ARTICLE IN PRESS

Discrete Applied Mathematics ▪ (▪▪▪▪) ▪▪▪–▪▪▪

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

t-CIS codes over $GF(p)$ and orthogonal arrays

Hyun Jin Kim [a,*], Yoonjin Lee [b]

[a] University College, Yonsei University, 85 Songdogwahak-ro, Yeonsu-gu, Incheon 406-840, Republic of Korea

[b] Department of Mathematics, Ewha Womans University, 11-1 Daehyun-Dong, Seodaemun-Gu, Seoul, 120-750, Republic of Korea

ARTICLE INFO

Article history:
Received 23 February 2016
Received in revised form 28 July 2016
Accepted 13 September 2016
Available online xxxx

Keywords:
Optimal code
Complementary information set code
Correlation immune
Self-dual code
Equivalence
Orthogonal array

ABSTRACT

We first show that orthogonal arrays over $GF(p)$ can be explicitly constructed from t-CIS codes over $GF(p)$, where *t-CIS* codes are CIS codes of order $t \geq 2$. With this motivation, we are interested in developing methods of constructing t-CIS codes over $GF(p)$. We present two types of constructions; the first one is a "t-extension method" which is finding t-CIS codes over $GF(p)$ of length tn from given $(t-1)$-CIS codes over $GF(p)$ of length $(t-1)n$ for $t > 2$, and the second one is a "building-up type construction" which is finding t-CIS codes over $GF(p)$ of length $t(n+1)$ from given t-CIS codes over $GF(p)$ of length tn. Furthermore, we find a criterion for checking equivalence of t-CIS codes over $GF(p)$. We find inequivalent t-CIS codes over $GF(p)$ of length n for $t = 3, 4$, $n = 9, 12, 16$, and $p = 3, 5, 7$ using our construction and criterion, and corresponding orthogonal arrays are found. We point out that 171 t-CIS codes we found are *optimal* codes.

1. Introduction

Orthogonal arrays generalize the idea of mutually orthogonal latin squares in a tabular form. They have many connections to other combinatorial designs and have applications in the statistical design of experiments, cryptography and various types of software testing. Hence, they are essential in the study of statistics, computer science and cryptography, combinatorics, error-correcting codes and so forth. Some results on the case $d \geq 4$ and $q \geq 2$ can be found in [1,16,18,19]. Applications of these covering arrays and related structures to circuit testing, digital communication, network design, and etc. are discussed in [7,20]. We can also refer to [8,11] for known results regarding orthogonal arrays.

Orthogonal arrays are strongly connected to CIS codes. A *complementary information set code* (for short, *CIS* code) is defined to be a linear code with parameters $[2n, n, d]$ which has two disjoint information sets for a positive integer n. CIS codes include self-dual codes and formally self-dual codes which are very important classes of codes. A notion of CIS codes over $GF(2)$ is introduced by Carlet et al. [6]. The authors introduce CIS codes over $GF(p)$ and classify CIS codes over $GF(p)$ of small lengths, where p is 3, 5, and 7 in [15]. Furthermore, a notion of higher order CIS codes over $GF(2)$ is also developed by Carlet et al. [5].

In this paper, we show that orthogonal arrays over $GF(p)$ can be explicitly constructed from t-CIS codes over $GF(p)$, where *t-CIS* codes are CIS codes of order $t \geq 2$. In more detail, an orthogonal array over $GF(p)$ with parameters $OA(p^n, tn, p, d)$ is defined to be a set of p^n vectors over $GF(p)$ of length tn with the property that, in any d coordinate positions, all p^d possibilities occur exactly λ times, where $\lambda = p^{n-d}$. The number d is called the *strength* of the orthogonal array. From t-CIS codes over $GF(p)$, we can explicitly construct orthogonal arrays over $GF(p)$ with parameters $OA(p^n, tn, p, d)$ and $\lambda = p^{n-d}$,

* Corresponding author.
E-mail addresses: guswls41@yonsei.ac.kr (H.J. Kim), yoonjinl@ewha.ac.kr (Y. Lee).

http://dx.doi.org/10.1016/j.dam.2016.09.032
0166-218X/

where $p^n \times tn$ is the size of the array and d is its strength. With this motivation, we are interested in developing methods of constructing t-CIS codes over $GF(p)$.

We present two types of constructions; the first one is a "t-extension method" which is finding t-CIS codes over $GF(p)$ of length tn from given $(t-1)$-CIS codes over $GF(p)$ of length $(t-1)n$ for $t > 2$. The second one is a "building-up type construction" which is finding t-CIS codes over $GF(p)$ of length $t(n+1)$ from given t-CIS codes over $GF(p)$ of length tn; in fact, any t-CIS code over $GF(p)$ of length $t(n+1)$ can be obtained from some t-CIS code of length tn by this construction up to equivalence. Furthermore, we find a criterion for checking equivalence of t-CIS codes over $GF(p)$. We find inequivalent t-CIS codes over $GF(p)$ of length n for $t = 3, 4$, $n = 9, 12, 16$, and $p = 3, 5, 7$ using our construction and criterion, and corresponding orthogonal arrays are found. We point out that 171 t-CIS codes we found are optimal codes.

