CIS CODES OVER $\mathbb{F}_4$

HYUN JIN KIM

Abstract. We study the complementary information set codes (for short, CIS codes) over $\mathbb{F}_4$. They are strongly connected to correlation-immune functions over $\mathbb{F}_4$. Also the class of CIS codes includes the self-dual codes. We find a construction method of CIS codes over $\mathbb{F}_4$ and a criterion for checking equivalence of CIS codes over $\mathbb{F}_4$. We complete the classification of all inequivalent CIS codes of length up to 8 over $\mathbb{F}_4$.

1. Introduction

A complementary information set code (for short, CIS code) is defined to be a linear code with $[2n, n, d]$ which has two disjoint information sets for a positive integer $n$. A CIS code over $\mathbb{F}_2$ is proposed by Carlet et al. [6]. CIS codes are strongly connected to correlation-immune functions. Correlation-immune functions are noticeably important class of cryptography functions due to their useful application in cryptography [15, 16]. A CIS code over $\mathbb{F}_p$ is introduced by Kim and Lee [11]. They classify CIS codes over $\mathbb{F}_p$ of small lengths, where $p$ is 3, 5, 7 in [11]. Also, they show that long CIS codes over $\mathbb{F}_p$ meet the Gilbert-Vashmov bound. The class of CIS codes includes self-dual codes. Furthermore, a notion of higher order CIS codes over $\mathbb{F}_2$ is developed by Carlet et al. [5].
Also, a $t$-CIS code over $\mathbb{F}_p$ is developed by Kim and Lee, where the $t$-CIS code is a CIS code of order $t \geq 2$ [12]. They show that orthogonal arrays over $\mathbb{F}_p$ can be explicitly constructed from $t$-CIS codes over $\mathbb{F}_p$.

In this paper we study on CIS codes over $\mathbb{F}_4$. We show the relation between the existence of a correlation immune function of strength $d$ of $n$-variables and the existence of a CIS code over $\mathbb{F}_4$ of parameters $[2n, n, d]$ with the systematic partition. We find a method for constructing complementary information set codes over $\mathbb{F}_4$ from the building-up method [8, 13, 14]. Using this method, we classify quaternary CIS codes of lengths up to 8. Also, we show a criterion for checking equivalence of CIS codes over $\mathbb{F}_4$.

This paper is organized as follows. We introduce some definitions and basic contents in Section 2. In Section 3, we show the relation between correlation-immune functions over $\mathbb{F}_4$ and quaternary CIS code. In Section 4, we find a construction method of CIS codes over $\mathbb{F}_4$ and a criterion for checking equivalence of CIS codes over $\mathbb{F}_4$. Finally, we classify quaternary CIS codes of lengths 2, 4, 6, 8 in Section 5.

In this paper, all computations are done using the computer algebra system MAGMA [1].

2. Preliminaries

Let $\mathbb{F}_4$ be a finite field of cardinality 4 with $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$. Let $C$ be a linear code of length $n$ over $\mathbb{F}_4$. We define two inner products over $\mathbb{F}_4^n$. For $u, v \in \mathbb{F}_4^n$, $u = (u_1, u_2, \ldots, u_n)$, and $v = (v_1, v_2, \ldots, v_n)$, the Euclidean inner product is defined as

$$ u \cdot v = \sum_{i=1}^{n} u_i v_i, $$

and the Hermitian inner product is defined as

$$ \langle u, v \rangle = \sum_{i=1}^{n} u_i v_i^2. $$

Let

$$ C^\perp_E = \{ x \in \mathbb{F}_4^n \mid x \cdot c = 0, \forall c \in C \} $$

be the Euclidean dual code of $C$, and let

$$ C^\perp_H = \{ x \in \mathbb{F}_4^n \mid \langle x, c \rangle = 0, \forall c \in C \} $$
be the Hermitian dual code of $C$. A code $C$ is Euclidean self-dual if $C = C^\perp_E$ and Hermitian self-dual if $C = C^\perp_H$. A code $C$ of length $n$ is called systematic if there exists a subset $I$ of $\{1, 2, \ldots, n\}$ (called an information set of $C$) such that every possible tuple of length $|I|$ occurs in exactly one codeword in $C$ within the specified coordinates $x_i$ for $i \in I$ [6, 11]. Thus, a CIS code is a systematic code with two complementary information sets. The generator matrix of a $[2n, n]$ code is called systematic form if it is blocked as $[I \mid A]$, where $I$ is the identity matrix of order $n$ and $A$ is an $n \times n$ matrix [11]. The class of CIS codes over $\mathbb{F}_4$ includes the Euclidean self-dual codes and the Hermitian self-dual codes over $\mathbb{F}_4$ as its subclasses.

