Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 9(4): 9091–9106.
DOI:10.3934/math.2024442
Received: 25 December 2023
Revised: 29 January 2024
Accepted: 20 February 2024
Published: 05 March 2024

Research article

A class of binary sequences with two-valued cross correlations

Jianying Rong[1], **Ting Li**[2,*], **Rui Hua**[2] **and Xuemei Wang**[2]

[1] Jiangsu Vocational College of Electronics and Information, Huai'an 223003, China
[2] School of Mathematics and Statistics, Zaozhuang University, Zaozhuang 277160, China

* **Correspondence:** Email: liting810505@163.com.

Abstract: Let p be an odd prime with $p \equiv 7 \pmod{12}$, $\frac{p-1}{2}$ be the least integer such that $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, and $q = 2^{\frac{p-1}{2}}$. Let α be a primitive element of the finite field $\mathbb{F}_q$ and $\beta = \alpha^{\frac{q-1}{p}}$. Suppose that $\sigma = \sum_{i=0}^{2} \beta^{m\zeta_3^i} \in \mathbb{F}_q^*$, where $m \in \mathbb{F}_p^*$ and ζ_3 is a 3rd root of unity in $\mathbb{F}_p$. Let $\{u_i\} = (\mathrm{Tr}_{q/2}(\sigma\beta^i))_{i=0}^{q-2}$ be a binary sequence of period $q-1$. In this paper, we obtained the cross correlation distribution between two sequences $\{u_i\}$ and its $\frac{q-1}{p}$-decimation sequence, which is two-valued.

Keywords: cross correlation; exponential sum
Mathematics Subject Classification: 94A55, 94A60

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of prime 2. Let $u = \{u_i\}_{i=0}^{N-1}$ and $v = \{v_i\}_{i=0}^{N-1}$ be two binary sequences of period N with elements from $\mathbb{F}_2$. The period cross correlation function between these two sequences at shift τ is defined as

$$C_{u,v}(\tau) = \sum_{i=0}^{N-1} (-1)^{u_{i+\tau}-v_i}, 0 \leq \tau \leq N-1.$$

The multiset $\{C_{u,v}(\tau) : 0 \leq \tau \leq N-1\}$ is called the cross correlation distribution of sequences u and v. Assume that $\{v_i\}$ is shifted cyclically such that $\{v_i\} = \{u_{di}\}$. Taking $1 \leq d \leq N-2$, the cross correlation function between u and its d-decimation is $C_d(\tau) = \sum_{i=0}^{N-1} (-1)^{u_{i+\tau}-u_{di}}$. For the cross correlation function between an m-sequence and its d-decimation, an overview of known results can be found in [5, 10, 17, 18], etc.

The numerical results indicate that the cross correlation distributions are very complex and difficult. Due to applications in cryptography, radar, and wireless communication systems [8], the sequences with low cross correlation play an important role in deducing the interference of different users in communication systems. Therefore, sequences with cross correlations are desired and the reader is referred to literatures [2, 3, 9, 11, 12, 14, 25] and the references therein. In the following, we list some results about the cross correlation of sequences.

In [6], Dobbertin et al. gave ternary sequences of period $3^n - 1$ with a three-valued cross correlation function for $d = 2 \cdot 3^r + 1$, where $4r + 1 \equiv 0 \pmod{n}$.

In [4], let $q = p^m$ and m and k be two positive integers such that $\frac{m}{\gcd(m,k)} \geq 3$ is odd. Suppose that $p \equiv 3 \pmod{4}$, $d(p^k + 1) \equiv 2 \pmod{p^m - 1}$, and $k|m$. Choi et al. determined the cross correlation distribution of $C_d(\tau)$, where $d = \frac{p^m+1}{p^k+1} + \frac{p^m-1}{2}$, which generalized the result of [22]. Furthermore, Xia et al. [21] defined a class of sequence and investigated the cross correlation distribution of $C_d(\tau)$, where the decimations have the form $\frac{p^l+1}{2}$, where $p \equiv 3 \pmod{4}$ and l is a positive integer.

In [24], let $q = 3^{3r}$, where r is a positive integer with $\gcd(r, 3) = 1$. Zhang et al. determined the cross correlation distribution for decimations $d = 3^r + 2$ and $d = 3^{2r} + 2$, respectively.

In [20], let $q = p^{\frac{\phi(r^m)}{3}}$ and $r \equiv 1 \pmod{3}$. Suppose that $\{u_i\}_{i=0}^{q-2} = (\mathrm{Tr}_{q/p}(\alpha^i))_{i=0}^{q-2}$, where α is a primitive element of $\mathbb{F}_q$. Wu et al. investigated the cross correlation distribution between $\{u_i\}$ and its $\frac{q-1}{r^m}$-decimation sequence for $p = 2$ and $p = 3$, respectively.

Let p be an odd prime and $p \equiv 7 \pmod{12}$. Suppose that $\frac{p-1}{2}$ is the multiplicative order of 2 modulo p and let $q = 2^{\frac{p-1}{2}}$, α be a primitive element of $\mathbb{F}_q$, and $\beta = \alpha^{\frac{q-1}{p}}$. Suppose that $\sigma = \sum_{i=0}^{2} \beta^{m\zeta_3^i} \in \mathbb{F}_q^*$, where $m \in \mathbb{F}_p^*$ and ζ_3 is a 3rd root of unity in $\mathbb{F}_p$. In this paper, we shall investigate the cross correlation distribution between two sequences $\{u_i\}$ and its $\frac{q-1}{p}$-decimation sequence, where $\{u_i\} = (\mathrm{Tr}_{q/2}(\sigma\beta^i))_{i=0}^{q-2}$.

This paper is organized as follows: In Section 2, we recall some concepts and several results about Gaussian sums in the index two case. In Section 3, we construct a class of binary sequences and investigate the cross correlation distribution $\{C_d(\tau) : 0 \leq \tau \leq q - 2\}$. Moreover, some examples are given. In Section 4, we make a conclusion.

2. Preliminaries

In this section, we recall some definitions and results about characters and Gaussian sums, which are useful in the sequel.

The trace function from $\mathbb{F}_q$ onto $\mathbb{F}_2$ is defined by $\mathrm{Tr}_{q/2}(x) = x + x^2 + \cdots + x^{q/2}$, $x \in \mathbb{F}_q$. The additive character of $\mathbb{F}_q$ is a nonzero function $\chi_b, b \in \mathbb{F}_q$, from $\mathbb{F}_q$ to the set of complex numbers: $\chi_b(c) = (-1)^{\mathrm{Tr}_{q/2}(bc)}$. When $b = 1$, the character χ_1 is called the canonical additive character of $\mathbb{F}_q$. It is well known that $\sum_{c \in \mathbb{F}_q} \chi_b(c) = 0$ for $b \neq 0$.

