Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 18-24, 2016, Albena, Bulgaria *pp. 102–107*

Some new quasi-cyclic self dual codes

Pinar Çomak [1] pcomak@metu.edu.tr
Middle East Technical University, Department of Mathematics, Ankara, Turkey
Jon Lark Kim jlkim@sogang.ac.kr
Sogang University, Department of Mathematics, Seoul, South Korea
Ferruh Özbudak ozbudak@metu.edu.tr
Middle East Technical University, Department of Mathematics and Institute of Applied Mathematics, Ankara, Turkey

Abstract. In this paper, we study the construction of quasi-cyclic self-dual codes, especially of binary cubic ones. We consider binary quasi-cyclic codes of length 3ℓ with the algebraic approach of [7]. In particular, we improve the previous results, by constructing 7 new binary cubic self-dual codes. We also complete the classification of $[54, 27, 10]$ binary cubic self-dual codes up to a conjecture.

1 Introduction

A q**-ary linear code** $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$. If $\mathcal{C}$ has dimension k, then $\mathcal{C}$ is called an $[n, k]$ linear code. The minimum (Hamming) distance $d(\mathcal{C})$ is the minimum number of distinct coordinates between any pair of distinct codewords in $\mathcal{C}$. The (Hamming) weight $w(c)$ of a codeword c in $\mathcal{C}$ is defined to be the number of non-zero entries of c. For a linear code, we have that $d(\mathcal{C}) = w(\mathcal{C})$. Two codes are said to be equivalent up to permutation if they differ only in the order of their coordinates. The (Hamming) weight enumerator of the code $\mathcal{C}$ is defined to be $W_{\mathcal{C}}(y) = \sum_{c\in\mathcal{C}} y^{wt(c)} = \sum_{i=0}^{n} A_i y^i$, where A_i is the number of vectors of the code $\mathcal{C}$ having Hamming weight i.

We can define the **dual** of a code $\mathcal{C}$ to be $\mathcal{C}^\perp = \{u \in \mathbb{F}_q^n : (u, v) = 0 \text{ for all } v \in \mathcal{C}\}$. Here the inner product is the standard (Euclidean) inner product. $\mathcal{C}$ is **self-dual** if $\mathcal{C} = \mathcal{C}^\perp$. If a code $\mathcal{C}$ of length n is self-dual, then n must be even; and $\mathcal{C}$ is a subspace of dimension $n/2$.

If $\mathcal{C} \subset \mathbb{F}_2^n$ is a binary self-dual code, then the weight of all codewords must be even. The binary self-dual codes in which there is at least one codeword with weight not divisible by 4 are called **Type I** or **singly-even** self-dual binary codes. Otherwise, the binary self-dual codes are called **Type II** or **doubly-**

[1]The research of the author was supported by Council of Higher Education in Turkey

even self-dual binary codes.

In this paper, we consider the algebraic approach of [7] for constructing cubic self-dual binary codes. In the literature, there are only seven cubic binary self-dual $[54, 27, 10]$ inequivalent codes up to permutation (see [5]). The method they used was their building-up construction [5, Theorem 2.2]. We construct seven new cubic binary self-dual $[54, 27, 10]$ inequivalent codes up to permutation. In Remark 4.2, we conjecture that these 14 codes are all cubic binary self-dual $[54, 27, 10]$ inequivalent codes up to permutation.

The rest of this paper is organized as follows: In Sections 2 and 3 we give some background. We present our results in Section 4.

2 Quasi-Cyclic Codes

Let $\mathbb{F}_q$ be a finite field and m be a positive integer coprime with the characteristic of $\mathbb{F}_q$. A linear code $\mathcal{C}$ of length ℓm over $\mathbb{F}_q$ is called **quasi-cyclic code** if the codeword $(c_{0,0}, \ldots, c_{0,\ell-1}, c_{1,0}, \ldots, c_{1,\ell-1}, \ldots, c_{m-1,0}, \ldots, c_{m-1,\ell-1}) \in \mathcal{C}$, then $(c_{m-1,0}, \ldots, c_{m-1,\ell-1}, c_{0,0}, \ldots, c_{0,\ell-1}, \ldots, c_{m-2,0}, \ldots, c_{m-2,\ell-1}) \in \mathcal{C}$.

This code is invariant under ℓ-shift and such codes are called as **ℓ-quasi-cyclic codes** or **quasi-cyclic codes of index** ℓ. The quasi-cyclic codes are the generalization of cyclic codes. Cyclic codes correspond to the case $\ell = 1$.

