Available online: September 12, 2018

Commun. Fac. Sci. Univ. Ank. Ser. A1 Math. Stat.
Volume 68, Number 1, Pages 672–685 (2019)
DOI: 10.31801/cfsuasmas.459971
ISSN 1303–5991 E-ISSN 2618-6470
http://communications.science.ankara.edu.tr/index.php?series=A1

# $k$-AUTOCORRELATION AND ITS APPLICATIONS

HAYRULLAH ÖZİMAMOĞLU, MURAT ŞAHIN, AND OKTAY ÖLMEZ

Abstract. The standard autocorrelation measures similarities between a binary sequence and its any shifted form. In this paper, we introduce the concept of the $k$-autocorrelation of a binary sequence as a generalization of the standard autocorrelation. We give two applications of the $k$-autocorrelation. The first one is related the additive circulant codes over $\mathbb{F}_4$ in coding theory. We use the $k$-autocorrelation to determine the minimum distance of additive circulant codes over $\mathbb{F}_4$. The second one is related the $(7,3,1)$-BIBD in design theory. The $k$-autocorrelation coefficients give us information about the lines in the $(7,3,1)$-BIBD.

## 1. Introduction

Autocorrelation is used to measure similarities between a sequence and its shifted forms. It has applications in communication systems and cryptography. Let $\boldsymbol{a} = (a_0, a_1, a_2, \ldots, a_{n-1})$ be a binary sequence and $\boldsymbol{a_\tau} = (a_{-\tau}, a_{1-\tau}, a_{2-\tau}, \ldots, a_{n-1-\tau})$ be its shifted forms for $\tau = 1, 2, \cdots, n-1$. In this paper, indices of all sequences are in *modulo* $n$. The *standard autocorrelation* of the sequences $\boldsymbol{a}$ and $\boldsymbol{a_\tau}$ is defined by

$$c_\tau(\boldsymbol{a}) = \sum_{i=0}^{n-1} (-1)^{a_i + a_{i-\tau}}.$$

$\{c_\tau(\boldsymbol{a})\}_{\tau=0}^{n-1}$ sequence is called *autocorrelation coefficients*.

In this study, we introduce $k$-autocorrelation for a binary sequence and its $k-1$ shifted forms. This concept is the generalization of standard autocorrelation. For given $\tau_1, \tau_2, \ldots, \tau_{k-1} \in \mathbb{Z}$ such that $1 \le \tau_1 < \tau_2 < \cdots < \tau_{k-1} \le n-1$, we define *k-autocorrelation* of the sequence $\boldsymbol{a}$ as follows:

$$c_{\tau_1,\tau_2,\ldots,\tau_{k-1}}(\boldsymbol{a}) = \sum_{i=0}^{n-1} (-1)^{a_i + a_{i-\tau_1} + a_{i-\tau_2} + \cdots + a_{i-\tau_{k-1}}},$$

Received by the editors: December 12, 2017; Accepted: March 27, 2018.
2010 *Mathematics Subject Classification.* Primary 62H20, 94B60; Secondary 94B05, 05B05.
*Key words and phrases.* Autocorrelation, additive circulant codes, Fano plane.

where

$$\begin{aligned} \boldsymbol{a} &= (a_0, a_1, a_2, \ldots, a_{n-1}), \\ \boldsymbol{a_{\tau_1}} &= (a_{-\tau_1}, a_{1-\tau_1}, a_{2-\tau_1}, \ldots, a_{n-1-\tau_1}), \\ &\vdots \\ \boldsymbol{a_{\tau_{k-1}}} &= (a_{-\tau_{k-1}}, a_{1-\tau_{k-1}}, a_{2-\tau_{k-1}}, \ldots, a_{n-1-\tau_{k-1}}), \end{aligned}$$

for any $k = 2, 3, \ldots, n$. The sequence $\{c_{\tau_1,\tau_2,\ldots,\tau_{k-1}}(\boldsymbol{a})\}$ is called *$k$-autocorrelation coefficients*. If we take $k = 2$, then we get the standard autocorrelation. Moreover, we call

$$\boldsymbol{s} = \boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}} + \ldots + \boldsymbol{a_{\tau_{k-1}}}$$

*total shift sequence* for any binary sequence $\boldsymbol{a}$, the $k$-autocorrelation measures the similarity between the sequence $\boldsymbol{a}$ and the total shift sequence $\boldsymbol{s}$.

For example, we calculate the standard autocorrelation and the 3-autocorrelation for the sequence $\boldsymbol{a} = (0, 0, 1, 0, 1, 1)$ in Table 1 and Table 2, respectively.

TABLE 1.

| $\tau$ | $\boldsymbol{a_\tau}$ | $c_\tau(\boldsymbol{a})$ |
|---|---|---|
| 1 | $(1,0,0,1,0,1)$ | $-2$ |
| 2 | $(1,1,0,0,1,0)$ | $-2$ |
| 3 | $(0,1,1,0,0,1)$ | $2$ |
| 4 | $(1,0,1,1,0,0)$ | $-2$ |
| 5 | $(0,1,0,1,1,0)$ | $-2$ |

TABLE 2.

| $\tau_1,\ \tau_2$ | $c_{\tau_1,\tau_2}(\boldsymbol{a})$ |
|---|---|
| $\tau_1 = 1,\ \tau_2 = 2$ | 0 |
| $\tau_1 = 1,\ \tau_2 = 3$ | $-4$ |
| $\tau_1 = 1,\ \tau_2 = 4$ | 4 |
| $\tau_1 = 1,\ \tau_2 = 5$ | 0 |
| $\tau_1 = 2,\ \tau_2 = 3$ | 4 |
| $\tau_1 = 2,\ \tau_2 = 4$ | 0 |
| $\tau_1 = 2,\ \tau_2 = 5$ | $-4$ |
| $\tau_1 = 3,\ \tau_2 = 4$ | $-4$ |
| $\tau_1 = 3,\ \tau_2 = 5$ | 4 |
| $\tau_1 = 4,\ \tau_2 = 5$ | 0 |

This paper is organized as follows: In Section 2, we give basic definitions and theorems. In Section 3, we determine the minimum distance of additive circulant codes over $\mathbb{F}_4$ by the $k$-autocorrelation. In Section 4, we would like to motivate our definition by providing an example related to design theory. In this specific example, we explain the relation between $k$-autocorrelation values of a sequence and corresponding lines in the $(7,3,1)$-BIBD.