Let L be a positive divisor of $q-1$, ω a primitive element of $\mathbb{F}_q$, and $C_i^{(L,q)} = \omega^i \langle \omega^L \rangle$, $i = 0, \ldots, L-1$, cosets. Gaussian periods of order L are defined by

$$\eta_i^{(L,q)} = \sum_{x \in C_i^{(L,q)}} \chi(x), i = 0, 1, \ldots, L - 1.$$

Lemma 2.1. *[16] If $q = p^w$ and $L = 2$, the Gaussian periods are given by the following:*

$$\eta_0^{(2,q)} = \begin{cases} \frac{-1+(-1)^{w-1} q^{\frac{1}{2}}}{2}, & \text{if } p \equiv 1 \pmod{4}, \\ \frac{-1+(-1)^{w-1} (\sqrt{-1})^w q^{\frac{1}{2}}}{2}, & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

and $\eta_1^{(2,q)} = -1 - \eta_0^{(2,q)}$.

Let β be a fixed primitive element of $\mathbb{F}_q$. For each $j = 1, 2, \ldots, q-1$, the function ψ_j with

$$\psi_j(\beta^k) = \zeta_{q-1}^{jk} \text{ for } k = 0, 1, \ldots, q-2 \tag{2.1}$$

defines a multiplicative character with order $\frac{q-1}{gcd(q-1,j)}$ of $\mathbb{F}_q$, where ζ_{q-1} denotes the $(q-1)$-th primitive root of unity.

Let q be odd and $j = \frac{q-1}{2}$ in (2.1). We then get a multiplicative character denoted by η such that $\eta(c) = 1$ if c is the square of an element, and $\eta(c) = -1$ otherwise. This η is called the quadratic character of $\mathbb{F}_q$.

Let ψ be a multiplicative character with order k with $k|(q-1)$ and χ an additive character of $\mathbb{F}_q$, then the Gaussian sum $G(\psi, \chi)$ of order k is defined by

$$G(\psi, \chi) = \sum_{x \in \mathbb{F}_q^*} \psi(x)\chi(x).$$

Since $G(\psi, \chi_b) = \bar{\psi}(b)G(\psi, \chi_1)$, we just consider $G(\psi, \chi_1)$, briefly denoted as $G(\psi)$.

The Gaussian sum is an important tool in investigating the weights of cyclic codes, the cross correlation of sequences, and the Walsh spectrum of functions. For example, Schmidt et al. [19] used Fourier transforms and Gaussian sums and obtained necessary and sufficient numerical conditions for an irreducible cyclic code to have at most two weight.

Lemma 2.2. *[15] Let χ be a nontrivial additive character of $\mathbb{F}_q$ and let ψ be a multiplicative character of $\mathbb{F}_q$ of order $s = \gcd(n, q-1)$, then*

$$\sum_{x \in \mathbb{F}_q} \chi(ax^n + b) = \chi(b) \sum_{j=1}^{s-1} \bar{\psi}^j(a) G(\psi^j, \chi)$$

for any $a, b \in \mathbb{F}_q$ with $a \neq 0$.

We use $\mathbb{Z}_N$ to denote the ring $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ and use $\mathbb{Z}_N^*$ to denote all the invertible elements of $\mathbb{Z}_N$. Suppose that 2 generates a subgroup of the group $\mathbb{Z}_N^*$ with index $[\mathbb{Z}_N^* : \langle 2 \rangle] = 2$. If $-1 \notin \langle 2 \rangle \subset \mathbb{Z}_N^*$, then it is the so-called "index 2" case. The Gaussian sum of the "index 2" case is explicitly determined; see [7, 23] and its references for details.

Lemma 2.3. *([7, 23]) Let $3 \neq p \equiv 3 \pmod 4$ be a prime and let $w = \mathrm{ord}_p(2) = \frac{p-1}{2}$, $q = 2^w$, and χ be a primitive multiplicative character of order p over $\mathbb{F}_q^*$, then for $1 \leq i \leq p-1$, we have that*

$$G(\chi^i) = \begin{cases} 2^{\frac{w-h-2}{2}}(e + f\sqrt{-p}) & \text{if } (\frac{i}{p}) = 1, \\ 2^{\frac{w-h-2}{2}}(e - f\sqrt{-p}) & \text{if } (\frac{i}{p}) = -1, \end{cases}$$

where $(\frac{i}{r})$ denotes the Legendre symbol, h is the ideal class number of quadratic number field $\mathbb{Q}(\sqrt{-p})$, and e, f are given by

$$\begin{cases} e^2 + pf^2 = 2^{2+h}, \\ e \equiv -2^{\frac{p+3+2h}{4}} \pmod p. \end{cases} \tag{2.2}$$

3. The cross correlation distributions of a class of binary sequence

In this section, let p be an odd prime with $p \equiv 7 \pmod{12}$. Suppose that $\mathrm{ord}_p(2) = \frac{p-1}{2}$, i.e., $\frac{p-1}{2}$ is the least integer such that $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, which is called 2 semi-primitive root modulo p. Let $q = 2^{\frac{p-1}{2}}$, α be a primitive element of $\mathbb{F}_q$, and $\beta = \alpha^{\frac{q-1}{p}}$. Let D_1 and D_0 be the sets consisting of all non-square elements and square elements in $\mathbb{F}_p^*$, respectively, i.e., $\mathbb{F}_p^* = D_1 \cup D_0$.

Define a binary sequence of period $q-1$:

$$u = \{u_0, u_1, \ldots, u_{q-2}\}, u_i = \mathrm{Tr}_{q/2}(\sigma\alpha^i), \sigma \in \mathbb{F}_q^*, i = 0, 1, \ldots, q-2. \tag{3.1}$$

For $0 \le \tau \le q-2$, the cross correlation function between u and its $d = \frac{q-1}{p}$-decimation is

$$C_d(\tau) = \sum_{i=0}^{q-2} (-1)^{u_{i+\tau} + u_{di}}. \tag{3.2}$$

In this section, we shall investigate the above cross correlation distribution defined as (3.2).

