{Comm}(U \otimes \overline{U} | U \in \mathcal{G})$ as algebras. Pulling the above basis of $\mathrm{Comm}(U \otimes \overline{U} | U \in \mathcal{G})$ back to $\mathrm{Comm}(\mathrm{Ad}_{\mathcal{G}})$, we then find:

$$\mathrm{mat}^{-1}(\mathbb{1}) = \mathrm{id}_{L(\mathbb{C}^d)}, \quad \mathrm{mat}^{-1}(\,|\Omega\rangle\langle\Omega|\,) = \mathrm{tr}(\bullet)\mathrm{id}_{L(\mathbb{C}^d)}. \tag{13.3}$$

Hence, we have shown that any element in $\mathrm{Comm}(\mathrm{Ad}_{\mathcal{G}})$ is a linear combination of these two maps. However, by restricting to $\mathfrak{su}(d)$, the second map becomes identically zero, thus we have

$$\mathrm{Comm}(\mathrm{Ad}_{\mathcal{G}}) \cap \mathrm{End}(\mathfrak{su}(d)) = \{\lambda\, \mathrm{id}_{\mathfrak{su}(d)} \,|\, \lambda \in \mathbb{R}\}. \tag{13.4}$$

By Lemma 13.3, this shows that any finitely generated infinite unitary 2-group $\mathcal{G} \leq \mathrm{SU}(d)$ is dense in $\mathrm{SU}(d)$. Since any unitary t-group is in particular a 2-group, this is also true for any $t > 2$.

CHAPTER 14

APPROXIMATE t-DESIGNS WITH FEW NON-CLIFFORD GATES

About this chapter

This chapter is based on the following article:

> Jonas Haferkamp, Felipe Montealegre-Mora, Markus Heinrich, Jens Eisert, David Gross and Ingo Roth. *Quantum homeopathy works: Efficient unitary designs with a system-size independent number of non-Clifford gates*. Submitted to Communications in Mathematical Physics. 2020. arXiv: 2002.09524

The paper is the result of a deep collaboration among the authors. As a consequence, my contribution is difficult to isolate in this work and hence the full article is not included in this dissertation. An exception is Section V which is included as Ch. 13. Because the work on this project has influenced and provides context for other works of mine, see Ch. 9 and 15, a concise summary is given in this chapter.

14.1 Introduction

As laid out in Chapter 13, the Clifford groups occupy a somewhat singular role – they are a locally generated family of finite subgroups in prime-power dimensions, which form unitary 2-designs in odd dimensions and 3-designs in even dimensions. Due to the non-existence of unitary 4-groups [115], efficient higher-order designs have to be constructed by other means.

Very recently, Bannai, Nakata, Okuda and Zhao [178] proposed an iterative method which – in principle – allows to build higher-order unitary designs from lower-order designs. As an example, they construct an exact 4-design for two qubits from three copies of the two-qubit Clifford group. Their construction is based on the knowledge of the irreps of the fourth tensor power representation of the Clifford group. To me, it is not clear whether their method can be generalised to the n-qubit setting and, if so, yields efficient unitary designs. At the minimum, it seems to require insights into the representation theory of the Clifford group which is still under current research [192]. However, it seems worthwhile to investigate this further in the future.

Since the requirements for *exact* unitary designs are rather strict, our approach is to construct *approximate* unitary designs instead. Assuming that the approximation is in a sufficiently strong sense, this is enough for most applications. A constructive way of building approximate designs is given by *random circuits*. Indeed, it has been known for some time that polynomial-depth random circuits composed of local gates from a universal set form *approximate* unitary 2-designs. [193]. Subsequently, this result has been improved and extended, showing that the circuit depth and design order are in general polynomially related [182, 194–197]. Moreover, it is widely believed that local

random circuits on n qubits generate an approximate unitary t-design in $O(nt)$ depth, a conjecture formulated in Ref. [182].

In our work [129], we choose a more structured gate set from which the random circuits are constructed. Namely, the gate set consists of all Clifford gates and an arbitrary, but fixed non-Clifford gate K. As the Clifford group can be efficiently described and its elements can be efficiently implemented in terms of local generators, this choice has the potential to yield efficient unitary designs (cp. Sec. 3.1.4 and 5.3.2). Indeed, the underlying motivation for this choice is three-fold:

First, any non-trivial non-Clifford gate K is enough to promote the classically simulable Clifford circuits to universality [60]. However, the power of Clifford circuits with *finite non-Clifford resources* is still an active line of research of both practical and theoretical importance. While resource theories of magic discussed in Part II try to quantify these resources, unitary designs measure how quickly Clifford circuits become dense in the unitary group when supplied with non-Clifford resources.

Second, Clifford gates are usually easier to implement than non-Clifford gates. Strictly speaking, this is only true when we consider common *fault-tolerant architectures*. However, it is questionable whether unitary designs can even be implemented on non-fault-tolerant quantum computers. Since errors accumulate quickly, already moderately-sized quantum circuits are beyond their reach. In practise, this means that a generic n-qubit Clifford unitary cannot be executed when $n \approx 5$. In this sense, the focus of the random circuits discussed here are fault-tolerant quantum computers. Then, unitary designs with mostly Clifford gates are preferable over designs with random gates.

Third, the Clifford group is the optimal starting point from the perspective of designs since it is the "maximal" unitary group design. Although the Clifford commutant deviates more and more from the unitary commutant with t, additional non-Clifford gates should close this gap since the underlying gate set is universal. Since the dimension of the Clifford commutant does not dependent on the number of qubits n, it turns out that a n-independent number of non-Clifford gates is actually enough.

More precisely, we prove that random Clifford circuits supplied with $\tilde{O}(t^4 \log(1/\varepsilon)$ fixed non-Clifford gates consist an approximate unitary t-design with an additive diamond norm error ε. In terms of the standard Clifford generators, this yields an overall gate count of $\tilde{O}(n^2 t^4 \log(1/\varepsilon))$ which is a significant improvement compared to the gate count $\tilde{O}(n^2 t^{10} \log(1/\varepsilon))$ for the local random circuits considered in Ref. [182]

Interestingly, the design order of a family of circuits was recently related to a notion of circuit complexity [198]. In this sense, our work shows that the complexity of Clifford+K circuits can be quantified by the number of K gates.

14.2 Results

14.2.1 Approximate unitary t-designs with few non-Clifford gates

Before we state our results, we have to introduce some notation. As in Ch. 12, we denote by ν a probability measure on the unitary group $\mathrm{U}(d)$. Let us define the quantum channel

$$\Delta_t(\nu) := \int_{\mathrm{U}(d)} U^{\otimes t} \cdot (U^{\otimes t})^\dagger \, \mathrm{d}\nu(U), \tag{14.1}$$

which we call the t-th moment operator of the measure ν. Recall from Ch. 12 that ν is a unitary t-design if and only if $\Delta_t(\nu) = \Delta_t(\mu_{\mathrm{H}})$ where μ_{H} is the normalised Haar measure on $\mathrm{U}(d)$. For an *approximate unitary design* we only require that the moment operator of ν is close to the Haar operator. Naturally, there a different notions of "closeness" expressed by the choice of a distance function. Here, we require approximation in diamond norm, which is defined for any superoperator $\phi : L(\mathbb{C}^d) \to L(\mathbb{C}^d)$ as

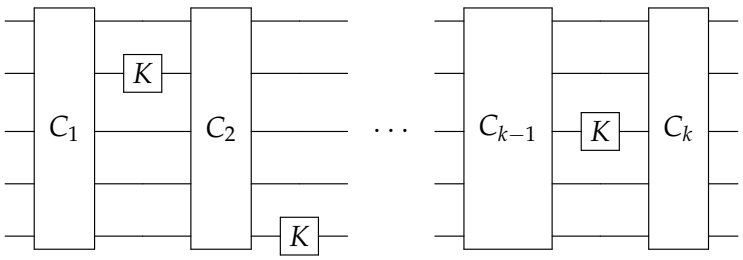
$$\|\phi\|_\diamond := \left\|\phi \otimes \mathrm{id}_{L(\mathbb{C}^d)}\right\|_{1\to 1} = \sup_{\|X\|_1 \leq 1} \left\|\phi \otimes \mathrm{id}_{L(\mathbb{C}^d)}(X)\right\|_1 . \tag{14.2}$$

This is motivated by the operational meaning of the diamond distance as the maximum success probability of distinguishing two quantum channels. In particular, the deviation in total variation distance of the outcome distributions of any measurement on the output of $\Delta_t(\nu)$ and $\Delta_t(\mu_{\mathrm{H}})$ is bounded by their diamond norm distance.

Definition 14.1 (Approximate unitary t-design)**.** A probability measure ν on $\mathrm{U}(d)$ is an (additive) ε-approximate unitary t-design if

$$\|\Delta_t(\nu) - \Delta_t(\mu_{\mathrm{H}})\|_\diamond \leq \varepsilon. \tag{14.3}$$

Next, we describe the probability measure which underlies our random circuit construction. The random circuits consist of k layers of which any layer is given by a random element C from the multi-qubit Clifford group $\mathrm{Cl}_n \equiv \mathrm{Cl}_n(2)$, followed by a non-Clifford single-qubit gate K acting on a random qubit:



(14.4)

To make this formal, let μ_{Cl} be the normalised counting measure on the n-qubit Clifford group Cl_n and let $K \in \mathrm{U}(2)$ be a non-trivial non-Clifford unitary. Note that without loss of generality, we can assume that K acts exclusively on the first qubit, since any qubit permutation is Clifford and can thus be absorbed into the Clifford part. Furthermore, we introduce a technical assumption, namely that instead of applying K, we apply a random gate from the set $\{\mathbb{1}_n, K \otimes \mathbb{1}_{n-1}, K^\dagger \otimes \mathbb{1}_{n-1}\}$. This ensures that the moment operator associated with the counting measure ξ_K on this set is self-adjoint. The reason for including the identity is to simplify certain steps in the proof. Clearly, we can leave out the identity and the depth k derived here is an upper bound on the depth without sampling the identity. Finally, note that the probability measure which describes the product of two unitaries U_1 and U_2 drawn from measures ν_1 and ν_2, respectively, is the convolution measure $\nu_1 * \nu_2$.

Definition 14.2 (Interleaved Clifford circuit)**.** Let $K \in \mathrm{U}(2)$ and let ξ_K be the counting measure on $\{\mathbb{1}_n, K \otimes \mathbb{1}_{n-1}, K^\dagger \otimes \mathbb{1}_{n-1}\}$. A *$K$-interleaved Clifford circuit* of depth k is a random quantum circuit described by the probability measure $\sigma_k := \sigma^{*k}$ where $\sigma := \mu_{\mathrm{Cl}} * \xi_K$.

This definition now allows us to state our main result.

Theorem 14.1 (Unitary designs with few non-Clifford gates [197, Thm. 1])**.** *Let $K \in \mathrm{U}(2)$ be a non-trivial non-Clifford unitary. Then, there are constants $c_1(K), c_2(K) > 0$ such that for any $k \geq c_1(K) \log^2(t) \left(t^4 + t \log(1/\varepsilon)\right)$, the K-interleaved Clifford circuits of depth k acting on n qubits form an additive ε-approximate unitary t-design for all $n \geq c_2(K) t^2$.*

We outline the proof of Thm. 14.1 in Sec. 14.3. Note that n-qubit Clifford unitaries can be sampled efficiently using $O(n^3)$ random bits [119], cp. Sec. 5.3.1. Then, the sampled Clifford unitaries can be efficiently compiled into $O(n^2/\log(n))$ generators [88]. This yields an overall gate count of $O(n^2/\log(n)\log^2(t)t^4)$ which improves considerably on $O(n^2 t^{10})$ reported for local random circuits in Ref. [182]. This is possible since part of the randomness is provided by a classical computer. We consider a variant of Thm. 14.1 based on random walks on local generators in Cor. 14.2.

Our construction has direct relations to the complexity of Clifford circuits with a limited number of non-Clifford gates. Stabiliser-based simulation methods are able to simulate these Circuits with a runtime which scales exponential in the number of non-Clifford gates, see Ch. 8 and Refs. [26, 27, 29–37]. This implies that our scheme yields a family of approximate $O(\log(n))$-designs which are simulable on a classical computer in quasi-polynomial time. It is conjectured that a linear scaling of the depth with t is sufficient which would improve the runtime to polynomial time.

Conversely, a recent connection between design order and complexity drawn by Brandão et al. [198] states that a random element from an approximate unitary t-design has high probability to have a circuit complexity $\sim t$. Since in our construction, the design order and the number of non-Clifford gates is related as $k = O(t^4)$, this implies that the complexity of a quantum circuit with k non-Clifford gates is very likely to be $k^{\frac{1}{4}}$.

Our proof technique can also be used to prove that K-interleaved Clifford circuits form approximate unitary designs with respect to a stronger notion of approximation.

Definition 14.3 (Relative approximate unitary t-design)**.** A probability measure ν is a *relative ε-approximate t-design* if

$$(1-\varepsilon)\Delta_t(\mu_{\mathrm{H}}) \preceq \Delta_t(\nu) \preceq (1+\varepsilon)\Delta_t(\mu_{\mathrm{H}}), \tag{14.5}$$

where $A \preceq B$ if and only if $B - A$ is completely positive.

For this stronger notion of relative approximation, we lose the system-size independence in the number of non-Clifford gates. However, at the same time, the scaling improves to almost linear in t.

Corollary 14.1 (K-interleaved Clifford circuits as relative approximate designs [197, Cor. 2])**.** *There are constants $c_1'(K), c_2'(K) > 0$ such that K-interleaved Clifford circuits are a relative ε-approximate unitary t-design in depth $k \geq c_1'(K) \log^2(t)(2nt + t\log(1/\varepsilon))$ for all $n \geq c_2'(K) t^2$.*

For applications, the constants given in the theorems have to be worked out explicitly for a choice of K. Here, we intentionally leave this choice open and thus have to rely on general bounds on certain spectral gaps. The resulting constants can be very large if for example K is close to the identity. However, given a choice of K, it is very likely that the given scaling can be further improved using tighter bounds. This is already the case if

we replace the fixed gate K with a Haar-random unitary from $\mathrm{U}(2)$ in every layer. Then, it is straightforward to adapt our proof to show the following.

Proposition 14.1 (Haar-interleaved Clifford circuits [197, Prop. 1])**.** *Clifford circuits interleaved with Haar-random single-qubit unitaries form an additive ε-approximate unitary t-design in depth $k \geq 36(33t^4 + 3t\log(1/\varepsilon))$ for all $n \geq 33t^2 + 7$.*

14.2.2 Local random Clifford circuits

As already mentioned before, instead of compiling a random Clifford unitary into generators, we can also consider a random Clifford circuit composed of local generators instead. To this end, we first establish how quickly such a local random Clifford circuit converges t-th moment operator $\Delta_t(\mu_{\mathrm{Cl}})$ of the Clifford group. We take $G \subset \mathrm{Cl}_2$ to be a set of 2-local generators for the Clifford group. For technical reasons, we assume G is closed under taking inverses. An example of such a *closed generating set* is $\{H \otimes \mathbb{1}, S \otimes \mathbb{1}, S^3 \otimes \mathbb{1}, CX\}$. By letting the generators act on all pairs of qubits we obtain a closed, generating set $G_n \subset \mathrm{Cl}_n$ for the n-qubit Clifford group.

Definition 14.4 (Local random Clifford circuit)**.** Let $G \subset \mathrm{Cl}_2$ be a closed, generating set and let $G_n \subset \mathrm{Cl}_n$ be the induced generating set for the n-qubit Clifford group. Let σ_G be the normalised counting measure on G_n, then a *local random Clifford circuit* of depth m is obtained by drawing m times from σ_G and described by the probability measure σ_G^{*m}.

An *approximate Clifford t-design* is defined analogously to the unitary case, but approximates the Clifford moment operator instead.

Theorem 14.2 (Local random Clifford designs[197, Thm. 3])**.** *Let $n \geq 12t$ and $G \subset \mathrm{Cl}_2$ be a closed, generating set. Then, there is a constant $c(G) > 0$ such that local random Clifford circuits of depth $m \geq c(G)nt^8 \log^{-2}(t)(2nt + \log(1/\varepsilon))$ form relative ε-approximate Clifford t-designs.*

Using Thm. 14.2, we can replace the random n-qubit Clifford unitaries in the interleaved random circuit Eq. (14.4) by a local random Clifford circuit of appropriate depth. This results in the following corollary, involving only local gates:

Corollary 14.2 (Approximate designs from local generators [197, Cor. 3])**.** *Let $K \in \mathrm{U}(2)$ be a non-trivial non-Clifford unitary and let $G \subset \mathrm{Cl}_2$ be a closed, generating set. Then, there are constants $c_1''(K,G), c_2''(K), c_3''(K,G) > 0$ such that for*

$$\begin{aligned} m &\geq c_1''(K,G)nt^8/\log^2(t)\,(2nt + \log(1/\varepsilon))\,, \\ k &\geq c_2''(K)\log^2(t)\left(t^4 + t\log(1/\varepsilon)\right), \end{aligned}$$

the local random circuits defined by $\sigma_{k,m} := (\sigma_G^{*m} * \xi_K)^{*k}$ form an additive ε-approximate unitary t-design for all $n \geq c_3''(K)t^2$.

14.3 Technical background

In this section, some details on the techniques used to prove the above results are given. An outline of the proofs of Thm. 14.1 and Thm. 14.2 is presented in Secs. 14.3.1 and

14.3.2, including some comments on the technicalities involved. Furthermore, a few selected proofs are given. For more details and all proofs the interested reader is referred to Ref. [58].