## 2. Preliminaries

The Hamming weight of $u \in \mathbb{F}_q^n$, denoted $wt(u)$, is the number of nonzero components of $u$. The Hamming distance between $u$ and $v$, denoted $d(u,v)$, is $wt(u-v)$. We assume that the binary sequence $\boldsymbol{a} = (a_0, a_1, a_2, \ldots, a_{n-1})$ is a vector in $\mathbb{F}_2^n$. There is a relation between the standard autocorrelation $c_\tau(\boldsymbol{a})$ and the Hamming distance $d(\boldsymbol{a}, \boldsymbol{a_\tau})$. It is given in the next lemma.

**Lemma 1.** *For any binary sequence* $\boldsymbol{a} = (a_0, a_1, a_2, \ldots, a_{n-1})$ *of length* $n$*,*

$$c_\tau(\boldsymbol{a}) = n - 2d(\boldsymbol{a}, \boldsymbol{a_\tau}),$$

*where* $\boldsymbol{a_\tau}$ *is the shifted form of the sequence* $\boldsymbol{a}$ [2].

Since $d(\boldsymbol{a}, \boldsymbol{a_\tau}) = wt(\boldsymbol{a}+\boldsymbol{a_\tau})$ for any binary sequence $\boldsymbol{a}$, then we have the following corollary.

**Corollary 2.** *For any binary sequence* $\boldsymbol{a} = (a_0, a_1, a_2, \ldots, a_{n-1})$ *of length* $n$*,*

$$2wt(\boldsymbol{a} + \boldsymbol{a_\tau}) + c_\tau(\boldsymbol{a}) = n,$$

*where* $\boldsymbol{a_\tau}$ *is the shifted form of the sequence* $\boldsymbol{a}$*.*

We generalize Corollary 2 in the next theorem.

**Theorem 3.** *For any binary sequence* $\boldsymbol{a} = (a_0, a_1, a_2, \ldots, a_{n-1})$ *of length* $n$*, and for any* $k = 2, 3, \ldots, n$*, we have*

$$2wt(\boldsymbol{a} + \boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}} + \cdots + \boldsymbol{a_{\tau_{k-1}}}) + c_{\tau_1,\tau_2,\ldots,\tau_{k-1}}(\boldsymbol{a}) = n,$$

*where* $\boldsymbol{a_{\tau_j}}$ *are the shifted forms of the sequence* $\boldsymbol{a}$ *for* $j = 1, 2, \ldots, k-1$*.*

*Proof.* Let

$$(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) = \boldsymbol{a} + \boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}} + \cdots + \boldsymbol{a_{\tau_{k-1}}},$$

where

$$\alpha_i = \begin{cases} 0, & if \ a_i + a_{i-\tau_1} + a_{i-\tau_2} + \cdots + a_{i-\tau_{k-1}} \equiv 0 \pmod 2, \\ 1, & if \ a_i + a_{i-\tau_1} + a_{i-\tau_2} + \cdots + a_{i-\tau_{k-1}} \equiv 1 \pmod 2, \end{cases} \tag{1}$$

for $i = 0, 1, \ldots, n-1$. Moreover,

$$wt(\boldsymbol{a} + \boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}} + \cdots + \boldsymbol{a_{\tau_{k-1}}}) = \sum_{i=0}^{n-1} \alpha_i. \tag{2}$$

Let $\beta_i = (-1)^{a_i + a_{i-\tau_1} + a_{i-\tau_2} + \cdots + a_{i-\tau_{k-1}}}$, for $i = 0, 1, \ldots, n-1$, then we have

$$\beta_i = \begin{cases} 1, & if \ a_i + a_{i-\tau_1} + a_{i-\tau_2} + \cdots + a_{i-\tau_{k-1}} \equiv 0 \pmod 2, \\ -1, & if \ a_i + a_{i-\tau_1} + a_{i-\tau_2} + \cdots + a_{i-\tau_{k-1}} \equiv 1 \pmod 2, \end{cases} \tag{3}$$

for $i = 0, 1, \ldots, n-1$. As a result, by (1) , (2) and (3), we obtain

$$\begin{aligned} 2wt(\boldsymbol{a} + \boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}} + \cdots + \boldsymbol{a_{\tau_{k-1}}}) + c_{\tau_1, \tau_2, \ldots, \tau_{k-1}}(\boldsymbol{a}) &= \sum_{i=0}^{n-1} 2\alpha_i + \sum_{i=0}^{n-1} \beta_i \\ &= \sum_{i=0}^{n-1} (2\alpha_i + \beta_i) \\ &= \sum_{i=0}^{n-1} 1 \\ &= n. \end{aligned}$$