Fixed a $\sigma \in \mathbb{F}_q^*$, for $0 \le \tau \le q-2$, we find that $\rho = \sigma\alpha^\tau$ runs over all elements of $\mathbb{F}_q^*$ as α^τ does. Hence

$$\begin{aligned} C_d(\tau) &= \sum_{i=0}^{q-2} (-1)^{\mathrm{Tr}_{q/2}(\sigma\alpha^{\tau+i} + \sigma\alpha^{di})} = \sum_{i=0}^{q-2} (-1)^{\mathrm{Tr}_{q/2}(\rho\alpha^i + \sigma\alpha^{di})} \\ &= \sum_{x \in \mathbb{F}_q^*} (-1)^{\mathrm{Tr}_{q/2}(\rho x + \sigma x^d)} = \sum_{x \in \mathbb{F}_q^*} (-1)^{\mathrm{Tr}_{q/2}(x + \sigma(\rho^{-1}x)^d)} \\ &= \sum_{i=0}^{q-2} (-1)^{\mathrm{Tr}_{q/2}(\alpha^i + \sigma\rho^{-d}\beta^i)}, \end{aligned} \tag{3.3}$$

for $0 \le i \le q-2$, by division algorithm $i = jp + r$, $0 \le j \le d-1$, $0 \le r \le p-1$. By Lemma 2.2,

$$\begin{aligned} C_d(\tau) &= \sum_{r=0}^{p-1} (-1)^{\mathrm{Tr}_{q/2}(\sigma\rho^{-d}\beta^r)} \sum_{j=0}^{d-1} (-1)^{\mathrm{Tr}_{q/2}(\alpha^{jp}\alpha^r)} \\ &= \frac{1}{p} \sum_{r=0}^{p-1} (-1)^{\mathrm{Tr}_{q/2}(\sigma\rho^{-d}\beta^r)} \sum_{x \in \mathbb{F}_q^*} (-1)^{\mathrm{Tr}_{q/2}(\alpha^r x^p)} \\ &= \frac{1}{p} \sum_{r=0}^{p-1} (-1)^{\mathrm{Tr}_{q/2}(\sigma\rho^{-d}\beta^r)} (\sum_{s=1}^{p-1} \bar{\psi}^s(\alpha^r) G(\psi^s) - 1) \\ &= \frac{1}{p} \sum_{r=0}^{p-1} (-1)^{\mathrm{Tr}_{q/2}(\sigma\rho^{-d}\beta^r)} (\sum_{s=1}^{p-1} \zeta_p^{-rs} G(\psi^s) - 1), \end{aligned} \tag{3.4}$$

where $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is the p-th primitive root of unity in the complex number field, ψ is a primitive multiplicative character of order p over $\mathbb{F}_q^*$, and $\psi(\alpha) = \zeta_p$.

Recall that $p \equiv 7 \pmod{12}$, which implies that $p \equiv 3 \pmod 4$. By Lemma 2.3,

$$\begin{aligned}\sum_{s=1}^{p-1} \zeta_p^{-rs} G(\psi^s) &= 2^{\frac{p-1-2h}{4}}\Big(\frac{e+f\sqrt{-p}}{2}\sum_{s\in D_0}\zeta_p^{-rs} + \frac{e-f\sqrt{-p}}{2}\sum_{s\in D_1}\zeta_p^{-rs}\Big)\\ &= 2^{\frac{p-5-2h}{4}}\Big(e\big(\sum_{s\in D_0}\zeta_p^{-rs} + \sum_{s\in D_1}\zeta_p^{-rs}\big) + f\sqrt{-p}\big(\sum_{s\in D_0}\zeta_p^{-rs} - \sum_{s\in D_1}\zeta_p^{-rs}\big)\Big),\end{aligned}$$

where h is the ideal class number of $\mathbb{Q}(\sqrt{-p})$, and e, f are given by (2.2).

If $r = 0$, then

$$\sum_{s=1}^{p-1} \zeta_p^{-rs} G(\psi^s) = 2^{\frac{p-5-2h}{4}} e(p-1).$$

If $r \neq 0$, then by Lemma 2.1,

$$\sum_{s=1}^{p-1} \zeta_p^{-rs} G(\psi^s) = 2^{\frac{p-5-2h}{4}}(-e + pf\eta(-r)) = -2^{\frac{p-5-2h}{4}}(e + pf\eta(r)),$$

where η is the quadric character of $\mathbb{F}_p$. Let $c = \frac{p-5-2h}{4}$, then

$$C_d(\tau) = -\frac{1}{p}(2^c e + 1)\Gamma_1(\sigma) - 2^c f\Gamma_2(\sigma) + 2^c e\Gamma_3(\sigma), \tag{3.5}$$

where $\Gamma_1(\sigma) = \sum_{r=0}^{p-1}\chi(\sigma\rho^{-d}\beta^r)$, $\Gamma_2(\sigma) = \sum_{r\in D_0}\chi(\sigma\rho^{-d}\beta^r) - \sum_{r\in D_1}\chi(\sigma\rho^{-d}\beta^r)$, and $\Gamma_3(\sigma) = \chi(\sigma\rho^{-d})$.

In the following we calculate the values of $\Gamma_1(\sigma)$, $\Gamma_2(\sigma)$, and $\Gamma_3(\sigma)$. We need some lemmas.

Lemma 3.1. *([13, Theorem 7]) Let p be a prime with $p = A^2 + 3B^2$. If 2 is a cubic non-residue of p and if $4p = L^2 + 27M^2$, $A \equiv L \equiv 1 \pmod 3$, then the number $N_3(u)$ of solutions (x, y) of $x^3 + u \equiv y^2 \pmod p$ is given by*

$$N_3(u) = \begin{cases} p - (\frac{u}{p})2A, & \text{if } u \equiv w^3 \pmod p,\\ p + (\frac{u}{p})L, & \text{if } u \equiv 2w^3 \pmod p,\\ p + (\frac{u}{p})(2A - L), & \text{if } u \equiv 4w^3 \pmod p.\end{cases}$$

Lemma 3.2. *([13, Theorem 8]) Let p be a prime with $p = A^2 + 3B^2$. If 2 is a cubic non-residue of p and if $4p = L^2 + 27M^2$, $A \equiv L \equiv 1 \pmod 3$, then the number $N_6(u)$ of solutions (x, y) of $x^6 + u \equiv y^2 \pmod p$ is given by*

$$N_6(u) = \begin{cases} p - 1 - 2A(1 + (\frac{u}{p})), & \text{if } u \equiv w^3 \pmod p,\\ p - 1 + 2A + L((\frac{u}{p}) - 1), & \text{if } u \equiv 2w^3 \pmod p,\\ p - 1 + (\frac{u}{p})2A - L((\frac{u}{p}) - 1), & \text{if } u \equiv 4w^3 \pmod p.\end{cases}$$

Lemma 3.3. *Suppose that D_1 is the set consisting of all non-square elements in $\mathbb{F}_p^*$, for $0 \leq r \leq p-1$, if $\sqrt{-p} \equiv 1 \pmod{\mathcal{P}_1}$, then*

$$\mathrm{Tr}_{q/2}(\beta^r) = \begin{cases} 1, & \text{if } r = 0 \text{ or } r \in D_1, \\ 0, & \text{otherwise.} \end{cases}$$

If $\sqrt{-p} \equiv -1 \pmod{\mathcal{P}_1}$, then,

$$\mathrm{Tr}_{q/2}(\beta^r) = \begin{cases} 1, & \text{if } r = 0 \text{ or } r \in D_0, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. It is well known that there is an irreducible factorization over $\mathbb{F}_2$:

$$x^p - 1 = (x-1)\Phi_p^{(0)}(x)\Phi_p^{(1)}(x),$$

where $\Phi_p^{(0)}(x) = \prod_{r\in D_0}(x-\beta^r)$, $\Phi_p^{(1)}(x) = \prod_{r\in D_1}(x-\beta^r)$. By Lemma 2.1,

$$\sum_{r\in D_0} \zeta_p^r = \frac{-1+\sqrt{-p}}{2}, \sum_{r\in D_1} \zeta_p^r = \frac{-1-\sqrt{-p}}{2},$$

where ζ_p is a primitive p-th root of unity in the complex number field.

