Korean J. Math. **28** (2020), No. 2, pp. 285–294
http://dx.doi.org/10.11568/kjm.2020.28.2.285

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].

Received April 20, 2020. Revised May 22, 2020. Accepted June 10, 2020.
2010 Mathematics Subject Classification: 94B05, 11T71.
Key words and phrases: complementary information set code, self-dual code, equivalence, correlation immune.
This work was supported by the National Research Foundation of Korea(NRF) grant founded by the Korea government(NRF-2017R1D1A1B03028251).

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 $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_4$. We define two inner products over $\mathbb{F}_4^n$. For $\mathbf{u}, \mathbf{v} \in \mathbb{F}_4^n, \mathbf{u} = (u_1, u_2, \ldots, u_n)$, and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$, the Euclidean inner product is defined as

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

and the Hermitian inner product is defined as

$$< \mathbf{u}, \mathbf{v} >= \sum_{i=1}^{n} u_i v_i^2.$$

Let

$$\mathcal{C}^{\perp E} = \{\mathbf{x} \in \mathbb{F}_4^n \mid \mathbf{x} \cdot \mathbf{c} = 0, \forall \mathbf{c} \in \mathcal{C}\}$$

be the Euclidean dual code of $\mathcal{C}$, and let

$$\mathcal{C}^{\perp H} = \{\mathbf{x} \in \mathbb{F}_4^n \mid < \mathbf{x}, \mathbf{c} >= 0, \forall \mathbf{c} \in \mathcal{C}\}$$

be the Hermitian dual code of $\mathcal{C}$. A code $\mathcal{C}$ is *Euclidean self-dual* if $\mathcal{C} = \mathcal{C}^{\perp E}$ and *Hermitian self-dual* if $\mathcal{C} = \mathcal{C}^{\perp H}$. A code $\mathcal{C}$ of length n is called *systematic* if there exists a subset I of $\{1, 2, \ldots, n\}$ (called an *information set* of $\mathcal{C}$) such that every possible tuple of length $\mid I \mid$ occurs in exactly one codeword in $\mathcal{C}$ 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 $\mathbf{z}$ is the number of its nonzero entries. The Hamming weight of $\mathbf{z}$ is denoted by $wt(\mathbf{z})$. The homogeneous polynomial $W_{\mathcal{C}}(X, Y)$ defined by

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

is called the weight enumerator of a code $\mathcal{C}$. Let $\mathcal{C}$ and $\mathcal{C}'$ be two codes over $\mathbb{F}_4$. If there is some monomial matrix M (resp. permutation matrix) over $\mathbb{F}_4$ such that $\mathcal{C}' = \mathcal{C}M$, where $\mathcal{C}M = \{cM \mid c \in \mathcal{C}\}$, then two codes $\mathcal{C}$ and $\mathcal{C}'$ over $\mathbb{F}_4$ are *monomially equivalent (resp. permutation equivalent)*, denoted by $\mathcal{C} \cong \mathcal{C}'$. The monomial automorphism group of $\mathcal{C}$ is the set of monomial matrices M with $\mathcal{C} = \mathcal{C}M$, denoted by $\mathrm{Aut}(\mathcal{C})$. In this paper, the equivalence means the monomial equivalence. We note that this is the usual concept of equivalence over $\mathbb{F}_4$, named IsEquivalent 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 $\mathcal{C}$ over $\mathbb{F}_4$ has generator matrix $[I \mid A]$ with A invertible, then $\mathcal{C}$ 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 $\mathcal{C}$ over $\mathbb{F}_4$ has generator matrix $[I \mid A]$ with $rank(A) < n/2$, then $\mathcal{C}$ is not a CIS code.*

Lemma 2.3. *If $\mathcal{C}$ is a $[2n, n]$ code over $\mathbb{F}_4$ whose dual has minimum weight 1 then $\mathcal{C}$ 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 $f : \mathbb{F}_q^n \to \mathbb{F}_q^l$. In this paper, we only think of the case of $l = n$ and $q = 4$.

