TWMS J. Pure Appl. Math., V.4, N.2, 2013, pp.177-186

SELF-DUAL CODES FROM SMALLER LENGTHS OF SELF-DUAL CODES AND RECURSIVE ALGORITHM*

H. TOPCU[1], H. AKTAS[2]

Abstract. Self-dual codes have been received great attention by researchers since the beginning of the coding theory. In this work, some construction methods for this kind of codes are composed which produce new self-dual codes from self-dual codes of smaller lengths. A special one of these methods that is called recursive algorithm is also mentioned. For the binary case, it was shown that recursive algorithm is actually same with another so-called building-up construction method. This comparison is mentioned here.

Keywords: self-dual codes,code construction, building-up construction, recursive algorithm.

AMS Subject Classification: 94B05.

1. Introduction

Self-dual codes are an important class of linear codes because of their rich algebraic structure and connections with other mathematical areas such as group theory, lattice theory, design theory etc. Also some famous codes for example extended binary Hamming code of length 8, binary Golay code of length 24, tetracode over GF(3) and hexacode over GF(4) are self-dual.

A *linear [n,k] code* C of *length* n over GF(q) is a k-dimensional vector subspace of GF(q)^n. An element of C is called a *codeword* and *Hamming weight* of a codeword is the number of non-zero coordinates in it. Hamming weight of a codeword x is denoted by $wt(x)$. *Minimum weight* of a linear code C is defined by w(C):=min$\{wt(x)|x \in C, x \neq 0\}$. *Distance* between two codewords x and y is defined as the number of the coordinates where x and y differ and denoted by *d(x,y)*. *Minimum distance* of a linear code C is defined by $d(C) = min\{d(x,y)|x,y \in C\}$. A linear code C over GF(q) can also be denoted by *[n,k,d]* linear code where d is the minimum distance of C. Euclidean inner product of two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ is $x \cdot y = \sum_{i=1}^{n} x_i y_i$. The *dual code* C$^\perp$ of C is defined as C$^\perp$ $= \{x \in GF(q)^n | x \cdot y = 0, \forall y \in C\}$. If C⊆C$^\perp$, C is called *self-orthogonal* and if C=C$^\perp$, C is called *self-dual.* A linear code over GF(2) is called *binary* code.

A binary self-dual code is called *Type II* or *doubly-even* if every codeword in C has weight divisible by 4. If there exists a codeword whose weight is congruent to 2 modulo 4, the code is called *Type I* or *singly-even.* Two codes C$_1$ and C$_2$ are *monomially equivalent* if there exists a monomial matrix M over GF(q) such that C$_2$=C$_1$M. Hence, for the binary case, two codes are *equivalent* if one of them can be obtained by a permutation of the coordinates of the other's. If C is a binary linear [n,k,d] code then it satisfies the below inequality [4];

*This work is presented in the 1st International Eurasian Conference on Mathematical Sciences and Applications (IECMSA-2012)

[1] Department of Mathematics, Nevsehir University, Turkey,

[2] Faculty of Science, Department of Mathmatics, Erciyes University, Kayseri, Turkey,
e-mail: hatice.kamit@nevsehir.edu.tr, haktas@erciyes.edu.tr, haticekamittopcu@gmail.com

Manuscript received August 2012.

$$d \leq \begin{cases} 4[\frac{n}{24}+4], & if\ \ n \neq 22\ \ (mod\ 24) \\ 4[\frac{n}{24}+6], & if\ \ n = 22\ \ (mod\ 24). \end{cases}$$

A binary self-dual code is called *extremal* if it meets the bounds of the above inequality. A self-dual code is *optimal* if it has the highest possible minimum weight with determined parameters.