14.3.1 Approximate unitary designs

Overview of the proof of Thm. 14.1

To prove that K-interleaved random Clifford circuits are additive ε-approximate t-designs, we have to bound the diamond distance between the t-moment operator $\Delta_t(\sigma_k)$ and the Haar moment operator $\Delta_t(\mu_{\mathrm{H}})$. Since the measure $\sigma_k = \sigma^{*k}$ is a k-fold convolution of $\sigma = \mu_{\mathrm{Cl}} * \xi_K$, its moment operator decomposes as

$$\Delta_t(\sigma_k) = \underbrace{\Delta_t(\mu_{\mathrm{Cl}})\Delta_t(\xi_K)\ldots\Delta_t(\mu_{\mathrm{Cl}})\Delta_t(\xi_K)}_{k \text{ times}}. \tag{14.6}$$

In the following, we use the shorthand notations $P_{\mathrm{H}} := \Delta_t(\mu_{\mathrm{H}})$, $P_{\mathrm{Cl}} := \Delta_t(\mu_{\mathrm{Cl}})$, and $R(K) := \Delta_t(\xi_K)$. Recall from Sec. 12.1 that P_{H} and P_{Cl} coincide with the projections on the commutant of the t-th tensor power representation of the unitary group and the Clifford group, respectively. From the fact that P_{H} is invariant under left and right multiplication with unitaries, the following identity follows for any mixed unitary channel $\mathcal{E}$:

$$\mathcal{E}^k - P_{\mathrm{H}} = (\mathcal{E} - P_{\mathrm{H}})^k. \tag{14.7}$$

Thus, we can rewrite the difference of $\Delta_t(\sigma_k)$ to the Haar projector P_{H} as

$$\Delta_t(\sigma_k) - P_{\mathrm{H}} = \left(P_{\mathrm{Cl}}R(K)\right)^k - P_{\mathrm{H}} = \left[(P_{\mathrm{Cl}} - P_{\mathrm{H}})R(K)\right]^k. \tag{14.8}$$

Clearly, the superoperator $P_{\mathrm{Cl}} - P_{\mathrm{H}}$ is the projection onto the orthocomplement of the unitary commutant within the Clifford commutant. In particular, if $t \leq 3$, then $P_{\mathrm{Cl}} - P_{\mathrm{H}} = 0$. Note that given an orthonormal basis E_i of the orthocomplement, we can write the projector $P_{\mathrm{Cl}} - P_{\mathrm{H}}$ as

$$P_{\mathrm{Cl}} - P_{\mathrm{H}} = \sum_i |E_i)(E_i|\,, \tag{14.9}$$

where $(A|$ is the linear form which acts on operators as $(A|: B \mapsto (A|B)$ and

$$(A|B) := \mathrm{tr}(A^\dagger B), \tag{14.10}$$

is the Hilbert-Schmidt inner product. Then, Eq. (14.8) can be explicitly expressed via the matrix elements of $R(K)$ in this basis:

$$\left[(P_{\mathrm{Cl}} - P_{\mathrm{H}})R(K)\right]^k = \sum_{i_1,\ldots,i_k} |E_{i_1})\,(E_{i_1}|\,R(K)\,|E_{i_2})\,(E_{i_2}|\,R(K)\,|E_{i_3})\ldots\left(E_{i_{k-1}}\right|R(K)\left|E_{i_k}\right)\,(E_{i_k}| \tag{14.11}$$

Because any non-Clifford gate K renders the Clifford group universal, it might be intuitively clear that $R(K)\,|E_i)$ should have a small overlap with the Clifford commutant and this effect is accumulating with k. This is the idea which underlies the proof of Thm. 14.1.

However, there are some technical details that have to be taken into account. For once, $R(K)$ acts only on a single qubit, thus its matrix elements could still be considerably

large in n. Here, the characterisation of the Clifford commutant given in Ref. [181] and discussed in Sec. 12.3.1, is of great importance. Recall that there is a natural basis for the Clifford commutant which is given by the operators $r(T)^{\otimes n}$ for $T \in \Sigma_t$ a stochastic Lagrangian subspace. As it is factorising, this choice of basis is very convenient and allows to take advantage of the fact that K is a single-qubit gate. Consequently, we derive a series of lemmata which bound the overlaps of $R(K)$ in this basis. In fact, it will be convenient to normalise the $r(T)$ basis as

$$Q_T := \frac{r(T)}{\|r(T)\|_2} = 2^{-t/2} r(T). \tag{14.12}$$

Then, the key lemma is the following.

Lemma 14.1 (Overlap bound)**.** *Let K be a single-qubit non-Clifford gate. Then, there is a $c(K) > 0$ such that*

$$\eta_{K,t} := \max_{\substack{T \in \Sigma_t \setminus S_t \\ T' \in \Sigma_t}} \frac{1}{3} \left| (Q_T| \operatorname{Ad}(K)^{\otimes t} + \operatorname{Ad}(K^\dagger)^{\otimes t} + \mathrm{id} \, |Q_{T'}) \right| \leq 1 - c(K) \log^{-2}(t). \tag{14.13}$$

Albeit, the $\{Q_T^{\otimes n}\}$ basis is not orthogonal and thus we cannot use the expansion in Eq. (14.11) directly. However, as $(Q_T|Q_{T'}) < 1$ for $T \neq T'$, the overlaps are exponentially small in n. This indicates that the bounds we obtain in the Q_T basis should be close to the ones in a suitable orthonormal basis. In our paper [58], we apply a Gram-Schmidt orthogonalisation to $\{Q_T^{\otimes n}\}$, resulting in an orthonormal basis

$$E_j := \sum_{i=1}^{j} A_{i,j} Q_{T_i}^{\otimes n}, \tag{14.14}$$

where $\{T_i\}$ is an enumeration of the elements in Σ_t such that the first $t!$ elements correspond to the permutations S_t. Importantly, it is possible to give reasonably good bounds on the magnitude of $A_{i,j}$ and the norm of E_j. Then, expanding in the orthogonalised basis as in Eq. (14.11), we obtain

$$\begin{aligned} &\left\| [(P_{\mathrm{Cl}} - P_{\mathrm{H}}) R(K)]^k \right\|_\diamond \leq \\ &\quad \sum_{i_1, \ldots, i_k} \left\| \, |E_{i_1})(E_{i_k}| \, \right\|_\diamond | \, (E_{i_1}| \, R(K) \, |E_{i_2}) \, | | \, (E_{i_2}| \, R(K) \, |E_{i_3}) \, | \ldots | \, \left(E_{i_{k-1}}\right| R(K) \left|E_{i_k}\right) \, |. \end{aligned} \tag{14.15}$$

We can now expand the E_j in the Q_T basis using Eq. (14.14) which introduces additional corrections, e. g.

$$| \, (E_i| \, R(K) \, |E_j) \, | \leq \sum_{r=1}^{i} \sum_{l=1}^{j} |A_{r,i} A_{l,j}| \, | \, (Q_{T_r}| \, R(K) \, |Q_{T_l}) \, |. \tag{14.16}$$

We refrain from giving the details of the following steps. These are quite technical and involve careful bounds for the appearing terms in different ways. Finally, the following bound can be obtained:

$$\left\| [(P_{\mathrm{Cl}} - P_{\mathrm{H}}) R(K)]^k \right\|_\diamond \leq 2^{33t^4 + t \log(k)} \left(1 + 2^{32t^2 - n}\right)^{5k} \eta_{K,t}^{k-1} \tag{14.17}$$

From this, the statement in Thm. 14.1 can be directly derived by taking the logarithm on both sides and using the bound in Lem. 14.1 and $\log(1 + x) \leq x$.

Corollary 14.1 and Proposition 14.1 follow with a slight modification to the argument.

Overlap bound

The Gram-Schmidt orthogonalisation of the commutant basis is merely a technical step which allows us to expand the difference of the moment operators in terms of the $Q_T^{\otimes n}$. Instead, the main ingredient to Thm. 14.1 is given by Lem. 14.1. Its proof is in turn based on a theorem due to Varjú [199] and the following lemma:

Lemma 14.2 (Haar symmetrisation)**.** *For all $t \in \mathbb{N}$ and $T \in \Sigma_t \setminus S_t$, it holds that*

$$(Q_T| P_{\mathrm{H}} |Q_T) = 2^{-t} \|P_{\mathrm{H}}[r(T)]\|_2^2 \leq \frac{7}{8}, \tag{14.18}$$

where $P_{\mathrm{H}} = \Delta_t(\mu_{\mathrm{H}})$ is the t-th moment operator of the single-qubit unitary group $\mathrm{U}(2)$.

The proof of Lemma 14.2 heavily uses the structure of the stochastic Lagrangian subspaces and can be found in our paper Ref. [197]. Varjú's theorem is repeated as this point for convenience.

Proposition 14.2 ([199, Thm. 6])**.** *Let ν be a probability measure on $\mathrm{U}(d)$. Consider the averaging operator $T_v(\nu)$ of a irreducible representation $\rho_v : \mathrm{U}(d) \to L(W_v)$ parameterized by highest weight $v \in \mathbb{Z}^d$:*

$$T_v(\nu) := \int_{\mathrm{U}(d)} \rho_v(U) \, \mathrm{d}\nu(U). \tag{14.19}$$

Then there are numbers $c(d) > 0$ and $r_0 > 0$ such that

$$\delta_r(\nu) := 1 - \max_{0<|v|\leq r} \|T_v(\nu)\|_\infty \geq c(d)\delta_{r_0}(\nu) \log^{-2}(r), \tag{14.20}$$

where $|v|^2 = \sum_i v_i^2$.

Here, $\delta_r(\nu)$ is called the *restricted spectral gap* of ν. We can now give a proof of Lem. 14.1.

Proof of Lemma 14.1. As before, let ξ_K be the normalised counting measure on $\{\mathbb{1}, K, K^\dagger\}$, μ_{Cl} the one on the single-qubit Clifford group Cl_1, and ν_K the average of $\xi_K * \xi_K$ and μ_{Cl}. Its moment operator is thus

$$\Delta_t(\nu_K) = \frac{1}{2}\Big(\Delta_t(\mu_{\mathrm{Cl}}) + \Delta_t(\xi_K * \xi_K)\Big) = \frac{1}{2}\Big(\Delta_t(\mu_{\mathrm{Cl}}) + \Delta_t(\xi_K)^2\Big). \tag{14.21}$$

We can decompose the representation $U \mapsto \mathrm{Ad}(U)^{\otimes t}$ of the unitary group into irreps ρ_v of highest weight v. From the representation theory of the unitary group, we know that no irreps with $|v| > \sqrt{2}t$ can hereby appear. This implies that we have the following decomposition with multiplicities m_v (possibly zero):

$$\begin{aligned}
\big\|\Delta_t(\nu_K) - P_{\mathrm{H}}\big\|_\infty &= \left\| \bigoplus_{|v|\leq\sqrt{2}t} \big(T_v(\nu_K) - T_v(\mu_{\mathrm{H}})\big) \otimes \mathrm{id}_{m_v} \right\|_\infty \\
&= \left\| \bigoplus_{0<|v|\leq\sqrt{2}t} T_v(\nu_K) \otimes \mathrm{id}_{m_v} \right\|_\infty \\
&= \max_{0<|v|\leq\sqrt{2}t} \|T_v(\nu_K)\|_\infty \\
&= 1 - \delta_{\sqrt{2}t}(\nu_K).
\end{aligned} \tag{14.22}$$

In the second step, we used that P_{H} is the projector onto the trivial isotype of $U \mapsto \mathrm{Ad}(U)^{\otimes t}$ and has thus only support on the trivial irrep $v = 0$. However, $T_0(\nu_K) = T_0(\mu_{\mathrm{H}})$ and this contribution cancels. In the third step, we then used that the spectral norm of a block-diagonal matrix is the biggest spectral norm over the blocks.

As the Clifford group supplemented with any non-Clifford gate is universal, so is ν_K, i. e. its powers converge to the Haar measure on $\mathrm{U}(2)$. This implies that the restricted spectral gap $\delta_r(\nu_K) > 0$ for all $r \geq 0$, cp. Ref. [193]. Thus, we find using Varjú's theorem:

$$\delta_{\sqrt{2}t}(\nu_K) \geq c(2)\delta_{r_0}(\nu_K)\log^{-2}(\sqrt{2}t) \geq \frac{c(2)}{4}\delta_{r_0}(\nu_K)\log^{-2}(t) =: C'(K)\log^{-2}(t) > 0. \tag{14.23}$$

And hence:

$$\left\|\Delta_t(\nu_K) - P_{\mathrm{H}}\right\|_\infty \leq 1 - \delta_{\sqrt{2}t}(\nu_K) \leq 1 - C'(K)\log^{-2}(t) =: \kappa_{t,K} < 1. \tag{14.24}$$

For any $T \in \Sigma_t \setminus S_t$, we can define the operator

$$X_T := \frac{(\mathrm{id} - P_{\mathrm{H}})Q_T}{\|(\mathrm{id} - P_{\mathrm{H}})Q_T\|_2}. \tag{14.25}$$

We then obtain

$$\begin{aligned}
\|\Delta_t(\nu_K) - P_{\mathrm{H}}\|_\infty &= \max_{\|X\|_2=1} |(X|\,\Delta_t(\nu_K) - P_{\mathrm{H}}\,|X)| \\
&\geq \frac{|(X_T|\,\Delta_t(\nu_K) - P_{\mathrm{H}}\,|X_T)|}{\|X_T\|_2^2} \\
&= \frac{|(Q_T|\,(\mathrm{id} - P_{\mathrm{H}})\Delta_t(\nu_K)(\mathrm{id} - P_{\mathrm{H}})\,|Q_T)|}{(Q_T|\,(\mathrm{id} - P_{\mathrm{H}})^2\,|Q_T)} \\
&= \frac{|\,(Q_T|\,\Delta_t(\nu_K)\,|Q_T) - (Q_T|\,P_{\mathrm{H}}\,|Q_T)\,|}{1 - (Q_T|\,P_{\mathrm{H}}\,|Q_T)} \\
&\geq \frac{(Q_T|\,\Delta_t(\nu_K)\,|Q_T) - (Q_T|\,P_{\mathrm{H}}\,|Q_T)}{1 - (Q_T|\,P_{\mathrm{H}}\,|Q_T)}.
\end{aligned} \tag{14.26}$$

Here, we used that $P_{\mathrm{H}}\Delta_t(\nu_K) = \Delta_t(\nu_K)P_{\mathrm{H}} = P_{\mathrm{H}}$ as before. From this, we immediately obtain using Eq. (14.24) and Lem. 14.2:

$$\begin{aligned}
(Q_T|\,\Delta_t(\nu_K)\,|Q_T) &\leq \kappa_{t,K}\big[1 - (Q_T|\,P_{\mathrm{H}}\,|Q_T)\,\big] + (Q_T|\,P_{\mathrm{H}}\,|Q_T) \\
&= \kappa_{t,K} + (1 - \kappa_{t,K})\,(Q_T|\,P_{\mathrm{H}}\,|Q_T) \\
&\leq 1 - \frac{1}{8}c'(K)\log^{-2}(t).
\end{aligned} \tag{14.27}$$

Next, we use that Q_T commutes with the t-th diagonal action of the single-qubit Clifford group and thus $(Q_T|\,\Delta_t(\mu_{\mathrm{Cl}})\,|Q_T) = 1$. This implies

$$(Q_T|\,\Delta_t(\xi_K)^2\,|Q_T) \leq 1 - \frac{1}{4}c'(K)\log^{-2}(t). \tag{14.28}$$

Finally, combine the Cauchy-Schwarz inequality with $\sqrt{1-x} \leq 1 - x/2$ for $x \leq 1$ to get

$$\begin{aligned} |(Q_T| \Delta_t(\xi_K) |Q_{T'})| &\leq \sqrt{(Q_T| \Delta_t(\xi_K)^2 |Q_T)} \\ &\leq \sqrt{1 - \frac{1}{4} c'(K) \log^{-2}(t)} \\ &\leq 1 - \frac{1}{8} c'(K) \log^{-2}(t) \\ &=: 1 - c(K) \log^{-2}(t), \end{aligned} \tag{14.29}$$

for all $T \in \Sigma_t \setminus S_t$ and $T' \in \Sigma_t$. This proves Lemma 14.1. □

14.3.2 Local random Clifford circuits

In the following, we give an outline of the proof of Thm. 14.2. The proof strategy is analogous to the unitary case treated in Refs. [182, 194]. For convenience, we restate Thm. 14.2.

Theorem 14.2 (Local random Clifford designs[197, Thm. 3])**.** *Let $n \geq 12t$ and $G \subset \mathrm{Cl}_2$ be a closed, generating set. Then, there is a constant $c(G) > 0$ such that local random Clifford circuits of depth $m \geq c(G) n t^8 \log^{-2}(t)(2nt + \log(1/\varepsilon))$ form relative ε-approximate Clifford t-designs.*

In this section, the definition of moment operators is with respect to the Clifford group Cl_n. More precisely, given a probability measure ν on Cl_n, its t-th moment operator is

$$\Delta_t(\nu) := \int_{\mathrm{Cl}_n} U^{\otimes t} \cdot (U^{\otimes t})^\dagger \, \mathrm{d}\nu(U). \tag{14.30}$$

Recall that the measure ν defines a relative ε-approximate Clifford design if it is close to the uniform measure μ_{Cl} in CP ordering, i. e.

$$(1-\varepsilon)\Delta_t(\mu_{\mathrm{Cl}}) \preceq \Delta_t(\nu) \preceq (1+\varepsilon)\Delta_t(\mu_{\mathrm{Cl}}) \tag{14.31}$$

Since all norms on finite-dimensional vector spaces are equivalent, it might be intuitively clear that the different notions of approximation are related but norm constants will generally appear. Since those can depend on the dimension $d = 2^{2nt}$ this may affect the rate of convergence. Let us define the deviation in *spectral norm* as

$$g(\nu, t) := \|\Delta_t(\nu) - \Delta_t(\mu_{\mathrm{Cl}})\|_\infty \tag{14.32}$$

Then, the following lemma derives an explicit norm constant which allows the lift closeness in spectral norm to closeness in CP ordering:

Lemma 14.3. *Suppose $\varepsilon \in [0, 1)$ is such that $g(\nu, t) \leq \varepsilon$. Then, ν is a relative $\varepsilon 2^{2nt}$-approximate Clifford t-design.*

As in Def. 14.4, given a closed, generating set $G \subset \mathrm{Cl}_2$ we define the probability measure σ_G which draws randomly from G and applies the gate to a random qubit i or a random pair of adjacent qubits $(i, i+1)$. Then, we can bound the spectral norm deviation as follows.