2.1 1-1 correspondence:

Let $\mathbb{F}_q[Y]$ denote the polynomial ring over $\mathbb{F}_q$. Consider the ring $\mathcal{R} := \mathcal{R}(\mathbb{F}_q, m) = \mathbb{F}_q[Y]/(Y^m - 1)$. Let $\mathcal{C}$ be a ℓ-quasi-cyclic code over $\mathbb{F}_q$ of length ℓm and let $c = (c_{0,0}, \ldots, c_{0,\ell-1}, c_{1,0}, \ldots, c_{1,\ell-1}, \ldots, c_{m-1,0}, \ldots, c_{m-1,\ell-1})$ denote a codeword in $\mathcal{C}$. Define a map $\phi : \mathbb{F}_q^{\ell m} \to \mathcal{R}^\ell$ by

$$\phi(c) = (c_0(Y), c_1(Y), \ldots, c_{\ell-1}(Y)) \in \mathcal{R}^\ell$$

where $c_j(Y) = \sum_{i=0}^{m-1} c_{ij} Y^i \in \mathcal{R}, \quad j = 0, \ldots, \ell - 1.$

A linear code $\mathcal{C}$ of length n over $\mathcal{R}$ is defined to be a $\mathcal{R}$-submodule of $\mathcal{R}^n$.

Lemma 2.1. (see [7]) *The map ϕ gives a one-to-one correspondence between ℓ-quasi-cyclic codes over $\mathbb{F}_q$ of length ℓm and linear codes over $\mathcal{R}$ of length ℓ.*

2.2 Existence of Self-Dual Codes

In [5], it is proved that there exist self-dual binary codes of length ℓ over $\mathcal{R} = \mathcal{R}(\mathbb{F}_2, m) = \mathbb{F}_2[Y]/(Y^m - 1)$ if and only if $2 \mid \ell$. For binary ℓ-quasi-cyclic self-dual codes of length ℓm, if m is a prime not dividing i, then m must divide

A_i, the number of codeword with Hamming weight i. This gives the possible weight enumerators of self-dual codes of a given length.

3 Ring Decomposition

Let $\mathcal{R} = \mathcal{R}(\mathbb{F}_q, m) = \mathbb{F}_q[Y]/(Y^m - 1)$. If $\gcd(m, q) = 1$, then the ring can be decomposed into a direct sum of fields by Chinese remainder theorem (CRT) or discrete Fourier transform (DFT) [7]. By this approach, the quasi-cyclic codes can be decomposed into codes of lower lengths. The polynomial $Y^m - 1$ factors completely into distinct irreducible factors in $\mathbb{F}_q[Y]$ as

$$Y^m - 1 = \delta g_1 \dots g_s h_1 h_1^* \dots h_t h_t^* \tag{1}$$

where δ is nonzero in $\mathbb{F}_q$, $g_1 \dots g_s$ are the polynomials which are self-reciprocal, and h_i^*'s are reciprocals of h_i's, for all $1 \leq i \leq t$. Then the ring $\mathcal{R}$ can be written by CRT [7] as

$$\mathcal{R} = \frac{F_q[Y]}{(Y^m - 1)} = \left(\bigoplus_{i=1}^{s} \frac{F_q[Y]}{(g_i)}\right) \oplus \left(\bigoplus_{j=1}^{t}\left(\frac{F_q[Y]}{(h_j)} \oplus \frac{F_q[Y]}{(h_j^*)}\right)\right). \tag{2}$$

Let $F_q[Y]/(g_i)$ be denoted by G_i, and in the same way $F_q[Y]/(h_j)$ by H_j' and $F_q[Y]/(h_j^*)$ by H_j'' for simplicity of notation. Every $\mathcal{R}$-linear code $\mathcal{C}$ of length ℓ can be decomposed as the direct sum

$$\mathcal{C} = \left(\bigoplus_{i=1}^{s} \mathcal{C}_i\right) \oplus \left(\bigoplus_{j=1}^{t}\left(\mathcal{C}_j' \oplus \mathcal{C}_j''\right)\right)$$

where $\mathcal{C}_i$, $\mathcal{C}_j'$ and $\mathcal{C}_j''$ are linear codes over G_i, H_j' and H_j'', respectively, all of length ℓ for each $1 \leq i \leq s$, and for each $1 \leq j \leq t$.

Let $x = (x_0, x_1, \cdots, x_{\ell-1})$ and $y = (y_0, y_1, \dots, y_{\ell-1})$. Here, for $1 \leq i \leq s$, the Hermitian inner product of x and y with x_i's, y_i's $\in G_i$ is defined in the sense used in [7, Section IV], which corresponds to the classical meaning of Hermitian product for $m = 3$ and $q = 2$, as $\langle x, y \rangle = x_0 y_0^{m-1} + \cdots + x_{\ell-1} y_{\ell-1}^{m-1}$. Moreover, for $1 \leq i \leq t$, the Euclidean inner product of x and y with x_i's, y_i's $\in H_j'$ is defined as $x \cdot y = x_0 y_0 + \cdots + x_{\ell-1} y_{\ell-1}$.