□

For $x, y \in \mathbb{F}_2^n$ , let $z = x \cap y \in \mathbb{F}_2^n$ such that

$$z_i = \begin{cases} 1, & if\ x_i = y_i = 1, \\ 0, & otherwise, \end{cases} \tag{4}$$

for $i = 0, 1, \ldots, n-1$. Then, we have Theorem 1.4.3 in [3] as follows:

$$wt(x + y) = wt(x) + wt(y) - 2wt(x \cap y). \tag{5}$$

A linear code $C$ of length $n$ over $\mathbb{F}_q$ is a $k$ dimensional subspace of $\mathbb{F}_q^n$ ,denoted $[n, k]$, and the vectors in $C$ are codewords of $C$. Specially, codes over $\mathbb{F}_2$ are called binary codes. The *minimum distance* $d$ of the linear code $C$ is the smallest Hamming distance between distinct codewords. For the linear code $C$, the minimum distance $d$ is the same the minimum Hamming weight of the nonzero codewords of $C$. A *generator matrix* for the linear $[n, k]$ code $C$ is any $k \times n$ matrix $G$ whose rows form a basis for $C$. The generator matrix of the form $[I_k|A]$, where $I_k$ is the $k \times k$ identity matrix, is said to be in standard form. There is the $(n-k) \times n$ matrix $H$, called a *parity check matrix* for the $[n, k]$ code $C$, defined by

$$C = \left\{ c \in \mathbb{F}_q^n \left| Hc^T = 0 \right. \right\}.$$

If $G = [I_k\,|A]$ is a generator matrix for the $[n, k]$ code $C$ in standard form, then $H = \left[-A^T\,|I_{n-k}\right]$ is a parity check matrix for $C$ (Theorem 1.2.1 in [3]).

The minimum distance $d$ of a linear code $C$ is related to a parity-check matrix of $C$. Any $d-1$ columns of $H$ are linearly independent and $H$ has $d$ columns that are linearly dependent if and only if $C$ has minimum distance $d$ (Corollary 4.5.7 in [4]).

Two linear codes $C_1$ and $C_2$ are permutation equivalent provided there is a permutation of coordinates which sends $C_1$ to $C_2$. Thus, $C_1$ and $C_2$ are permutation equivalent provided there is a permutation matrix $P$ such that $G_1$ is a generator matrix of $C_1$ if and only if $G_1P$ is a generator matrix of $C_2$. Then, if two linear codes $C_1$ and $C_2$ are permutation equivalent, the minimum distance of these codes are the same.

Let $B = \{b_1, b_2, \ldots, b_p\}$ be any binary column set of the same length and $1 \leq q \leq p$. We define

$$\alpha_B = \sum_{j=1}^{q} b_{i_j}$$

for $1 \leq i_j \leq p$. Note that $\alpha_B$ contain all linear combinations of the set $B$.

**Theorem 4.** *Let $G_{n\times 3n} = [I_{n\times n} : A_{n\times 2n}]$ be the generator matrix in the standard form of the binary $[3n, n]$ code $C$, and*

$$H_{2n\times 3n} = [A^T_{n\times 2n} : I_{2n\times 2n}] = [x_1 \ x_2 \ \cdots x_n : I_{2n\times 2n}],$$

*be the parity check matrix of the $C$, where $x_i$ is a binary column in the matrix $A^T$, and $wt(x_i) = m$ for $1 \leq i \leq n$.*

*Let $S$ be any binary column set in the matrix $A^T$, and $1 \leq s \leq n$. We denote*

$$\alpha_S = \sum_{j=1}^{s} x_{i_j}$$

*for $1 \leq i_j \leq n$. Then, $wt(\alpha_S) \geq m - s + 1$ for all $1 \leq s \leq n$ if and only if the minimum distance $d$ of the code $C$ is $m + 1$.*

*Proof.* $(\Rightarrow)$ : We choose a column $x_i$ in the matrix $A^T$ for any $1 \leq i \leq n$. Let $e_{i_j}$ be a column in the identity matrix $I_{2n\times 2n}$ for any $1 \leq i_j \leq 2n$. Since $wt\,(x_i) = m$, there is a column set $\{e_{i_1}, e_{i_2}, \ldots, e_{i_m}\}$ in the matrix $I_{2n\times 2n}$ such that

$$x_i = e_{i_1} + e_{i_2} + \cdots + e_{i_m}.$$

The set $\{x_i, e_{i_1}, e_{i_2}, \ldots, e_{i_m}\}$ with $m + 1$ elements is linearly dependent. Then, we need to show that any column set with $m$ elements in the parity check matrix $H$ is linearly independent.

(i) Let $S$ be any column set with $m$ elements in the matrix $A^T$ and $1 \leq s \leq m$. $\alpha_S = x_{i_1} + x_{i_2} + \ldots + x_{i_s}$ is any linear combination of the columns in the set $S$ for $1 \leq i_j \leq n$. Since by hypothesis

$$\begin{aligned} wt(\alpha_S) &\geq m - s + 1 \\ &\geq 1, \end{aligned}$$

$\alpha_S$ isn't equal to zero vector. Then the set $S$ is linearly independent.

(ii) Let $T$ be any column set with $m$ elements in the matrix $I_{2n\times 2n}$ and $1 \leq t \leq m$. $\alpha_T = e_{i_1} + e_{i_2} + \ldots + e_{i_t}$ is any linear combination of the columns in the set $T$ for $1 \leq i_j \leq n$. Since $wt(\alpha_T) = t \neq 0$, $\alpha_T$ isn't equal to zero vector. Hence the set $T$ is linearly independent.

(iii) Let $S$ be any column set with $s$ elements in the matrix $A^T$, $T$ be any column set with $t$ elements in the matrix $I_{2n\times 2n}$, $1 \leq s, t < m$ and $s + t = m$. We have

$$\begin{aligned} \alpha_{S\cup T} &= x_{i_1} + x_{i_2} + \ldots + x_{i_s} + e_{i_1} + e_{i_2} + \ldots + e_{i_t} \\ &= \alpha_S + \alpha_T, \end{aligned}$$

for $1 \le i_j \le n$, and so $\alpha_S + \alpha_T$ is any linear combination of the columns in the set $S \cup T$ with $m$ elements.

Since $wt(\alpha_T) = t$, by the definition in (4) we have

$$wt(\alpha_S \cap \alpha_T) \le t. \tag{6}$$

Since by hypothesis, (5) and (6),

$$\begin{aligned} wt(\alpha_S + \alpha_T) &= wt(\alpha_S) + wt(\alpha_T) - 2wt(\alpha_S \cap \alpha_T) \\ &\ge m - s + 1 + t - 2t \\ &= 1, \end{aligned}$$

$\alpha_S + \alpha_T$ isn't equal to zero vector. Then the set $S \cup T$ is linearly independent.