The Hamming weight of a vector $z$ is the number of its nonzero entries. The Hamming weight of $z$ is denoted by $wt(z)$. The homogeneous polynomial $W_C(X, Y)$ defined by

$$W_C(X, Y) = \sum_{c \in C} X^{n-wt(c)} Y^{wt(c)}.$$ 

is called the weight enumerator of a code $C$. Let $C$ and $C'$ be two codes over $\mathbb{F}_4$. If there is some monomial matrix $M$ (resp. permutation matrix) over $\mathbb{F}_4$ such that $C' = CM$, where $CM = \{cM \mid c \in C\}$, then two codes $C$ and $C'$ over $\mathbb{F}_4$ are monomially equivalent (resp. permutation equivalent), denoted by $C \cong C'$. The monomial automorphism group of $C$ is the set of monomial matrices $M$ with $C = CM$, denoted by $\text{Aut}(C)$. In this paper, the equivalence means the monomial equivalence. We note that this is the usual concept of equivalence over $\mathbb{F}_4$, named IsE Equivalent in MAGMA [1].

The following three lemmas are given in [6], and they also hold for CIS codes over $\mathbb{F}_4$ as well.

**Lemma 2.1.** If a $[2n, n]$ code $C$ over $\mathbb{F}_4$ has generator matrix $[I \mid A]$ with $A$ invertible, then $C$ is a CIS code with the systematic partition. Conversely, every CIS code is equivalent to a code with generator matrix in that form.

In particular, this lemma applies to systematic self-dual codes whose generator matrix $[I \mid A]$ satisfies $AA^T = I$.

**Lemma 2.2.** If a $[2n, n]$ code $C$ over $\mathbb{F}_4$ has generator matrix $[I \mid A]$ with $\text{rank}(A) < n/2$, then $C$ is not a CIS code.
Lemma 2.3. If $C$ is a $[2n, n]$ code over $\mathbb{F}_4$ whose dual has minimum weight 1 then $C$ is not a CIS code.

3. Correlation-immune functions

We consider correlation-immune functions of strength $d$ over $\mathbb{F}_4^n$. In [2–4, 7], we can find the characterization of the $t$-th order correlation-immune function $f : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^t$. In this paper, we only think of the case of $l = n$ and $q = 4$.

Definition 3.1. ([3, 7]) A bijective function $F : \mathbb{F}_4^n \rightarrow \mathbb{F}_4^n$ is correlation-immune of strength $d$ if for $\forall \ a, b \in \mathbb{F}_4^n$ such that $wt(a) + wt(b) \leq d$ and $a \neq 0$, we have $W_F(a, b) = 0$, where $wt$ denotes the Hamming weight and $W_F$ the Walsh-Hadamard transform of $F$: $W_F(a, b) = \sum_{x \in \mathbb{F}_4^n} (-1)^{tr(a \cdot x + b \cdot F(x))}$.

We note that $\sum_{x \in \mathbb{F}_4^n} (-1)^{tr(x \cdot a)} \neq 0$ if and only if $a = 0$. We can find the connection between correlation-immune functions of strength $d$ and CIS codes over $\mathbb{F}_4$ with parameters $[2n, n, > d]$ from the following theorem.

Theorem 3.2. The existence of a linear correlation-immune function of strength $d$ of $n$-variables over $\mathbb{F}_4$ is equivalent to the existence of a CIS code over $\mathbb{F}_4$ of parameters $[2n, n, > d]$ with the systematic partition.

The proof is analogous to that of Theorem 3.2 in [11] and hence is omitted.