Proposition 14.3. *Given a probability measure as in Def. 14.4 and assume that $n \geq 12t$. Then, there is a constant $c(G) > 0$ such that $g(\sigma_G, t) \leq 1 - c(G)n^{-1}\log^2(t)t^{-8}$.*

Proof of Thm. 14.2. Note that for all probability measures ν on the Clifford group we have $g(\nu^{*m}, t) = g(\nu, t)^m$ since

$$\Delta_t(\mu_{\mathrm{Cl}})\Delta_t(\nu) = \Delta_t(\nu)\Delta_t(\mu_{\mathrm{Cl}}) = \Delta_t(\mu_{\mathrm{Cl}}). \tag{14.33}$$

Thus, Prop. 14.3 and Lem. 14.3 imply that for $m \geq c(G)nt^8\log^{-2}(t)(2nt + \log(1/\varepsilon))$ the local random Clifford circuit σ_G^{*m} is a relative ε-approximate Clifford t-design. □

Let us now turn to the proof of Proposition 14.3. In the following we consider the gate set G to be fixed and simply write $\sigma_G \equiv \sigma$. By assumption, G is closed under taking inverses and thus $\Delta_t(\sigma)$ is self-adjoint. Its largest eigenvalue is 1 since σ is a probability measure. The according eigenspace is the subspace of operators which is fixed under $\mathrm{Ad}(g)^{\otimes t}$ for any $g \in G$. This is exactly the subspace of operators which commute with any $g^{\otimes t}$. Since G generates the Clifford group, this subspace has to coincide with the Clifford commutant Cl_n'. Denoting with $P_{\mathrm{Cl}} = \Delta_t(\mu_{\mathrm{Cl}})$ the projector onto Cl_n', the spectral decomposition of $\Delta_t(\sigma)$ is thus

$$\Delta_t(\sigma) = P_{\mathrm{Cl}} + \sum_{r\geq 2} \lambda_r(\Delta_t(\sigma))\Pi_r, \tag{14.34}$$

where $\lambda_r(X)$ denotes the r-th largest eigenvalue of X. Hence, the deviation in spectral norm becomes

$$g(\sigma, t) = \|\Delta_t(\sigma) - P_{\mathrm{Cl}}\|_\infty = \lambda_2(\Delta_t(\sigma)). \tag{14.35}$$

We can reformulate this as the spectral gap of a suitable family of *local Hamiltonians* with vanishing ground state energy. These are:

$$H_{n,t} := n\left(\mathrm{id} - \Delta_t(\sigma)\right) = \sum_{i=1}^{n} h_{i,i+1}, \quad \text{with} \quad h_{i,i+1} := \frac{1}{|G|}\sum_{g\in G}\left(\mathrm{id} - \mathrm{Ad}(g_{i,i+1})^{\otimes t}\right). \tag{14.36}$$

Here, $g_{i,i+1}$ is the local generator g applied to the qubit pair $(i, i+1)$. It is clear that $H_{n,t}$ is a positive operator with ground state energy 0. By construction, the corresponding ground space is exactly the Clifford commutant Cl_n'. Let $\Delta(H_{n,t})$ be the spectral gap of $H_{n,t}$, i. e. the second-smallest eigenvalue of $H_{n,t}$. Then, we have

$$g(\sigma, t) = 1 - \frac{\Delta(H_{n,t})}{n}. \tag{14.37}$$

The key step in proving Prop. 14.3 is to show that the spectral gap $\Delta(H_{n,t})$ has a lower bound independent of n. It is crucial that the Hamiltonians $H_{n,t}$ are *frustration-free* such that we can apply the *martingale method* due to Nachtergaele [200]. This leads to the following bound:

Lemma 14.4 (Lower bound on spectral gap)**.** *Let $H_{n,t}$ be the family of Hamiltonians defined in Eq.* (14.36) *and let $n \geq 12t$. Then, the following inequality holds for the spectral gap of $H_{n,t}$:*

$$\Delta(H_{n,t}) \geq \frac{\Delta(H_{12t,t})}{48t}. \tag{14.38}$$

Finally, we can combine Lem. 14.4 with a suitable lower bound on $\Delta(H_{12t,t})$ to prove Prop. 14.3. To this end, we use a result by Diaconis and Saloff-Coste [201] about random walks on finite groups. As in Varjú's theorem, this involves an averaging operator, however, in this case with respect to the regular representation of Cl_n on its group algebra $L^2(\mathrm{Cl}_n)$ which acts as $\rho(h)f(g) := f(h^{-1}g)$. The averaging operator is then

$$T_\sigma f(g) := \int_{\mathrm{Cl}_n} f(h^{-1}g)\ \mathrm{d}\sigma(h). \tag{14.39}$$

By the Peter-Weyl theorem, the regular representation decomposes into all irreducible representations of Cl_n. Then, the highest eigenvalue of T_σ is 1 with eigenspace corresponding to the trivial isotype in this decomposition. According to Ref. [201, Cor. 1], the second largest eigenvalue is bounded as

$$\lambda_2(T_\sigma) \leq 1 - \frac{\eta}{d^2}, \tag{14.40}$$

where $\eta = |G|^{-1}n^{-1}$ is the probability of the least probable generator in G and d is the diameter of the Cayley graph of Cl_n, which is $d = O(n^3/\log n)$ by Ref. [88].

By the Peter-Weyl theorem, the spectrum of $\Delta_t(\sigma)$ is contained in the spectrum of T_σ. In fact, it is given by the spectrum of T_σ restricted to the irreps that appear in the representation $U \mapsto \mathrm{Ad}(U)^{\otimes t}$. Since this representation has a trivial isotype, the bound Eq. (14.40) has to also hold for $\Delta_t(\sigma)$. In particular, the spectral gap of the Hamiltonian $H_{n,t}$ has to be at least η/d^2. This yields for a constant $\tilde{c}(G) > 0$:

$$\Delta(H_{n,t}) \geq \tilde{c}(G)n^{-1}n^{-6}\log(n)^2 = \tilde{c}(G)n^{-7}\log^2(n). \tag{14.41}$$

Using Lemma 14.4, and the just given lower bound with $n = 12t$, we find for a suitable constant $c(G) > 0$:

$$\Delta(H_{n,t}) \geq \frac{\Delta(H_{12t,t})}{48t} \geq c(G)t^{-8}\log^2(t). \tag{14.42}$$

This proves Prop. 14.3.

CHAPTER 15

APPROXIMATIONS OF THE CLIFFORD PROJECTOR

15.1 Introduction

As we have seen in Sec. 12.3.1, the Clifford commutant comes with a conveniently factorising and well-studied basis $r(T)^{\otimes n}$ which, however, is *non-orthogonal*. Consequently, the projector onto the Clifford commutant P_{Cl} cannot be naturally expressed in this basis. This makes it difficult to relate bounds on P_{Cl} to expressions involving the basis $r(T)^{\otimes n}$. As laid out in the last Ch. 14, my collaborators and I used an explicit Gram-Schmidt orthogonalisation in Ref. [58] to fill this gap. Both from a conceptual and mathematical point of view, this is *unsatisfactory*. Moreover, it complicates the understanding of the central proof. Independently from my work, suitable expansions of the *Clifford twirl* P_{Cl} have also been studied by Roth et al. [15] for $t = 4$ in the context of quantum process characterisation.

After the release of the first version of Ref. [58], I have studied whether suitable expansions in the commutant basis $r(T)^{\otimes n}$ approximate the exact Clifford projection in diamond norm. Unfortunately, such an expansion has not been found at the time of writing. This chapter is meant to document these efforts and the appearing difficulties, thus reflecting ongoing work. The studied "natural" expansion map has the form of a so-called *frame operator* associated with the commutant basis $r(T)^{\otimes n}$. The exponentially small overlaps of the basis elements imply that this frame operator is close to P_{Cl} in spectral norm. We were able to derive a useful result, the *lifting lemma* 15.1, which allows to "lift" such a spectral norm bound to a diamond norm bound under certain assumptions. However, those are not fulfilled by the studied "natural" frame operator – in fact the diamond norm difference is independent of n. Nevertheless, the studies indicate that the problems and their resolution might be very much intertwined with the representation theory of the Clifford group which is by itself subject to ongoing research [181, 192].

To motivate the search for suitable approximations of the Clifford projector, let us consider the unitary case first. Already there, the permutations $r(\pi)$ form a non-orthogonal basis for the unitary commutant. In this situation, however, there is a powerful result by Collins and Sniady [202], relating the *normalised permutation frame operator*,

$$S_{\mathrm{H}} = d^{-t} \sum_{\pi \in S_t} |r(\pi)\rangle\!\rangle\langle\!\langle r(\pi)| \,, \tag{15.1}$$

to the projection P_{H} onto the unitary commutant.

Lemma 15.1 (Collins-Sniady [202])**.** *Let P_{H} be the Haar projector associated with the unitary group $\mathrm{U}(d)$ acting diagonally on $(\mathbb{C}^d)^{\otimes t}$ and be S_{H} the frame operator given by Eq.* (15.1)*. Then, it holds*

(i) $P_{\mathrm{H}}(X) = S_{\mathrm{H}}(X) \cdot S_{\mathrm{H}}(\mathbb{1})^{-1}$ *for all* $X \in L((\mathbb{C}^d)^{\otimes t})$,

(ii) $\|S_{\mathrm{H}} - P_{\mathrm{H}}\|_\diamond \leq t^2 d^{-1}$ *for* $d \geq t$.

The overlap of two distinct (normalised) permutations scales as d^{-1}. Thus, it might be clear that the permutation basis eventually becomes orthogonal when d is large. However, this only implies that S_{H} approximates P_{H} in spectral norm, not in diamond norm. The result of Collins and Sniady [202] is on an algebraic level, relating P_{H} and S_{H} by a multiplicative correction. Indeed, the second statement follows directly from the first one:

Proof of (ii). First, let us consider a superoperator which acts by right multiplication, $M_A(X) := X \cdot A$. Then, its diamond norm is by the duality of trace and spectral norm given by

$$\|M_A\|_\diamond = \sup_{\|X\|_1=1} \|X \cdot (\mathbb{1} \otimes A)\|_1 = \|A\|_\infty . \tag{15.2}$$

Thus, setting $I := S_{\mathrm{H}}(\mathbb{1})$, we find using (i):

$$\|S_{\mathrm{H}} - P_{\mathrm{H}}\|_\diamond = \|(M_I - \mathrm{id}) \circ P_{\mathrm{H}}\|_\diamond \leq \|I - \mathbb{1}\|_\infty \|P_{\mathrm{H}}\|_\diamond = \|I - \mathbb{1}\|_\infty . \tag{15.3}$$

Note that $\operatorname{tr} r(\pi) = d^k$, where k is the number of fixed points of the permutation $\pi \in S_t$. Let $p(t,k)$ be the number of permutations with exactly k fixed points. Then, we group the permutations appearing in $I - \mathbb{1}$ by number of fixed points and use $\|r(\pi)\|_\infty = 1$:

$$\|I - \mathbb{1}\|_\infty = \left\| d^{-t} \sum_{\pi \in S_t \setminus \mathrm{id}} \operatorname{tr}[r(\pi)]\, r(\pi)^\dagger \right\|_\infty \leq \sum_{k=0}^{t-1} d^{-(t-k)} p(t,k). \tag{15.4}$$

We can bound the final sum using the following well-known bound [203]:

$$p(t,k) \leq 2e^{-1} \frac{t!}{k!}. \tag{15.5}$$

We have for any $t, l \in \mathbb{N}$ such that $d > t - l$ and $t \geq l \geq 1$:

$$\sum_{k=0}^{t-l} d^{-(t-k)} p(t,k) \leq \frac{2}{e} \sum_{k=0}^{t-l} d^{-t} t! \frac{d^k}{k!} \leq \frac{2}{e} d^{-t} (t-l+1) t! \frac{d^{(t-l)}}{(t-l)!} \leq t^{l+1} d^{-l}. \tag{15.6}$$

Here, we use in the second inequality that $d^k/k!$ is monotonically increasing for $k \leq t - l < d$ and a standard bound on binomial coefficients in the last step. This implies the required result for $d \geq t$:

$$\|S_{\mathrm{H}} - P_{\mathrm{H}}\|_\diamond = \|I - \mathbb{1}\|_\infty \leq t^2 d^{-1}. \tag{15.7}$$

□

Lemma 15.1 allows to exchange an integration over the unitary group for an expansion into permutations at the cost of a diamond norm error which is reciprocal in the dimension. For quantum information applications, this means that this errors is suppressed exponentially in the number of qudits.

15.2 The Clifford frame operator

The Clifford projector P_{Cl} is defined as the projection onto the commutant of the t-th tensor power representation of the Clifford group:

$$P_{\mathrm{Cl}} = \frac{1}{|\mathrm{Cl}_n(p)|} \sum_{U \in \mathrm{Cl}_n(p)} U^{\otimes t} \cdot (U^{\otimes t})^\dagger. \tag{15.8}$$

To study whether P_{Cl} can be approximated by the basis $r(T)^{\otimes n}$ similar to the unitary case in Lem. 15.1, we introduce the *Clifford frame operator*:

$$S_{\mathrm{Cl}} = \sum_{T \in \Sigma_t} |Q_T)(Q_T|^{\otimes n}, \qquad Q_T := \frac{r(T)}{\|r(T)\|_2}. \tag{15.9}$$

Here, we work in arbitrary local prime dimensions p and thus stochastic Lagrangians are subspaces of $\mathbb{F}_p^{2t}$.

In the remainder of this section, we derive some properties of S_{Cl}. First, we give an interesting Kraus decomposition of the Clifford frame operator which in particular shows that it is a completely positive map. To this end, consider the Choi-Jamiołkowski isomorphism on $(\mathbb{C}^p)^{\otimes nt}$,

$$\mathcal{J}(\mathcal{E}) := p^{-nt} \sum_{x,y \in \mathbb{F}_p^{nt}} \mathcal{E}(|x\rangle\langle y|) \otimes |x\rangle\langle y|, \tag{15.10}$$

where $\mathcal{E}$ is an arbitrary superoperator. Note that under $\mathcal{J}$, the power of a n-qudit Clifford unitary $U^{\otimes t}$ corresponds to the power of a maximally entangled $2n$-qudit stabiliser state $|s\rangle^{\otimes t}$. In contrast, the Clifford frame operator involves an average over *all* stabiliser states, or equivalently, over the *Clifford semigroup* introduced in Sec. 12.3.2. This is made precise by the next lemma. In the following, $(a;q)_n := \prod_{i=0}^{n-1}(1 - aq^i)$ is the q-Pochhammer symbol.

Lemma 15.2. *The Clifford frame operator can be written as*

$$S_{\mathrm{Cl}} = \frac{(-p^{-2n};p)_{t-1}}{|\mathrm{CS}_n(p)|} \sum_{Q \in \mathrm{CS}_n(p)} \frac{p^{nt}}{\|Q\|_2^{2t}} Q^{\otimes t} \cdot \left(Q^{\otimes t}\right)^\dagger, \tag{15.11}$$

where $\mathrm{CS}_n(p)$ *is the Clifford semigroup defined in Eq.* (12.63)*. In particular,* S_{Cl} *is completely positive.*

Proof. Using that rank-one superoperators $\mathcal{E} = |A)(B|$ map to $p^{-nt} A \otimes \bar{B}$ under $\mathcal{J}$, we find

$$\mathcal{J}(S_{\mathrm{Cl}}) = p^{-2nt} \sum_{T \in \Sigma_t} r(T)^{\otimes 2n} = \frac{p^{2nt}(-p^{-2n};p)_{t-1}}{p^{2nt}|\mathrm{stab}_{2n}(p)|} \sum_{s \in \mathrm{stab}_{2n}(p)} |s\rangle\langle s|^{\otimes t}, \tag{15.12}$$

where we used Thm. 5.3 of Ref. [181] in the second step. By Eq. (12.59) in Sec. 12.3.2, we have $|s\rangle = p^{n/2}\|Q\|_2^{-1} Q \otimes \mathbb{1} \, |\phi^+\rangle$ for some stabiliser operator $Q \in \mathrm{CS}_n(p)$. The claim follows by applying $\mathcal{J}^{-1}$ to both sides. □

In Sec. 12.3.2, it is shown that any stabiliser operator $Q \in \mathrm{CS}_n(p)$ has the form $Q = UP$ for a Clifford unitary U and stabiliser code projector P. The fact that stabiliser operators correspond to stabiliser states under the Choi-Jamiołkowski isomorphism can be summarised as follows:

$$|s\rangle = p^{k/2} UP \otimes \mathbb{1} \left|\Phi^+\right\rangle, \qquad U \in \mathrm{Cl}_n(p),\ P \in \mathrm{stab}_{n,k}(p). \tag{15.13}$$

In particular, the Schmidt rank of $|s\rangle$ is given by $\mathrm{rk}\, P = p^{n-k}$. Thus, the difference between P_{Cl} and S_{Cl} comes from the additional operators in the Clifford semigroup arising from stabiliser codes. In the Choi picture, these are exactly the non-maximally entangled stabiliser states.

From Eq. (15.13) we can directly express S_{Cl} in terms of Clifford unitaries and stabiliser codes. This allows us to get the following form of S_{Cl}:

Lemma 15.3. *We have*

$$S_{\mathrm{Cl}} = (-p^{-2n}; p)_{t-1}\, P_{\mathrm{Cl}} \circ \mathcal{C} = (-p^{-2n}; p)_{t-1}\, \mathcal{C} \circ P_{\mathrm{Cl}}, \tag{15.14}$$

where

$$\mathcal{C} := \frac{|\mathrm{Cl}_n(p)|}{|\mathrm{CS}_n(p)|} \sum_{k=0}^{n} \frac{p^{kt}}{|\mathcal{S}(k)|} \sum_{P \in \mathrm{stab}_{n,k}(p)} P^{\otimes t} \cdot P^{\otimes t}, \tag{15.15}$$

and $\mathcal{S}(k)$ is the left Clifford stabiliser of a rank k stabiliser code.