Let $O = \mathbb{Z}[\zeta_p]$ be the algebraic integer ring of $\mathbb{Q}(\zeta_p)$, then there is a prime ideal factorization of the prime 2 in the algebraic integer ring O:

$$2O = \mathcal{P}_1\mathcal{P}_2,$$

where $\mathcal{P}_1 = \langle \frac{a+b\sqrt{-p}}{2}, 2\rangle$ and $\mathcal{P}_2 = \langle \frac{a-b\sqrt{-p}}{2}, 2\rangle$ are prime ideals of $\mathbb{Q}(\zeta_p)$ over 2.

Let

$$\zeta_p \equiv \beta \pmod{\mathcal{P}_1} \text{ and } O/\mathcal{P}_1 = \mathbb{F}_{2^{\frac{p-1}{2}}} = \mathbb{F}_2(\beta),$$

where $\frac{p-1}{2}$ is the order of 2 modulo p, then

$$\sum_{r\in D_0} \zeta_p^r \equiv \sum_{r\in D_0} \beta^r \equiv \frac{-1+\sqrt{-p}}{2} \pmod{\mathcal{P}_1},$$

$$\sum_{r\in D_1} \zeta_p^r \equiv \sum_{r\in D_1} \beta^r \equiv \frac{-1-\sqrt{-p}}{2} \pmod{\mathcal{P}_1},$$

where $\sqrt{-p}$ is an element in $\mathbb{F}_2$ such that $(\sqrt{-p})^2 \equiv -p \pmod 2$.

Suppose that $\sqrt{-p} \equiv 1 \pmod{\mathcal{P}_1}$, then for $0 \le r \le p-1$,

$$\mathrm{Tr}_{q/2}(\beta^r) = \begin{cases} 1, & \text{if } r = 0 \text{ or } r \in D_1, \\ 0, & \text{otherwise.} \end{cases}$$

Suppose that $\sqrt{-p} \equiv -1 \pmod{\mathcal{P}_1}$, then for $0 \le r \le p-1$,

$$\mathrm{Tr}_{q/2}(\beta^r) = \begin{cases} 1, & \text{if } r = 0 \text{ or } r \in D_0, \\ 0, & \text{otherwise.} \end{cases}$$

Without loss of generality, in the following, we always assume that $\sqrt{-p} \equiv 1 \pmod{\mathcal{P}_1}$, i.e., for $0 \le r \le p-1$,

$$\mathrm{Tr}_{q/2}(\beta^r) = \begin{cases} 1, & \text{if } r = 0 \text{ or } r \in D_1, \\ 0, & \text{otherwise.} \end{cases}$$

In the following, suppose that $p \equiv 7 \pmod{12}$ and $\sigma = \sum_{i=0}^{2} \beta^{m\zeta_3^i} \in \mathbb{F}_q^*$, where ζ_3 is a 3rd primitive root of unity in $\mathbb{F}_p$. We calculate the values of $\Gamma_1(\sigma)$, $\Gamma_2(\sigma)$, and $\Gamma_3(\sigma)$ in two cases: $m \in D_0$ and $m \in D_1$.

3.1. $m \in D_0$

In this subsection, we always assume that $m \in D_0$. In the following, we investigate the values of $\Gamma_1(\sigma)$, $\Gamma_2(\sigma)$, and $\Gamma_3(\sigma)$.

Theorem 3.4. *Let p be a prime with $p = A^2 + 3B^2$, where $A \equiv 1 \pmod 3$. Suppose that $p \equiv 7 \pmod{12}$ and $\sigma = \sum_{i=0}^{2} \beta^{m\zeta_3^i} \in \mathbb{F}_q^*$, where $m \in D_0$ and ζ_3 is a 3rd primitive root of unity in $\mathbb{F}_p$. If 2 is a cubic nonresidue of p, then,*

$$\Gamma_1(\sigma) = -2A + 3.$$

Proof. Since $\mathrm{ord}(\rho^{-d}) = p$,

$$\begin{aligned} \Gamma_1(\sigma) &= \sum_{r=0}^{p-1} \chi(\sigma\rho^{-d}\beta^r) = \sum_{r=0}^{p-1} \chi(\sigma\beta^r) = \sum_{x \in \mathbb{F}_p} (-1)^{\mathrm{Tr}_{q/2}(\sum_{i=0}^{2} \beta^{x+m\zeta_3^i})} \\ &= \sum_{x \in \mathbb{F}_p \setminus M} (-1)^{\mathrm{Tr}_{q/2}(\sum_{i=0}^{2} \beta^{x+m\zeta_3^i})} + \sum_{x \in M} (-1)^{\mathrm{Tr}_{q/2}(\sum_{i=0}^{2} \beta^{x+m\zeta_3^i})}, \end{aligned}$$

where $M = \{-m, -m\zeta_3, -m\zeta_3^2\}$. Note that $-1 \in D_1$, $-m \in D_1$, and $p \equiv 7 \pmod{12}$, then it is easy to check that for $x \in M$,

$$(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=0}^{2} \beta^{x+m\zeta_3^i})} = -(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=1}^{2} \beta^{-m+m\zeta_3^i})} = 1.$$

By the fact that the product of any two square elements or any two non-square elements is a square element and the product of a square element with a non-square element is a non-square element, a simple conclusion is that for $x \in \mathbb{F}_p \setminus M$,

$$(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=0}^{2} (\beta^{x+m\zeta_3^i})} = (-1)^{\mathrm{Tr}_{q/2}(\beta^{\Pi_{i=0}^{2}(x+m\zeta_3^i)})} = \eta(\Pi_{i=0}^{2}(x + m\zeta_3^i)).$$

Consider the equation: For $x \in \mathbb{F}_p \setminus M$,

$$y^2 = \Pi_{i=0}^{2}(x + m\zeta_3^i) = x^3 + m^3.$$

By Lemma 3.1, the number $N_3(m^3)$ of solutions (x, y) of $x^3 + m^3 = y^2$ over $\mathbb{F}_p$ is $p - (\frac{m}{p})2A = p - 2A$, where $p = A^2 + 3B^2$ and $A \equiv 1 \pmod 3$.