$(\Leftarrow)$ : Let $S$ be any column set in the matrix $A^T$, and $1 \le s \le n$. $\alpha_S = x_{i_1} + x_{i_2} + \ldots + x_{i_s}$ is any linear combination of the columns in the set $S$ for $1 \le i_j \le n$. Assume that for any $1 \le s \le n$ ,

$$wt(\alpha_S) < m - s + 1 \tag{7}$$

Let $r_{i_j} = [e_{i_j} : x_{i_j}]$ be a row of the generator matrix $G$, where $e_{i_j}$ is a row in the identity matrix $I_{n\times n}$, and $x_{i_j}$ is a row in the matrix $A_{n\times 2n}$ for any $1 \le i_j \le n$. By (7), we have

$$\begin{aligned} wt(r_{i_1} + r_{i_2} + \cdots + r_{i_s}) &< s + m - s + 1 \\ &= m + 1, \end{aligned}$$

and this is contrary to the fact that the minimum distance of the code $C$ is $m + 1$. Then the proof is completed.

□

## 3. Finding minimum distance of the additive circulant codes over $\mathbb{F}_4$

Given a finite field $\mathbb{F}$ and a subfield $\mathbb{K} \subseteq \mathbb{F}$ such that $[\mathbb{F} : \mathbb{K}] = e$, a $\mathbb{K}$-linear subset $C \subseteq \mathbb{F}^n$ is called $\mathbb{F}/\mathbb{K}$-*additive code* (Definition 1 in [6]). We denote $\mathbb{F}_4 = \{0, 1, w, w^2\}$, where $w^2 = w + 1$. An *additive code* $C$ over $\mathbb{F}_4$ of length $n$ is additive subgroup of $\mathbb{F}_4^n$. $C$ contains $2^k$ codewords for some $0 \le k \le 2n$, and can be defined by a $k \times n$ generator matrix with entries from $\mathbb{F}_4$, whose rows span $C$ additively. $C$ is called an $(n, 2^k)$ code. The *minimum distance* $d$ of the code $C$ is the minimal Hamming distance between any two distinct codewords of $C$. Since $C$ is an additive code, the minimum distance is also given by the smallest nonzero weight of any codeword in $C$.

An additive $(n, 2^n)$ code $C$ over $\mathbb{F}_4$ with generator matrix

$$G = \begin{bmatrix} w & g_1 & g_2 & \cdots & g_{n-1} \\ g_{n-1} & w & g_1 & \cdots & g_{n-2} \\ g_{n-2} & g_{n-1} & w & \cdots & g_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_1 & g_2 & g_3 & \cdots & w \end{bmatrix}_{n\times n}$$

is called *additive circulant code*, where $g_i \in \{0,1\} \subseteq \mathbb{F}_4$ for $i = 1, 2, \ldots, n-1$. The vector $g = (w, g_1, g_2, \ldots, g_{n-1})$ is called *generator vector* for the code $C$ [1].

The additive $(n, 2^k)$ code $C$ over $\mathbb{F}_4$ is transformed into a $[3n, k]$ binary code by the isometric embedding technique. There is a relation between the minimum distances of these two codes as follows:

**Lemma 5.** ***(Isometric Embedding Technique)*** *The isometric monomorphism is given by* $\sigma : \mathbb{F}_4 \longrightarrow \mathbb{F}_2^3,\ 0 \longrightarrow (0,0,0),\ 1 \longrightarrow (1,1,0),\ w \longrightarrow (1,0,1),\ w^2 \longrightarrow (0,1,1)$. *The minimum distance of an additive code $C$ over $\mathbb{F}_4$ is given by*

$$d(C) = \frac{d(\sigma(C))}{2}$$

[6].

Let

$$g = (w, g_1, g_2, \ldots, g_{n-1}) \tag{8}$$

be the generator vector of an additive circulant code $C$ with length $n$ over $\mathbb{F}_4$, where $g_i \in \{0,1\} \subseteq \mathbb{F}_4$ for $i = 1, 2, \ldots, n-1$. Now we construct a binary sequence by the vector $g$ as follows:

We apply the map $\phi : \mathbb{F}_4 \longrightarrow \mathbb{F}_2^2,\ 0 \longrightarrow (0,0),\ 1 \longrightarrow (1,1),\ w \longrightarrow (1,0),\ w^2 \longrightarrow (0,1)$ to the coordinates of the generator vector $g$, and so we define the binary sequence

$$\boldsymbol{a} = (\phi(w), \phi(g_1), \phi(g_2), \ldots, \phi(g_{n-1})). \tag{9}$$

Note that the length of the sequence $\boldsymbol{a}$ is $2n$, and

$$wt(a) \quad = \quad 2wt(g) - 1 \tag{10}$$

We determine whether the minimum distance of additive circulant code $C$ over $\mathbb{F}_4$ is $wt(g)$.

**Lemma 6.** *Let $g$ be defined in (8), and $\boldsymbol{a}$ be defined in (9). For even integers $\tau_i$ such that $2 \leq \tau_1 < \tau_2 < \ldots < \tau_{k-1} \leq 2n-2$, we have $wt(\boldsymbol{a} + \boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}} + \ldots + \boldsymbol{a_{\tau_{k-1}}}) \geq k$.*

*Proof.* Let $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3 \ldots, \alpha_{2n-2}, \alpha_{2n-1}) = \boldsymbol{a} + \boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}} + \cdots + \boldsymbol{a_{\tau_{k-1}}}$. Since $\phi(w) = (1,0)$ and $\phi(g_i) = (0,0)$ or $(1,1)$ for $i = 1, 2, \ldots, n-1$, there are exactly $k$ pair $(\alpha_j, \alpha_{j+1}) = (1,0)$ or $(0,1)$ for some $j = 0, 2, \ldots, 2n-2$ in the vector $\alpha$. Then, we have $wt(\alpha) \geq k$. $\square$