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

We note that $\sum_{\mathbf{x}\in\mathbb{F}_4^n} (-1)^{tr(\mathbf{x}\cdot\mathbf{a})} \neq 0$ if and only if $\mathbf{a} = 0$. 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 $\mathcal{C}$ by $gen(\mathcal{C})$.

Theorem 4.1. *Suppose that $\mathcal{C}$ is a $[2n, n]$ CIS code over $\mathbb{F}_4$ with generator matrix $(I_n \mid A_n)$, where A_n is an invertible matrix with n row vectors $\mathbf{r_1}, \mathbf{r_2}, \ldots, \mathbf{r_n}$. Then for any two vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and*

$\mathbf{y} = (y_1, y_2, \ldots, y_n)$ in $\mathbb{F}_4^n$, the following G' generates a $[2(n+1), n+1]$ CIS code $\mathcal{C}'$:

$$G' = \left[\begin{array}{c|ccc|ccc|c} 1 & x_1 & \cdots & x_n & 0 & \cdots & 0 & 1 \\ \hline 0 & & & & & & & y_1 \\ \vdots & & I_n & & & A_n & & \vdots \\ 0 & & & & & & & y_n \end{array}\right]$$

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

$$gen(\overline{\mathcal{C}}) \cong \left[\begin{array}{c|ccc|ccc|c} 1 & x_1' & \cdots & x_n' & 0 & \cdots & 0 & y' \\ \hline 0 & & & & & & & y_1' \\ \vdots & & I_n & & & A_n' & & \vdots \\ 0 & & & & & & & y_n' \end{array}\right],$$

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

$$gen(\overline{\mathcal{C}}) \cong \left[\begin{array}{c|ccc|ccc|c} 1 & x_1' & \cdots & x_n' & 0 & \cdots & 0 & 1 \\ \hline 0 & & & & & & & \overline{y_1} \\ \vdots & & I_n & & & A_n' & & \vdots \\ 0 & & & & & & & \overline{y_n} \end{array}\right],$$

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 $\mathbf{x}$ by $\mathbf{x}^T$.

Algorithm 1. construction of CIS code over $\mathbb{F}_4$

Input:

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

Output:

$\mathcal{C}'$: a CIS code of length $2n+2$ with generator matrix

begin

For $\mathbf{x}, \mathbf{y} \in \mathbb{F}_4^n$,

$I' := \left[\frac{\mathbf{x}}{I_n}\right]$, $A' := [A_n \mid \mathbf{y}^T]$,

$\overline{I} := [\mathbf{z}^T \mid I']$, $\overline{A} := \left[\frac{\mathbf{z}'}{A'}\right]$, where $\mathbf{z}, \mathbf{z}' \in \mathbb{F}_4^{n+1}$

with $\mathbf{z} = (1, 0, 0, \ldots, 0)$, $\mathbf{z}' = (0, \ldots, 0, 0, 1)$,

$G' = [\overline{I} \mid \overline{A}]$;

$\mathcal{C}'$:= code generated by G'

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

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

$$G_1 = \left[\begin{array}{c|ccccc|c} 1 & \mathbf{x} & & 0 & \cdots & 0 & 1 \\ \hline 0 & & & & & & \\ \vdots & I_n & & & A_n & & \mathbf{y}^T \\ 0 & & & & & & \end{array}\right]$$

and

$$G_2 = \left[\begin{array}{c|ccccc|c} 1 & \mathbf{x}' & & 0 & \cdots & 0 & 1 \\ \hline 0 & & & & & & \\ \vdots & I_n & & & A_n & & \mathbf{y}^T \\ 0 & & & & & & \end{array}\right]$$