Theorem 3.1. (see [7]) *An ℓ-quasi-cyclic code $\mathcal{C}$ of length ℓm over $\mathbb{F}_q$ is self-dual if and only if*

$$\mathcal{C} = \left(\bigoplus_{i=1}^{s} \mathcal{C}_i\right) \oplus \left(\bigoplus_{j=1}^{t}\left(\mathcal{C}_j' \oplus (\mathcal{C}_j')^{\perp}\right)\right)$$

where, for $1 \leq i \leq s$, $\mathcal{C}_i$ is a self-dual code over G_i of length ℓ with respect to the Hermitian inner product and for $1 \leq j \leq t$, $\mathcal{C}_j'$ is a linear code of length

ℓ over H'_j and $(\mathcal{C}')^{\perp}$ is its dual with respect to the Euclidean inner product as defined above.

4 Cubic Self-Dual Binary Codes

There are some construction methods for combining codes to get new codes with greater length for different values of q, m and ℓ (see for example [1]).

In this work, we focus on the case $q = 2$ and $m = 3$, so called **binary cubic codes**. We use a cubic construction in [1] and [7] to find new codes.

Since Y^2+Y+1 is irreducible in $\mathbb{F}_2[Y]$, we can write $Y^3-1 = (Y-1)(Y^2+Y+1)$ as a product of irreducible factors. By (2), $\mathcal{R}$ can be decomposed as

$$\mathcal{R} = \frac{\mathbb{F}_2[Y]}{(Y^3-1)} = \mathbb{F}_2 \oplus \mathbb{F}_{2^2}.$$

This gives a correspondence between the ℓ-quasi-cyclic codes $\mathcal{C}$ of length 3ℓ over $\mathbb{F}_2$ and a pair $(\mathcal{C}_1, \mathcal{C}_2)$, where $\mathcal{C}_1$ is a linear code over $\mathbb{F}_2$ of length ℓ and $\mathcal{C}_2$ is a linear code over F_4 of length ℓ. Using the discrete Fourier transform [7], we have

$$\mathcal{C} = \{ \ (\ x+b \mid x+a \mid x+a+b \ ) \mid x \in \mathcal{C}_1, \ a+\omega b \in \mathcal{C}_2\} \tag{3}$$

where $\omega^2+\omega+1 = 0$. Moreover, $\mathcal{C}$ is self-dual if and only if $\mathcal{C}_1$ is self-dual with respect to the Euclidean inner product and $\mathcal{C}_2$ is self-dual with respect to the Hermitian inner product.

In [7], it is shown that all such codes can be obtained by this method, from a binary code over $\mathbb{F}_2$ and a quaternary code over $\mathbb{F}_4$ both of length ℓ. Cubic binary codes of length 3ℓ are viewed as codes of length ℓ over the ring $\mathbb{F}_2 \times \mathbb{F}_{2^2}$ [1].

The authors of [3] and [5] completed the classification of binary cubic self-dual codes of lengths up to 48 (up to permutation equivalence) by their building-up construction (see [5, Theorem 2.2]). The numbers of cubic self-dual codes are given in [5] as follows:

(i) for $\ell = 2$, unique binary cubic self-dual code of length 6,
(ii) for $\ell = 4$, 2 binary cubic self-dual codes of length 12,
(iii) for $\ell = 6$, 3 binary cubic self-dual codes of length 18,
(iv) for $\ell = 8$, 16 binary cubic self-dual codes of length 24,

(v) for $\ell = 10$, 8 binary cubic self-dual codes of length 30,
(vi) for $\ell = 12$, 13 binary cubic self-dual codes of length 36,
(vii) for $\ell = 14$, 1569 binary cubic self-dual codes of length 42,
(viii) for $\ell = 16$, 264 binary cubic self-dual codes of length 48.

The shortest length of binary cubic self-dual codes for which the classification is not completed, and the focus of this study, is $\ell = 18$. The number of inequivalent codes that were found in [5] is 7. In this paper, we find 7 more such codes by the cubic construction (3).