4. Construction of CIS Codes over $\mathbb{F}_4$

The following theorem is obtained from ([11, Theorem 4.1]). It gives a construction method of CIS code over $\mathbb{F}_4$. The motivation of this method is building up construction on self-dual codes over $\mathbb{F}_2$ and $\mathbb{F}_q$ [8, 13, 14]. We denote a generator matrix of a code $C$ by $\text{gen}(C)$.

Theorem 4.1. Suppose that $C$ is a $[2n, n]$ CIS code over $\mathbb{F}_4$ with generator matrix $(I_n | A_n)$, where $A_n$ is an invertible matrix with $n$ row vectors $r_1, r_2, \ldots, r_n$. Then for any two vectors $x = (x_1, x_2, \ldots, x_n)$ and
\[y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_4^n, \text{ the following } G' \text{ generates a } [2(n + 1), n + 1] \text{ CIS code } C':\]

\[
G' = \begin{bmatrix}
1 & x_1 & \cdots & x_n & 0 & \cdots & 0 & 1 \\
0 & I_n & & & A_n & & & y_1 \\
\vdots & & & & \vdots & & & \vdots \\
0 & & & & & & & y_n
\end{bmatrix}
\]

Conversely, any \([2(n + 1), n + 1]\) CIS code over \(\mathbb{F}_4\) is obtained from some \([2n, n]\) CIS code by this construction, up to equivalence.

**Proof.** It is obvious that the matrix \(G'\) has two information sets. Hence the matrix \(G''\) generates a \([2(n + 1), n + 1]\) CIS code over \(GF(4)\).

Conversely, let \(C\) be a \([2(n + 1), n + 1]\) CIS code over \(GF(4)\). By Lemma 2.1, this code has a generator matrix \((I_{n+1} | A_{n+1})\), where \(A_{n+1}\) is an \((n+1) \times (n+1)\) invertible matrix, up to equivalence. By elementary row operations, we have that

\[
\text{gen}(C) \cong \begin{bmatrix}
1 & x'_1 & \cdots & x'_n & 0 & \cdots & 0 & y' \\
0 & I_n & & & A'_n & & & y'_1 \\
\vdots & & & & \vdots & & & \vdots \\
0 & & & & & & & y'_n
\end{bmatrix},
\]

where \(A'_n\) is an \(n \times n\) invertible matrix. In this case, \(y'\) is a nonzero element in \(\mathbb{F}_4\) since \(A_{n+1}\) is an invertible matrix. By scaling the last column, we have

\[
\text{gen}(C) \cong \begin{bmatrix}
1 & x'_1 & \cdots & x'_n & 0 & \cdots & 0 & 1 \\
0 & I_n & & & A'_n & & & y'_1 \\
\vdots & & & & \vdots & & & \vdots \\
0 & & & & & & & y'_n
\end{bmatrix},
\]

Since \(A'_n\) is an \(n \times n\) invertible matrix, \((I_n \mid A'_n)\) generates a \([2n, n]\) CIS code. Therefore, any \([2(n + 1), n + 1]\) CIS code can be obtained from some \([2n, n]\) CIS code by this construction up to equivalence.

We denote a transpose of a vector \(x\) by \(x^T\).
Algorithm 1. construction of CIS code over $\mathbb{F}_4$

Input: 
$C$ : a CIS code of length $2n$ with generator matrix $[I_n \mid A_n]$

Output: 
$C'$ : a CIS code of length $2n + 2$ with generator matrix

begin 
For $x, y \in \mathbb{F}_4^n$, 
$I' := \left[ \begin{array}{c} x \\ I_n \end{array} \right]$, $A' := [A_n \mid y^T]$, 
$\bar{T} := [z^T \mid I']$, $\bar{A} := \left[ \begin{array}{c} z' \\ A' \end{array} \right]$, with $z = (1, 0, 0, \ldots, 0)$, $z' = (0, \ldots, 0, 0, 1)$, 
$G' = [\bar{T} \mid \bar{A}]$; 
$C' :=$ code generated by $G'$