Since the beginning of the coding theory,there are many papers about self-dual codes, their constructions and their classifications [1, 2, 3, 4, 8, 6, 9, 12]. A special technique about constructing self-dual codes is using smaller lengths of self-dual codes. The earlier form of this idea is made by Pless and Brauldi [15]. They have used shadow code concept and constructed a new singly-even self-dual [10, 24, 48] code with a weight enumerator. Tsai [17] has used a similar way and obtained two new singly-even extremal [10, 26, 52] and [10, 27, 54] codes. After him, Dougherty [5] has carried this technique from binary case to over arbitrary fields. Then we can see Harada's matrix form which generates longer self-dual codes from existing self-dual codes for binary case [7]. By using this method, he has published the first example of a [12, 35, 70] singly-even self-dual code. Kim[6] has constructed new extremal self-dual codes of lengths 36, 38 and 58 by using a more general matrix form than Harada's method. This is the so-called building-up construction method. Then, Kim has carried his technique from binary case to over another finite fields and different algebraic structures [10, 11, 14]. He has found many new self-dual codes of various lengths.Another method with the same direction is used by Melchor and Gaborit which is called recursive algorithm [1]. They have classified all of the 41 extremal binary [8, 18, 36] self-dual codes. Melchor et al.[2] have classified all extremal self-dual codes of length 38. They have compared three different methods and used recursive algorithm. They showed that there are exactly 2744 extremal [8, 19, 38] self-dual codes. Recently, Betsumiya et al[3]. have given a complete classification of doubly-even self-dual codes of length 40. Bouyuklieva and Bouyukliev have used a similar way with Harada and Munemasa but the difference of their algorithm is that they have found exactly one representative of every equivalance classes [4, 8]. They gave a complete classification of self-dual codes of length 38.

In this note, constructions of self-dual codes from smaller lengths of self-dual codes over finite fields are investigated. Methods which are used for this aim are composed.

2. Shadow code concept

Let C be a singly-even self-dual binary code of length n and C_0 is the subcode of C consisting of all codewords of weight 0 modulo 4. S=S(C) is called the shadow of C and defined by S=$C_0^\perp$-C. C_0 has codimension 1 in C. Hence C_0 has codimension 2 in $C_0^\perp$ and there are cosets C_1, C_2, C_3 of C_0 such that $C_0^\perp$=C_0∪C_1∪C_2∪C_3 where C=C_0∪C_2 and S=C_1∪C_3.

Let C be a doubly-even self-dual binary code of length n and let C_0 be any subcode of C of codimension 1. Then C⊆$C_0^\perp$ and hence there are cosets C_1, C_2, C_3 of C_0 such that $C_0^\perp$=C_0∪C_1∪C_2∪C_3 where C=C_0∪C_2 and S=C_1∪C_3. Then, the shadow of C with respect to C_0 is defined by S=S(C:C_0)=C_1∪C_3.

Pless and Brauldi has used above definitions to obtain new longer binary self-dual codes [15]. They have done this for two cases of the code, singly-even case and doubly-even case. Firstly, they have investigated the orthogonality of the cosets C_0, C_1, C_2, C_3 to each other and following tables for two cases obtained. For Table I and Table II, C_0 denotes the doubly-even subcode of a singly-even self-dual code C. For Table III and Table IV, C_0 denotes the subcode with codimension 1 of the doubly-even self-dual code C.

$TableI$

$n \equiv 2\ or\ 6\ \ (mod\ 8)$

	C_0	C_2	C_1	C_3
C_0	$\perp$	$\perp$	$\perp$	$\perp$
C_2	$\perp$	$\perp$	/	/
C_1	$\perp$	/	/	$\perp$
C_3	$\perp$	/	$\perp$	/

$TableII$

$n \equiv 0\ or\ 4\ \ (mod\ 8)$

	C_0	C_2	C_1	C_3
C_0	$\perp$	$\perp$	$\perp$	$\perp$
C_2	$\perp$	$\perp$	/	/
C_1	$\perp$	/	$\perp$	/
C_3	$\perp$	/	/	$\perp$