Proof. By Eq. (15.13), we can write $Q = UP$ and $\|Q\|_2^2 = p^{n-k}$ for $P \in \mathrm{stab}_{n,k}(p)$. Note that this representation is unique up to redefining $U' = UV$ where V is fixing P under left multiplication. Thus, varying U for a fixed P will overcount by exactly $|\mathcal{S}(k)|$. Hence, we can write

$$\begin{aligned} \sum_{Q \in \mathrm{CS}_n(p)} \frac{p^{nt}}{\|Q\|_2^{2t}} Q^{\otimes t} \cdot \left(Q^{\otimes t}\right)^\dagger &= \sum_{k=0}^{n} \frac{p^{kt}}{|\mathcal{S}(k)|} \sum_{U \in \mathrm{Cl}_n(p)} \sum_{P \in \mathrm{stab}_{n,k}(p)} (UP)^{\otimes t} \cdot (PU^\dagger)^{\otimes t} \\ &= P_{\mathrm{Cl}} \circ \left(\sum_{k=0}^{n} \frac{p^{kt} |\mathrm{Cl}_n(p)|}{|\mathcal{S}(k)|} \sum_{P \in \mathrm{stab}_{n,k}(p)} P^{\otimes t} \cdot P^{\otimes t} \right), \end{aligned} \tag{15.16}$$

which shows the desired result. □

Remark 15.1 (Relation to other parts of this thesis)**.** Surprisingly, not much has been known in the literature about the "stabiliser operators". This has led me to investigate this matter more closely which has resulted in Sec. 12.3.2 in this thesis, treating the orthogonal commutant and the Clifford semigroup. There, it is shown that the operators $Q = Q(L) \in \mathrm{CS}_n(p)$ are parametrised by Lagrangian subspaces L in a *signed double* of phase space. These Lagrangians correspond to the Lagrangians of $2n$-qudit stabiliser states under a Choi-like isomorphism. In the context of the duality of Clifford and stochastic orthogonal group $\mathrm{O}_t^{\mathrm{st}}(p)$, the stabiliser operators $Q(L)$ play the same role for $\mathrm{O}_t^{\mathrm{st}}(p)$ as the stochastic Lagrangian operators $r(T)$ play for the Clifford group. Namely, the operators $Q(L)^{\otimes t}$ commute with the action of $\mathrm{O}_t^{\mathrm{st}}(p)$ and span the orthogonal commutant.

Furthermore, these considerations initiated the study of completely stabiliser-preserving channels presented in Ch. 9. The form of S_{Cl} presented in Lem. 15.2 is reminiscent of the Kraus decomposition of CSP channels. However, the decomposition of S_{Cl} is neither convex nor is S_{Cl} trace-preserving.

15.3 Approximation of the Clifford projector

As in the case of permutations, the Clifford commutant basis becomes *almost* orthogonal for large n. More precisely, the following Lemma shows that their overlaps decay exponentially in n.

Lemma 15.4 (Lemma 3 in Ref. [58]). *Consider $T, T' \in \Sigma_t$ and denote with N, N' their respective defect spaces. Then, it holds that*

$$|\,(Q_T|Q_{T'})\,| \leq p^{-|\dim N - \dim N'|}. \tag{15.17}$$

Thus, there is a priori hope that the Clifford frame operator could provide a suitable approximation to the Clifford projection for large enough n. In fact, my collaborators and I have already proved in Ref. [58] that this is at least true in spectral norm:

Lemma 15.5 ([58, Lem. 12]). *Let S_{Cl} be the Clifford frame operator and Γ the corresponding Gram matrix, i.e. $\Gamma_{T,T'} = (Q_T|Q'_T)^n$. Then the following holds*

$$\|S_{\mathrm{Cl}} - P_{\mathrm{Cl}}\|_\infty = \|\Gamma - \mathbb{1}\|_\infty \leq (-p^{-n}; p)_{t-1} - 1 \leq t\, p^{t-n}, \tag{15.18}$$

where the last inequality holds for $n + 2 \geq t + \log_p t$.

The (superoperator) spectral norm is the same as the $2 \to 2$ operator norm induced by the Schatten 2-norm or Hilbert-Schmidt norm on $L(\mathbb{C}^2)^{\otimes nt}$. Approximation with respect to this norm is geometrically meaningful but does not have a clear operational meaning. We desire approximation in diamond norm as in Lem. 15.1(ii) which would also be useful in a setting such as Ch. 14. The question is thus:

$$\text{Is} \quad \|S_{\mathrm{Cl}} - P_{\mathrm{Cl}}\|_\diamond \quad \text{small?} \tag{15.19}$$

As it turns out, computing the diamond norm is not straightforward. One technical difficulty comes from the fact that both superoperators have support only on the Clifford commutant $\mathrm{Cl}_n(p)'$ which is a $*$-subalgebra of $L(\mathbb{C}^2)^{\otimes nt}$ (and thus also a C^*-algebra). Thus, we are comparing a completely positive map to the identity, but on a $*$-subalgebra. Generally, this is simplified by the introduction of pure states. However, a general C^*-algebra $\mathcal{A}$ is not a matrix algebra, and thus there is no canonical notion of pure states. Nevertheless, $\mathcal{A}$ can be decomposed into matrix algebras which results in the following theorem which was proven by David Gross and myself. It states that a spectral norm approximation can be lifted to a diamond norm approximation under certain assumptions:

Theorem 15.1 (Lifting lemma). *Let $\mathcal{A}$ be a C^*-subalgebra of $L(\mathcal{H})$ for some finite-dimensional Hilbert space $\mathcal{H}$ and let P be the orthogonal projection onto $\mathcal{A}$ with respect to the Hilbert-Schmidt inner product on $L(\mathcal{H})$. Given a completely positive map $\Phi : L(\mathcal{H}) \to L(\mathcal{H})$ and $\frac{1}{24} \geq \varepsilon \geq 0$ such that*

$$\max\left(\|\Phi\|_\diamond - 1, \|\Phi - P\|_\infty\right) \leq \varepsilon, \qquad \Phi \circ P = P \circ \Phi = \Phi, \tag{15.20}$$

then it holds:

$$\|\Phi - P\|_\diamond \leq \sqrt{\varepsilon(10 + \varepsilon)}. \tag{15.21}$$

The proof of Theorem 15.1 can be found in Sec. 15.3.1. It seems that the lifting lemma 15.1 allows us to answer the raised question (15.19) affirmatively – however, it relies on the assumption that $\|S_{\mathrm{Cl}}\|_\diamond$ is close to 1, i. e. that S_{Cl} is approximately trace-preserving. As it turns out, this is not the case as the following observation by Felipe Montealegre Mora shows:

Theorem 15.2. *It holds*

$$\|S_{\mathrm{Cl}}\|_\diamond \geq 1 + p^{\lfloor t^2/8 \rfloor}, \qquad \Rightarrow \quad \|S_{\mathrm{Cl}} - P_{\mathrm{Cl}}\|_\diamond \geq p^{\lfloor t^2/8 \rfloor}. \tag{15.22}$$

Proof. For any CP map Φ, we have $\|\Phi\|_\diamond = \|\Phi^\dagger(\mathbb{1})\|_\infty$ (see e. g. Ref. [204]). In particular, since S_{Cl} is self-adjoint, $\|S_{\mathrm{Cl}}\|_\diamond = \|S_{\mathrm{Cl}}(\mathbb{1})\|_\infty$. Then:

$$S_{\mathrm{Cl}}(\mathbb{1}) = \sum_{T \in \Sigma_t} Q_T^{\otimes n} \operatorname{tr}\left((Q_T^{\otimes n})^\dagger \mathbb{1} \right) = \sum_{T \in \Sigma_t} Q_T^{\otimes n} \underbrace{\operatorname{tr}(Q_T^{\otimes n})}_{\geq 0}. \tag{15.23}$$

This implies that $S_{\mathrm{Cl}}(\mathbb{1})$ is Hermitian since $\dagger$ simply interchanges the left and right half of a stochastic Lagrangian T and thus preserves the set Σ_t. Hence:

$$\|S_{\mathrm{Cl}}(\mathbb{1})\|_\infty = \max_\psi |\langle \psi | S_{\mathrm{Cl}}(\mathbb{1}) | \psi \rangle|^2. \tag{15.24}$$

Next, given a maximal defect subspace $N \subset \mathbb{F}_p^t$, i. e. $\dim N = \lfloor t/2 \rfloor$, any subspace $N' \subset N$ is also a defect subspace and we can define associated operators

$$Q_{N'} := \frac{P_{N'}}{\|P_{N'}\|_2}. \tag{15.25}$$

The corresponding contribution to Eq. (15.23) is given by

$$\operatorname{tr}(Q_{N'}) Q_{N'} = \|P_{N'}\|_2^{-2} \operatorname{tr}(P_{N'}) P_{N'} = P_{N'}. \tag{15.26}$$

Finally, we define a pure state $|\psi\rangle$ which lies in the CSS code $\operatorname{ran}(P_N^{\otimes n})$ and consequently in any $\operatorname{ran}(P_{N'}^{\otimes n}) \supset \operatorname{ran}(P_N^{\otimes n})$ for $N' \subset N$:

$$|\psi\rangle := p^{-n \dim N/2} \sum_{x \in N^n} |x\rangle, \qquad \Rightarrow P_{N'}^{\otimes n} |\psi\rangle = |\psi\rangle \quad \forall N' \subset N. \tag{15.27}$$

Since, the components of ψ are non-negative and so are the matrix entries of Q_T, we have $\langle \psi | Q_T^{\otimes n} | \psi \rangle \geq 0$ for all $T \in \Sigma_t$ and therefore

$$\begin{aligned} \|S_{\mathrm{Cl}}(\mathbb{1})\|_\infty^{1/2} &\geq \langle \psi | S_{\mathrm{Cl}}(\mathbb{1}) | \psi \rangle \\ &= \sum_{N' \subset N} \langle \psi | P_{N'}^{\otimes n} | \psi \rangle + \underbrace{\text{rest}}_{\geq 0} \\ &\geq \left| \{ N' \subset N \text{ subspace} \} \right| \\ &= G(p; \lfloor t/2 \rfloor). \end{aligned} \tag{15.28}$$

Here, $G(p; m)$ is the total number of subspaces of a vector space of dimension m over $\mathbb{F}_p$. The number of k-dimensional subspaces is given by the Gaussian binomial coefficient,

$$\binom{m}{k}_p := \frac{(1-p^m)\cdots(1-p^{m-k+1})}{(1-p)\cdots(1-p^k)}, \tag{15.29}$$

which is a polynomial in p of degree $k(m-k)$. Hence, the number $G(p;m)$ is again a polynomial of degree $\lfloor m/2 \rfloor \lceil m/2 \rceil = \lfloor m^2/4 \rfloor$:

$$G(p;m) = \sum_{k=0}^{m} \binom{m}{k}_p = \sum_{k=0}^{\lfloor m^2/4 \rfloor} T(m,k) p^k \geq 1 + p^{\lfloor m^2/4 \rfloor}. \tag{15.30}$$

The numbers $T(m,k)$ are positive integers counting the number of binary words of length m with exactly k inversions [205, 206]. From this the last lower bound follows directly. Thus, we find the following lower bound for $\|S_{\mathrm{Cl}}\|_\diamond$ which shows the claim:

$$\|S_{\mathrm{Cl}}(\mathbb{1})\|_\infty \geq G(p; \lfloor t/2 \rfloor)^2 \geq \left(1 + p^{\lfloor t^2/8 \rfloor}\right)^2 \geq 1 + p^{\lfloor t^2/8 \rfloor}. \tag{15.31}$$

□

Theorem 15.2 shows that while the Clifford frame operator S_{Cl} is a good approximation to the Clifford projector P_{Cl} in *spectral norm*, this is not the case in *diamond norm*. The reason is the existence of an n-independent number of nested defect subspaces which prohibit the diamond norm to decrease with n. Interestingly, the same defect subspaces induce so-called *rank-deficient representations* in the representation theory of the Clifford group [192]. There, they prevent the duality of the Clifford group and stochastic orthogonal group to be *injective* in the sense that the degeneracy spaces of orthogonal irreps are not necessarily irreducible under the Clifford action and vice versa. The question whether insights from representation theory could help to find a better definition of a "frame operator" remains open for future investigation.

Open problem 6 (Approximations of the Clifford projector)**.** Is there a suitable redefinition of the Clifford frame operator which approximates the Clifford projector in diamond norm?

15.3.1 Proof of Theorem 15.1

Given a C^*-subalgebra $\mathcal{A} \subset L(\mathcal{H})$ for some finite-dimensional Hilbert space $\mathcal{H}$, there is an orthogonal decomposition (see e.g. Ref. [207, Ch. I.11] and Ref. [208, Sec. 2.7]):

$$\mathcal{H} = \bigoplus_{i=0}^{N} \mathcal{H}_i, \tag{15.32}$$

in terms of subspaces that carry a tensor product structure

$$\begin{aligned} &\mathcal{H}_i = \mathcal{L}_i \otimes \mathcal{R}_i && \dim \mathcal{L}_i =: d_i, \quad \dim \mathcal{R}_i =: m_i, \qquad i = 1, \ldots, N \\ &\mathcal{H}_0 = \mathcal{R}_0, && \dim \mathcal{R}_0 =: m_0. \end{aligned}$$

for suitable *dimensions* d_i and *multiplicities* m_i, such that

$$\mathcal{A} \simeq 0_{m_0} \oplus \left(\bigoplus_{i=1}^{n} L(\mathcal{L}_i) \otimes \mathbb{1}_{m_i} \right). \tag{15.33}$$

Now suppose P is the orthogonal projection onto the C^*-subalgebra $\mathcal{A}$ with respect to the Hilbert-Schmidt inner product on $L(\mathcal{H})$. In C^*-algebraic terms, P is the unique

conditional expectation of $L(\mathcal{H})$ onto $\mathcal{A}$ which preserves the trace. As conditional expectations are completely positive, P is a CPTP map [207, 209]. Given a linear CP map $\Phi : L(\mathcal{H}) \to L(\mathcal{H})$ which is invariant under P, i. e. $\Phi \circ P = P \circ \Phi = \Phi$, we then find:

$$\begin{aligned} \|\Phi - P\|_\diamond &= \sup_{X \in L(\mathcal{H})\otimes L(\mathcal{H}):\, \|X\|_1 = 1} \|(\Phi \otimes \mathrm{id} - P \otimes \mathrm{id})\,(X)\|_1 \\ &= \sup_{X \in L(\mathcal{H})\otimes L(\mathcal{H}):\, \|X\|_1 = 1} \|(\Phi \otimes \mathrm{id} - \mathrm{id})(P \otimes \mathrm{id})\,(X)\|_1 \\ &= \sup_{Y \in \mathcal{A}\otimes L(\mathcal{H}):\, \|Y\|_1 = 1} \|(\Phi \otimes \mathrm{id} - \mathrm{id})\,(Y)\|_1 . \end{aligned} \tag{15.34}$$

The last step follows since the difference $\Phi - P$ is Hermiticity-preserving and thus the supremum is attained for a pure state $X = |\varphi\rangle\langle\varphi|$ (see e. g. Ref. [210, Thm. 3.51]). Then, $\|(P \otimes \mathrm{id})(X)\|_1 = \mathrm{tr}((P \otimes \mathrm{id})(X)) = \mathrm{tr}(X) = \|X\|_1$. We can write any $Y \in \mathcal{A} \otimes L(\mathcal{H})$ as

$$Y = \sum_{i=1}^{N} A_i \otimes I_i, \qquad \text{where} \quad A_i \in L(\mathcal{L}_i \otimes \mathcal{H}),\ I_i := \mathbb{1}_i / m_i. \tag{15.35}$$

Since the terms are orthogonal, we have $\|Y\|_1 = \sum_i \|A_i\|_1$ and the extremal points of the 1-norm unit ball in $\mathcal{A} \otimes L(\mathcal{H})$ are hence of the form $e^{i\varphi}\ |\psi\rangle\langle\psi| \otimes I_i$ for some i and $\psi \in \mathcal{L}_i$, $\varphi \in \mathbb{R}$. In the following, we use the shorthand notation $|\psi| := |\psi\rangle\langle\psi|$. We then find:

$$\|\Phi - P\|_\diamond = \sup_i \sup_{\psi \in \mathcal{L}_i} \|(\Phi \otimes \mathrm{id} - \mathrm{id})(|\psi| \otimes I_i)\|_1 . \tag{15.36}$$

Furthermore, we need the following lemma which is a generalisation of the Fuchs-van der Graaf inequality:

Lemma 15.6 (Trace distance of positive operators)**.** *For any two positive semi-definite operators $A, B \geq 0$, it holds*

$$\|A - B\|_1 \leq \sqrt{(\mathrm{tr}(A + B))^2 - 4F(A, B)^2}, \tag{15.37}$$

where $F(A, B) = \left\| \sqrt{A}\sqrt{B} \right\|_1$ is the (Uhlmann) fidelity.