This paper is organized as follows. We introduce t-CIS codes over $GF(p)$ and orthogonal arrays in Section 2. In Section 3, we discuss a direct connection between t-CIS codes and orthogonal arrays over $GF(p)$. Section 4 presents two construction methods t-CIS codes, and we show implementation results of t-CIS codes over $GF(p)$ of length n for $t = 3, 4$, $n = 9, 12, 16$, and $p = 3, 5, 7$ with corresponding orthogonal arrays. All computations are done using MAGMA [4].

2. Preliminaries

Let $\mathcal{C}$ be a linear code over $GF(p)$. A code $\mathcal{C}$ is *self-dual* if $\mathcal{C} = \mathcal{C}^{\perp}$, where $\mathcal{C}^{\perp}$ denotes the dual code of $\mathcal{C}$ defined with respect to the standard inner product. 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 $|I|$ in $\mathcal{C}$ occurs in exactly one codeword within the specified coordinates x_i for $i \in I$. We note that a CIS (unrestricted) code is a systematic code which admits two complementary information sets. In fact, every non-trivial linear code is systematic in this sense. Furthermore, a generator matrix of $[tn, n]$ code is said to be in *systematic form* if it can be written as $(I_n \mid A)$, with I_n the identity matrix of order n.

Definition 2.1. A t-CIS code is a systematic code of length tn which admits t pairwise disjoint information sets.

We define the *Hamming weight* $wt(z)$ of a vector z to be the number of its nonzero entries. A *monomial matrix* is a matrix on a field with exactly one nonzero entry per row and per column. We say that two codes $\mathcal{C}$ and $\mathcal{C}'$ over $GF(p)$ are *monomially equivalent* (simply, called equivalent in this paper) if there is some monomial matrix M over $GF(p)$ such that $\mathcal{C}' = \mathcal{C}M = \{cM \mid c \in \mathcal{C}\}$. The set of monomial matrices M with $\mathcal{C} = \mathcal{C}M$ is called the *monomial automorphism group* of $\mathcal{C}$, and it is denoted by $\mathrm{Aut}(\mathcal{C})$.

Definition 2.2. An orthogonal array A of size m, n constraints, strength d and index λ over $GF(p)$ (or with q levels) is an $m \times n$ array of which rows are the vectors from a subset M of $GF(p)^n$ such that $|M| = m$ which has the property that in any subset of d columns of A, each of the p^d vectors of $GF(p)^d$ appears exactly λ times as a row. Such an array is denoted by $OA(m, n, p, d)$. Clearly $m = \lambda p^d$.

The binary version of the following lemma is given in [6], and this lemma holds for CIS codes over $GF(p)$ for every prime p as well.

Lemma 2.3. *If a $[2n, n]$ code $\mathcal{C}$ over $GF(p)$ 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.*

3. Motivation: orthogonal arrays arising from t-CIS codes

In this section, we discuss a direct connection between t-CIS codes over $GF(p)$ and orthogonal arrays $GF(p)$. Throughout this paper, ζ_p is a primitive pth root of unity in $\mathbb{C}$.

We know that the homomorphisms from the Abelian group $\mathcal{F}$ into the multiplicative group of $\mathbb{C}$ form an Abelian group $\mathcal{F}'$, called the *character group*, which is isomorphic with $\mathcal{F}$. For $x \in \mathcal{F}$ and $y \in \mathcal{F}'$ we denote by $\langle x, y \rangle$ the complex image of x under the character y. (Refer to [3] for more details.)

For example, if $\mathcal{F}$ is the additive group $(GF(p), +)$ of the finite field $GF(q)$, where $q = p^s$ and p a prime, then $\langle \mathbf{x}, \mathbf{y} \rangle = \zeta_p^{\mathbf{x} \cdot \mathbf{y}}$.

Let $\mathcal{F}$ be an Abelian group. The nth Cartesian power $G = \mathcal{F}^n$ is then an Abelian group in its turn. Let G' be the character group which is isomorphic with G. The following is a characterization of orthogonal arrays of strength d in terms of Fourier transform over $GF(p)$ [9], and this result is also used in [3] for studying correlation-immune functions.

Proposition 3.1 ([9, Theorem 4.4]). *The array consisting of a set $M \subset G$ of λp^d rows is orthogonal with n constraints, p levels, strength d and index λ if and only if*

$$\forall \mathbf{y} \in G',\ 1 \le wt(\mathbf{y}) \le d, \quad \sum_{\mathbf{x} \in M} \langle \mathbf{x}, \mathbf{y} \rangle = 0.$$