Assume that there exists $M \in Aut(\mathcal{C})$ such that its corresponding element $L_M \in \mathrm{Im}(\phi)$ with $G_1 M = L_M G_1$ under a homomorphism $\phi : Aut(\mathcal{C}) \to GL(n, \mathbb{F}_4)$ is a stabilizer of $\mathbf{y}$ and $\overline{\mathbf{x}'} = \overline{\mathbf{x}}M$, where $\overline{\mathbf{x}} = (\mathbf{x}, 0, \ldots, 0)$ and $\overline{\mathbf{x}'} = (\mathbf{x}', 0, \ldots, 0)$. 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. □

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:

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

The code generated by $\mathcal{C}_{4,1}$ is Hermitian self-dual and Euclidean self-dual. The code generated by $\mathcal{C}_{4,3}$ 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:

$$\begin{aligned} W_{\mathcal{C}_{4,1}} &= X^4 + 3X^2Y^2 + 6XY^3 + 6Y^4, \\ W_{\mathcal{C}_{4,2}} &= X^4 + 12XY^3 + 3Y^4, \\ W_{\mathcal{C}_{4,3}} &= X^4 + 6X^2Y^2 + 9Y^4. \end{aligned}$$

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.

$$\mathcal{C}_{6,1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad \mathcal{C}_{6,2} = \begin{bmatrix} 1 & 0 & 0 & w^2 & 1 & w \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

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

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

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

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

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

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

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

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

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

References

[1] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput **24** (1997), 235–265.

[2] P. Camion, A. Canteaut. *Correlation-immune and resilient functions over a finite alphabet and their applications in cryptography*, Designs Codes Crypt. **16** (2) (1999), 121–149.

[3] P. Camion, C. Carlet, P. Charpin, N. Sendrier. *On correlation-immune functions*, Lecture Notes in Computer Science, **576** (1992), 86–100.

[4] C. Carlet, *More correlation-immune and resilient functions over Galois fields and Galois rings*, Advances in Cryptology, EUROCRYPT'97, Lecture Note in Computer Sciences, Springer Verlag 1233 (1997), 422-433.

[5] C. Carlet, F. Freibert, S. Guilley, M. Kiermaier, J.-L. Kim, P. Solé, *Higher-order CIS codes*, IEEE Trans. Inform. Theory **60** (9) (2014), 5283–5295.

[6] C. Carlet, P. Gaborit, J-L. Kim, P. Solé, *A new class of codes for Boolean masking of cryptographic computations*, IEEE Trans. Inform. Theory **58** (2012), 6000–6011.

[7] K. Gopalakrishnan, D. R. Stinson *Three characterizations of non-binary correlation-immune and resilient functions*, Designs Codes Crypt. **5** (1995), 241–251.

[8] M. Harada, *The existence of a self-dual* $[70, 35, 12]$ *code and formally self-dual codes*, Finte Fields Appl. **3** (1997), 131–139.

[9] M. Harada, A. Munemasa, *Classification of self-dual codes of length 36*, Adv. Math. Commun. **6** (2012), 229–235.

[10] H. J. Kim: *https://drive.google.com/file/d/1sVZ-Em5hHFs36-hBLGda0NLqmt8RThkh/view?usp=sharing.*

[11] H. J. Kim and Y. Lee, *Complementary information set codes over $GF(p)$*, Designs Codes Crypt. **81** (2016), 541–555.

[12] H. J. Kim and Y. Lee, *t-CIS codes over $GF(p)$ and orthogonal arrays*, Discrete Applied Mathematics **217** (2017), 601–612.

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

[14] J.-L. Kim and Y. Lee, *Euclidean and Hermitian self-dual MDS codes over large finite fields*, J. Combin. Theory Ser. A **105** (1) (2004), 79–95.

[15] C.P. Schnorr, S. Vaudenay, *Black box cryptanalysis of hash networks based on multipermutations*, Advances in Cryptology, EUROCRYPT'94, Lecture Note in Computer Science 950, Springer Verlag (1995), 47–57.

[16] T. Siegenthaler, *Correlation-immunity of non-linear Combining functions for cryptographic applications*, IEEE Trans. Inform. Theory **30** (5) (1984), 776–780.

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