Proof. Set $\alpha = \mathrm{tr}\, A \geq 0$ and $\beta = \mathrm{tr}\, B \geq 0$. By Uhlmann's theorem, there are purifications ψ and φ such that $A = \mathrm{tr}_2(\alpha|\psi|)$ and $B = \mathrm{tr}_2(\beta|\varphi|)$, as well as $\sqrt{\alpha\beta}\,|\langle\psi|\varphi\rangle| = F(A, B)$. Using that the trace norm is non-increasing under the partial trace, we find

$$\begin{aligned} \|A - B\|_1 \leq \|\alpha|\psi| - \beta|\varphi|\|_1 &= \sqrt{(\alpha + \beta)^2 - 4\alpha\beta\,|\langle\psi|\varphi\rangle|^2} \\ &= \sqrt{(\mathrm{tr}(A + B))^2 - 4F(A, B)^2}. \end{aligned} \tag{15.38}$$

Here, we used a well-known identity for the trace distance of rank-one operators, see e. g. Ref. [210, Eq. 1.183]. □

Proof of Theorem 15.1. Let (i, ψ) be an optimal argument in Eq. (15.36) and write

$$\Phi \otimes \mathrm{id}(|\psi| \otimes I_i) = \sum_{j=1}^{N} A_j \otimes I_j, \qquad \text{for } A_j \geq 0. \tag{15.39}$$

Set $1+\delta := \operatorname{tr} A_i$ with $\delta \geq -1$. Then, using Lem. 15.6 and $F(A_i, |\psi|)^2 = \langle\psi| A_i |\psi\rangle$, we find:

$$\begin{aligned}
\|\Phi - P\|_\diamond &= \|A_i - |\psi|\|_1 + \left\|\sum_{j\neq i} A_j \otimes I_j\right\|_1 \\
&\leq \sqrt{(2+\delta)^2 - 4\operatorname{tr}(A_i|\psi|)} + \sum_{j\neq i} \operatorname{tr} A_j \\
&= \sqrt{4\left[1 - \operatorname{tr}(A_i|\psi|)\right] + 4\delta + \delta^2} + \sum_{j\neq i} \operatorname{tr} A_j \\
&= \sqrt{4\left[1 - \operatorname{tr}\left(|\psi| \otimes \mathbb{1}_i\right)\left(\Phi \otimes \mathrm{id}(|\psi| \otimes I_i)\right)\right] + 4\delta + \delta^2} + \sum_{j\neq i} \operatorname{tr} A_j.
\end{aligned} \tag{15.40}$$

We can now establish bound on the individual terms as follows:

$$\begin{aligned}
1 - \operatorname{tr}\left(|\psi| \otimes \mathbb{1}_i\right)\left(\Phi \otimes \mathrm{id}(|\psi| \otimes I_i)\right) &= \operatorname{tr}\left(|\psi| \otimes \mathbb{1}_i\right)\left((\mathrm{id} - \Phi \otimes \mathrm{id})(|\psi| \otimes I_i)\right) \\
&\leq \|I_i\|_2 \, \|\mathbb{1}_i\|_2 \, \|(\mathrm{id} - \Phi) \otimes \mathrm{id}\|_\infty \\
&= \|\Phi - \mathrm{id}\|_\infty \\
&\leq \varepsilon.
\end{aligned} \tag{15.41}$$

We have a straightforward upper bound on δ:

$$\delta = \operatorname{tr} A_i - 1 \leq \operatorname{tr}\left(\Phi \otimes \mathrm{id}(|\psi| \otimes I_i)\right) - 1 \leq \|\Phi\|_\diamond - 1 \leq \varepsilon. \tag{15.42}$$

Furthermore, Eq. (15.41) also implies a lower bound on δ via Hölder's inequality:

$$\delta = \operatorname{tr} A_i - 1 \geq \operatorname{tr}\left(A_i|\psi|\right) - 1 \geq -\varepsilon. \tag{15.43}$$

Hence, we also find

$$\sum_{j\neq i} \operatorname{tr} A_j \leq \|\Phi\|_\diamond - (1+\delta) \leq 1 + \varepsilon - 1 + \varepsilon = 2\varepsilon. \tag{15.44}$$

Finally, it is straightforward to check that for $\varepsilon \leq 1/24$, the following inequality with $x = \varepsilon(8+\varepsilon)$ and $y = 2\varepsilon$ can be applied:

$$x \leq \frac{1}{4}(1-y)^2 \quad \Rightarrow \quad \sqrt{x} + y \leq \sqrt{x+y}, \qquad \text{for } x, y > 0, \tag{15.45}$$

Then, we obtain the desired bound:

$$\|\Phi - P\|_\diamond \leq \sqrt{8\varepsilon(1+\varepsilon)} + 2\varepsilon \leq \sqrt{\varepsilon(10+\varepsilon)}. \tag{15.46}$$

□

CONCLUSION

The unifying theme of this thesis is the study of advanced stabiliser methods. The powerful mathematical framework underlying the stabiliser formalism and the design properties of the Clifford group make them a versatile tool for quantum information theory. I have shown that these methods are particularly useful in the context of classical simulation of quantum circuits and the construction of higher-order unitary designs. The latter construction finds application in protocols where designs beyond the third order are beneficial. Although most known protocols do not require designs beyond the third order, it can be advantageous when control over higher moments of the estimator or tail bounds are needed. For instance, the use of 4-designs can be beneficial for RB and shadow tomography [12, 13, 15, 16, 183, 184]. Furthermore, the availability of unitary t-designs has already triggered the search for applications. A recent work shows that unitary t-designs can be used to construct efficient *quantum physical uncloneable functions* which provide provable cryptographic security against quantum adversaries [185].

In the following, I summarise the results presented in this thesis and discuss future research directions as well as open questions.

Classical simulation and the resource theory of magic

Summary

Stabiliser-based algorithms perform best for quantum circuits with few non-Clifford gates since their runtime only scales with the overall "non-stabiliserness" of the quantum circuit. Such algorithms also provide a way of quantifying the resources needed for a quantum computation and thus have a close relation to a *resource theory of quantum computing*. This can be made more precise in the *magic state model* of quantum computing where the operational meaning of the existing magic monotones is to quantify the runtime of an associated classical simulation algorithm. I have contributed to a better understanding of the resource theory of magic through two publications [33, 129], included in this thesis as Ch. 8 and 9.

The first work treats the computation of magic monotones which provides the necessary input for a classical simulation algorithm. Generally, this computation can only be carried out for few-qubit states and more general states have to be treated in a non-optimal fashion. Here, I have shown that the symmetries present in stabiliser and magic states can be exploited to significantly reduce the computational complexity for copies of magic states. To this end, I have proven that the symmetries of the stabiliser polytope are fixed by the fact that stabiliser states form a design (and are thus different in even and odd dimensions). This study has been performed at the example of robustness of magic, but can be generalised to other magic monotones as well.

The second paper contains a discussion of two different classes of free operations in the resource theory of magic. *Stabiliser operations* (SO) define an operationally motivated, well-studied class, which is used throughout the theory of fault-tolerant quantum

computing. In contrast, *completely-stabiliser preserving channels* (CSP) are axiomatically defined and relatively new [35, 36, 39, 128, 129]. However, resource-theoretic arguments naturally involve the latter class. My collaborators and I have contributed to a better understanding of the CSP class through the introduction of generalised stabiliser measurements. We have constructed an explicit example of a CSP channel which is not a stabiliser operation, thereby showing that the CSP class is strictly larger than the SO class.

Outlook

Following the publication of Ch. 8 as Ref. [33], more magic monotones and related simulation algorithms have been proposed in Refs. [34, 36]. Most importantly, these monotones are multiplicative for tensor products of single-qubit states. Therefore, the computation of these monotones becomes trivial in the important case of many copies of single-qubit magic states. From multiplicativity results on the stabiliser extent [34], it is expected that these monotones are also multiplicative for products of three-qubit states. However, a proof of this statement is still missing. Nevertheless, the multiplicativity can only hold in the few-qubit regime since it is known that these monotones eventually become non-multiplicative [38].

Building on the results in Ch. 9, there are two directions for future research which have been discussed in more detail in Ch. 10. First, I conjecture that CSP channels can be efficiently simulated. Since the CSP class is strictly larger than the SO class, this would yield a simulation algorithm beyond the Gottesman-Knill theorem. Initial work in this direction has been done in Ref. [36]. However, this method requires an assumption on the number of non-unitary Kraus operators of a CSP channel. This is needed since the simulation is performed on the level of Kraus operators. Because the non-unitary Kraus operators are trace-decreasing, the sampling complexity is increased and the algorithm has a non-vanishing failure probability. In my opinion, this is an artifact of the simulation ansatz. In principle, CSP channels can be decomposed into extremal CSP channels which are trace-preserving. Efficient simulation is thus possible if extremal CSP channels can be simulated. Future research would thus be dedicated to a better understanding of extremal CSP channels and a simulation method.

Second, the possible implications for resource-theoretic tasks have to explored. Most importantly, the resource-theoretic approach allows to derive bounds on magic state distillation rates. It is conceivable that these bounds can only be saturated by CSP channels. The found inequality between CSP and SO could be manifest in a significant gap in achievable distillation rates. Similar gaps have been found in the resource theory of entanglement for the analogous SEP and LOCC classes [155–157]. Since common magic state distillation schemes are based on stabiliser operations, this would have implications on the optimal overhead of the magic state model. A related question is whether CSP channels should be considered physical. In the entanglement case, separable channels are usually considered unphysical since they cannot be realised via local operations (thus making a global interaction necessary). A priori, it is not clear whether an analogous argument can be made to discard CSP channels.

Exact and approximate unitary designs from the Clifford group

Summary

The fact that stabiliser states and the Clifford group form designs makes them a preferred choice in many applications. Although e. g. randomised benchmarking works equally well with any unitary 2-design, it is usually done with the Clifford group due to the efficient sampling of group elements, their compilation into generators, and the multiplication and inversion of elements (cp. Sec. 5.3). The Clifford group is somewhat singular in this aspect since recent results imply that an analogous group for higher orders cannot exist and that the Clifford group is essentially unique [115] (cp. Ch. 13).

However, the Clifford group is a good basis to construct efficient *approximate* higher-order designs. My collaborators and I have used recent results in the representation theory of the Clifford group [87, 181] to show that random Clifford circuits interleaved with few non-Clifford gates define approximate unitary t-designs [58]. Strikingly, the properties of the Clifford group allow that the number of non-Clifford gates depends only on the design order t but not on the number of qubits n. More precisely, $\tilde{O}(t^4 \log(1/\varepsilon))$ non-Clifford gates are enough to approximate an exact unitary t-design up to an additive diamond norm error ε. Decomposing the Clifford circuits into standard generators, this results in an overall gate count of $\tilde{O}(n^2 t^4 \log(1/\varepsilon))$ which improves significantly on $\tilde{O}(n^2 t^{10} \log(1/\varepsilon))$ in the random circuit construction by Brandao, Harrow and Horodecki [182].

Outlook

Based on our construction of efficient approximate unitary designs, it seems imperative to find applications for higher order designs. Motivated by the results in Ref. [185], possible usecases could be found in quantum cryptography.

Our result on approximate unitary designs is based on a hands-on approximation of the projection onto the Clifford commutant ("Clifford twirl"). However, I think that a better understanding of such approximations is necessary and that this could find applications beyond the above scheme (e. g. along the lines of Ref. [15]). I have presented an ansatz to the problem in Ch. 15. Unfortunately, fundamental problems in this ansatz need to be overcome which seem to make a better understanding of the representation theory of the Clifford group necessary. The latter topic is subject to ongoing research [192] and relevant insights might be available in the near future.

ACKNOWLEDGMENTS

I would like to use this opportunity to thank David Gross, whom I first met during my Bachelor studies in Freiburg, and who had apparently influenced me to such a degree that I joined his group in Cologne later on. David has succeeded in creating a friendly and productive scientific environment and it has been a pleasure working there. I have profited deeply from his guidance, the various smaller and bigger discussions and the joint work on our projects.

Moreover, a big thanks goes to all my friends and colleagues of the Cologne family who have helped me feel immediately welcome. Among others, this includes Richard Küng, Christian Gogolin, David Wierichs, Arne Heimendahl, Yaiza Aragonés, and Mariami Gachechiladze. I am especially grateful to Johan Åberg for answering a lot of questions and participating in many discussions, even when they are on "Clifford stuff". I would also like to thank Mariela Boevska for holding everything together. Special thanks go to my friends and office mates Felipe Montealegre Mora and Mateus Araújo for providing a legendary office atmosphere and having countless discussions over the years, not to forget awesome barbecues in the park. It was a pleasure to share the office with you two. Felipe, I would like to thank you for patiently being my Clifford rubber duck.

Furthermore, I would like to thank all my collaborators over the years for enjoyable and productive discussions. These are namely Felipe Montealegre Mora, Ingo Roth, Jonas Haferkamp, Arne Heimendahl, Jens Eisert, Mateus Araújo, and Christian Gogolin. Although not all ideas have made it into the final stage, it has been worth pursuing every one of them.

I am grateful for the countless discussions and the advice I have received over the years. In particular, I would like to thank Richard Küng, Ingo Roth, and Christian Gogolin, as well as Martin Kliesch, Markus Huber, James Seddon, Earl Campbell, and Felix Huber. I also want to thank Christian Majenz for encouraging me to apply for a PhD position in Cologne.

Für die anhaltende Unterstützung, die Ermutigung und das Vertrauen in das, was ich tue, möchte ich mich bei meinen Eltern Karin und Johannes besonders bedanken.

Diese Dissertation wäre ohne die Unterstützung meiner Frau Nina nicht denkbar gewesen und dafür bin ich ihr zutiefst dankbar. Solch ein Vorhaben während einer Pandemie zu verfolgen, stellt uns alle vor besondere Herausforderungen und ich bin glücklich darüber, dass wir diese gemeinsam gemeistert haben. Danke, Nina, für Deine Liebe und dafür, dass Du auch in schwierigen Zeiten stets für mich da bist und mich in meinen Entscheidungen stärkst.

BIBLIOGRAPHY

[1] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter and Anton Zeilinger. "Experimental quantum teleportation". In: *Nature* 390.6660 (1997), pp. 575–579. DOI: 10.1038/37539 (cit. on p. v).

[2] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller and J. E. Nordholt. "Long-distance quantum key distribution in optical fibre". In: *New Journal of Physics* 8.9 (2006), pp. 193–193. DOI: 10.1088/1367-2630/8/9/193 (cit. on p. v).

[3] R. Ursin et al. "Entanglement-based quantum communication over 144 km". In: *Nature Physics* 3.7 (2007), pp. 481–486. DOI: 10.1038/nphys629 (cit. on p. v).

[4] Sheng-Kai Liao et al. "Satellite-to-ground quantum key distribution". In: *Nature* 549.7670 (2017), pp. 43–47. DOI: 10.1038/nature23655 (cit. on p. v).

[5] Frank Arute et al. "Quantum supremacy using a programmable superconducting processor". In: *Nature* 574.7779 (2019), pp. 505–510. DOI: 10.1038/s41586-019-1666-5 (cit. on p. v).

[6] Han-Sen Zhong et al. "Quantum computational advantage using photons". In: *Science* 370.6523 (2020), pp. 1460–1463. DOI: 10.1126/science.abe8770 (cit. on p. v).

[7] P. Sen. "Random measurement bases, quantum state distinction and applications to the hidden subgroup problem". In: *21st Annual IEEE Conference on Computational Complexity (CCC'06)*. 2006. DOI: 10.1109/CCC.2006.37 (cit. on pp. v, vii, 151).

[8] A. J. Scott. "Tight informationally complete quantum measurements". In: *Journal of Physics A: Mathematical and General* 39.43 (2006), pp. 13507–13530. DOI: 10.1088/0305-4470/39/43/009 (cit. on pp. v, vii, 3, 151).

[9] A. J. Scott. "Optimizing quantum process tomography with unitary 2-designs". In: *Journal of Physics A: Mathematical and Theoretical* 41.5 (2008), p. 055308. DOI: 10.1088/1751-8113/41/5/055308. arXiv: 0711.1017 (cit. on pp. v, vii, 3, 151, 155).

[10] William Matthews, Stephanie Wehner and Andreas Winter. "Distinguishability of Quantum States Under Restricted Families of Measurements with an Application to Quantum Data Hiding". In: *Communications in Mathematical Physics* 291.3 (2009), pp. 813–843. DOI: 10.1007/s00220-009-0890-5 (cit. on pp. v, vii, 151).

[11] Huangjun Zhu and Berthold-Georg Englert. "Quantum state tomography with fully symmetric measurements and product measurements". In: *Physical Review A* 84.2 (2011), p. 022327. DOI: 10.1103/PhysRevA.84.022327 (cit. on pp. v, vii, 3, 151).

[12] Maryia Kabanava, Richard Kueng, Holger Rauhut and Ulrich Terstiege. "Stable low-rank matrix recovery via null space properties". In: *Information and Inference: A Journal of the IMA* 5.4 (2016), pp. 405–441. DOI: 10.1093/imaiai/iaw014 (cit. on pp. v, 151, 152, 197).

[13] Richard Kueng, Holger Rauhut and Ulrich Terstiege. "Low rank matrix recovery from rank one measurements". In: *Applied and Computational Harmonic Analysis* 42.1 (2017), pp. 88–116. DOI: 10.1016/j.acha.2015.07.007 (cit. on pp. v, 151, 152, 197).

[14] Richard Kueng, Huangjun Zhu and David Gross. *Distinguishing quantum states using Clifford orbits*. 2016. arXiv: 1609.08595 (cit. on pp. v, vii, 151, 152).

[15] I. Roth, R. Kueng, S. Kimmel, Y.-K. Liu, D. Gross, J. Eisert and M. Kliesch. "Recovering Quantum Gates from Few Average Gate Fidelities". In: *Physical Review Letters* 121.17 (2018), p. 170502. DOI: 10.1103/PhysRevLett.121.170502 (cit. on pp. v, vii, 151, 152, 187, 197, 199).

[16] Hsin-Yuan Huang, Richard Kueng and John Preskill. "Predicting many properties of a quantum system from very few measurements". In: *Nature Physics* 16.10 (2020), pp. 1050–1057. DOI: 10.1038/s41567-020-0932-7 (cit. on pp. v, vii, 151, 152, 197).

[17] Joseph Emerson, Robert Alicki and Karol {\textbackslash}.Zyczkowski. "Scalable noise estimation with random unitary operators". In: *Journal of Optics B: Quantum and Semiclassical Optics* 7.10 (2005), S347–S352. DOI: 10.1088/1464-4266/7/10/021 (cit. on pp. v, vii, 151).

[18] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin and D. J. Wineland. "Randomized benchmarking of quantum gates". In: *Physical Review A* 77.1 (2008), p. 012307. DOI: 10.1103/PhysRevA.77.012307 (cit. on pp. v, vii, 151).

[19] Easwar Magesan, Jay M. Gambetta and Joseph Emerson. "Characterizing quantum gates via randomized benchmarking". In: *Physical Review A* 85.4 (2012), p. 042311. DOI: 10.1103/PhysRevA.85.042311 (cit. on pp. v, vii, 151).

[20] Timothy Proctor, Kenneth Rudinger, Kevin Young, Mohan Sarovar and Robin Blume-Kohout. "What Randomized Benchmarking Actually Measures". In: *Physical Review Letters* 119.13 (2017), p. 130502. DOI: 10.1103/PhysRevLett.119.130502 (cit. on pp. v, vii, 151).

[21] Jonas Helsen, Xiao Xue, Lieven M. K. Vandersypen and Stephanie Wehner. "A new class of efficient randomized benchmarking protocols". In: *npj Quantum Information* 5.1 (2019), pp. 1–9. DOI: 10.1038/s41534-019-0182-7 (cit. on pp. v, vii, 151).

[22] Jonas Helsen, Sepehr Nezami, Matthew Reagor and Michael Walter. *Matchgate benchmarking: Scalable benchmarking of a continuous family of many-qubit gates*. 2020. arXiv: 2011.13048 (cit. on pp. v, vii, 151).

[23] Jonas Helsen, Ingo Roth, Emilio Onorati, Albert H. Werner and Jens Eisert. *A general framework for randomized benchmarking*. 2020. arXiv: 2010.07974 (cit. on pp. v, vii, 151).

