Dual Cyclic Codes with Two Zeros

Jon-Lark Kim

Dept. of Mathematics and Statistics
University of Nebraska - Lincoln
Lincoln, NE 68588-0323
jlkim@math.unl.edu

Abstract

Let $\mathcal{C}_{1,l}$ be the binary cyclic code of length $n = 2^m - 1$ with two zeros α and α^l, where α is a primitive element of the finite field $\mathbb{F}_{2^m}$. The weight distribution of the dual of $\mathcal{C}_{1,l}$ is known for $m \le 9$ with all odd $l \le (n-1)/2$. The purpose of this paper is to compute the weight distribution of the dual of $\mathcal{C}_{1,l}$ of lengths $n = 2^m - 1$ with $m = 10, 11, 12$, and 13 using the Delsarte duality theorem on subfield subcodes. We give a theoretical bound by improving the Weil sum related to the minimum weight of the dual cyclic codes with two zeros. We also recalculate the true minimum weight of dual BCH codes of length 255 with designed distance $\delta = 9, 11, 13$, and 15.

Keywords BCH codes, Cyclic codes, Weil sum.

1 Introduction

Cyclic codes are a practically and theoretically interesting class of linear codes. RS codes and BCH codes are well-known classes of cyclic codes. Cyclic codes of a primitive length $n = p^m - 1, (m \ge 1)$ over $\mathrm{GF}(p) := \mathbb{F}_p$ are defined as ideals of the principal ideal ring $\mathbb{F}_p[x]/(x^n - 1)$. A defining set of a cyclic code $\mathcal{C}$ is a subset T of $\{0, 1, \cdots, n-1\}$ such that $\{\alpha^j | j \in T\}$ is the zero set of the generator polynomial of $\mathcal{C}$, where α is a primitive element in $\mathrm{GF}(p^m)$. The narrow sense BCH code of designed distance δ is the code with defining set $T = \cup_{1 \le s < d} \mathrm{cl}(s)$, where $\mathrm{cl}(s)$ is the p-cyclotomic coset modulo n whose smallest element is s.

We will mostly consider the class of binary cyclic codes of primitive length $n = 2^m - 1$ with two zeros, i.e., having two disjoint 2-cyclotomic cosets modulo n as a defining set of the codes. These codes are linked with the properties of sequences used in CDMA. The well-known families are Melas codes and Kasami codes. One of the difficult problems about cyclic codes with two zeros is to find their weight distribution. We show that this can be done for moderate lengths by looking at their dual codes. Our idea is to use the Dalsarte duality theorem on subfield subcodes. We computed the weight distribution of the dual of all binary cyclic codes with two zeros of lengths $n = 2^m - 1, m = 10, 11, 12, 13$. This result upgrades P. Charpin's data [5] which appeared in the Handbook of Coding Theory. We also give a theoretical bound to the minimum weight of the dual cyclic codes with two zeros by improving Weil exponential sums with polynomials with two monomials. We further recalculate the true minimum weight of dual BCH codes of length 255 with designed distance $\delta = 9, 11, 13$, and 15, which has been done in [2],[8],[12], [13].

2 Methods

Delsarte [6] introduced subfield subcodes of modified Reed-Solomon codes as a simple description of BCH and Goppa codes. The dual of a subfield subcode is characterized as follows.

Theorem 1 (Delsarte [6]). *Let $\mathcal{C}$ be a linear code over GF(q), where q is a power of prime p. The dual of the subfield subcode $\mathcal{C}|_p$ of $\mathcal{C}$ is the trace of the dual of $\mathcal{C}$.*

Let $\mathcal{C}$ be a binary cyclic code of length $n = 2^m - 1$ with zeros $\alpha^{i_1}, \alpha^{i_2}, \cdots, \alpha^{i_s}$, where α is a primitive element of GF(2^m). $\mathcal{C}|_2$ denotes the binary subfield subcode of $\mathcal{C}$ over GF(2). Then it follows from the Delsarte theorem that the dual of $\mathcal{C}|_2$ is generated by the trace of linear combinations of rows of H over GF(2^m), where H is of the form

$$H = \begin{bmatrix} 1 & \alpha^{i_1} & (\alpha^{i_1})^2 & \cdots & (\alpha^{i_1})^{n-1} \\ 1 & \alpha^{i_2} & (\alpha^{i_2})^2 & \cdots & (\alpha^{i_2})^{n-1} \\ & & & \vdots & \\ 1 & \alpha^{i_s} & (\alpha^{i_s})^2 & \cdots & (\alpha^{i_s})^{n-1} \end{bmatrix} = \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_s \end{bmatrix}.$$

where r_i denotes the ith row of H. We multiply each row of H by $\alpha^j, j = 0, 1, \cdots, m-1$, and form a new matrix of size $sm \times n$ by replacing each row of H with its m multiples. Then we observe the following.