$TableIII$

$n \equiv 0\ \ (mod\ 8); 1 \in C_0$

	C_0	C_2	C_1	C_3
C_0	$\perp$	$\perp$	$\perp$	$\perp$
C_2	$\perp$	$\perp$	/	/
C_1	$\perp$	/	$\perp$	/
C_3	$\perp$	/	/	$\perp$

$TableIV$

$n \equiv 0\ \ (mod\ 8); 1 \notin C_0$

	C_0	C_2	C_1	C_3
C_0	$\perp$	$\perp$	$\perp$	$\perp$
C_2	$\perp$	$\perp$	/	/
C_1	$\perp$	/	/	$\perp$
C_3	$\perp$	/	$\perp$	/

By the help of these tables, construction method that is given by the following theorems has been developed. Proofs of the following theorems are omitted.

Theorem 2.1. [15] *Suppose that C is a singly-even self-dual code with length n where n≡2 or 6 (mod 8) and C_0 is the subcode of C consisting of all codewords of weight 0 in modulo 4. Let C_1,C_2,C_3 be cosets of C_0 and C* be the code of length n+2 obtained by extending $C_0^{\perp}$ as follows; (0,0,C_0), (1,1,C_2), (1,0,C_1), (0,1,C_3). Then C* is a self-dual code. If n≡2 (mod 8), then C* is singly-even. If n≡6 (mod 8), then C* is doubly-even.*

Theorem 2.2. [15] *Suppose that C is a singly-even self-dual code with length n where n≡0 or 4 (mod 8) and C_0 is the subcode of C consisting of all codewords of weight 0 in modulo 4.Let C_1,C_2,C_3 be cosets of C_0 and C* be the code of length n+4 generated by (1,1,1,1,0,. . .,0) and the following extension of $C_0^{\perp}$; (0,0,0,0,C_0), (1,1,0,0,C_2), (1,0,1,0,C_1), (0,1,1,0,C_3). Then C* is a self-dual code. If n≡0 (mod 8), then C* is singly-even. If n≡4 (mod 8), then C* is doubly-even.*

Theorem 2.3. [15] *Suppose that C is a doubly-even self-dual code with length n and C_0 is the subcode of C with codimension 1 which contains all one vector* **1**. *Let C_1,C_2,C_3 be cosets of C_0 and C* be the code of length n+4 generated by (1,1,1,1,0,. . .,0) and the following extension of $C_0^{\perp}$; (0,0,0,0,C_0), (1,1,0,0,C_2), (1,0,1,0,C_1), (0,1,1,0,C_3). Then C* is a self-dual code.*

Theorem 2.4. [15] *Suppose that C is a doubly-even self-dual code with length n and C_0 is the subcode of C with codimension 1 which does not contain all one vector* **1**. *Let C_1,C_2,C_3 be cosets of C_0 and C* be the code of length n+2 obtained by extending $C_0^{\perp}$ as follows; (0,0,C_0), (1,1,C_2), (1,0,C_1), (0,1,C_3). Then C* is a singly-even self-dual code.*

3. Harada's construction

Harada has obtained a new [12, 35, 70] singly-even self-dual code from the code D17 which is an extremal singly-even code of length 68 by using his following method[7, 17]. This [12, 35, 70] singly-even self-dual code is the first published example with this minimum weight and it was denoted by C_{70}.

Proposition 3.1. [7] *Let Ω be a subset of the set $\{1,2,\ \dots,\ n\}$ such that $|\Omega|$ is odd if $2n{\equiv}0$ (mod 4) and $|\Omega|$ is even if $2n{\equiv}2$ (mod 4). Let $G{=}[I_n,\ A]$ be a generator matrix of a self-dual code C of length $2n$, where I_n is the identity matrix of order n. Then the following matrix,*

$$G^* = \begin{bmatrix} 1 & 0 & x_1 \dots x_n & 1 \dots 1 \\ y_1 & y_1 & & \\ \vdots & \vdots & I_n & A \\ y_n & y_n & & \end{bmatrix},$$

where $x_i{=}1$ if $i \in \Omega$ and $x_i{=}0$ otherwise and $y_i = x_i{+}1$ ($1{\leq}\ i \leq\ n$), generates a self-dual code C^* of length $2n{+}2$.