With the solutions (y, x) and $(-y, x)$ with respect to the y-axis, except three rational points $(-m, 0), (-m\zeta_3, 0), (-m\zeta_3^2, 0)$, then for $x \in \mathbb{F}_p \setminus M$,

$$\Delta = |\{x \in \mathbb{F}_p \setminus M, x^3 + m^3 = y^2, y \in \mathbb{F}_p\}|$$

$$= \frac{1}{2}(N_3(m^3) - 3) = \frac{p-3-2A}{2}.$$

Hence,

$$\begin{aligned}\Gamma_1(\sigma) &= \sum_{x\in\mathbb{F}_p\setminus M}(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=0}^{2}\beta^{x+m\zeta_3^i})} + \sum_{x\in M}(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=0}^{2}\beta^{x+m\zeta_3^i})}\\ &= \Delta - (p-3-\Delta) + 3 = -2A + 3.\end{aligned}$$

Theorem 3.5. *Let p be a prime with $p = A^2+3B^2$, where $A \equiv 1 \pmod 3$. Suppose that $\sigma = \sum_{i=0}^{2}\beta^{m\zeta_3^i} \in \mathbb{F}_q^*$, where $m \in D_0$ and ζ_3 is a 3rd primitive root of unity in $\mathbb{F}_p$. If 2 is a cubic non-residue of p, then,*

$$\Gamma_2(\sigma) = -5 - 4A.$$

Proof. Since 2 is a semi-primitive root modulo p, let $D_0 = \langle 2\rangle$ and $D_1 = \beta D_0$, $\mathbb{F}_p^* = \langle\beta\rangle = D_0 \cup D_1$. It is obvious that $\mathrm{ord}(\rho^{-d}) = 1$ or $\mathrm{ord}(\rho^{-d}) = p$. Let $\rho^{-d} = \beta^y$, $0 \le y \le p-1$, then

$$\begin{aligned}\Gamma_2(\sigma) &= \sum_{r\in D_0}\chi(\sigma\rho^{-d}\beta^r) - \sum_{r\in D_1}\chi(\sigma\rho^{-d}\beta^r)\\ &= \sum_{r\in D_0}(\chi(\sigma\rho^{-d}\beta^r) - \chi(\sigma\rho^{-d}\beta^{-r}))\\ &= \frac{1}{2}(\sum_{x\in\mathbb{F}_p^*}\chi(\sigma\rho^{-d}\beta^{x^2}) - \sum_{x\in\mathbb{F}_p^*}\chi(\sigma\rho^{-d}\beta^{-x^2})).\end{aligned}$$

For $0 \le y \le p-1$, either $y = 0$, $y \in D_0$, or $y \in D_1(-y \in D_0)$, then

$$\begin{aligned}\Gamma_2(\sigma) &= \frac{1}{2}(\sum_{x\in\mathbb{F}_p^*}(\chi(\sigma\beta^{x^2}) - \sum_{x\in\mathbb{F}_p^*}\chi(\sigma\beta^{-x^2}))\\ &= \frac{1}{2}(\sum_{x\in\mathbb{F}_p^*}(-1)^{\sum_{i=0}^{2}\mathrm{Tr}_{q/2}(\beta^{x^2+m\zeta_3^i})} - \sum_{x\in\mathbb{F}_p^*}(-1)^{\sum_{i=0}^{2}\mathrm{Tr}_{q/2}(\beta^{-x^2+m\zeta_3^i})})\\ &= \frac{1}{2}(\sum_{x\in\mathbb{F}_p}(-1)^{\sum_{i=0}^{2}\mathrm{Tr}_{q/2}(\beta^{x^2+m\zeta_3^i})} - \sum_{x\in\mathbb{F}_p}(-1)^{\sum_{i=0}^{2}\mathrm{Tr}_{q/2}(\beta^{-x^2+m\zeta_3^i})} - 2).\end{aligned} \tag{3.6}$$

From the above discussion,

$$(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=0}^{2}\beta^{x^2+m\zeta_3^i})} = (-1)^{\mathrm{Tr}_{q/2}(\prod_{i=0}^{2}\beta^{x^2+m\zeta_3^i})} = \eta(\prod_{i=0}^{2}(x^2+m\zeta_3^i)).$$

Since $p \equiv 1 \pmod 6$, and $m \in D_0$, we have for $0 \le i \le 2$, $-m\zeta_3^i \in D_1$, then for $x \in \mathbb{F}_p$, $x^2 + m\zeta_3^i \neq 0, i = 0, 1, 2$.

Consider the equation: For $x \in \mathbb{F}_p$,

$$y^2 = \prod_{i=0}^{2}(x^2 + m\zeta_3^i) = x^6 + m^3.$$

By Lemma 3.2, the number $N_6(m^3)$ of solutions (x, y) of $x^6+m^3 = y^2$ over $\mathbb{F}_p$ is $p-1-2A((\frac{m}{p})+1) = p-1-4A$, where $p = A^2+3B^2$ and $A \equiv 1 \pmod 3$.

With the solutions (y, x) and $(-y, x)$ with respect to the y-axis, then for $x \in \mathbb{F}_p$,

$$\begin{aligned} \Delta_1 &= |\{x \in \mathbb{F}_p, x^6 + m^3 = y^2, y \in \mathbb{F}_p\}| \\ &= \frac{1}{2} N_6(m^3) = \frac{p-1-4A}{2}. \end{aligned}$$

Hence,

$$\sum_{x \in \mathbb{F}_p} (-1)^{\sum_{i=0}^{2} \mathrm{Tr}_{q/2}(\beta^{x^2+m\zeta_3^i})} = \Delta_1 - (p - \Delta_1) = -1 - 4A.$$

Moreover, let $M = \{\pm\sqrt{m}, \pm\sqrt{m\zeta_3}, \pm\sqrt{m\zeta_3^2}\}$. It is easy to check that for $x \in M$,

$$(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=0}^{2} \beta^{-x^2+m\zeta_3^i})} = -(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=1}^{2} \beta^{-m+m\zeta_3^i})} = 1.$$

For $x \in \mathbb{F}_p \setminus M$, we consider the equation:

$$y^2 = \Pi_{i=0}^{2}(-x^2 + m\zeta_3^i) = -x^6 + m^3 = -(x^6 - m^3).$$

Note that $-m^3 \equiv (-m)^3 \pmod{p}$, then the number $N_6(-m^3)$ of solutions (x, y) of $x^6 - m^3 = y^2$ over $\mathbb{F}_p$ is the number $N_6(m^3)$ of solutions (x, y) of $x^6 + m^3 = y^2$. For $x \in \mathbb{F}_p$,

$$\begin{aligned} \Delta_2 &= |\{x \in \mathbb{F}_p, -x^6 + m^3 = y^2, y \in \mathbb{F}_p\}| \\ &= p - \frac{1}{2}(N_6(m^3) - 6) = \frac{p+7+4A}{2}. \end{aligned}$$

