ANGEWANDTE MATHEMATIK UND INFORMATIK
UNIVERSITÄT ZU KÖLN

Report No. 93.144

The True Minimum Distance of Some Narrow-Sense BCH-Codes of Length 255

by

Georg Wambach

Köln, 1993

Institut für Informatik
Universität zu Köln
Pohligstraße 1
D–50969 Köln (Zollstock)
Germany
Telephone (0221) 470–5308
Telefax (0221) 470–5317
e–Mail GW@INFORMATIK.UNI-KOELN.DE

Address of the author:

Georg Wambach
Institut für Informatik
Universität zu Köln
Pohligstraße 1
D–50969 Köln (Zollstock)
Germany
Telephone (0221) 470–5308
e–Mail GW@INFORMATIK.UNI-KOELN.DE

The True Minimum Distance of Some Narrow-Sense BCH-Codes of Length 255

Georg Wambach
University of Cologne

October 6, 1993

Abstract

Using equivalent codes it is shown that the BCH-bound for the following narrow-sense BCH-codes already yields the true minimum distance: [255,87,53], [255,107,45], [255,115,43], [255,123,39], [255,131,37], [255,147,29], [255,163,25], [255,179,21]. For the remaining two narrow-sense BCH-codes of length 255 in the book of F. J. MacWilliams and N. J. A. Sloane, page 261, Figure 9.1, whose true minimum distances are still unknown, upper bounds on the minimum distances are given which differ only by two from the corresponding BCH-bounds.

Even 16 years after the first printing of "The Theory of Error-Correcting Codes" the table of primitive BCH-codes of length up to 255 ([3], 7^{th} printing, p.261) contains ten entries where the true minimum distances are unknown. We show that the BCH-bound gives the true minimum distance for the following codes: [255,87,53], [255,107,45], [255,115,43], [255,123,39], [255,131,37], [255,147,29], [255,163,25], [255,179,21] by explicitly giving a check polynomial and a codeword of minimum weight. For the remaining two codes we give upper bounds on the minimum distances which differ only by two from the corresponding BCH-bounds. Instead of a brute-force attack we have used equivalent codes in parallel. The use of equivalence has been successful in five out of the eight cases.

Section 1 contains a description of our algorithm for the general case. In Section 2 the results are presented.

1 The Approach

Let α be a primitive n-th root of unity over some finite field $\mathbb{F}_q$ with n, q relatively prime. Every (linear) cyclic code C corresponds to an ideal $I = (g(X))$ in $\mathbb{F}_q[X]/(X^n - 1)$, where $g(X)$ is a generator polynomial for C. We assume $g(X)$ to be the smallest-degree divisor of $X^n - 1$ with leading coefficient 1 generating I. C is uniquely determined by the set N of zeroes of $g(X)$. Let $N_\alpha = \{i | \alpha^i \in N\}$ be the set of powers of α which are roots of $g(X)$, so $g(X) = \prod_{i \in N_\alpha}(X - \alpha^i)$. Now two cyclic codes C, C' of length n over $\mathbb{F}_q$ are *equivalent* if there are two primitive n-th roots of unity α, β such that for the corresponding sets N, N' of zeroes $N_\alpha = N'_\beta$. In other words: C and C' differ only in the choice of the primitive n-th root of unity, or, to be more precise, in the choice of the minimal polynomial for α over $\mathbb{F}_q$.

This definition of equivalence is stronger than the usual one (where two codes are equivalent when they can be transformed into each other by a permutation of the coordinates and the alphabet). Two such equivalent codes not only possess the same weight distribution, even their respective coset leaders are permutations of each other. Berlekamp ([1],p.144) mentioned that in spite of these similiarities, equivalent codes may differ concerning the correction of burst errors and the number of connections in the encoding and decoding circuitry.

Former explicit computing of cyclic codes considered only one code of each equivalence class ([4]) – the codesizes were small enough to find the minimum distance more or less straightforward. Obviously it is sufficient to consider only equivalent codes with different generator polynomials. After computing and systemizing the generator matrix we computed all combinations of up to v rows. It surprisingly turned out that small v are often sufficient. The algorithm goes as follows (see Fig. 1).

The transformation of the generator matrix into systematic form also enables a weak lower bound on the minimum distance according to CHEN (following [4]):

Let C be a cyclic linear code over $\mathbb{F}_q$ of length n and dimension k. All linear combinations of up to v rows of the generator matrix (in systematic form) have been generated. If $v \geq \left\lfloor \frac{(d_v - 1)k}{n} \right\rfloor$, where d_v is the minimum weight found so far, then $d_v = d$ is the minimum distance of C. Otherwise if $v < \left\lfloor \frac{(d_v - 1)k}{n} \right\rfloor$, then $d \geq \left\lceil \frac{(v+1)n}{k} \right\rceil$.