Proof. Since G generates a self-dual code, it is sufficent to show the orthogonalities of the first row and other rows of G^*. Let r_i be the ith row of G^*. For $2{\leq}\ i \leq n{+}1$, we have

$$r_1 \cdot r_i = (x_{i-1} + 1) + x_{i-1} + k_{i-1} \equiv 0 \ \ (mod\ 2),$$

where k_i is the number of 1's in the ith row of A. Therefore G^* generates a self-dual code of length 2n+2. □

4. Building-up construction

This so-called method has been represented firstly in by Kim [6]. In [6], Kim has studied on binary self-dual codes and constructed new extremal self-dual binary codes of length 36, 38 and 58. He has shown that there are at least 14 inequivalent extremal self-dual [8, 18, 36] codes and there are at least 368 inequivalent extremal self-dual [8, 19, 38] codes. For length 58, 11 extremal self-dual [10, 29, 58] codes have been constructed. For all of these constructions the following method has been used. Building-up construction for binary case is more general than Harada's method in [7].

Theorem 4.1. [6] *Let S be a subset of the set $\{1, 2, ..., 2n\}$ of coordinate indices such that $|S|$ is odd. Let $G_o = (L|R) = (l_i|r_i)$ be a generator matrix (may not be in standard form) of a self-dual codes C_0 of length 2n, where l_i and r_i are rows of L and R, respectively, for $1{\leq}i{\leq}n$. Let $x = (x_1, x_2, ..., x_n, x_{n+1}, ..., x_{2n})$ be the characteristic vector of S, i.e., $x_j := 1$ if $j \in S$ and $x_j := 0$ if $j \notin S$ for $1{\leq}j{\leq}2n$. Suppose that $y_i := (x_1, x_2, ..., x_n, x_{n+1}, ..., x_{2n}) \cdot (l_i|r_i)$ for $1{\leq}i{\leq}n$. Then the following matrix generates a self-dual code C of length $2n{+}2$*

$$G = \left[\begin{array}{cc|cc} 1 & 0 & x_1 \dots x_n & x_{n+1} \dots x_{2n} \\ \hline y_1 & y_1 & & \\ \vdots & \vdots & L & R \\ y_n & y_n & & \end{array}\right].$$

Proof. C has dimension n+1 since the row rank of C is n+1. It remains to show that any two rows of G are orthogonal. Note that the first row of G is orthogonal to itself. Since any two rows of G excluding the first row of G are orthogonal to each other, it suffices to show that the first row of G is orthogonal to any other rows of G. This is true since for 1≤i≤n

$$(1, 0, x_1, x_2, ..., x_n, x_{n+1}, ..., x_{2n}) \cdot (y_i, y_i, l_i, r_i) =$$
$$= y_i + (x_1, x_2, ..., x_n, x_{n+1}, ..., x_{2n}) \cdot (l_i|r_i) =$$
$$= y_i + y_i = 0 \text{ in GF(2).}$$

□

Kim and Lee has generalized building-up construction method from self-dual codes over GF(2) to self-dual codes over GF(q) where q is a power of an odd prime [10]. For the cases, q≡1 (mod

4) and q=2^m , where m is a positive integer, following propositions are obtained. Proves of these propositions are analogue to Theorem 1 in [6].