Hence,

$$\sum_{x \in \mathbb{F}_p} (-1)^{\sum_{i=0}^{2} \mathrm{Tr}_{q/2}(\beta^{-x^2+m\zeta_3^i})} = \Delta_2 - (p - \Delta_2) = 7 + 4A.$$

Therefore,

$$\Gamma_2(\sigma) = \sum_{r \in D_0} \chi(\sigma\rho^{-d}\beta^r) - \sum_{r \in D_1} \chi(\sigma\rho^{-d}\beta^r) = -5 - 4A.$$

Theorem 3.6. *Let p be a prime with $p = A^2+3B^2$, where $A \equiv 1 \pmod 3$. Suppose that $\sigma = \sum_{i=0}^{2} \beta^{m\zeta_3^i} \in \mathbb{F}_q^*$, where $m \in D_0$ and ζ_3 is a 3rd primitive root of unity in $\mathbb{F}_p$. If 2 is a cubic non-residue of p, then for $\rho \in \mathbb{F}_q^*$,*

$$\Gamma_3(\sigma) = \begin{cases} 1, & \text{occurs } \frac{(q-1)(p+3+2A)}{2p} \text{ times}, \\ -1, & \text{occurs } \frac{(q-1)(p-3-2A)}{2p} \text{ times}. \end{cases}$$

Proof. For $\forall\rho \in \mathbb{F}_q^* = \langle\alpha\rangle$, $\rho = \alpha^u$, $0 \leq u \leq q-2$. It is obvious that $\mathrm{ord}(\rho^{-d}) = 1$ or $\mathrm{ord}(\rho^{-d}) = p$. Let $\rho^{-d} = \beta^x$, $0 \leq x \leq p-1$.

Suppose that $x = 0$, i.e., $\mathrm{ord}(\rho^{-d}) = 1$, then $\rho = \alpha^{pv}$, $0 \leq v \leq \frac{q-1}{p} - 1$, so there are $\frac{q-1}{p}$ elements $\rho \in \mathbb{F}_q^*$ such that $\mathrm{ord}(\rho^{-d}) = 1$.

Suppose that $1 \leq x \leq p-1$, i.e., $\mathrm{ord}(\rho^{-d}) = p$, then $\rho = \alpha^v$, $0 \leq v \leq q-2$ and $\gcd(v, p) = 1$, so there are $q - 1 - \frac{q-1}{p}$ elements $\rho \in \mathbb{F}_q^*$ such that $\mathrm{ord}(\rho^{-d}) = p$.

Thus

$$\Gamma_3(\sigma) = (-1)^{\mathrm{Tr}_{q/2}(\sigma\rho^{-d})} = (-1)^{\sum_{i=0}^{2}\mathrm{Tr}_{q/2}(\beta^{x+m\zeta_3^i})}.$$

Suppose that $x \in M = \{-m, -m\zeta_3, -m\zeta_3^2\}$. Note that $-1 \in D_1$, $-m, -m\zeta_3, -m\zeta_3^2 \in D_1$, then it is easy to check that

$$\Gamma_3(\sigma) = (-1)^{\sum_{i=0}^{2}\mathrm{Tr}_{q/2}(\beta^{-m+m\zeta_3^i})} = -(-1)^{\mathrm{Tr}_{q/2}(\beta^{\Pi_{i=1}^{2}(-m+m\zeta_3^i)})} = 1.$$

By Lemma 4.1, there are such $\frac{3(q-1)}{p}$ elements $\rho \in \mathbb{F}_q^*$ such that $\rho^{-d} = \beta^x$.

Suppose that $x \in \mathbb{F}_p \setminus M$, then

$$\Gamma_3(\sigma) = (-1)^{\mathrm{Tr}_{q/2}(\beta^{\Pi_{i=1}^{k}(x+m\zeta_3^i)}) = \eta(\Pi_{i=1}^{k}(x+m\zeta_3^i))}.$$

Consider the equation: For $x \in \mathbb{F}_p \setminus M$,

$$y^2 = \Pi_{i=0}^{2}(x + m\zeta_3^i) = x^3 + m^3.$$

By Theorem 3.3, there are $\Delta = \frac{p-3+2A}{2}$ elements $x \in \mathbb{F}_p \setminus M$ such that $\Gamma_3(\sigma) = 1$, and there are $p - 3 - \Delta = \frac{p-3-2A}{2}$ elements $x \in \mathbb{F}_p \setminus M$ such that $\Gamma_3(\sigma) = -1$, where $p = A^2 + 3B^2$, $A \equiv 1 \pmod 3$.

Therefore, there are $\frac{p+3+2A}{2} \cdot \frac{q-1}{p}$ elements $\rho \in \mathbb{F}_q^*$ such that $\Gamma_3(\sigma) = 1$, and there are $\frac{p-3-2A}{2} \cdot \frac{q-1}{p}$ elements $\rho \in \mathbb{F}_q^*$ such that $\Gamma_3(\sigma) = -1$.

The last thing is to give the correlation distribution of $C_d(\tau), 0 \leq \tau \leq q-2$, defined as (3.2). Putting Theorems 3.4–3.6 together, from (3.5), we obtain the following theorem.

Theorem 3.7. *The notation is as above. Suppose that* $p \equiv 3 \pmod 4$ *and* $p \equiv 7 \pmod{12}$ *with* $p = A^2 + 3B^2$, $A \equiv 1 \pmod 3$. *Let 2 be a semi-primitive root modulo p. Suppose that there exist integers e and f such that*

$$\begin{cases} e^2 + pf^2 = 2^{2+h} \\ e \equiv -2^{\frac{p+3+2h}{4}} \pmod p, f > 0, 2 \nmid f, \end{cases}$$

where h is the ideal class number of $\mathbb{Q}(\sqrt{-p})$. Let u be a binary m-sequence defined as (3.1) and $\sigma = \sum_{i=0}^{2}\beta^{m\zeta_3^i} \in \mathbb{F}_q^*$. If $m \in D_0$, then the cross correlation distribution of $C_d(\tau)$, $0 \leq \tau \leq q-2$, is as follows:

values	frquencies
$\frac{1}{p}(2A-3)(2^c e + 1) + 2^c(5f + 4Af + e)$	occurs $\frac{(q-1)(p+3+2A)}{2p}$ times,
$\frac{1}{p}(2A-3)(2^c e + 1) + 2^c(5f + 4Af - e)$	occurs $\frac{(q-1)(p-3-2A)}{2p}$ times,

where $c = \frac{p-5-2h}{4}$.