end 

We consider equivalence relation of CIS codes generated by Algorithm 1. Let $C$ be a CIS $[2n, n]$ code over $\mathbb{F}_4$ with a generator matrix $G$. The elements of the automorphism group $Aut(C)$ can be considered as monomial matrices. For any monomial matrix $M \in Aut(C)$, the matrix $GM$ generates the code $C$. Hence we can choose an invertible matrix $L_M$ in $GL(n, \mathbb{F}_4)$ such that $GM = L_M G$, where $GL(n, \mathbb{F}_4)$ is the general linear group of dimension $n$ over $\mathbb{F}_4$. In this way, we obtain a homomorphism $\phi : Aut(C) \to GL(n, \mathbb{F}_4)$ with $\phi(M) = L_M$. We define the action of the image of $\phi$ on $\mathbb{F}_4^n$ as $L(x) = Lx^T$ for every $x \in \mathbb{F}_4^n$ and $L$ in the image of $\phi$ [9, 11].

**Theorem 4.2.** Let $[I_n \mid A_n]$ be a generator matrix of a CIS code $C$, and let

$$G_1 = \begin{bmatrix}
1 & x & 0 & \cdots & 0 & 1 \\
0 & I_n & A_n & y^T \\
0 & I_n & A_n & y^T
\end{bmatrix}$$

and

$$G_2 = \begin{bmatrix}
1 & x' & 0 & \cdots & 0 & 1 \\
0 & I_n & A_n & y^T \\
0 & I_n & A_n & y^T
\end{bmatrix}$$
Assume that there exists $M \in \text{Aut}(C)$ such that its corresponding element $L_M \in \text{Im} (\phi)$ with $G_1 M = L_M G_1$ under a homomorphism $\phi : \text{Aut}(C) \to GL(n, \mathbb{F}_4)$ is a stabilizer of $y$ and $\overline{x'} = \mathbf{x} M$, where $\mathbf{x} = (x, 0, \ldots, 0)$ and $\mathbf{x'} = (x', 0, \ldots, 0)$. Then $G_1$ and $G_2$ generate equivalent CIS codes.

The proof is analogous to that of Theorem 4.4 in [11]. Hence it is omitted.

5. Implementation

**Theorem 5.1.** There is only one quaternary CIS code of length 2, up to equivalence.

**Proof.** A generator matrix of quaternary CIS code of length 2 is $[x, y]$, where $x, y \in \mathbb{F}_4$ are nonzero. The code generated by $[x, y]$ is equivalent to the code with a generator matrix $[1, 1]$. Therefore, there exists one CIS code of length 2 over $\mathbb{F}_4$, up to equivalence. $\square$

We obtain the following theorem by Theorem 4.1.

**Theorem 5.2.** There are exactly three inequivalent quaternary CIS codes of length 4. One of these codes is Hermitian self-dual.

We list up the generator matrices of all inequivalent quaternary CIS codes of length 4 as follows:

$$C_{4,1} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \quad C_{4,2} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}, \quad C_{4,3} = \begin{bmatrix} 1 & w & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

The code generated by $C_{4,1}$ is Hermitian self-dual and Euclidean self-dual. The code generated by $C_{4,3}$ is equivalent to a Euclidean self-dual code.

**Remark 5.3.** Hermitian self-dual codes are preserved under monomial equivalence. However, Euclidean self-dual codes are not preserved under monomial equivalence.

We write the weight enumerators of all inequivalent quaternary CIS code of length 4 as follows:

$$W_{C_{4,1}} = X^4 + 3X^2Y^2 + 6XY^3 + 6Y^4,$$
$$W_{C_{4,2}} = X^4 + 12XY^3 + 3Y^4,$$
$$W_{C_{4,3}} = X^4 + 6X^2Y^2 + 9Y^4.$$
Theorem 5.4. There exist 16 CIS codes of length 6 over $\mathbb{F}_4$, up to equivalence. Two of these codes are Hermitian self-dual codes.