**Lemma 7.** *Let $g$ be defined in (8), and $\boldsymbol{a}$ be defined in (9). For even integers $\tau_i$ such that $2 \leq \tau_1 < \tau_2 < \ldots < \tau_{k-1} \leq 2n-2$, if $k \geq wt(g)$, we have $c_{\tau_1,\tau_2,\ldots,\tau_{k-1}}(\boldsymbol{a}) \leq s_k$, where $s_k = 2n - 2wt(\boldsymbol{a}) + 2k - 2$.*

*Proof.* By hypothesis and (10),

$$k \geq wt(g) \quad \Rightarrow \quad -2k \leq -wt(\boldsymbol{a}) - 1 \tag{11}$$

$$\Rightarrow \quad 0 \leq 2k - wt(\boldsymbol{a}) - 1, \tag{12}$$

and since $wt(\boldsymbol{a} + \boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}} + \ldots + \boldsymbol{a_{\tau_{k-1}}}) \geq k$ by Lemma 6, we get

$$-2wt(\boldsymbol{a} + \boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}} + \ldots + \boldsymbol{a_{\tau_{k-1}}}) \leq -2k. \tag{13}$$

By Theorem 3, (11), (12) and (13), we obtain

$$\begin{aligned} c_{\tau_1,\tau_2,\ldots,\tau_{k-1}}(\boldsymbol{a}) &= 2n - 2wt(\boldsymbol{a} + \boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}} + \ldots + \boldsymbol{a_{\tau_{k-1}}}) \\ &\leq 2n - 2k \\ &\leq 2n - wt(\boldsymbol{a}) - 1 \\ &\leq (2n - wt(\boldsymbol{a}) - 1) + (2k - wt(\boldsymbol{a}) - 1) \\ &= s_k. \end{aligned}$$

□

**Theorem 8.** *Let $g$ be defined in (8), and $\boldsymbol{a}$ be defined in (9). For even integers $\tau_i$ such that $2 \leq \tau_1 < \tau_2 < \ldots < \tau_{k-1} \leq 2n-2$, if for all $k = 2, 3, \ldots, wt(g) - 1$*

$$c_{\tau_1,\tau_2,\ldots,\tau_{k-1}}(\boldsymbol{a}) \leq s_k,$$

*where $s_k = 2n - 2wt(\boldsymbol{a}) + 2k - 2$, the minimum distance $d$ of the additive circulant code $C$ over $\mathbb{F}_4$ is equal to $wt(g)$ , otherwise the minimum distance $d$ isn't equal to $wt(g)$.*

*Proof.* Let $G_1$ be a generator $n \times n$ matrix of the additive circulant code $C$. If we apply the map $\sigma$ in Lemma 5 to $G_1$, we have a $n \times 3n$ matrix $G_2$. Let $\sigma(C)$ be the generated code with matrix $G_2$. If we apply one permutation to columns of the matrix $G_2$, so we can obtain the generator matrix in the standard form

$$G_3 = \begin{bmatrix} & \boldsymbol{a} \\ & \boldsymbol{a_2} \\ I_{n\times n} & \boldsymbol{a_4} \\ & \vdots \\ & \boldsymbol{a_{2n-2}} \end{bmatrix}.$$

Since the generated codes by $G_2$ and $G_3$ are equivalent, the minimum distances $d(\sigma(C))$ of these codes are the same. The parity check matrix of the generated code by $G_3$ is

$$H_3 = \begin{bmatrix} \boldsymbol{a} & \boldsymbol{a_2} & \boldsymbol{a_4} & \cdots & \boldsymbol{a_{2n-2}} & : I_{2n\times 2n} \end{bmatrix}, \; wt(\boldsymbol{a_{\tau_i}}) = wt(\boldsymbol{a}).$$

If $k = 1$, we have

$$wt(\boldsymbol{a_{\tau_i}}) = wt(\boldsymbol{a}) - k + 1. \tag{14}$$

By Lemma 7, if $k \geq wt(g)$,

$$c_{\tau_1,\tau_2,\ldots,\tau_{k-1}}(\boldsymbol{a}) \leq s_k, \tag{15}$$

and by hypothesis, for all $k = 2, 3, \ldots, wt(g) - 1$

$$c_{\tau_1,\tau_2,\ldots,\tau_{k-1}}(\boldsymbol{a}) \leq s_k. \tag{16}$$

Since by Theorem 3, (15) and (16), for all $k = 2, 3, \ldots, n$,

$$\begin{aligned} c_{\tau_1,\tau_2,\ldots,\tau_{k-1}}(\boldsymbol{a}) &= 2n - 2wt(\boldsymbol{a} + \boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}} + \ldots + \boldsymbol{a_{\tau_{k-1}}}) \\ &\leq 2n - 2wt(\boldsymbol{a}) + 2k - 2, \end{aligned}$$

we have

$$wt(\boldsymbol{a} + \boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}} + \ldots + \boldsymbol{a_{\tau_{k-1}}}) \geq wt(\boldsymbol{a}) - k + 1. \tag{17}$$

Since for all $k = 1, 2, \ldots, n$,

$$wt(\boldsymbol{a} + \boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}} + \ldots + \boldsymbol{a_{\tau_{k-1}}}) \geq wt(\boldsymbol{a}) - k + 1 \tag{18}$$

by (14) and (17), and so by Theorem 4 , $d(\sigma(C)) = wt(\boldsymbol{a}) + 1$. Then by Lemma 5 and (10), the minimum distance $d$ of the code $C$ is equal to

$$d(C) = \frac{wt(\boldsymbol{a}) + 1}{2} = wt(g).$$

Assume that for $\exists k = 2, 3, \ldots, wt(g) - 1$, $c_{\tau_1,\tau_2,\ldots,\tau_{k-1}}(\boldsymbol{a}) > s_k$. Since by Theorem 3

$$\begin{aligned} c_{\tau_1,\tau_2,\ldots,\tau_{k-1}}(\boldsymbol{a}) &= 2n - 2wt(\boldsymbol{a} + \boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}} + \ldots + \boldsymbol{a_{\tau_{k-1}}}) \\ &> 2n - 2wt(\boldsymbol{a}) + 2k - 2, \end{aligned}$$

we get

$$wt(\boldsymbol{a} + \boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}} + \ldots + \boldsymbol{a_{\tau_{k-1}}}) < wt(\boldsymbol{a}) - k + 1. \tag{19}$$