[24] Ernesto F. Galvão. "Discrete Wigner functions and quantum computational speedup". In: *Physical Review A* 71.4 (2005), p. 042302. DOI: 10.1103/PhysRevA.71.042302 (cit. on pp. v, vi, 3, 45, 73, 116).

[25] D. Gross. "Non-negative Wigner functions in prime dimensions". In: *Applied Physics B* 86.3 (2007), pp. 367–370. DOI: 10.1007/s00340-006-2510-9 (cit. on pp. v, vi, 3, 45, 73, 116).

[26] Victor Veitch, Christopher Ferrie, David Gross and Joseph Emerson. "Negative quasi-probability as a resource for quantum computation". In: *New Journal of Physics* 14.11 (2012), p. 113011. DOI: 10.1088/1367-2630/14/11/113011 (cit. on pp. v, vi, 48, 49, 73, 78, 116, 178).

[27] Victor Veitch, S. A. Hamed Mousavian, Daniel Gottesman and Joseph Emerson. "The resource theory of stabilizer quantum computation". In: *New Journal of Physics* 16.1 (2014), p. 013009. DOI: 10.1088/1367-2630/16/1/013009 (cit. on pp. v, vi, 73, 78, 116, 125, 178).

[28] A. Mari and J. Eisert. "Positive Wigner Functions Render Classical Simulation of Quantum Computation Efficient". In: *Physical Review Letters* 109.23 (2012), p. 230503. DOI: 10.1103/PhysRevLett.109.230503 (cit. on pp. v, vi, 73, 78, 116).

[29] Hakop Pashayan, Joel J. Wallman and Stephen D. Bartlett. "Estimating Outcome Probabilities of Quantum Circuits Using Quasiprobabilities". In: *Physical Review Letters* 115.7 (2015), p. 070501. DOI: 10.1103/PhysRevLett.115.070501 (cit. on pp. v, vi, 49, 50, 73, 80, 116, 178).

[30] Sergey Bravyi, Graeme Smith and John A. Smolin. "Trading Classical and Quantum Computational Resources". In: *Physical Review X* 6.2 (2016), p. 021043. DOI: 10.1103/PhysRevX.6.021043 (cit. on pp. v, vi, 74, 78, 81, 178).

[31] Sergey Bravyi and David Gosset. "Improved Classical Simulation of Quantum Circuits Dominated by Clifford Gates". In: *Physical Review Letters* 116.25 (2016), p. 250501. DOI: 10.1103/PhysRevLett.116.250501 (cit. on pp. v, vi, 74, 81, 116, 178).

[32] Mark Howard and Earl Campbell. "Application of a Resource Theory for Magic States to Fault-Tolerant Quantum Computing". In: *Physical Review Letters* 118.9 (2017), p. 090501. DOI: 10.1103/PhysRevLett.118.090501 (cit. on pp. v, vi, 74, 78, 80–83, 93, 103, 104, 116, 178).

[33] Markus Heinrich and David Gross. "Robustness of Magic and Symmetries of the Stabiliser Polytope". In: *Quantum* 3 (2019), p. 132. DOI: 10.22331/q-2019-04-08-132 (cit. on pp. v, vi, 74, 75, 77, 91, 116, 178, 197, 198).

[34] Sergey Bravyi, Dan Browne, Padraic Calpin, Earl Campbell, David Gosset and Mark Howard. "Simulation of quantum circuits by low-rank stabilizer decompositions". In: *Quantum* 3 (2019), p. 181. DOI: 10.22331/q-2019-09-02-181 (cit. on pp. v, vi, 74, 116, 178, 198).

[35] James R. Seddon and Earl T. Campbell. "Quantifying magic for multi-qubit operations". In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 475.2227 (2019), p. 20190251. DOI: 10.1098/rspa.2019.0251 (cit. on pp. v, vi, 74, 116, 119, 120, 178, 198).

[36] James R. Seddon, Bartosz Regula, Hakop Pashayan, Yingkai Ouyang and Earl T. Campbell. *Quantifying quantum speedups: improved classical simulation from tighter magic monotones*. 2020. arXiv: 2002.06181 (cit. on pp. v, vi, 74, 116, 120, 125, 147, 178, 198).

[37] Michael Beverland, Earl Campbell, Mark Howard and Vadym Kliuchnikov. "Lower bounds on the non-Clifford resources for quantum computations". In: *Quantum Science and Technology* 5.3 (2020), p. 035009. DOI: 10.1088/2058-9565/ab8963 (cit. on pp. v, vi, 74, 116, 178).

[38] Arne Heimendahl, Felipe Montealegre-Mora, Frank Vallentin and David Gross. *Stabilizer extent is not multiplicative*. 2020. arXiv: 2007.04363 (cit. on pp. v, vi, 74, 116, 198).

[39] Zi-Wen Liu and Andreas Winter. *Many-body quantum magic*. 2020. arXiv: 2010.13817 (cit. on pp. v, vi, 74, 116, 125, 148, 198).

[40] Daniel Gottesman. *The Heisenberg Representation of Quantum Computers*. 1998. arXiv: quant-ph/9807006 (cit. on pp. v, vi, 3, 9, 31, 41).

[41] D. Schlingemann and R. F. Werner. "Quantum error-correcting codes associated with graphs". In: *Physical Review A* 65.1 (2001), p. 012308. DOI: 10.1103/PhysRevA.65.012308 (cit. on pp. v, 37).

[42] D. Schlingemann. *Stabilizer codes can be realized as graph codes*. 2001. arXiv: quant-ph/0111080 (cit. on pp. v, 90–92).

[43] Maarten Van den Nest, Jeroen Dehaene and Bart De Moor. "Graphical description of the action of local Clifford transformations on graph states". In: *Physical Review A* 69.2 (2004). DOI: 10.1103/PhysRevA.69.022316 (cit. on pp. v, 90).

[44] Matthew B. Elliott, Bryan Eastin and Carlton M. Caves. "Graphical description of the action of Clifford operators on stabilizer states". In: *Physical Review A* 77.4 (2008), p. 042307. DOI: 10.1103/PhysRevA.77.042307 (cit. on pp. v, 91, 92).

[45] M. Hein, J. Eisert and H. J. Briegel. "Multiparty entanglement in graph states". In: *Physical Review A* 69.6 (2004). DOI: 10.1103/PhysRevA.69.062311 (cit. on pp. v, 37, 90).

[46] David Fattal, Toby S. Cubitt, Yoshihisa Yamamoto, Sergey Bravyi and Isaac L. Chuang. *Entanglement in the stabilizer formalism*. 2004. arXiv: 0406168 (cit. on p. v).

[47] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest and H.-J. Briegel. *Entanglement in Graph States and its Applications*. 2006. arXiv: quant-ph/0602096 (cit. on pp. v, 91).

[48] Charles H. Bennett. "Mixed-state entanglement and quantum error correction". In: *Physical Review A* 54.5 (1996), pp. 3824–3851. DOI: 10.1103/PhysRevA.54.3824 (cit. on pp. v, 3).

[49] A. R. Calderbank and Peter W. Shor. "Good quantum error-correcting codes exist". In: *Physical Review A* 54.2 (1996), pp. 1098–1105. DOI: 10.1103/PhysRevA.54.1098 (cit. on pp. v, 3).

[50] Andrew Steane. "Multiple-particle interference and quantum error correction". In: *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 452.1954 (1996), pp. 2551–2577. DOI: 10.1098/rspa.1996.0136 (cit. on pp. v, 3).

[51] Daniel Gottesman. *Stabilizer Codes and Quantum Error Correction*. 1997. arXiv: quant-ph/9705052 (cit. on pp. v, vi, 3, 5, 116, 118).

[52] Daniel Gottesman. "Theory of fault-tolerant quantum computation". In: *Physical Review A* 57.1 (1998), pp. 127–137. DOI: 10.1103/PhysRevA.57.127 (cit. on pp. v, vi, 3, 151).

[53] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane. "Quantum Error Correction and Orthogonal Geometry". In: *Physical Review Letters* 78.3 (1997), pp. 405–408. DOI: 10.1103/PhysRevLett.78.405 (cit. on pp. vi, 3, 5).

[54] A. R. Calderbank, E. M. Rains, P. M. Shor and N. J. A. Sloane. "Quantum error correction via codes over GF(4)". In: *IEEE Transactions on Information Theory* 44.4 (1998), pp. 1369–1387. DOI: 10.1109/18.681315 (cit. on pp. vi, 3, 29, 31).

[55] Sergey Bravyi and Alexei Kitaev. "Universal quantum computation with ideal Clifford gates and noisy ancillas". In: *Physical Review A* 71.2 (2005), p. 022316. DOI: 10.1103/PhysRevA.71.022316 (cit. on pp. vii, 73, 78, 116).

[56] Andris Ambainis, Jan Bouda and Andreas Winter. "Nonmalleable encryption of quantum information". In: *Journal of Mathematical Physics* 50.4 (2009), p. 042106. DOI: 10.1063/1.3094756 (cit. on pp. vii, 151).

[57] D. P. DiVincenzo, D. W. Leung and B. M. Terhal. "Quantum data hiding". In: *IEEE Transactions on Information Theory* 48.3 (2002), pp. 580–598. DOI: 10.1109/18.985948 (cit. on pp. vii, 151).

[58] Jonas Haferkamp, Felipe Montealegre-Mora, Markus Heinrich, Jens Eisert, David Gross and Ingo Roth. *Quantum homeopathy works: Efficient unitary designs with a system-size independent number of non-Clifford gates*. Submitted to Communications in Mathematical Physics. 2020. arXiv: 2002.09524 (cit. on pp. viii, 152, 153, 171, 175, 180, 181, 187, 191, 199).

[59] A. R. Calderbank, R. H. Hardin, E. M. Rains, P. W. Shor and N. J. A. Sloane. "A Group-Theoretic Framework for the Construction of Packings in Grassmannian Spaces". In: *J. Algebraic Combinatorics* 9 (1999), pp. 129–140 (cit. on p. 3).

[60] Gabriele Nebe, E. M. Rains and N. J. A. Sloane. "The Invariants of the Clifford Groups". In: *Designs, Codes and Cryptography* 24.1 (2001), pp. 99–122. DOI: 10.1023/A:1011233615437 (cit. on pp. 3, 6, 30, 31, 151, 176).

[61] William K Wootters and Brian D Fields. "Optimal state-determination by mutually unbiased measurements". In: *Annals of Physics* 191.2 (1989), pp. 363–381. DOI: 10.1016/0003-4916(89)90322-9 (cit. on pp. 3, 51).

[62] S. Chaturvedi. "Mutually unbiased bases". In: *Pramana* 59.2 (2002), pp. 345–350. DOI: 10.1007/s12043-002-0126-0 (cit. on p. 3).

[63] Somshubhro Bandyopadhyay, P. Oscar Boykin, Vwani Roychowdhury and Farrokh Vatan. "A new proof for the existence of mutually unbiased bases". In: *Algorithmica* 34 (2002), pp. 512–528 (cit. on p. 3).

[64] Andreas Klappenecker and Martin Roetteler. "Constructions of Mutually Unbiased Bases". In: *Proceedings of the 7th International Conference on Finite Fields*. Lecture Notes in Computer Science (2004), pp. 137–144 (cit. on p. 3).

[65] Kathleen S. Gibbons, Matthew J. Hoffman and William K. Wootters. "Discrete phase space based on finite fields". In: *Physical Review A* 70.6 (2004), p. 062101. DOI: 10.1103/PhysRevA.70.062101 (cit. on pp. 3, 45, 48, 117).

[66] D. M. Appleby. "Symmetric informationally complete–positive operator valued measures and the extended Clifford group". In: *Journal of Mathematical Physics* 46.5 (2005), p. 052107. DOI: 10.1063/1.1896384 (cit. on pp. 3, 4, 23, 60, 83, 108, 117).

[67] D. M. Appleby. *Properties of the extended Clifford group with applications to SIC-POVMs and MUBs*. 2009. arXiv: 0909.5233 (cit. on pp. 3, 4, 23, 41, 60).

[68] David Marcus Appleby, Ingemar Bengtsson, Stephen Brierley, Markus Grassl, David Gross and Jan-Åke Larsson. "The monomial representations of the Clifford group". In: *Quantum Inf. Comput.* 12.5-6 (2012), pp. 404–431 (cit. on pp. 3, 4, 23, 60).

[69] D. M. Appleby, Ingemar Bengtsson and Hoan Bui Dang. *Galois Unitaries, Mutually Unbiased Bases, and MUB-balanced states*. 2014. arXiv: 1409.7987 (cit. on p. 3).

[70] Claudio Carmeli, Jussi Schultz and Alessandro Toigo. "Covariant mutually unbiased bases". In: *Reviews in Mathematical Physics* 28.4 (2016), p. 1650009. DOI: 10.1142/S0129055X16500094 (cit. on p. 3).

[71] Huangjun Zhu. "Mutually unbiased bases as minimal Clifford covariant 2-designs". In: *Physical Review A* 91.6 (2015), p. 060301. DOI: 10.1103/PhysRevA.91.060301 (cit. on pp. 3, 51).

[72] William K Wootters. "A Wigner-function formulation of finite-state quantum mechanics". In: *Annals of Physics* 176.1 (1987), pp. 1–21. DOI: 10.1016/0003-4916(87)90176-X (cit. on pp. 3, 45, 117).

[73] Ulf Leonhardt. "Quantum-State Tomography and Discrete Wigner Function". In: *Physical Review Letters* 74.21 (1995), pp. 4101–4105. DOI: 10.1103/PhysRevLett.74.4101 (cit. on pp. 3, 45).

[74] Ulf Leonhardt. "Discrete Wigner function and quantum-state tomography". In: *Physical Review A* 53.5 (1996), pp. 2998–3013. DOI: 10.1103/PhysRevA.53.2998 (cit. on pp. 3, 45).

[75] D. Gross. "Hudson's theorem for finite-dimensional quantum systems". In: *Journal of Mathematical Physics* 47.12 (2006), p. 122107. DOI: 10.1063/1.2393152 (cit. on pp. 3, 29, 35, 37, 39, 41, 45, 48, 78, 108, 117).

[76] Cecilia Cormick, Ernesto F. Galvão, Daniel Gottesman, Juan Pablo Paz and Arthur O. Pittenger. "Classicality in discrete Wigner functions". In: *Physical Review A* 73.1 (2006), p. 012301. DOI: 10.1103/PhysRevA.73.012301 (cit. on pp. 3, 45, 108).

[77] Beverley Bolt, T. G. Room and G. E. Wall. "On the Clifford collineation, transform and similarity groups. I." In: *Journal of the Australian Mathematical Society* 2.1 (1961), pp. 60–79. DOI: 10.1017/S1446788700026379 (cit. on pp. 3, 50, 60, 74).

[78] Beverley Bolt, T. G. Room and G. E. Wall. "On the Clifford collineation, transform and similarity groups. II." In: *Journal of the Australian Mathematical Society* 2.1 (1961), pp. 80–96. DOI: 10.1017/S1446788700026380 (cit. on pp. 3, 61, 67).

[79] W. M. Kantor A. R. Calderbank P. J. Cameron and J. J. Seidel. "$\mathbb{Z}_4$ Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets". In: *Proceedings of the London Mathematical Society* 75 (1997), pp. 436–480 (cit. on p. 3).

[80] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups*. 2nd. Grundlehren der math. Wissenschaften 290. Springer, 1993 (cit. on p. 3).

[81] John H. Conway, Ronald H. Hardin and Neil J. A. Sloane. "Packing Lines, Planes, etc.: Packings in Grassmannian Spaces". In: *Experimental Mathematics* 5.2 (1996), pp. 139–159. DOI: 10.1080/10586458.1996.10504585 (cit. on p. 3).

[82] P. W. Shor and N. J. A. Sloane. "A family of optimal packings in Grassmannian manifolds". In: *J. Algebraic Combin.* 7 (1998), pp. 157–163 (cit. on p. 3).

[83] André Weil. "Sur certains groupes d'opérateurs unitaires". In: *Acta Mathematica* 111 (1964), pp. 143–211. DOI: 10.1007/BF02391012 (cit. on pp. 3, 18, 60).

[84] Markus Grassl. *On SIC-POVMs and MUBs in Dimension 6*. 2009. arXiv: quant-ph/0406175 (cit. on pp. 4, 23, 52, 60).

[85] Niel De Beaudrap. "A linearized stabilizer formalism for systems of finite dimension". In: *Quantum Information & Computation* 13.1 (2013), pp. 73–115 (cit. on pp. 4, 23, 29, 60, 117).

[86] Shamgar Gurevich and Ronny Hadani. "The Weil representation in characteristic two". In: *Advances in Mathematics* 230.3 (2012), pp. 894–926. DOI: 10.1016/j.aim.2012.03.008 (cit. on pp. 4, 18, 23, 25, 60, 65, 67, 68).

[87] Huangjun Zhu, Richard Kueng, Markus Grassl and David Gross. *The Clifford group fails gracefully to be a unitary 4-design*. 2016. arXiv: 1609.08172 (cit. on pp. 6, 30, 152, 155, 161, 162, 199).

[88] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A* 70.5 (2004), p. 052328. DOI: 10.1103/PhysRevA.70.052328 (cit. on pp. 9, 43, 116, 118, 178, 186).

[89] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. 2nd ed. Encyclopedia of Mathematics and its Applications. Cambridge: Cambridge University Press, 1996. DOI: 10.1017/CBO9780511525926 (cit. on p. 11).

[90] Gary L. Mullen and Daniel Panario. *Handbook of Finite Fields*. 1st. Chapman & Hall/CRC, 2013. 1068 pp. (cit. on p. 11).

[91] Rolf Berndt. *An Introduction to Symplectic Geometry*. Vol. 26. Graduate Studies in Mathematics. American Mathematical Society, 2001 (cit. on p. 11).

[92] Nolan R. Wallach. *Symplectic Geometry and Fourier Analysis*. 2nd. Dover Publications, 2018 (cit. on p. 11).

[93] Ernst Witt. "Theorie der quadratischen Formen in beliebigen Körpern". In: *Journal für die Reine und Angewandte Mathematik* 176 (1936), pp. 31–44 (cit. on p. 14).