As far as we know no non-trivial bound for $d \cdot k$ exists which would lead to an estimate of the running time for an exact algorithm. The time-consuming part of the algorithm given here clearly is step five with a complexity of $\mathcal{O}\left(\sum_{i=1}^{v} \binom{k}{i}(q-1)^{i-1}\right)$ which should be parallelized, too.

Input: N_α, n, q, v

Output: d or upper bound on d

begin

(1) factorize $X^n - 1$ over $\mathbb{F}_q$

(2) mark primitive irreducible factors (whose roots are primitive n-th roots of unity)

(3) fix one primitive polynomial as $m_1(X)$, the minimal polynomial of α^1

(4) distribute the remaining irreducible polynomials for the cyclotomic cosets of $\{0, 1, \ldots, n-1\}$ such that $m_j(X)$ has zeroes $\{\alpha^i | i \in C_j\}$
(using $\mathbb{F}_q[\alpha] \cong \mathbb{F}_q[X]/(m_1(X))$)

(5) for all coset leaders $j, (j, n) = 1$, do in parallel

(6) compute $g(X) = \prod_{i \in N_\alpha}(X - (\alpha^j)^i)$ by multiplying the minimal polynomials corresponding to $\{ji | i \in N_\alpha\}$ (using $\beta = \alpha^{-j}$ this code is equivalent)

(7) compute the generator matrix $\mathbf{G}$ (whose i-th row is given by $X^i g(X)$)

(8) systemize $\mathbf{G}$ to $\mathbf{G}_s = (\mathbf{I}_k | \mathbf{A})$

(9) $d_0 := w(g(X))$

(10) for $i := 1$ to v do

(11) $d_i := \min\Big(\{\ w(\mathbf{z}) \mid \mathbf{z}$ is a linear combination of exactly i rows of $\mathbf{G}_s\}$
$\cup\{d_{i-1}\}\Big)$

enddo

(12) if $v \geq \left\lfloor \frac{(d_v - 1)k}{n} \right\rfloor$ then $d := d_v$
else d_v is an upper bound on d

enddo

end

Figure 1: The Algorithm

It should be pointed out that by the explicit construction of the generator polynomial we use *all* zeroes of the code whereas most of the well-known bounds on the minimum distance (for an overview see [2]) in general only use a subset of them. In most cases these bounds are also valid for some larger codes over extension fields of $\mathbb{F}_q$ which may explain their occasional failure.

2 The Results

We set the first found primitive polynomial $X^8+X^6+X^3+X^2+1$ to $m_1(X)$, the minimal polynomial of α. This yields the following factorization of $X^{255}-1$, where as usual $m_i(X)$ denotes the minimal polynomial of α^i. According to [3] the factors are given in octal, lowest degree on left.

$$\begin{aligned} X^{255}-1 &= m_0m_1m_3m_5m_7m_9m_{11}m_{13}m_{15}m_{17}m_{19}m_{21}m_{23}m_{25}m_{27}m_{29}m_{31}m_{37} \\ &\quad m_{39}m_{43}m_{45}m_{47}m_{51}m_{53}m_{55}m_{59}m_{61}m_{63}m_{85}m_{87}m_{91}m_{95}m_{111}m_{119}m_{127} \\ &= 600.545.771.637.747.643.615.561.727.460.607.675.765.661.567.537.717.551. \\ &\quad 735.453.471.435.760.651.433.703.543.477.700.573.455.763.613.620.515 \end{aligned}$$

Since $255 = 3 \cdot 5 \cdot 17$, 16 of the 35 irreducible factors are primitive.

For every code we list the primitive n-th root of unity actually used, the generator polynomial, a check polynomial h which is the reciprocal polynomial of $(X^{255}-1)/g(X)$, a codeword c of minimum weight and the value of v which led to success. To verify the results it is sufficient to check wether $X^i h(X)c(X) = 0 \bmod (X^{255}-1)$ for $0 \le i < n-k$.

[255,87,53]:
Using α^{13} instead of α, $v = 5$.
$g = m_{51}m_{43}m_{45}m_{19}m_{63}m_{23}m_{37}m_{61}m_3m_{25}m_{11}m_9m_{127}m_{119}m_{15}m_{53}m_{31}m_{87}m_{91}m_5m_{39}m_{13}$
h = 44413 20551 65254 52772 43637 25714
c = 40200 20000 00000 00000 00000 04025 70014 40124 36041 00110 70200 10540
01224 40241 40322 41100 26011

[255,107,45]:
Using α^7 instead of α, $v = 4$.
$g = m_{23}m_9m_1m_{59}m_{47}m_{111}m_{95}m_{13}m_{39}m_{11}m_{119}m_{45}m_{91}m_{53}m_{63}m_{19}m_{25}m_{21}m_7$

h = 66702 71654 52453 55664 12654 65436 65641 3

c = 00000 00000 00000 00010 00020 00020 10000 10202 11042 02253 00000 20013 44104 00050 14074 02151 64350

[255,115,43]:

Using α^7 instead of α, $v = 5$.