By Theorem 4 and (19), $d(\sigma(C)) \neq wt(\boldsymbol{a}) + 1$ and then by Lemma 5, the minimum distance $d(C)$ of the code $C$ isn't equal to $wt(g)$. □

**Example 9.** *Let $g = (w, 1, 1, 1, 0, 0)$ be a generator vector of the additive circulant code $C$ of length 6 over $\mathbb{F}_4$. So, the generator matrix of the code $C$ is*

$$G_1 = \begin{bmatrix} w & 1 & 1 & 1 & 0 & 0 \\ 0 & w & 1 & 1 & 1 & 0 \\ 0 & 0 & w & 1 & 1 & 1 \\ 1 & 0 & 0 & w & 1 & 1 \\ 1 & 1 & 0 & 0 & w & 1 \\ 1 & 1 & 1 & 0 & 0 & w \end{bmatrix}_{6\times 6}.$$

*Now we determine whether this code has a minimum distance of $wt(g) = 4$. If we apply the map $\sigma$ in Lemma 5 to the matrix $G_1$, we have the matrix*

$$G_2 = \begin{bmatrix} 1&0&1&1&1&0&1&1&0&1&1&0&0&0&0&0&0&0 \\ 0&0&0&1&0&1&1&1&0&1&1&0&1&1&0&0&0&0 \\ 0&0&0&0&0&0&1&0&1&1&1&0&1&1&0&1&1&0 \\ 1&1&0&0&0&0&0&0&0&1&0&1&1&1&0&1&1&0 \\ 1&1&0&1&1&0&0&0&0&0&0&0&1&0&1&1&1&0 \\ 1&1&0&1&1&0&1&1&0&0&0&0&0&0&0&1&0&1 \end{bmatrix}_{6\times 18}.$$

*If we apply the permutation $p$ to the columns of the matrix $G_2$, where*

$$p = \begin{pmatrix} 1&2&3&4&5&6&7&8&9&10&11&12&13&14&15&16&17&18 \\ 3&6&9&12&15&18&1&2&4&5&7&8&10&11&13&14&16&17 \end{pmatrix},$$

*we obtain the generator matrix in the standard form*

$$G_2 \simeq G_3 = \left[\begin{array}{c|cccccccccccc} & 1&0&1&1&1&1&1&1&0&0&0&0 \\ & 0&0&1&0&1&1&1&1&1&1&0&0 \\ I_{6\times 6} & 0&0&0&0&1&0&1&1&1&1&1&1 \\ & 1&1&0&0&0&0&1&0&1&1&1&1 \\ & 1&1&1&1&0&0&0&0&1&0&1&1 \\ & 1&1&1&1&1&1&0&0&0&0&1&0 \end{array}\right]_{6\times 18}.$$

*Then, the parity check matrix of generated code by the matrix $G_3$ is*

$$H_3 = \begin{bmatrix} \boldsymbol{a} & \boldsymbol{a_2} & \boldsymbol{a_4} & \boldsymbol{a_6} & \boldsymbol{a_8} & \boldsymbol{a_{10}} & : I_{12\times 12}\end{bmatrix} = \left[\begin{array}{cccccc|c} 1&0&0&1&1&1& \\ 0&0&0&1&1&1& \\ 1&1&0&0&1&1& \\ 1&0&0&0&1&1& \\ 1&1&1&0&0&1& \\ 1&1&0&0&0&1& \\ 1&1&1&1&0&0& I_{12\times 12} \\ 1&1&1&0&0&0& \\ 0&1&1&1&1&0& \\ 0&1&1&1&0&0& \\ 0&0&1&1&1&1& \\ 0&0&1&1&1&0& \end{array}\right]_{12\times 18}.$$

*In Table 3 , we calculate the 2-autocorrelation coefficients of the sequence*

$$\boldsymbol{a} = (\phi(w), \phi(1), \phi(1), \phi(1), \phi(0), \phi(0)) = (1,0,1,1,1,1,1,1,0,0,0,0).$$

*Hence, 2-autocorrelation coefficients of the sequence $\boldsymbol{a}$ are*

$$(c_2(\boldsymbol{a}), c_4(\boldsymbol{a}), c_6(\boldsymbol{a}), c_8(\boldsymbol{a}), c_{10}(\boldsymbol{a})) = (4, -4, -8, -4, 4).$$

*Since $s_2 = 0$ by Theorem 8, for $k = 2$, and $c_\tau(\boldsymbol{a}) > s_2$ for $\tau = 2, 10$, the minimum distance of the code $C$ isn't equal to 4.*

Table 3.

| $\tau$ | $\boldsymbol{a_\tau}$ | $c_\tau(\boldsymbol{a})$ |
|---|---|---|
| 2 | $(0,0,1,0,1,1,1,1,1,1,0,0)$ | 4 |
| 4 | $(0,0,0,0,1,0,1,1,1,1,1,1)$ | $-4$ |
| 6 | $(1,1,0,0,0,0,1,0,1,1,1,1)$ | $-8$ |
| 8 | $(1,1,1,1,0,0,0,0,1,0,1,1)$ | $-4$ |
| 10 | $(1,1,1,1,1,1,0,0,0,0,1,0)$ | 4 |

**Example 10.** *In Table 4 , we calculate the* 2*-autocorrelation coefficients of all the additive circulant codes of length* 6 *over* $\mathbb{F}_4$ *such that* $wt(g) = 4$.