For self-dual $[54, 27, 10]$ codes, there are two weight enumerators [4]:

$$\begin{aligned} W_1 &= 1 + (351 - 8\beta)y^{10} + (5031 + 24\beta)y^{12} + (48492 + 32\beta)y^{14} + \dots \quad 0 \leq \beta \leq 43 \\ W_2 &= 1 + (351 - 8\beta)y^{10} + (5543 + 24\beta)y^{12} + (43884 + 32\beta)y^{14} + \dots \quad 12 \leq \beta \leq 43. \end{aligned}$$

In [5], by building-up construction, four inequivalent codes with W_1 for $\beta = 0, 3, 6, 9$ and three inequivalent codes with W_2 for $\beta = 12, 15, 18$ are found.

By the construction (3), binary codes $\mathcal{C}$ of length 54 are formed from a binary code $\mathcal{C}_1$ of length 18 and a quaternary code $\mathcal{C}_2$ of length 18. Let A, B and X be binary vectors of length 18 and write $\mathbb{F}_4 = \mathbb{F}_2(\omega)$, where $\omega^2 + \omega + 1 = 0$. We can define a Gray map from $\mathbb{F}_2^{18} \times \mathbb{F}_4^{18} \to \mathbb{F}_2^{54}$ as

$$\phi(X,\ A + \omega B) = (X + A \mid X + B \mid X + A + B) = \mathcal{C} = \phi(\mathcal{C}_1,\ \mathcal{C}_2). \quad (4)$$

For $\ell = 18$, by this construction, we found four $[54, 27, 10]$ codes with weight enumerator W_1 for $\beta = 12, 15, 18, 21$ and three $[54, 27, 10]$ codes with weight enumerator W_2 for $\beta = 21, 24, 27$ by taking $\mathcal{C}_1 = H_{18}, I_{18}$ (the only $[18, 9, 4]$ self-dual binary codes listed in [8]) and $\mathcal{C}_2 = A_{18}, B_{18}$ (18^{th} and 38^{th} $[18, 9, 6]$ self-dual quaternary codes taken from [6]).

Throughout this work, we extensively used the Computational Algebra System MAGMA [2].

Remark 4.1. These $[54, 27, 10]$ codes are of Type II 18 quasi-cyclic self-dual codes of length 54 since their binary components H_{18} and I_{18} are of Type II and self-dual with respect to the Euclidean inner product.

Remark 4.2. It is known that there are 9 binary $[18, 9]$ self-dual (with $d = 2, 4$) and 245 quaternary codes (with $d = 6, 8$) listed in [6]. We tried all possible binary and quaternary self-dual codes with a huge number of permutation in our construction method to find more codes. Based on computational evidence, we conjecture that there is no other $[54, 27, 10]$ self-dual cubic code over $\mathbb{F}_2$.

Our computational results, with β a multiple of 3, are listed above:

	Possible values	Known values [5]	New values, Thm.3	Conjecture, Rk.4.2
W_1	$0 \leq \beta \leq 43$	$\beta \in \{0, 3, 6, 9\}$	$\beta \in \{12, 15, 18, 21\}$	$\beta \notin \{24, \cdots, 42\}$
W_2	$12 \leq \beta \leq 43$	$\beta \in \{12, 15, 18\}$	$\beta \in \{21, 24, 27\}$	$\beta \notin \{30, \cdots, 42\}$

References

[1] A. Bonnecaze, A.D. Bracco, S.T. Dougherty, L.R. Nochefranca, P. Solé, Cubic self-dual binary codes, *IEEE Trans. Inform. Theory.*, vol. 49, no. 9, Sep. 2003, pp. 2253-2259.

[2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, vol. 24, 1997, pp. 235-265.

[3] S. Bouyuklieva, N. Yankov, J.-L. Kim, Classification of binary self-dual $[48, 24, 10]$ codes with an automorphism of odd prime order, *Finite Fields and Their Appl.*, vol. 18, no. 6, 2012, pp. 1104-1113.

[4] J. H. Conway and N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Transactions on Information Theory*, vol. 36, no. 6, Nov 1990, pp. 1319-1333.

[5] S. Han, J.-L. Kim, H. Lee and Y. Lee, Construction of quasi-cyclic self-dual codes, *Finite Fields and Their Appl.*, vol. 18, no. 3, 2012, pp. 613-633.

[6] A.Munemasa, M. Harada, (2016, Feb. 9). Retrieved from http://www.math.is.tohoku.ac.jp/∼munemasa/selfdualcodes.htm

[7] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes I, Finite fields, *IEEE Trans. Inform. Theory.* vol. 47, 2001, pp. 2751-2760.

[8] V. Pless, A classification of self-orthogonal codes over GF(2), *Discrete Math.*, vol. 3, 1972 pp. 209-246.

[9] E. Rains and N.J.A. Sloane, Self-dual codes, *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, pp. 177-294.