Proposition 4.2. [10] *Assume that q is a power of an odd prime such that q≡1 (mod 4). Let c be in GF(q) such that c^2=-1 in GF(q). Let $G_0 = (L|R) = (l_i|r_i)$ be a generator matrix (not necessarily in standard form) of an Euclidean self-dual code C_0 over GF(q) of length 2n, where l_i and r_i are the rows of the matrices L and R, respectively, for 1≤i≤n. Then the following matrix generates a self-dual code C over GF(q) of length 2n+2*

$$G = \left[\begin{array}{cc|cc} 1 & 0 & x_1 \dots x_n & x_{n+1} \dots x_{2n} \\ \hline -y_1 & cy_1 & & \\ \vdots & \vdots & L & R \\ -y_n & cy_n & & \end{array}\right].$$

Proposition 4.3. [10] *Let $G_0 = (L|R) = (l_i|r_i)$ be a generator matrix (not necessarily in standard form) of an Euclidean self-dual code C_0 over GF(2^m) of length 2n, where l_i and r_i are the rows of the n x n matrices L and R, respectively, for 1≤i≤n. Let $x = (x_1, x_2, ..., x_n, x_{n+1}, ..., x_{2n})$ be a vector in GF(2^m)^{2n} with $x \cdot x = 1$. Set $y_i := (x_1, x_2, ..., x_n, x_{n+1}, ..., x_{2n}) \cdot (l_i|r_i)$ for 1≤i≤n. Then the following matrix generates an Euclidean self-dual code C over GF(2^m) of length 2n+2*

$$G = \left[\begin{array}{cc|cc} 1 & 0 & x_1 \dots x_n & x_{n+1} \dots x_{2n} \\ \hline y_1 & y_1 & & \\ \vdots & \vdots & L & R \\ y_n & y_n & & \end{array}\right].$$

Building-up construction technique for self-dual codes also have been developed over finite fields GF(q), where q≡3 (mod 4), by Kim and Lee [14]. 945 new extremal self-dual ternary [32,16,9] self-dual codes have been constructed by using the following proposition. Proof of this proposition is analogous to Theorem 1 in [6].

Proposition 4.4. [14] *Let q be a power of an odd prime with q≡3 (mod 4) and let n be even. Let α and β be in GF(q)* such that $\alpha^2 + \beta^2 + 1 = 0$ in GF(q). Let $G_0 = (r_i)$ be a generator matrix(not necessarily in standard form) of a self-dual code C_0 of length 2n, where r_i are the row vectors for 1≤i≤n. Let x_1 and x_2 be vectors in GF(q)^{2n} such that $x_1 \cdot x_2 = 0$ in GF(q) and $x_i \cdot x_i = -1$ in GF(q) for each i=1,2. For each i, 1≤i≤n, let $s_i := x_1 \cdot r_i$, $t_i := x_2 \cdot r_i$ and $y_i := (-s_i, -t_i, -\alpha s_i - \beta t_i, -\beta s_i + \alpha t_i)$ be vector of length 4. Then the following matrix generates a self-dual code C over GF(q) of length 2n+4.*

$$G = \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & x_1 \\ 0 & 1 & 0 & 0 & x_2 \\ \hline & y_1 & & & r_1 \\ & \vdots & & & \vdots \\ & y_n & & & r_n \end{array}\right].$$

5. Recursive construction for binary self-dual codes

Melchor and Gaborit [1] have given a new recursive method to classify extremal self-dual codes. By using this method, they have classified all of the 41 extremal binary [8, 18, 36] self-dual codes. Subtraction is a well-known method for self-dual binary codes which says that it is possible to construct a self-dual binary [n, $\frac{n}{2}$, ≥d] code from a self-dual binary [n+2, $\frac{n}{2}$+1, d+2] code. For a self-dual binary code C of length n, let C$_1$={(x$_1$,x$_2$,...,x$_{2n}$)∈C | x$_1$=x$_2$=0 or x$_1$=x$_2$=1} and C$_2$={(x$_3$,x$_4$,...,x$_{2n}$)| (x$_1$,x$_2$,...,x$_{2n}$)∈C$_1$}. Then C$_2$ is a [2n-2, n-1] subcode of C which has been obtained by subtraction of C. In [1], they have shown that the converse of this idea is possible, all self-dual binary [n+2, $\frac{n}{2}$, d+2] codes can be constructed from all binary self-dual [n, $\frac{n}{2}$, ≥d] codes.