Table 4.

| | ***The generator vectors*** | **2*-autocorrelation coefficients*** |
|---|---|---|
| ***1*** | $(w,1,1,1,0,0)$ | $(4,-4,-8,-4,4)$ |
| ***2*** | $(w,1,1,0,1,0)$ | $(-4,0,0,0,-4)$ |
| ***3*** | $(w,1,1,0,0,1)$ | $(0,-4,0,-4,0)$ |
| ***4*** | $(w,1,0,1,1,0)$ | $(-4,-4,8,-4,-4)$ |
| ***5*** | $(w,1,0,1,0,1)$ | $(-8,8,-8,8,-8)$ |
| ***6*** | $(w,1,0,0,1,1)$ | $(0,-4,0,-4,0)$ |
| ***7*** | $(w,0,1,1,1,0)$ | $(0,0,-8,0,0)$ |
| ***8*** | $(w,0,1,1,0,1)$ | $(-4,-4,8,-4,-4)$ |
| ***9*** | $(w,0,1,0,1,1)$ | $(-4,0,0,0,-4)$ |
| ***10*** | $(w,0,0,1,1,1)$ | $(4,-4,-8,-4,4)$ |

*In Table 4 , since* $c_\tau(\boldsymbol{a}) > s_2 = 0$ *for the codes in* 1, 4, 5, 8 *and* 10*, these codes haven't the minimum distance of* 4*. We calculate the* 3*-autocorrelation coefficients for remained codes in Table 5 .*

Table 5.

| | ***The generator vectors*** | **3*-autocorrelation coefficients*** |
|---|---|---|
| ***1*** | $(w,1,1,0,1,0)$ | $(2,6,-2,2,-2,-6,6,6,-2,2)$ |
| ***2*** | $(w,1,1,0,0,1)$ | $(-2,-2,6,-2,6,6,-2,-2,6,-2)$ |
| ***3*** | $(w,1,0,0,1,1)$ | $(-2,6,-2,-2,-2,6,6,6,-2,-2)$ |
| ***4*** | $(w,0,1,1,1,0)$ | $(2,2,2,2,2,-6,2,2,2,2)$ |
| ***5*** | $(w,0,1,0,1,1)$ | $(2,-2,6,2,6,-6,-2,-2,6,2)$ |

*For example,* 3*-autocorrelation coefficients are*

$$(c_{2,4}(\boldsymbol{a}), c_{2,6}(\boldsymbol{a}), c_{2,8}(\boldsymbol{a}), c_{2,10}(\boldsymbol{a}), c_{4,6}(\boldsymbol{a}), c_{4,8}(\boldsymbol{a}), c_{4,10}(\boldsymbol{a}), c_{6,8}(\boldsymbol{a}), c_{6,10}(\boldsymbol{a}), c_{8,10}(\boldsymbol{a})) \\ = (2,6,-2,2,-2,-6,6,6,-2,2)$$

*for the vector* $(w, 1, 1, 0, 1, 0)$ *in* 1. *Since by Theorem 8,* $c_{2,6}(\boldsymbol{a}), c_{4,10}(\boldsymbol{a}), c_{6,8}(\boldsymbol{a}) > s_3 = 2$*, the generated code by this vector hasn't the minimum distance of* 4. *As a result, since by Theorem 8,* $s_3 = 2$ *for* $k = 3$ *and* $c_{\tau_1,\tau_2}(\boldsymbol{a}) > 2$ *for the codes in the* 1, 2, 3 *and* 5, *the minimum distances of these codes aren't equal to* 4. *The generated code by the vector* $(w, 0, 1, 1, 1, 0)$ *in* 4 *have only the minimum distance of* 4.

## 4. Cases of the lines in the $(7, 3, 1)$-BIBD

Let $v, k$ and $\lambda$ be positive integers such that $v > k \geq 2$. A $(v, k, \lambda)$-balanced incomplete block design (which we abbreviate to $(v, k, \lambda)$-BIBD) is a design $(X, A)$ such that the following properties are satisfied:

(1) $|X| = v$,
(2) Each block contains exactly $k$ points,
(3) Every pair of distinct points is contained in exactly $\lambda$ blocks (Definition 1.2 in [5]).

Now, we can give $(7, 3, 1)$-BIBD. The $(7, 3, 1)$-BIBD is the set of points and blocks, respectively

$$\begin{aligned} X &= \{0, 1, 2, 3, 4, 5, 6\}, \\ A &= \{013, 124, 235, 346, 045, 156, 026\}. \end{aligned}$$

We denote the block $x_1x_2x_3 \in A$ by the binary sequence $\boldsymbol{a} = (a_0, a_1, a_2, a_3, a_4, a_5, a_6)$ such that

$$a_i = \begin{cases} 1, & if\ i \in \{x_1, x_2, x_3\}, \\ 0, & otherwise, \end{cases}$$

for $i = 0, 1, \ldots, 6$. The shifted forms of the sequence $\boldsymbol{a} = (1, 1, 0, 1, 0, 0, 0)$ corresponds the blocks of $(7, 3, 1)$-BIBD by this method. It is shown in Table 6.

Table 6.

| $\boldsymbol{\tau}$ | $\boldsymbol{a_\tau}$ | Blocks |
|---|---|---|
| 0 | $(1, 1, 0, 1, 0, 0, 0)$ | 013 |
| 1 | $(0, 1, 1, 0, 1, 0, 0)$ | 124 |
| 2 | $(0, 0, 1, 1, 0, 1, 0)$ | 235 |
| 3 | $(0, 0, 0, 1, 1, 0, 1)$ | 346 |
| 4 | $(1, 0, 0, 0, 1, 1, 0)$ | 045 |
| 5 | $(0, 1, 0, 0, 0, 1, 1)$ | 156 |
| 6 | $(1, 0, 1, 0, 0, 0, 1)$ | 026 |

The $(7, 3, 1)$-BIBD consists of seven points and seven blocks (lines). It is shown in Figure 1. The $k$-autocorrelation coefficients of the sequence $\boldsymbol{a}$ give us the information about intersections of these lines.