Observation. The dual of $\mathcal{C}|_2$ has the generator matrix H' over GF(2).

$$H' = \begin{bmatrix} \mathrm{Tr}(r_1) \\ \mathrm{Tr}(\alpha r_1) \\ \vdots \\ \mathrm{Tr}(\alpha^{m-1} r_1) \\ \vdots \\ \mathrm{Tr}(r_s) \\ \mathrm{Tr}(\alpha r_s) \\ \vdots \\ \mathrm{Tr}(\alpha^{m-1} r_s) \end{bmatrix}$$

Our computation is based on this observation and implemented on Magma [4]. We remark that although Magma has functions about cyclic codes, our observation gives another way to look at cyclic codes.

Definition 1. Let $\mathcal{C}_{r,s}$ be a primitive binary cyclic code of length $n = 2^m - 1$ with two zeros α^r and α^s for some integers r and s. For short, we will say $T = \{r, s\}$ for such a defining set, where r and s are the representatives of 2-cyclotomic cosets modulo n.

We mention some known fact about $\mathcal{C}_{r,s}$ whose proof can be found in [5].

Theorem 2. *Let $n = 2^m - 1, m \geq 1$. Let $\mathcal{C}_{r,s}$ be defined as above with minimum weight d. Then we have*

(i) $2 \leq d \leq 5$ and

(ii) $d = 2$ if and only if $\gcd(r, s, n) > 1$.

From now on, we only consider the code with defining set $T = \{1, l\}$ i.e. $\mathcal{C}_{1,l}$ is the binary cyclic code whose zeros are α, α^l and their conjugates where α is a primitive root of $\mathrm{GF}(2^m)$. See [11] for the code $\mathcal{C}_{1,7}$ with $m \geq 18$ and [9] for $\mathcal{C}_{1,l}$ with fixed l but various m. We note that $\mathcal{C}_{1,l}$ has $3 \leq d \leq 5$ by Theorem 2.

Example 1. Melas codes are cyclic codes of the form $\mathcal{C}_{1,-1}$. The dual of Melas codes are called the *Kloosterman codes*. The nonzero weights of Kloosterman codes were completely determined [10].

3 Results

3.1 Weight distribution of $\mathcal{C}_{1,l}^{\perp}$

There is a detailed explanation [5] of the dual of $\mathcal{C}_{1,l}$ of length 511. (See Table 6,7, and 8 of [5].) It is computed there that there are exactly 24 distinct dual weight distributions for odd $3 \leq l \leq 255$. Our aim is to extend the lengths up to $2^{13} - 1$. So we note that in most cases of l the dimension of $\mathcal{C}_{1,l}^{\perp}$ of length $2^m - 1$ is $2m$ and sometimes less. Hence we apply the observation of the Delsarte theorem to obtain the upgraded data for $\mathcal{C}_{1,l}^{\perp}$.

Proposition 1. *The weight distribution of $\mathcal{C}_{1,l}^{\perp}$ of lengths $n = 2^m - 1$ with $m = 10, 11, 12,$ and 13 and all odd $3 \leq l \leq (n-1)/2$ are summarized as follows. There are $61, 68, 269,$ and 289 distinct dual weight distributions respectively when $m = 10, 11, 12,$ and 13.*

The enumeration of the weight distribution of $\mathcal{C}_{1,l}^{\perp}$ is omitted to save space but available from the author. Using the weight distribution of $\mathcal{C}_{1,l}^{\perp}$ and MacWilliams' identity, we computed the minimum weight of $\mathcal{C}_{1,l}$ for $m = 10, 11,$ and 12. (We omit $m = 13$ case to save space.) See Table 1.

3.2 Improvement of the Weil sum

The Weil sum related to the minimum weight of the dual of $\mathcal{C}_{1,l}$ is

$$S(Ax^l + Bx) := \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(Ax^l + Bx)},$$

where A and B are elements of $\mathbb{F}_{2^m}$ and Tr is the trace map from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. It is well known that the minimum weight d of the dual of $\mathcal{C}_{1,l}$ has a lower bound $d \geq 2^{m-1} - |S(Ax^l + Bx)|$. Therefore a smaller value of $|S(Ax^l + Bx)|$ for any A and B in $\mathbb{F}_{2^m}$ will result in a better estimation of the minimum weight of the dual of $\mathcal{C}_{1,l}$. The Carlitz-Uchiyama bound (also known as Weil's bound) estimates $|S(Ax^l + Bx)| \leq (l-1)2^{m/2}$, which becomes trivial when $l - 1 > 2^{m/2}$. Akuliničev estimated such a Weil sum as follows.