Assume that one starts from a [n, $\frac{n}{2}$,d] code C$_n$ with generator matrix $\begin{bmatrix} y' \\ E \end{bmatrix}$ where y′ is a codeword of weight d. Let $a_i \in \{0,1\}$ and MC denote the set of all [n+2, $\frac{n}{2}$] codes with generator matrices of the form

$$\begin{bmatrix} 1 & 1 & y' \\ a_1 & a_1 & \\ \vdots & \vdots & E \\ a_{\frac{n}{2}-1} & a_{\frac{n}{2}-1} & \end{bmatrix}.$$

It is clear that C is self-orthogonal. Hence, to obtain C$_{n+2}$ from C, it is sufficent to complete all the codes C of MC by one of the three non-null elements of C$^{\perp}$/C. If one starts from the set of all inequivalent [n, $\frac{n}{2}$,d] self-dual codes, it is possible to rebuild all the [n+2, $\frac{n}{2}$+1, d+2] self-dual codes. Let C$_d$ is the subcode of C$_n$ which is generated by the vectors of weight d. These vectors have to be extended in codewords of weight d+2. So they must be extended with 11 and it will be easier to consider 2^{n-k} possibilities for the a$_i$ instead of 2^{n-1} possibilities where k≤ $\frac{n}{2}$ is the dimension of C$_d$. This makes the algorithm faster. Now, by using these facts the following algorithm can be written.

Recursive Algorithm

Input: S$_n$, the set of [n,$\frac{n}{2}$,d] self-dual codes up to permutation.
Output: The set of [n+2, $\frac{n}{2}$+1, d+2] self-dual codes.
For each code C$_n$ of S$_n$ do:
1) List all the words of weight d and construct the subcode C$_d$ of dimension k generated by these words. Construct a generator matrix G$_d$ of C$_d$ composed only with words of weight d.
2) Let E be a code of dimesion $\frac{n}{2}$-k with generator matrix G$_E$ such that C$_n$=C$_d$+E, construct the extended codes C with generator matrices

$$\begin{bmatrix} 1 & 1 & \\ \vdots & \vdots & G_d \\ 1 & 1 & \\ a_1 & a_1 & \\ \vdots & \vdots & G_E \\ a_{\frac{n}{2}-k} & a_{\frac{n}{2}-k} & \end{bmatrix}$$

such that $a_i \in \{0,1\}$, $(1 \le i \le n-k)$.
3) Complete all the previous codes C by non-null elements of C$^{\perp}$/C in order to obtain a self-dual code and check for codes with minimum distance d+2. For codes with weight d+2, check for the equivalence with already obtained self-dual [n+2, $\frac{n}{2}$+1, d+2] codes.

6. Comparison of building-up construction and recursive algorithm for binary case

Generator matrices of self-dual binary [n+2, $\frac{n}{2}$] codes which are obtained in step2 of the recursive algorithm is in the following form

$$\begin{bmatrix} 1 & 1 & y' \\ a_1 & a_1 & \\ \vdots & \vdots & E \\ a_{\frac{n}{2}-1} & a_{\frac{n}{2}-1} & \end{bmatrix}.$$

Let C be a self-orthogonal code that is generated by the matrix in the above form. In recursive algorithm C is completed with one of the three non-null elements of C$^\perp$/C to satisfy the self-duality. Assume that, C is completed with the coset C+y and the result code is denoted by C$_{n+2}$. A generator matrix of C$_{n+2}$ can be written as the following form up to permutation equivalance

$$G = \begin{bmatrix} 1 & 1 & y' \\ a_1 & a_1 & \\ \vdots & \vdots & E \\ a_{\frac{n}{2}-1} & a_{\frac{n}{2}-1} & \\ 1 & 0 & x_1 \dots x_n \end{bmatrix},$$

where $(1, 0, x_1, \dots x_n) \in C + y$ and $x = (x_1, \dots x_n)$ satisfies the following conditions.