[94] Emil Artin. "The orders of the classical simple groups". In: *Communications on Pure and Applied Mathematics* 8.4 (1955), pp. 455–472. DOI: https://doi.org/10.1002/cpa.3160080403 (cit. on p. 15).

[95] Markus Neuhauser. "An Explicit Construction of the Metaplectic Representation over a Finite Field". In: *Journal of Lie Theory* 12.1 (2002), pp. 15–30 (cit. on pp. 16, 18, 23).

[96] Daniel Gottesman. "Fault-Tolerant Quantum Computation with Higher-Dimensional Systems". In: *Chaos, Solitons & Fractals* 10.10 (1999), pp. 1749–1758. DOI: 10.1016/S0960-0779(98)00218-5 (cit. on pp. 16, 31).

[97] Gerald B. Folland. *Harmonic Analysis in Phase Space.* Vol. 122. Annals of Mathematics Studies. 1989 (cit. on p. 18).

[98] Paul Gérardin. "Weil representations associated to finite fields". In: *Journal of Algebra* 46.1 (1977), pp. 54–101. DOI: 10.1016/0021-8693(77)90394-5 (cit. on p. 18).

[99] Shamgar Gurevich and Ronny Hadani. "The geometric Weil representation". In: *Selecta Mathematica* 13.3 (2007), p. 465. DOI: 10.1007/s00029-007-0047-3 (cit. on p. 18).

[100] Shamgar Gurevich and Ronny Hadani. "Notes on Canonical Quantization of Symplectic Vector Spaces over Finite Fields". In: *Arithmetic and Geometry Around Quantization*. Ed. by Özgür Ceyhan, Yu. I. Manin and Matilde Marcolli. Progress in Mathematics. Boston, MA: Birkhäuser, 2010, pp. 233–251. DOI: 10.1007/978-0-8176-4831-2_8 (cit. on p. 18).

[101] Jeroen Dehaene and Bart De Moor. "The Clifford group, stabilizer states, and linear and quadratic operations over GF(2)". In: *Physical Review A* 68.4 (2003). DOI: 10.1103/PhysRevA.68.042318 (cit. on pp. 29, 37).

[102] Erik Hostens, Jeroen Dehaene and Bart De Moor. "Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic". In: *Physical Review A* 71.4 (2005), p. 042315. DOI: 10.1103/PhysRevA.71.042315 (cit. on p. 29).

[103] Narayanan Rengaswamy, Robert Calderbank, Swanand Kadhe and Henry D. Pfister. *Synthesis of Logical Clifford Operators via Symplectic Geometry*. 2018. arXiv: 1803.06987 (cit. on pp. 29, 55).

[104] Narayanan Rengaswamy, Robert Calderbank and Henry D. Pfister. *Unifying the Clifford Hierarchy via Symmetric Matrices over Rings*. 2019. arXiv: 1902.04022 (cit. on p. 29).

[105] Robert Raussendorf, Juani Bermejo-Vega, Emily Tyhurst, Cihan Okay and Michael Zurel. *Phase space simulation method for quantum computation with magic states on qubits*. 2019. arXiv: 1905.05374 (cit. on pp. 29, 74).

[106] Simeon Ball, Aina Centelles and Felix Huber. *Quantum error-correcting codes and their geometries*. 2020. arXiv: 2007.05992 (cit. on pp. 29, 32).

[107] Gabriele Nebe. "Finite quaternionic matrix groups". In: *Representation Theory of the American Mathematical Society* 2.5 (1998), pp. 106–223. DOI: 10.1090/S1088-4165-98-00011-9 (cit. on p. 31).

[108] Richard Kueng and David Gross. *Qubit stabilizer states are complex projective 3-designs*. 2015. arXiv: 1510.02767 (cit. on pp. 35, 84, 108).

[109] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. 10th Anniversary Edition. Cambridge: Cambridge University Press, 2010 (cit. on p. 36).

[110] Shamgar Gurevich and Roger Howe. "Rank and duality in representation theory". In: *Japanese Journal of Mathematics* 15 (2020), pp. 1–87. DOI: 10.1007/s11537-020-1728-3 (cit. on pp. 37, 153, 166, 170).

[111] D. Gross, K. Audenaert and J. Eisert. "Evenly distributed unitaries: On the structure of unitary designs". In: *Journal of Mathematical Physics* 48.5 (2007), p. 052104. DOI: 10.1063/1.2716992 (cit. on pp. 39, 151, 153, 155, 157, 158, 160).

[112] Huangjun Zhu. "Permutation Symmetry Determines the Discrete Wigner Function". In: *Physical Review Letters* 116.4 (2016), p. 040501. DOI: 10.1103/PhysRevLett.116.040501 (cit. on pp. 50, 74).

[113] Huangjun Zhu. "Multiqubit Clifford groups are unitary 3-designs". In: *Physical Review A* 96.6 (2017), p. 062336. DOI: 10.1103/PhysRevA.96.062336 (cit. on pp. 50, 84, 108, 153, 160, 161).

[114] Zak Webb. "The Clifford Group Forms a Unitary 3-design". In: *Quantum Info. Comput.* 16.15 (2016), pp. 1379–1400 (cit. on pp. 50, 84, 108, 160).

[115] Eiichi Bannai, Gabriel Navarro, Noelia Rizo and Pham Huu Tiep. "Unitary t-groups". In: *Journal of the Mathematical Society of Japan* (2020). DOI: 10.2969/jmsj/82228222 (cit. on pp. 50, 151–153, 171, 172, 175, 199).

[116] Julian Schwinger. "Unitary operator bases". In: *Proceedings of the National Academy of Sciences* 46.4 (1960), pp. 570–579. DOI: 10.1073/pnas.46.4.570 (cit. on p. 51).

[117] I. D. Ivonovic. "Geometrical description of quantal state determination". In: *Journal of Physics A: Mathematical and General* 14.12 (1981), pp. 3241–3245. DOI: 10.1088/0305-4470/14/12/019 (cit. on p. 51).

[118] Persi Diaconis and Mehrdad Shahshahani. "The Subgroup Algorithm for Generating Uniform Random Variables". In: *Probability in the Engineering and Informational Sciences* 1.1 (1987), pp. 15–32. DOI: 10.1017/S0269964800000255 (cit. on p. 52).

[119] Robert Koenig and John A. Smolin. "How to efficiently select an arbitrary Clifford group element". In: *Journal of Mathematical Physics* 55.12 (2014), p. 122202. DOI: 10.1063/1.4903507 (cit. on pp. 52, 178).

[120] Peter J Cameron and Queen Mary and Westfield College (University of London). *Projective and polar spaces*. OCLC: 26548463. London: University of London, Queen Mary and Westfield College, 1992 (cit. on p. 61).

[121] Donald E Taylor. *The geometry of the classical groups*. OCLC: 26769296. Berlin: Heldermann Verlag, 1992 (cit. on p. 61).

[122] Mark Howard, Joel Wallman, Victor Veitch and Joseph Emerson. "Contextuality supplies the 'magic' for quantum computation". In: *Nature* 510.7505 (2014), pp. 351–355. DOI: 10.1038/nature13460 (cit. on pp. 73, 116).

[123] Nicolas Delfosse, Cihan Okay, Juan Bermejo-Vega, Dan E. Browne and Robert Raussendorf. "Equivalence between contextuality and negativity of the Wigner function for qudits". In: *New Journal of Physics* 19.12 (2017), p. 123024. DOI: 10.1088/1367-2630/aa8fe3 (cit. on pp. 73, 116).

[124] Nicolas Delfosse, Philippe Allard Guerin, Jacob Bian and Robert Raussendorf. "Wigner Function Negativity and Contextuality in Quantum Computation on Rebits". In: *Physical Review X* 5.2 (2015). DOI: 10.1103/PhysRevX.5.021003 (cit. on p. 74).

[125] Robert Raussendorf, Dan E. Browne, Nicolas Delfosse, Cihan Okay and Juan Bermejo-Vega. "Contextuality and Wigner-function negativity in qubit quantum computation". In: *Physical Review A* 95.5 (2017), p. 052334. DOI: 10.1103/PhysRevA.95.052334 (cit. on p. 74).

[126] Juan Bermejo-Vega, Nicolas Delfosse, Dan E. Browne, Cihan Okay and Robert Raussendorf. "Contextuality as a Resource for Models of Quantum Computation with Qubits". In: *Physical Review Letters* 119.12 (2017), p. 120505. DOI: 10.1103/PhysRevLett.119.120505 (cit. on p. 74).

[127] Michael Zurel, Cihan Okay and Robert Raussendorf. *A hidden variable model for universal quantum computation with magic states on qubits*. 2020. arXiv: 2004.01992 (cit. on p. 74).

[128] Mehdi Ahmadi, Hoan Bui Dang, Gilad Gour and Barry C. Sanders. "Quantification and manipulation of magic states". In: *Physical Review A* 97.6 (2018), p. 062332. DOI: 10.1103/PhysRevA.97.062332 (cit. on pp. 74, 198).

[129] Arne Heimendahl*, Markus Heinrich* and David Gross. *The axiomatic and the operational approaches to resource theories of magic do not coincide*. 2020. arXiv: 2011.11651 (cit. on pp. 75, 115, 130, 176, 197, 198).

[130] Earl T. Campbell, Barbara M. Terhal and Christophe Vuillot. "Roads towards fault-tolerant universal quantum computation". In: *Nature* 549.7671 (2017), pp. 172–179. DOI: 10.1038/nature23460 (cit. on p. 78).

[131] Bryan Eastin and Emanuel Knill. "Restrictions on Transversal Encoded Quantum Gate Sets". In: *Physical Review Letters* 102.11 (2009), p. 110502. DOI: 10.1103/PhysRevLett.102.110502 (cit. on p. 78).

[132] Ben W. Reichardt. *Quantum universality by state distillation*. 2006. arXiv: quant-ph/0608085 (cit. on p. 78).

[133] Huangjun Zhu. "Permutation symmetry determines the discrete Wigner function". In: *Physical Review Letters* 116.4 (2016-01-26), p. 040501. DOI: 10.1103/PhysRevLett.116.040501 (cit. on p. 78).

[134] Angela Karanjai, Joel J Wallman and Stephen D Bartlett. *Contextuality bounds the efficiency of classical simulation of quantum processes*. 2018. arXiv: arXiv:1802.07744 (cit. on p. 78).

[135] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 10th. New York, NY, USA: Cambridge University Press, 2011. DOI: 10.1017/CBO9780511976667 (cit. on p. 79).

[136] S. Virmani, Susana F. Huelga and Martin B. Plenio. "Classical simulability, entanglement breaking, and quantum computation thresholds". In: *Physical Review A* 71.4 (2005), p. 042328. DOI: 10.1103/PhysRevA.71.042328 (cit. on p. 79).

[137] J. Gubernatis, N. Kawashima and P. Werner. *Quantum Monte Carlo Methods: Algorithms for Lattice Models*. Cambridge University Press, 2016. DOI: 10.1017/CBO9780511902581 (cit. on p. 79).

[138] Sergey Bravyi, Dan Browne, Padraic Calpin, Earl Campbell, David Gosset and Mark Howard. *Simulation of quantum circuits by low-rank stabilizer decompositions*. 2018. arXiv: 1808.00128 (cit. on p. 81).

[139] Guifré Vidal and Rolf Tarrach. "Robustness of entanglement". In: *Physical Review A* 59.1 (1999), pp. 141–155. DOI: 10.1103/PhysRevA.59.141 (cit. on pp. 82, 103).

[140] Stephen Boyd and Lieven Vandenberghe. *Convex Optimization*. Seventh printing with corrections. Cambridge University Press, 2009. DOI: 10.1017/CBO9780511804441.007 (cit. on pp. 83, 110).

[141] Christine Bachoc, Dion C. Gijswijt, Alexander Schrijver and Frank Vallentin. "Invariant semidefinite programs". In: *Handbook on Semidefinite, Conic and Polynomial Optimization*. Ed. by Miguel F. Anjos and Jean B. Lasserre. International Series in Operations Research & Management Science. Springer US, 2012. DOI: 10.1007/978-1-4614-0769-0 (cit. on p. 83).

[142] David Gross, Sepehr Nezami and Michael Walter. *Schur-Weyl Duality for the Clifford Group with Applications: Property Testing, a Robust Hudson Theorem, and de Finetti Representations*. 2017. arXiv: 1712.08628 (cit. on p. 85).

[143] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North Holland, 1977. DOI: 0.1137/1022103 (cit. on p. 87).

[144] Gabriele Nebe, Eric M. Rains and Neil J. A. Sloane. *Self-Dual Codes and Invariant Theory*. Springer Science & Business Media, 2006. 449 pp. DOI: 10.1007/3-540-30731-1 (cit. on p. 87).

[145] Patrick Rall. *Signed quantum weight enumerators characterize qubit magic state distillation*. 2017. arXiv: arXiv:1702.06990 (cit. on p. 87).

[146] Patrick Rall. *Fractal Properties of Magic State Distillation*. 2017. arXiv: 1708.09256 (cit. on p. 87).

[147] Lars Eirik Danielsen and Matthew G. Parker. "On the classification of all self-dual additive codes over GF(4) of length up to 12". In: *Journal of Combinatorial Theory, Series A* 113.7 (2006), pp. 1351–1367. DOI: 10.1016/j.jcta.2005.12.004 (cit. on pp. 91, 108).

[148] Lars Eirik Danielsen. *Database of Self-Dual Quantum Codes*. URL: http://www.ii.uib.no/~larsed/vncorbits/ (visited on 12/06/2018) (cit. on pp. 91, 108).

[149] Matthew B Hastings. "Superadditivity of communication capacity using entangled inputs". In: *Nature Physics* 5.4 (2009), p. 255. DOI: 10.1038/nphys1224 (cit. on p. 102).

[150] Israel Nathan Herstein. "Jordan Homomorphisms". In: *Transaction of the American Mathematical Society* 81.2 (1956), pp. 331–341. DOI: 10.2307/1992920 (cit. on p. 107).

[151] J. H. Dulá and R. V. Helgason. "A new procedure for identifying the frame of the convex hull of a finite collection of points in multidimensional space". In: *European Journal of Operational Research* 92.2 (1996), pp. 352–367. DOI: 10.1016/0377-2217(94)00366-1 (cit. on p. 109).

[152] Robert Raussendorf, Juani Bermejo-Vega, Emily Tyhurst, Cihan Okay and Michael Zurel. "Phase space simulation method for quantum computation with magic states on qubits". In: *Phys. Rev. A 101, 012350 (2020)* (2019). DOI: 10.1103/PhysRevA.101.012350 (cit. on p. 116).

[153] Charles H. Bennett, David P. DiVincenzo, Christopher A. Fuchs, Tal Mor, Eric Rains, Peter W. Shor, John A. Smolin and William K. Wootters. "Quantum nonlocality without entanglement". In: *Physical Review A* 59.2 (1999), pp. 1070–1091. DOI: 10.1103/PhysRevA.59.1070 (cit. on p. 116).

[154] Eric Chitambar, Debbie Leung, Laura Mančinska, Maris Ozols and Andreas Winter. "Everything You Always Wanted to Know About LOCC (But Were Afraid to Ask)". In: *Communications in Mathematical Physics* 328.1 (2014), pp. 303–326. DOI: 10.1007/s00220-014-1953-9 (cit. on p. 116).

[155] Masato Koashi, Fumitaka Takenaga, Takashi Yamamoto and Nobuyuki Imoto. *Quantum nonlocality without entanglement in a pair of qubits*. 2007. arXiv: 0709.3196 (cit. on pp. 117, 198).

[156] R. Duan, Y. Feng, Y. Xin and M. Ying. "Distinguishability of Quantum States by Separable Operations". In: *IEEE Transactions on Information Theory* 55.3 (2009), pp. 1320–1330. DOI: 10.1109/TIT.2008.2011524 (cit. on pp. 117, 198).

[157] Eric Chitambar, Wei Cui and Hoi-Kwong Lo. "Increasing Entanglement Monotones by Separable Operations". In: *Physical Review Letters* 108.24 (2012), p. 240504. DOI: 10.1103/PhysRevLett.108.240504 (cit. on pp. 117, 125, 198).

[158] Arne Heimendahl. "The stabilizer polytope and contextuality for qubit systems". MA thesis. University of Cologne, 2019 (cit. on p. 122).

[159] Jeffrey Epstein. "Stabilizer Quantum Mechanics and Magic State Distillation". Master's Essay, Perimeter Institute. 2015 (cit. on p. 122).

[160] Zi-Wen Liu. "One-Shot Operational Quantum Resource Theory". In: *Physical Review Letters* 123.2 (2019). DOI: 10.1103/PhysRevLett.123.020401 (cit. on p. 125).

[161] Kun Fang and Zi-Wen Liu. "No-Go Theorems for Quantum Resource Purification". In: *Physical Review Letters* 125.6 (2020), p. 060405. DOI: 10.1103/PhysRevLett.125.060405 (cit. on p. 125).

[162] Xin Wang, Mark M. Wilde and Yuan Su. "Efficiently Computable Bounds for Magic State Distillation". In: *Physical Review Letters* 124.9 (2020), p. 090505. DOI: 10.1103/PhysRevLett.124.090505 (cit. on p. 125).

[163] Roger Howe. "Invariant theory and duality for classical groups over finite fields with applications to their singular representation theory". preprint, Yale University. 1973 (cit. on pp. 131, 153, 166, 170).

[164] Roger Howe. "The oscillator semigroup". In: *The Mathematical Heritage of Hermann Weyl*. Proc. Sympos. Pure Math. 48. Amer. Math. Soc., 1988, pp. 61–132 (cit. on pp. 131, 153, 166, 170).

[165] Günter M. Ziegler. *Lectures on Polytopes*. Springer, 1995 (cit. on p. 133).

[166] Eric Chitambar and Gilad Gour. "Quantum resource theories". In: *Reviews of Modern Physics* 91.2 (2019), p. 025001. DOI: 10.1103/RevModPhys.91.025001 (cit. on p. 148).

[167] Fernando G. S. L. Brandão and Gilad Gour. "Reversible Framework for Quantum Resource Theories". In: *Physical Review Letters* 115.7 (2015), p. 070503. DOI: 10.1103/PhysRevLett.115.070503 (cit. on p. 148).

[168] Daniel Gottesman and Isaac L. Chuang. "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations". In: *Nature* 402.6760 (1999), pp. 390–393. DOI: 10.1038/46503 (cit. on p. 151).