3.2. $m \in D_1$

In this subsection, we suppose that $m \in D_1$. Note that $-1 \in D_1$, $-m \in D_0$ and for $x \in M = \{-m, -m\zeta_3, -m\zeta_3^2\}$,

$$(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=0}^{2}\beta^{x+m\zeta_3^i})} = -(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=1}^{2}\beta^{-m+m\zeta_3^i})} = 1.$$

Similar argument to Theorems 3.4 and 3.6, we obtain Theorems 3.8 and 3.10 immediately.

Theorem 3.8. *Let p be a prime with $p = A^2 + 3B^2$, where $A \equiv 1 \pmod 3$. Suppose that $p \equiv 7 \pmod{12}$ and $\sigma = \sum_{i=0}^{2}\beta^{m\zeta_3^i} \in \mathbb{F}_q^*$, where $m \in D_1$ and ζ_3 is a 3rd primitive root of unity in $\mathbb{F}_p$. If 2 is a cubic non-residue of p, then*

$$\Gamma_1(\sigma) = -2A + 3.$$

Theorem 3.9. *Let p be a prime with $p = A^2 + 3B^2$, where $A \equiv 1 \pmod 3$. Suppose that $\sigma = \sum_{i=0}^{2}\beta^{m\zeta_3^i} \in \mathbb{F}_q^*$, where $m \in D_1$ and ζ_3 is a 3rd primitive root of unity in $\mathbb{F}_p$. If 2 is a cubic non-residue of p, then*

$$\Gamma_2(\sigma) = -1.$$

Proof. Let $\rho^{-d} = \beta^y$, $0 \le y \le p-1$, then by (3.6),

$$\begin{aligned}
\Gamma_2(\sigma) &= \frac{1}{2}(\sum_{x\in\mathbb{F}_p}(-1)^{\sum_{i=0}^{2}\mathrm{Tr}_{q/2}(\beta^{x^2+m\zeta_3^i})} - \sum_{x\in\mathbb{F}_p}(-1)^{\sum_{i=0}^{2}\mathrm{Tr}_{q/2}(\beta^{-x^2+m\zeta_3^i})} - 2) \\
&= \frac{1}{2}(\sum_{x\in\mathbb{F}_p\setminus M}(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=0}^{2}\beta^{x^2+m\zeta_3^i})} + \sum_{x\in M}(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=0}^{2}\beta^{x^2+m\zeta_3^i})} \\
&\quad - \sum_{x\in\mathbb{F}_p}(-1)^{\sum_{i=0}^{2}\mathrm{Tr}_{q/2}(\beta^{-x^2+m\zeta_3^i})} - 2),
\end{aligned}$$

where $M = \{\pm\sqrt{-m}, \pm\sqrt{-m\zeta_3}, \pm\sqrt{-m\zeta_3^2}\}$. Note that $m \in D_1$ and $p \equiv 7 \pmod{12}$, then it is easy to check that for $x \in M$,

$$(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=0}^{2}\beta^{x^2+m\zeta_3^i})} = -(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=1}^{2}\beta^{-m+m\zeta_3^i})} = 1.$$

A simple fact is that for $x \in \mathbb{F}_p \setminus M$,

$$(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=0}^{2}(\beta^{x^2+m\zeta_3^i})} = (-1)^{\mathrm{Tr}_{q/2}(\beta^{\Pi_{i=0}^{2}(x^2+m\zeta_3^i)})} = \eta(\Pi_{i=0}^{2}(x^2 + m\zeta_3^i)).$$

From the above discussion,

$$(-1)^{\mathrm{Tr}_{q/2}(\sum_{i=0}^{2}\beta^{x^2+m\zeta_3^i})} = (-1)^{\mathrm{Tr}_{q/2}(\Pi_{i=0}^{2}\beta^{x^2+m\zeta_3^i})} = \eta(\Pi_{i=0}^{2}(x^2 + m\zeta_3^i)).$$

Since $p \equiv 1 \pmod 6$ and $m \in D_1$, we have $-m\zeta_3^i \in D_0$ for $0 \le i \le 2$.

Consider the equation: For $x \in \mathbb{F}_p \setminus M$,

$$y^2 = \Pi_{i=0}^{2}(x^2 + m\zeta_3^i) = x^6 + m^3.$$

By Lemma 3.2, the number $N_6(m^3)$ of solutions (x, y) of $x^6 + m^3 = y^2$ over $\mathbb{F}_p$ is $p - 1$, where $p = A^2 + 3B^2$ and $A \equiv 1 \pmod 3$.

With the solutions (y, x) and $(-y, x)$ with respect to the y-axis, then for $x \in \mathbb{F}_p \setminus M$,

$$\begin{aligned}\Delta_1 &= |\{x \in \mathbb{F}_p \setminus M, x^6 + m^3 = y^2, y \in \mathbb{F}_p\}| \\ &= \frac{1}{2}(N_6(m^3) - 6) = \frac{p-7}{2}.\end{aligned}$$

Hence,

$$\sum_{x\in\mathbb{F}_p\setminus M} (-1)^{\sum_{i=0}^{2} \mathrm{Tr}_{q/2}(\beta^{x^2+m\zeta_3^i})} = \Delta_1 - (p - \Delta_1) = -7.$$

Moreover, consider the equation: for $x \in \mathbb{F}_p$,

$$y^2 = \Pi_{i=0}^{2}(-x^2 + m\zeta_3^i) = -x^6 + m^3 = -(x^6 - m^3).$$

Note that $-m^3 \equiv (-m)^3 \pmod p$, then the number $N_6(-m^3)$ of solutions (x, y) of $x^6 - m^3 = y^2$ over $\mathbb{F}_p$ is the number $N_6(m^3)$ of solutions (x, y) of $x^6 + m^3 = y^2$. Moreover since $p \equiv 1 \pmod 6$ and $m \in D_1$, we have $m\zeta_3^i \in D_1$ for $0 \le i \le 2$, then for $x \in \mathbb{F}_p$, $-x^2 + m\zeta_3^i \neq 0, i = 0, 1, 2$. Thus for $x \in \mathbb{F}_p$,

$$\begin{aligned}\Delta_2 &= |\{x \in \mathbb{F}_p, -x^6 + m^3 = y^2, y \in \mathbb{F}_p\}| \\ &= \frac{1}{2}N_6(m^3) = \frac{p-1}{2}.\end{aligned}$$

Hence,

$$\sum_{x\in\mathbb{F}_p}(-1)^{\sum_{i=0}^{2} \mathrm{Tr}_{q/2}(\beta^{-x^2+m\zeta_3^i})} = \Delta_2 - (p - \Delta_2) = -1.$$

Therefore,

$$\Gamma_2(\sigma) = \sum_{r\in D_0}\chi(\sigma\rho^{-d}\beta^r) - \sum_{r\in D_1}\chi(\sigma\rho^{-d}\beta^r) = -1.$$