$$E \cdot x = [e_{ij}] \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_1 \\ \vdots \\ a_{\frac{n}{2}-1} \end{bmatrix} \text{ and } y' \cdot x = (y_1', \dots, y_n') \cdot (x_1, \dots, x_n) = 1$$

such that $E = [e_{ij}]$ is an $(\frac{n}{2}{-1}) \times n$ matrix. Also x must be an odd-like vector. Then, by the change of the first row and last row of the generator matrix we can obtain

$$G = \begin{bmatrix} 1 & 0 & x_1 \dots x_n \\ 1 & 1 & y' \\ a_1 & a_1 & \\ \vdots & \vdots & E \\ a_{\frac{n}{2}-1} & a_{\frac{n}{2}-1} & \end{bmatrix}.$$

Now, if we write $\begin{bmatrix} y' \\ E \end{bmatrix} = [L|R]$ and for $n = 2m$ (n is even since C$_n$ is self-dual) by transformations such that $(x_1, \dots, x_{\frac{n}{2}}, \dots, x_n) = (x_1, \dots, x_m, \dots, x_{2m})$ and $y_1 = 1$, $y_2 = a_1$, $y_3 = a_2$, …, $y_m = a_{\frac{n}{2}-1}$, then we have

$$G = \left[\begin{array}{cc|cc} 1 & 0 & x_1 \dots x_m & x_{m+1} \dots x_{2m} \\ \hline y_1 & y_1 & & \\ \vdots & \vdots & L & R \\ y_m & y_m & & \end{array}\right].$$

Hence it shows that the generator matrix of the code C$_{n+2}$ which is obtained in the recursive algorithm can be written in the form of a generator matrix of C$_{n+2}$ which is obtained in the building-up construction [6]. As a conclusion, we can say that for the binary case recursive algorithm and building-up construction are actually the same.

7. Modified building-up construction

Kim and Lee have modified building-up construction method via the idea of the recursive algorithm [11].

Step 1: For each i, let s_i and t_i be in GF(q) and define y_i:=$(s_i, t_i, \alpha s_i + \beta t_i, \beta s_i - \alpha t_i)$ be a vector of length 4. Then

$$G_1 = \left[\begin{array}{c|c} y_1 & r_1 \\ \vdots & \vdots \\ y_n & r_n \end{array}\right]$$

generates a self-orthogonal code C_1.

Step 2: Let C be the dual of C_1. Consider the quotient space C/C_1. Let U_1 be the set of all coset representatives of the form x_1'=(1 0 0 0 x_1) such that $x_1' \cdot x_1'$=0 and U_2 the set of all coset representatives of the form x_2'=(0 1 0 0 x_2) such that $x_2' \cdot x_2'$=0.

Step 3: For any $x_1' \in U_1$ and $x_2' \in U_2$ such that $x_1' \cdot x_2'$=0, the following matrix

$$G = \left[\begin{array}{c|c} 1\ 0\ 0\ 0 & x_1 \\ 0\ 1\ 0\ 0 & x_2 \\ \hline y_1 & r_1 \\ \vdots & \vdots \\ y_n & r_n \end{array}\right]$$

generates a self-dual code C over GF(q) of length 2n+4.

This method is a kind composition of the building-up construction and recursive algorithm for the case of self-dual codes over GF(q), where q≡3 (mod 4). Recursive method was only defined for the binary codes but it is more efficient than building-up construction. Hence, modified building-up construction is more efficient than building-up construction and it carries the recursive method on the case of self-dual codes over GF(q), where q≡3 (mod 4).

8. Conclusion

It can be seen that there are too many papers about self-dual codes and their classifications. Usually, researchers focus on finding unknown self-dual codes by using various constructions and hence completing the uncomplete classifications. Many examples about self-dual code construction can be seen in [1, 2, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 16, 17]. In this work, with a different perspective, we have focused on composing some effective construction methods for self-dual codes. We think that, it is beneficial to look together various methods. By comparing them, sometimes it can be said that, they are actually the same methods such as building-up construction and recursive algorithm for binary case [2, 16]. Moreover, by composing them more efficient methods can be obtained such as modified building-up construction [11].