[169] Bei Zeng, Xie Chen and Isaac L. Chuang. "Semi-Clifford operations, structure of C_k hierarchy, and gate complexity for fault-tolerant quantum computation". In: *Physical Review A* 77.4 (2008), p. 042313. DOI: 10.1103/PhysRevA.77.042313 (cit. on p. 151).

[170] B. Zeng, A. Cross and I. L. Chuang. "Transversality Versus Universality for Additive Quantum Codes". In: *IEEE Transactions on Information Theory* 57.9 (2011), pp. 6272–6284. DOI: 10.1109/TIT.2011.2161917 (cit. on p. 151).

[171] Sergey Bravyi and Robert König. "Classification of Topologically Protected Gates for Local Stabilizer Codes". In: *Physical Review Letters* 110.17 (2013), p. 170503. DOI: 10.1103/PhysRevLett.110.170503 (cit. on p. 151).

[172] Jonas T. Anderson and Tomas Jochym-O'Connor. *Classification of transversal gates in qubit stabilizer codes*. 2014. arXiv: 1409.8320 (cit. on p. 151).

[173] Fernando Pastawski and Beni Yoshida. "Fault-tolerant logical gates in quantum error-correcting codes". In: *Physical Review A* 91.1 (2015), p. 012305. DOI: 10.1103/PhysRevA.91.012305 (cit. on p. 151).

[174] Shawn X. Cui, Daniel Gottesman and Anirudh Krishna. "Diagonal gates in the Clifford hierarchy". In: *Physical Review A* 95.1 (2017). DOI: 10.1103/PhysRevA.95.012329. arXiv: 1608.06596 (cit. on p. 151).

[175] Tomas Jochym-O'Connor, Aleksander Kubica and Theodore J. Yoder. "Disjointness of Stabilizer Codes and Limitations on Fault-Tolerant Logical Gates". In: *Physical Review X* 8.2 (2018), p. 021047. DOI: 10.1103/PhysRevX.8.021047 (cit. on p. 151).

[176] Christoph Dankert. *Efficient Simulation of Random Quantum States and Operators*. M.Sc. thesis, University of Waterloo. 2005. arXiv: quant-ph/0512217 (cit. on pp. 151, 155).

[177] Christoph Dankert, Richard Cleve, Joseph Emerson and Etera Livine. "Exact and approximate unitary 2-designs and their application to fidelity estimation". In: *Physical Review A* 80.1 (2009), p. 012304. DOI: 10.1103/PhysRevA.80.012304 (cit. on pp. 151, 155).

[178] Eiichi Bannai, Yoshifumi Nakata, Takayuki Okuda and Da Zhao. *Explicit construction of exact unitary designs*. 2020. arXiv: 2009.11170 (cit. on pp. 151, 156, 175).

[179] Jonas Helsen, Joel J. Wallman and Stephanie Wehner. "Representations of the multi-qubit Clifford group". In: *Journal of Mathematical Physics* 59.7 (2018), p. 072201. DOI: 10.1063/1.4997688 (cit. on pp. 152, 161, 162).

[180] Richard Kueng, Huangjun Zhu and David Gross. *Low rank matrix recovery from Clifford orbits*. 2016. arXiv: 1610.08070 (cit. on p. 152).

[181] David Gross, Sepehr Nezami and Michael Walter. *Schur-Weyl Duality for the Clifford Group with Applications: Property Testing, a Robust Hudson Theorem, and de Finetti Representations*. 2019. arXiv: 1712.08628 (cit. on pp. 152, 153, 162–165, 170, 181, 187, 189, 199).

[182] Fernando G. S. L. Brandao, Aram W. Harrow and Michal Horodecki. "Local random quantum circuits are approximate polynomial-designs". In: *Communications in Mathematical Physics* 346.2 (2016), pp. 397–434. DOI: 10.1007/s00220-016-2706-8. arXiv: 1208.0692 (cit. on pp. 152, 175, 176, 178, 184, 199).

[183] Shelby Kimmel, Marcus P. da Silva, Colm A. Ryan, Blake R. Johnson and Thomas Ohki. "Robust Extraction of Tomographic Information via Randomized Benchmarking". In: *Physical Review X* 4.1 (2014), p. 011050. DOI: 10.1103/PhysRevX.4.011050 (cit. on pp. 152, 197).

[184] S. Kimmel and Y. Liu. "Phase retrieval using unitary 2-designs". In: *2017 International Conference on Sampling Theory and Applications (SampTA)*. 2017 International Conference on Sampling Theory and Applications (SampTA). 2017, pp. 345–349. DOI: 10.1109/SAMPTA.2017.8024414 (cit. on pp. 152, 197).

[185] Niraj Kumar, Rawad Mezher and Elham Kashefi. *Efficient Construction of Quantum Physical Unclonable Functions with Unitary t-designs*. 2021. arXiv: 2101.05692 (cit. on pp. 152, 197, 199).

[186] A. Sawicki and K. Karnas. "Universality of single qudit gates". In: *Ann. Henri Poincaré* (2017), Volume 18, Issue 11, pp 3515–3552 (cit. on pp. 153, 171–173).

[187] P. D Seymour and Thomas Zaslavsky. "Averaging sets: A generalization of mean values and spherical designs". In: *Advances in Mathematics* 52.3 (1984), pp. 213–240. DOI: 10.1016/0001-8708(84)90022-7 (cit. on p. 156).

[188] Eiichi Bannai, Mikio Nakahara, Da Zhao and Yan Zhu. "On the explicit constructions of certain unitary t-designs". In: *Journal of Physics A: Mathematical and Theoretical* 52.49 (2019), p. 495301. DOI: 10.1088/1751-8121/ab5009 (cit. on p. 156).

[189] L. E. Dickson. *Linear Groups: With an Exposition of the Galois Field Theory*. New York: Dover, 1958 (cit. on p. 160).

[190] Hoi Fung Chau. "Unconditionally secure key distribution in higher dimensions by depolarization". In: *IEEE Transactions on Information Theory* 51.4 (2005), pp. 1451–1468. DOI: 10.1109/TIT.2005.844076 (cit. on p. 160).

[191] Shamgar Gurevich and Roger Howe. "Small representations of finite classical groups". In: *Representation Theory, Number Theory, and Invariant Theory*. Springer, 2017, pp. 209–234 (cit. on p. 162).

[192] Felipe Montealegre-Mora and David Gross. *Rank-deficient representations in Howe duality over finite fields arise from quantum codes*. 2019. arXiv: 1906.07230 (cit. on pp. 162, 175, 187, 193, 199).

[193] Aram W. Harrow and Richard A. Low. "Random Quantum Circuits are Approximate 2-designs". In: *Communications in Mathematical Physics* 291.1 (2009), pp. 257–302. DOI: 10.1007/s00220-009-0873-6 (cit. on pp. 175, 183).

[194] Winton G. Brown and Lorenza Viola. "Convergence rates for arbitrary statistical moments of random quantum circuits". In: *Physical Review Letters* 104.25 (2010), p. 250501. DOI: 10.1103/PhysRevLett.104.250501. arXiv: 0910.0913 (cit. on pp. 175, 184).

[195] Richard Cleve, Debbie Leung, Li Liu and Chunhao Wang. "Near-linear constructions of exact unitary 2-designs". In: *arXiv:1501.04592 [quant-ph]* (2016). arXiv: 1501.04592 (cit. on p. 175).

[196] Nicholas Hunter-Jones. *Unitary designs from statistical mechanics in random quantum circuits*. 2019. arXiv: 1905.12053 (cit. on p. 175).

[197] Jonas Haferkamp and Nicholas Hunter-Jones. *Improved spectral gaps for random quantum circuits: large local dimensions and all-to-all interactions*. 2020. arXiv: 2012.05259 (cit. on pp. 175, 178, 179, 182, 184).

[198] Fernando G. S. L. Brandão, Wissam Chemissany, Nicholas Hunter-Jones, Richard Kueng and John Preskill. *Models of quantum complexity growth*. 2019. arXiv: 1912.04297 (cit. on pp. 176, 178).

[199] Péter Pál Varjú. "Random walks in compact groups". In: *Doc. Math.* 18 (2013), pp. 1137–1175 (cit. on p. 182).

[200] B. Nachtergaele. "The spectral gap for some spin chains with disrete symmetry breaking". In: *Commun. Math. Phys.* 175 (1996), pp. 565–606 (cit. on p. 185).

[201] P. Diaconis and L. Saloff-Coste. "Comparison techniques for random walk on finite groups". In: *Ann. Probab.* 21 (1993), pp. 2131–2156 (cit. on p. 186).

[202] Benoit Collins and Piotr Sniady. "Integration with respect to the Haar measure on unitary, orthogonal and symplectic group". In: *Communications in Mathematical Physics* 264.3 (2006), pp. 773–795. DOI: 10.1007/s00220-006-1554-3 (cit. on pp. 187, 188).

[203] Pierre Remond de Montmort. *Essay d'analyse sur les jeux de hazard*. Seconde édition. Jacque Quillau, Paris, 1713 (cit. on p. 188).

[204] Nathaniel Johnston, David W. Kribs and Vern I. Paulsen. "Computing stabilized norms for quantum operations via the theory of completely bounded maps". In: *Quantum Information & Computation* 9.1 (2009), pp. 16–35 (cit. on p. 192).

[205] George E. Andrews. *The Theory of Partitions*. Cambridge University Press, 1998, p. 242. 274 pp. (cit. on p. 193).

[206] *The On-Line Encyclopedia of Integer Sequences - OEIS. Sequence A083906*. URL: http://oeis.org/A083906 (visited on 11/01/2021) (cit. on p. 193).

[207] Masamichi Takesaki. *Theory of Operator Algebras I*. Springer New York, 1979 (cit. on pp. 193, 194).

[208] Cédric Bény and Florian Richter. *Algebraic approach to quantum theory: a finite-dimensional guide*. 2015. arXiv: 1505.03106 (cit. on p. 193).

[209] M. Nakamura, M. Takesaki and H. Umegaki. "A remark on the expectations of operator algebras". In: *Kodai Math. Sem. Rep.* 12.2 (1960), pp. 82–90. DOI: 10.2996/kmj/1138844264 (cit. on p. 194).

[210] John Watrous. *The Theory of Quantum Information*. Cambridge: Cambridge University Press, 2018. DOI: https://doi.org/10.1017/9781316848142 (cit. on p. 194).

ZUSAMMENFASSUNG

Der *Stabilisator-Formalismus* ist eine erfolgreiche und weitverbreitete Untertheorie der Quantenmechanik bestehend aus *Stabilisator-Zuständen*, *Clifford-Unitären* und *Pauli-Messungen*. Die Mächtigkeit des Formalismus begründet sich auf der Beschreibung seiner Elemente durch einfache Gruppentheorie. Obwohl die Ursprünge des Formalism6s in der Quantenfehlerkorrektur und im fehlertoleranten Quantenrechnen liegen, geht die Nützlichkeit des Formalismus weit darüber hinaus.

Das Gottesman-Knill-Theorem besagt, dass die Dynamik eines Stabilisator-Zustandes unter Clifford-Unitären und Pauli-Messungen effizient auf einem klassischen Computer simuliert werden kann. Der zugrundeliegende Algorithmus kann auf verschiedene Arten auch auf beliebige Zustände und Unitäre ausgeweitet werden. Dies geschieht jedoch im Allgemeinen auf Kosten der Laufzeit. Die erhöhte Laufzeit kann dabei als eine Quantifizierung der benötigten nicht-Stabilisator-Resourcen eines Quantenschaltkreises angesehen werden. Da solche nicht-Stabilisator-Resourcen notwendig für universelles Quantenrechnen sind, kann eine erhöhte Laufzeit darüber hinaus auch als ein Maß für die nichtklassische Natur einer Rechnung verstanden werden. Diese Perspektive wird besonders im *„magic state"-Modell* des Quantenrechnens deutlich, in dem die einzigen nicht-Stabilisator-Elemente aus sogenannten *magic states* (magischen Zuständen) bestehen. Daher werden in der *Theorie der magischen Resourcen* die Resourcen in Form von Zuständen durch sogenannte *magische Maße* quantifziert, die direkt der Laufzeit eines klassischen Simulationsalgorithmus entsprechen.

In dieser Dissertation diskutiere ich verschiedene Aspekte der Theorie der magischen Resourcen. Die erwähnten klassischen Simulationsalgorithmen setzen die Berechnung von magischen Maßen voraus, was im Allgemeinen ein rechnerisch unlösbares Problem darstellt. Allerdings zeige ich, dass der Rechnenaufwand exponentiell reduziert werden kann, wenn diese Maße für symmetrische Zustände berechnet werden. Dies umfasst insbesondere Kopien von magischen Zuständen. Dazu charakterisiere ich die Symmetrien der konvexen Hülle von Stabilisator-Zuständen and zeige, dass diese durch ihre Eigenschaften als sogenannte *Designs* bestimmt sind. Zusätzlich studiere ich die kürzlich eingeführte Klasse der *vollständig Stabilisator-erhaltenden Abbildungen* (CSP), welches genau jene Quantenkanäle umfasst, die nicht in der Lage sind magische Resourcen zu erzeugen. Ich zeige, dass diese Klasse echt größer als die Klasse von Stabilisator-Operationen, bestehend aus Clifford-Unitären und Pauli-Messungen, ist. Diese Erkenntnis könnte einige interessante Konsequenzen haben. Zum Einen ist es wahrscheinlich, dass sich CSP klassisch effizient simulieren lässt, was klassische Simulation über das Gottesman-Knill-Theorem erlauben würde. Zum Anderen ist es vorstellbar, dass optimale Raten in der Destillation von magischen Zuständen nur mittels CSP- und nicht mit Stabilisator-Operationen erreichbar sind. Der Unterschied könnte dabei signifikant sein.

Weitere Anwendungen des Stabilisator-Formalismus kommen aus der *Theorie der Designs*. Ein unitären t-Design ist ein Ensemble von Unitären, welches in der Lage ist, die ersten t Momente des Haar-Maßes auf der unitären Gruppe zu reproduzieren. *Zufall* in

der Form von Haar-zufälligen Unitären ist ein essentieller Baustein in vielen Quanteninformationsprotokollen. Die Implementierung solcher Haar-zufälligen Unitären ist jedoch oft schwierig. Hier setzen Designs wesentlich weniger Resourcen voraus und sind gleichzeitig zufällig genug für die meisten Anwendungen. Viele bekannte Beispiele für solche Protokolle betreffen dabei die Charakterisierung und Zertifizierung von Quantensystemen, wie beispielsweise *randomised benchmarking*. Interessanterweise ist die Clifford-Gruppe ein unitäres 3-Design und ist, dank effizienter Gruppenoperationen, oft die erste Wahl in der Anwendung.

Im Rahmen dieser Dissertation fasse ich eine kürzlich mit Koautoren veröffentlichte Arbeit zu *approximativen unitären t-Designs* zusammen. In unserer Konstruktion werden zufällige Clifford-Unitäre mit wenigen Nicht-Clifford-Gattern ergänzt. Interessanterweise benötigt unser Ansatz nur $\tilde{O}(t^4)$ viele Nicht-Clifford-Gatter und dies ist unabhängig von der Anzahl an Qubits n. Insgesamt werden dadurch $\tilde{O}(n^2t^4)$ viele elementare Gatter benötigt, was eine signifikante Verbesserung gegenüber $\tilde{O}(n^2t^{10})$ für die Brandao-Harrow-Horodecki-Konstruktion basierend auf lokalen, zufälligen Schaltkreisen darstellt.

Um dieses Ergebnis präsentieren zu können, fasse ich einige Resultate zur Darstellungstheorie der Clifford-Gruppe zusammen. In diesem Kontext führe ich auch die Clifford-Halbgruppe ein. Motiviert durch Approximationsresulte für die unitäre Gruppe untersuche ich die Eignung der Clifford-Halbgruppe für die Approximation des Erwartungswerts über die Clifford-Gruppe.

ERKLÄRUNG ZUR DISSERTATION

Hiermit versichere ich an Eides statt, dass ich die vorliegende Dissertation selbstständig und ohne die Benutzung anderer als der angegebenen Hilfsmittel und Literatur angefertigt habe. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten und nicht veröffentlichten Werken dem Wortlaut oder dem Sinn nach entnommen wurden, sind als solche kenntlich gemacht. Ich versichere an Eides statt, dass diese Dissertation noch keiner anderen Fakultät oder Universität zur Prüfung vorgelegen hat; dass sie – abgesehen von unten angegebenen Teilpublikationen und eingebundenen Artikeln und Manuskripten – noch nicht veröffentlicht worden ist sowie, dass ich eine Veröffentlichung der Dissertation vor Abschluss der Promotion nicht ohne Genehmigung des Promotionsausschusses vornehmen werde. Die Bestimmungen dieser Ordnung sind mir bekannt. Darüber hinaus erkläre ich hiermit, dass ich die Ordnung zur Sicherung guter wissenschaftlicher Praxis und zum Umgang mit wissenschaftlichem Fehlverhalten der Universität zu Köln gelesen und sie bei der Durchführung der Dissertation zugrundeliegenden Arbeiten und der schriftlich verfassten Dissertation beachtet habe und verpflichte mich hiermit, die dort genannten Vorgaben bei allen wissenschaftlichen Tätigkeiten zu beachten und umzusetzen. Ich versichere, dass die eingereichte elektronische Fassung der eingereichten Druckfassung vollständig entspricht.

Teilpublikationen

[1] Markus Heinrich and David Gross. "Robustness of Magic and Symmetries of the Stabiliser Polytope". In: *Quantum* 3 (2019), p. 132. DOI: 10.22331/q-2019-04-08-132.

[2] Jonas Haferkamp, Felipe Montealegre-Mora, Markus Heinrich, Jens Eisert, David Gross and Ingo Roth. *Quantum homeopathy works: Efficient unitary designs with a system-size independent number of non-Clifford gates*. Submitted to Communications in Mathematical Physics. 2020. arXiv: 2002.09524.

[3] Arne Heimendahl*, Markus Heinrich* and David Gross. *The axiomatic and the operational approaches to resource theories of magic do not coincide*. 2020. arXiv: 2011.11651.

*Diese Autoren haben in gleichem Umfang beigetragen.

Ort, Datum

Markus Heinrich