We present generator matrices of CIS codes of length 6 over $\mathbb{F}_4$ as follows.

$$
C_{6,1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad C_{6,2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & w \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},
$$

$$
C_{6,3} = \begin{bmatrix} 1 & 0 & 0 & 1 & w & w^2 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad C_{6,4} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},
$$

$$
C_{6,5} = \begin{bmatrix} 1 & 0 & 0 & w & 0 & w^2 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad C_{6,6} = \begin{bmatrix} 1 & 0 & 0 & w^2 & 1 & w^2 \\ 0 & 1 & 0 & 1 & 0 & w \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},
$$

$$
C_{6,7} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & w^2 \\ 0 & 1 & 0 & 1 & 0 & w \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad C_{6,8} = \begin{bmatrix} 1 & 0 & 0 & w^2 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & w \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},
$$

$$
C_{6,9} = \begin{bmatrix} 1 & 0 & 0 & 1 & w & w^2 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad C_{6,10} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},
$$

$$
C_{6,11} = \begin{bmatrix} 1 & 0 & 0 & w^2 & w & w \\ 0 & 1 & 0 & w & w^2 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad C_{6,12} = \begin{bmatrix} 1 & 0 & 0 & w & 1 & w^2 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},
$$

$$
C_{6,13} = \begin{bmatrix} 1 & 0 & 0 & w & 0 & w^2 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad C_{6,14} = \begin{bmatrix} 1 & 0 & 0 & w^2 & w & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix},
$$

$$
C_{6,15} = \begin{bmatrix} 1 & 0 & 0 & w^2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}, \quad C_{6,16} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}.
$$

The codes generated by $C_{6,11}$ and $C_{6,16}$ are Hermitian self-dual. Also, the codes of generated by $C_{6,6}$ and $C_{6,13}$ are equivalent to Euclidean self-dual codes, and the code of generated by $C_{6,16}$ is Euclidean self-dual. We list up the weight enumerators of all inequivalent CIS codes of length 6.
over $\mathbb{F}_4$ as follows:

$$
\begin{align*}
W_{c_{6,1}} &= X^6 + 12X^3Y^3 + 9X^2Y^4 + 36XY^5 + 6Y^6, \\
W_{c_{6,2}} &= X^6 + 6X^3Y^3 + 27X^2Y^4 + 18XY^5 + 12Y^6, \\
W_{c_{6,3}} &= X^6 + 9X^3Y^3 + 18X^2Y^4 + 27XY^5 + 9Y^6, \\
W_{c_{6,4}} &= X^6 + 3X^4Y^2 + 9X^3Y^3 + 12X^2Y^4 + 27XY^5 + 12Y^6, \\
W_{c_{6,5}} &= X^6 + 15X^3Y^3 + 12X^2Y^4 + 21XY^5 + 15Y^6, \\
W_{c_{6,6}} &= X^6 + 6X^3Y^3 + 27X^2Y^4 + 18XY^5 + 12Y^6, \\
W_{c_{6,7}} &= X^6 + 12X^3Y^3 + 21X^2Y^4 + 12XY^5 + 18Y^6, \\
W_{c_{6,8}} &= X^6 + 3X^4Y^2 + 6X^3Y^3 + 21X^2Y^4 + 18XY^5 + 15Y^6, \\
W_{c_{6,9}} &= X^6 + 3X^4Y^2 + 27X^2Y^4 + 24XY^5 + 9Y^6, \\
W_{c_{6,10}} &= X^6 + 3X^4Y^2 + 12X^3Y^3 + 15X^2Y^4 + 12XY^5 + 21Y^6, \\
W_{c_{6,11}} &= X^6 + 45X^2Y^4 + 18Y^6, \\
W_{c_{6,12}} &= X^6 + 3X^4Y^2 + 3X^3Y^3 + 18X^2Y^4 + 33XY^5 + 6Y^6, \\
W_{c_{6,13}} &= X^6 + 3X^4Y^2 + 12X^3Y^3 + 3X^2Y^4 + 36XY^5 + 9Y^6, \\
W_{c_{6,14}} &= X^6 + 6X^4Y^2 + 21X^2Y^4 + 24XY^5 + 12Y^6, \\
W_{c_{6,15}} &= X^6 + 6X^4Y^2 + 6X^3Y^3 + 15X^2Y^4 + 18XY^5 + 18Y^6, \\
W_{c_{6,16}} &= X^6 + 9X^4Y^2 + 27X^2Y^4 + 27Y^6.
\end{align*}
$$

References


Hyun Jin Kim
University College
Yonsei University
Incheon 21983, Republic of Korea
E-mail: guswls41@yonsei.ac.kr