Theorem 3 ([1]). *Let $p \geq 3$ be a prime, let A, B, n be natural numbers and let $p > n$, $\delta = (n, p-1), (A, p) = (B, p) = 1$. Then*

$$\left| \sum_{x=0}^{p-1} \exp\left(2\pi i \frac{\mathrm{Tr}(Ax^n + Bx)}{p}\right) \right| \leq \frac{p}{\sqrt{\delta}}.$$

Table 1: Minimum weight d of $\mathcal{C}_{1,l}$ of length $n = 2^m - 1$

length n	minimum weight	list of odd l such that $3 \le l \le (n-1)/2$	number of l's
2^{10}	$d=3$	the rest	191
2^{10}	$d=4$	15, 21, 27, 45, 51, 69, 75, 81, 87, 93, 105, 111,117, 141, 147, 153, 177, 189, 195, 201, 207, 231, 237,243, 255, 261, 267, 273, 279, 285, 291, 303, 315, 321, 327, 351, 363, 369, 375, 381, 387, 393, 417, 423, 429, 447, 453, 465, 471, 477, 483, 489, 495, 501, 507	55
2^{10}	$d=5$	3, 9, 57, 129, 135, 213, 309, 333, 339	9
2^{11}	$d=3$	none	0
2^{11}	$d=4$	the rest	456
2^{11}	$d=5$	3, 5, 9, 13, 17, 33, 35, 43, 57, 63, 65, 95, 107, 117, 129, 143, 151, 193, 231, 241, 249, 257, 263, 287, 315, 365, 369, 411, 413, 435, 455, 467, 473, 513, 515, 541, 603, 615, 647, 683, 685, 693, 705, 707, 725, 773, 781, 807, 819, 843, 853, 873, 905, 993, 1023	55
2^{12}	$d=3$	the rest	875
2^{12}	$d=4$	27, 45, 63, 69, 75, 87, 111, 153, 171, 189, 201, 213, 237, 243, 255, 279, 285, 297, 315, 321, 327, 339, 363, 369, 381, 405, 423, 441, 447, 453, 465, 489, 495, 531, 537, 549, 567, 573, 579, 591, 615, 621, 633, 657, 675, 693, 699, 705, 717, 747, 759, 783, 789, 801, 819, 825, 831, 843, 873, 885, 909, 915, 927, 945, 951, 957, 969, 999, 1011, 1035, 1041, 1071, 1077, 1083, 1095, 1119, 1125, 1137, 1161, 1167, 1179, 1197, 1203, 1221, 1245, 1251, 1263, 1293, 1305, 1323, 1329, 1335, 1347, 1371, 1377, 1389, 1413, 1419, 1431, 1449, 1455, 1461, 1473, 1497, 1503, 1515, 1539, 1545, 1557, 1575, 1581, 1623, 1629, 1641, 1665, 1671, 1683, 1701, 1707, 1713, 1725, 1749, 1767, 1791, 1797, 1809, 1827, 1839, 1851, 1875, 1881, 1893, 1917, 1923, 1935, 1953, 1959, 1965, 1977, 2001, 2007, 2019, 2043	143
2^{12}	$d=5$	3, 33, 129, 159, 993	5

For our purpose we need to consider prime powers instead of prime p in the above theorem. It is not difficult to generalize the theorem as follows.

Proposition 2. *Let p be prime, $q = p^m$ for some $m \geq 1$. Let $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ denote the trace map. Let A and B be in $\mathbb{F}_q$ and l be integer ≥ 2 and set $\delta = \gcd(l, q-1)$. Then we have*

$$\left| \sum_{x \in \mathbb{F}_q} \exp\left(2\pi i \frac{\mathrm{Tr}(Ax^l + Bx)}{p}\right) \right| \leq \frac{q}{\sqrt{\delta}}.$$

Proof. The proof is obtained by following the proof of Theorem 3 in [1]. We omit the details. □

Example 2. Let $n = 2^{10} - 1 = 3 \cdot 11 \cdot 31$. Suppose $l = 341 = 11 \cdot 31$. Then $\delta = 341$. It follows from Proposition 2 that the minimum weight d of $\mathcal{C}_{1,341}^{\perp}$ is at least

$$\left\lceil 2^9 - \frac{2^{10}}{\sqrt{341}} \right\rceil = 457.$$

We have computed the weight distribution of $\mathcal{C}_{1,341}^{\perp}$ as $A_0 = 1, A_{490} = 1023, A_{512} = 1023, A_{522} = 2046, A_{682} = 3$. So our estimation is close to the true minimum distance 490. On the other hand, Weil's bound becomes trivial since $l - 1 > 2^5$ and so cannot give a lower bound for d of $\mathcal{C}_{1,341}^{\perp}$.