References

[1] Aguilar-Melchor, C., Gaborit, P., (2008), On the classification of extremal [8, 18, 36] binary self-dual codes, IEEE Transactions on Information Theory, 54(10), pp.4743-4750.

[2] Aguilar-Melchor, C., Gaborit, P., Kim, J.-L., Sok, L., Sol, P., (2012), Classification of extremal snd s-extremal binary self-dual codes of length 38, IEEE Trans. Inform. Theory, 58, pp.2253-2262.

[3] Betsumiya, K., Harada M., Munemasa, A., (2012), A complete classification of doubly-even self-dual codes of length 40, The Electronic Journal of Combinatorics, 19, pp.18.

[4] Bouyuklieve, S., Bouyukliev, I., (2012), An algorithm for classification of binary self-dual codes, IEEE Transactions on Information Theory, 58(6), pp.3933-3940.

[5] Dougherty, S. T., (1995), Shadow codes and weight enumerators, IEEE Transactions on Information Theory, 41(3), pp.762-768.

[6] Kim, J.-L., (2001), New extremal self-dual codes of length 36,38 and 58, IEEE Trans. Inform Theory, 47, pp.386-393.

[7] Harada M., (1997), The existence of a self-dual [12, 35, 70] code and formally self-dual codes, Finite Fields Appl., 3, pp.131-139.

[8] Harada, M., Munemasa, A., (2012), Classification of self-dual codes of length 36, Advances in Mathematics of Communications, 6(2), pp.229-235.

[9] Huffman, W.C., (2005), On the classification and enumeration of self-dual codes, Finite Fields Appl., 11, pp.451-490.

[10] Kim, J.-L., Lee, Y., (2004), Euclidean and Hermitian self-dual MDS codes over large finite fields, J. Combin Theory Ser. A, 105, pp.79-95.

[11] Kim, J.-L., Lee, Y., (2012), An efficent construction of self-dual codes, arXiv.org, arXiv:1201.5689.

[12] Pless, V., (1975), On the classification and enumeration of self-dual codes, J. Combin Theory Ser. A, 18(3), pp.313-335.

[13] Rains, E, Sloane, N.J.A., (1998), Self-dual Codes, in: Pless V., Huffman W.C. (Eds.), ”Handbook of Coding Theory”, Elsevier, Amsterdam. Netherlands.

[14] Kim, J.-L., Lee, Y., (2009), Self-dual codes using the building-up construction, ISIT 2009, Seoul, Korea, June 28-July 3.

[15] Pless, V., Brualdi, R., (1991), Weight enumerator of self-dual codes, IEEE Transactions on Information Theory, 37(4), pp.1222-1225.

[16] Topcu, H., Aktas, H., (2012), Self-dual Kodlar ve Insa Yontemleri, Nevsehir Universitesi Fen Bilimleri Enstitusu.

[17] Tsai, H.-P., (1992), Existence of some extremal self-dual codes, IEEE Transactions on Information Theory, 38(6), pp.1829-1833.

Hatice Topcu received her B.Sc. degree in 2007 from Hacettepe University, Turkey. Then, she has got her M.Sc. degree in 2012 from Nevsehir University, Turkey. During her M.Sc., between Feb-June 2011, she has studied at University of Louisville, KY, USA as a researcher. She has started to Ph.D. in 2012 at Nevsehir University and still-continuing.

Hacı Aktas is an Associated Professor of Mathematics at Erciyes University (Kayseri, Turkey). He received M.Sc. and Ph.D. degrees in Mathematics from Erciyes University in 1994 and 1997, respectively. His research interests include fuzzy and soft algebraic structures and coding theory. He has published about 20 papers at national and international journals.