$g = m_9m_1m_{59}m_{47}m_{111}m_{95}m_{13}m_{39}m_{11}m_{119}m_{45}m_{91}m_{53}m_{63}m_{19}m_{25}m_{21}m_7$

h = 71001 12672 32061 33475 63530 03441 10274 2062

c = 01400 00000 02000 00020 00000 00000 00000 04022 60002 63040 50001 20014 60320 00014 06042 02262 36041

[255,123,39]:

Using α^7 instead of α, $v = 4$.

$g = m_1m_{59}m_{47}m_{111}m_{95}m_{13}m_{39}m_{11}m_{119}m_{45}m_{91}m_{53}m_{63}m_{19}m_{25}m_{21}m_7$

h = 44007 55164 20324 00303 40347 10201 66726 21066 14

c = 00400 00000 00200 00000 00000 00001 00200 00000 04200 55102 40005 52220 14001 22104 50304 40010 50403

[255,131,37]:

Using α^{13} instead of α, $v = 4$.

$g = m_{37}m_{61}m_3m_{25}m_{11}m_9m_{127}m_{119}m_{15}m_{53}m_{31}m_{87}m_{91}m_5m_{39}m_{13}$

h = 43244 47667 12302 03276 12575 11741 32124 36746 4171

c = 00000 01000 02000 00400 00000 00000 00000 00040 00014 24404 00214 01002 26602 40020 05000 16443 04446

[255,147,29]:

Using $\alpha = \alpha^1$, $v = 5$.

$g = m_1m_3m_5m_7m_9m_{11}m_{13}m_{15}m_{17}m_{19}m_{21}m_{23}m_{25}m_{27}$

h = 72404 27513 56272 65153 31435 71430 52236 76131 57720 20504

c = 00200 00000 00000 00000 00000 00504 00000 00000 00000 00204 01006 20100 00402 21032 25120 30040 01005

[255,163,25]:

Using $\alpha = \alpha^1$, $v = 4$.

$g = m_1m_3m_5m_7m_9m_{11}m_{13}m_{15}m_{17}m_{19}m_{21}m_{23}$

h = 50243 51715 32043 10313 40422 40612 61427 64717 70027 26153 46336

c = 00000 00001 01000 00000 20000 00000 00000 00000 00000 01000 00002 00002 67015 10104 50001 02040 20012

[255,179,21]:

Using $\alpha = \alpha^1$, $v = 3$.

$g = m_1 m_3 m_5 m_7 m_9 m_{11} m_{13} m_{15} m_{17} m_{19}$

h = 56265 14557 20554 42633 11265 05530 16562 56143 60230 31555 77206 16127

c = 00000 00000 00010 00000 00001 00000 00000 00000 00000 20000 00000 00001 40002 13202 40003 04304 40030

[255,63,61*]:

Using $\alpha = \alpha^1$, tested up to $v = 6$. Minimum weight found so far is 63 (with v=5).

$g = m_1 m_3 m_5 m_7 m_9 m_{11} m_{13} m_{15} m_{17} m_{19} m_{21} m_{23} m_{25} m_{27} m_{29} m_{31} m_{37} m_{39} m_{43} m_{45} m_{47} m_{51} m_{53} m_{55} m_{59}$

h = 74533 63531 61317 66221 34

c = 20022 00000 00100 04000 07700 30417 40040 23634 00007 06217 01410 03402 00006 04140 71100 23140 01404

[255,71,59*]:

Using $\alpha = \alpha^1$, tested up to $v = 6$. Minimum weight found so far is 61.

$g = m_1 m_3 m_5 m_7 m_9 m_{11} m_{13} m_{15} m_{17} m_{19} m_{21} m_{23} m_{25} m_{27} m_{29} m_{31} m_{37} m_{39} m_{43} m_{45} m_{47} m_{51} m_{53} m_{55}$

h = 42230 52501 52404 26536 1745

c = 00200 00005 00020 01002 00012 01601 05300 60161 40002 21035 20262 20670 10164 00100 62310 54044 50040

References

[1] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[2] J.H. van Lint and R. M. Wilson, "On the Minimum Distance of Cyclic Codes," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 23-40, Jan. 1986.

[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[4] G. Promhouse and S. E. Tavares, "The Minimum Distance of All Binary Cyclic Codes of Odd Lengths from 69 to 99", *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 438-442, Jul. 1978.