3.3 Dual primitive BCH codes of length 255

In this section we are concerned with the dual of BCH codes (simply dual BCH codes). The minimum weight of all dual BCH codes of length $n = 2^s - 1, s = 7$ is known [7]. Augot and Levy-dit-Vehel in Table II of [2] gave a lower bound of the minimum weight of dual BCH codes of length 255 and the true minimum weight for designed distance $\delta = 3, 5,$ and 7. Fujiwara and Kasami [8] gave the true minimum weight of dual BCH codes of length 255 for $\delta = 9, 11, 13$, Rodier [12] for $\delta = 9$ and Sala and Tamponi [13] for $\delta = 15$.

We recalculate these results for $\delta = 9, 11, 13,$ and 15 using the observation of the Delsarte theorem.

Proposition 3. *Let δ be the designed distance of the binary primitive BCH code $\mathcal{C}$ of length 255. Then the true minimum weight of the dual of $\mathcal{C}$ is 96, 64, 64, and 64 respectively when $\delta = 9, 11, 13, 15$.*

See Table 2 for the summary of true minimum weight of the duals of BCH codes of length 255.

4 Future work

We have considered the application of Delsarte's duality theorem to dual cyclic codes with two zeros and dual BCH codes of length 255. We also improved the Weil sum related to the dual cyclic codes with two zeros. It still seems to be possible to upgrade the data which appeared in this paper. For example, find all weight distributions of $\mathcal{C}_{1,l}^{\perp}$ of length 2^m for $m = 14, 15$, etc. Also find exact minimum weight of the dual of BCH

Table 2: True dual distance of BCH codes of length 255

designed distance δ	Schaub's bound [2]	True dual distance	References
3	128	128	[2]
5	112	112	[2]
7	96	96	[2]
9	88	96	Sec. 3.3, [8],[12]
11	64	64	Sec. 3.3, [8]
13	64	64	Sec. 3.3, [8]
15	60	64	Sec. 3.3, [13]
17	42	open	?

codes of length 255 with designed distance $\delta = 17, 19$, etc. Our computer could not go further. Finally improve the estimation of the Weil sum in Propostion 2 or in general the Weil sum with polynomials with a few monomials of odd degrees.

Acknowledgment: The author would like to thank J. Walker for useful discussion about Section 3.2 and P. Charpin for references [12],[13].

References

[1] N. M. Akuliničev, *Bounds for rational trigonometric sums of a special type* (Russian) Dokl. Akad. Nauk SSSR, 161 (1965) 743–745, English translation [Soviet Math. Dokl. 6 (1965), 480–482].

[2] D. Augot and F. Levy-dit-Vehel, *Bounds on the minimum distance of the duals of BCH codes*, IEEE Trans. Inform. Theory, 42 (1996), pp. 1257–1260.

[3] A.E. Brouwer, *Bounds on the size of linear codes*, Handbook of Coding Theory, V. S. Pless and W. C. Huffman, ed. Elsevier, Amsterdam (1998), pp. 295–461.

[4] J. Cannon and C. Playoust, *An Introduction to Magma*, University of Sydney, Sydney, Australia, 1994.

[5] P. Charpin, *Open problems on cyclic codes*, in Handbook of Coding Theory, V. S. Pless and W. C. Huffman, eds., Elsevier, Amsterdam (1998), pp. 963–1063.

[6] P. Delsarte, *On subfield subcodes of Reed-Solomon codes*, IEEE Trans. Inform. Theory 21 (1975), pp. 575–576.

[7] Y. Desaki, T. Fujiwara and T. Kasami, *The weight distribution of extended binary primitive BCH codes of length* 128, IEEE Trans. Inform. Theory 43 (1997), pp. 1364–1371.

[8] T. Fujiwara and T. Kasami, *The weight distribution of* $(256, k)$ *extended binary primitive BCH codes with* $k \leq 63$ *and* $k \geq 207$, IEICE, Tech. Rep. IT97-46 (1997-09), pp. 29–33.

[9] H. Janwa and R.M. Wilson, *Hyperplane sections of Fermat varieties in* P^3 *in* char. 2 *and some applications to cyclic codes,* Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), 180–194, Lecture Notes in Comput. Sci., 673, Springer, Berlin, 1993.

[10] G. Lachaud and J. Wolfmann, *The weights of the orthogonals of the extended quadratic binary Goppa codes,* IEEE Trans. Inform. Theory 36 (1990), pp. 686–692.

[11] J.H. van Lint and R.M. Wilson, *Binary cyclic codes generated by* $m_1 m_7$*,* IEEE Trans. Inform. Theory 32 (1986), pp. 283.

[12] F. Rodier, *On the minimum distance of the duals of* $4-$*error correcting extended BCH codes,* IEEE Trans. Inform. Theory 45 (1999), pp. 1677–1678.

[13] M. Sala and A. Tamponi, *A linear programming estimate of the weight distribution of BCH*$(255, k)$*,* IEEE Trans. Inform. Theory 46 (2000), pp. 2235–2237.