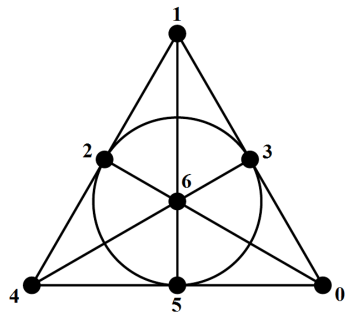


FIGURE 1. The Fano Plane: A $(7,3,1)$-BIBD

**Case 11.** ***$c_{\tau}(a) = -1$ means that the any two lines intersect in a unique point:***

*Since $c_{\tau}(\boldsymbol{a}) = -1$ by Corollary 2 and the equation (5), we have $wt(\boldsymbol{a} \cap \boldsymbol{a_{\tau}}) = 1$. Hence, any two lines intersect in a unique point.*

**Case 12.** *In Table 7 , we calculate the 3-autocorrelation coefficients of the sequence $\boldsymbol{a}$.*

TABLE 7.

| $\tau_1,\ \tau_2$ | $c_{\tau_1,\tau_2}(\boldsymbol{a})$ |
|---|---|
| $\tau_1 = 1,\ \tau_2 = 2$ | 1 |
| $\tau_1 = 1,\ \tau_2 = 3$ | 1 |
| $\tau_1 = 1,\ \tau_2 = 4$ | 1 |
| $\tau_1 = 1,\ \tau_2 = 5$ | $-7$ |
| $\tau_1 = 1,\ \tau_2 = 6$ | 1 |
| $\tau_1 = 2,\ \tau_2 = 3$ | $-7$ |
| $\tau_1 = 2,\ \tau_2 = 4$ | 1 |
| $\tau_1 = 2,\ \tau_2 = 5$ | 1 |
| $\tau_1 = 2,\ \tau_2 = 6$ | 1 |
| $\tau_1 = 3,\ \tau_2 = 4$ | 1 |
| $\tau_1 = 3,\ \tau_2 = 5$ | 1 |
| $\tau_1 = 3,\ \tau_2 = 6$ | 1 |
| $\tau_1 = 4,\ \tau_2 = 5$ | 1 |
| $\tau_1 = 4,\ \tau_2 = 6$ | $-7$ |
| $\tau_1 = 5,\ \tau_2 = 6$ | 1 |

(i) $\boldsymbol{c_{\tau_1,\tau_2}(a)} = 1$ ***means that any three lines don't intersect in any point:***

*Let* $c_{\tau_1,\tau_2}(\boldsymbol{a}) = 1$. *We can easily obtain* $wt(\boldsymbol{a} \cap (\boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}})) = 2$ *by Theorem 3 and the equation* (5). *Also, we get*

$$\begin{aligned} wt(\boldsymbol{a} \cap (\boldsymbol{a_{\tau_1}} + \boldsymbol{a_{\tau_2}})) &= |\boldsymbol{a} \cap \boldsymbol{a_{\tau_1}}| + |\boldsymbol{a} \cap \boldsymbol{a_{\tau_2}}| - 2|\boldsymbol{a} \cap \boldsymbol{a_{\tau_1}} \cap \boldsymbol{a_{\tau_2}}| \\ &= 1 + 1 - 2|\boldsymbol{a} \cap \boldsymbol{a_{\tau_1}} \cap \boldsymbol{a_{\tau_2}}| \end{aligned}$$

*and so* $|\boldsymbol{a} \cap \boldsymbol{a_{\tau_1}} \cap \boldsymbol{a_{\tau_2}}| = 0$. *Then the lines* $\boldsymbol{a}$, $\boldsymbol{a_{\tau_1}}$ *and* $\boldsymbol{a_{\tau_2}}$ *don't intersect in any point.*

(ii) $\boldsymbol{c_{\tau_1,\tau_2}(a) = -7}$ ***means that any three lines intersect in a unique point:***

*Let* $c_{\tau_1,\tau_2}(\boldsymbol{a}) = -7$. *Similarly in the (i), we have* $|\boldsymbol{a} \cap \boldsymbol{a_{\tau_1}} \cap \boldsymbol{a_{\tau_2}}| = 1$, *and so these lines intersect in a unique point.*

## References


[1] Danielsen, L.E. and Parker, M.G., Directed Graph Representation of Half-Rate Additive Codes over GF(4), *Des. Codes Cryptogr.*, 59(2011), 119-130.

[2] Hertel, D., Crosscorrelation Properties between Perfect Sequences, *Sequences and Their Applications-SETA*, 2004.

[3] Huffman, W.C. and Pless, V., Fundamentals of Error Correcting Codes, Cambridge University Press, 2003.

[4] Ling, S. and Xing, C., Coding Theory, U.K.:, Cambridge Univ. Press, 2004.

[5] Stinson, D.R., Combinatorial Designs:, Construction and Analysis, Springer, 2003.

[6] White, G. and Grassl, M., A New Minimum Weight Algorithm for Additive Codes, *International Symposium on Information Theory;* (2006), 1119-1123.



*Current address*: Hayrullah Özimamoğlu: Department of Mathematics, Faculty of Arts and Sciences, Nevşehir Haci Bektaş Veli University, Nevşehir, Turkey.

*E-mail address*: h.ozimamoglu@nevsehir.edu.tr

ORCID Address: http://orcid.org/0000-0001-7844-1840

*Current address*: Murat Şahin: Department of Mathematics, Faculty of Science, Ankara University, Ankara, Turkey.

*E-mail address*: msahin@ankara.edu.tr

ORCID Address: http://orcid.org/0000-0002-9480-0433

*Current address*: Oktay Ölmez: Department of Mathematics, Faculty of Science, Ankara University, Ankara, Turkey.

*E-mail address*: oolmez@ankara.edu.tr

ORCID Address: http://orcid.org/0000-0002-9130-0038