Theorem 3.10. *Let p be a prime with $p = A^2 + 3B^2$, where $A \equiv 1 \pmod 3$. Suppose that $\sigma = \sum_{i=0}^{2}\beta^{m\zeta_3^i} \in \mathbb{F}_q^*$, where $m \in D_1$ and ζ_3 is a 3rd primitive root of unity in $\mathbb{F}_p$. If 2 is a cubic non-residue of p, then for $\rho \in \mathbb{F}_q^*$,*

$$\Gamma_3(\sigma) = \begin{cases} 1, & \text{occurs } \frac{(q-1)(p+3+2A)}{2p} \text{ times,} \\ -1, & \text{occurs } \frac{(q-1)(p-3-2A)}{2p} \text{ times.} \end{cases}$$

Theorem 3.11. *The notation is as above. Suppose that $p \equiv 3 \pmod 4$ and $p \equiv 7 \pmod{12}$ with $p = A^2 + 3B^2$, $A \equiv 1 \pmod 3$. Let 2 be a semi-primitive root modulo p. Suppose that there exist integers e and f such that*

$$\begin{cases} e^2 + pf^2 = 2^{2+h} \\ e \equiv -2^{\frac{p+3+2h}{4}} \pmod p, f > 0, 2 \nmid f, \end{cases}$$

where h is the ideal class number of $\mathbb{Q}(\sqrt{-p})$. Let u be a binary m-sequence defined as (3.1)and $\sigma = \sum_{i=0}^{2}\beta^{m\zeta_3^i} \in \mathbb{F}_q^*$. If $m \in D_1$, then the cross correlation distribution of $C_d(\tau)$, $0 \le \tau \le q-2$, is as follows:

values	frquencies
$\frac{1}{p}(2A-3)(2^ce+1) + 2^c(f+e)$	occurs $\frac{(q-1)(p+3+2A)}{2p}$ times,
$\frac{1}{p}(2A-3)(2^ce+1) + 2^c(f-e)$	occurs $\frac{(q-1)(p-3-2A)}{2p}$ times,

where $c = \frac{p-5-2h}{4}$.

In the following, we give some examples to illustrate the results of Theorems 3.7 and 3.11.

Example 3.12. *Let $p = 7$, $q = 2^3$, and $\sigma = \sum_{i=0}^{2}\beta^{2\zeta_3^i} \in \mathbb{F}_q^*$. The class number h of $\mathbb{Q}(\sqrt{-7})$ is 1 (see [1, P.504]), then by Theorem 3.7, the cross correlation distribution of $C_d(\tau)$ is shown in Table 1.*

Table 1. the cross correlation distribution of $C_d(\tau)$.

values	frquencies
-3	occurs 3 times,
-2	occurs 4 times.

Example 3.13. *Let $p = 79$, $q = 2^{39}$, and $\sigma = \sum_{i=0}^{2}\beta^{2\zeta_3^i} \in \mathbb{F}_q^*$. The class number h of $\mathbb{Q}(\sqrt{-79})$ is 5 (see [1, P.504]). Then by Theorem 3.7, the cross correlation distribution of the $C_d(\tau)$ is shown in Table 2.*

Table 2. the cross correlation distribution of $C_d(\tau)$.

values	frquencies
221495	occurs $\frac{39(2^{39}-1)}{79}$ times,
-696009	occurs $\frac{40(2^{39}-1)}{79}$ times.

Example 3.14. *Let $p = 7$, $q = 2^3$, and $\sigma = \sum_{i=0}^{2}\beta^{3\zeta_3^i} \in \mathbb{F}_q^*$. The class number h of $\mathbb{Q}(\sqrt{-7})$ is 1 (see [1, P.504]). Then by Theorem 3.11, the cross correlation distribution of the $C_d(\tau)$ is shown in Table 3.*

Table 3. the cross correlation distribution of $C_d(\tau)$.

values	frquencies
0	occurs 3 times,
2	occurs 4 times.

Example 3.15. *Let $p = 79$, $q = 2^{39}$, and $\sigma = \sum_{i=0}^{2} \beta^{3\zeta_3^i} \in \mathbb{F}_q^*$. The class number h of $\mathbb{Q}(\sqrt{-79})$ is 5 (see [1, P.504]). Then by Theorem 3.11, the cross correlation distribution of the $C_d(\tau)$ is shown in Table 4.*

Table 4. the cross correlation distribution of $C_d(\tau)$.

values	frquencies
564937	occurs $\frac{39(2^{39}-1)}{79}$ times,
−352567	occurs $\frac{40(2^{39}-1)}{79}$ times.

4. Conclusions

Let p be an odd prime with $p \equiv 7 \pmod{12}$. Suppose that $\frac{p-1}{2}$ is the least integer such that $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ and $q = 2^{\frac{p-1}{2}}$. Let α be a primitive element of the finite field $\mathbb{F}_q$ and $\beta = \alpha^{\frac{q-1}{p}}$. In this paper, we constructed a class of binary sequence $u = \{u_0, u_1, \dots, u_{q-2}\}, u_i = \mathrm{Tr}_{q/2}(\sigma\alpha^i), i = 0, 1, \dots, q-2$, where $\sigma = \sum_{i=0}^{2} \beta^{m\zeta_3^i} \in \mathbb{F}_q^*$, $m \in \mathbb{F}_p^*$, and ζ_3 is a 3rd primitive root of unity in $\mathbb{F}_p$. By calculating the related exponential sums, we investigated the cross correlation distributions between u and its $\frac{q-1}{p}$-decimation sequence, which were two-valued.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

We are very grateful to the reviewers and the editor for their valuable comments and suggestions that much improved the quality of this paper. The work was supported by National Natural Science Foundation of China under Grant 12171420.

Conflict of interest

The authors declare no conflict of interest.

References

1. H. Cohen, *A course in computational algebraic number theory*, Heidelberg: Springer, 1996. https://doi.org/10.1007/978-3-662-02945-9
2. A. Canteaut, P. Charpin, H. Dobbertin, Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture, *IEEE T. Inform. Theory*, **46** (2000), 4–8. http://doi.org/10.1109/18.817504
3. T. W. Cusick, H. Dobbertin, Some new three-valued crosscorrelation functions for binary m-sequences, *IEEE T. Inform. Theory*, **42** (1996), 1238–1240. https://doi.org/10.1109/18.508848
4. S. T. Choi, J. Y. Kim, J. S. No, On the cross-correlation of a p-ary m-sequence and its decimated sequences by $d = \frac{p^m+1}{p^k+1} + \frac{p^m-1}{2}$, *IEICE T. Commun.*, **E96.B** (2013), 2190–2197. https://doi.org/10.1587/transcom.E96.B.2190
5. H. Dobbertin, P. Felke, T. Helleseth, P. Rosendahl, Niho type crosscorrelation functions via Dickson polynomials and Kloosterman sums, *IEEE T. Inform. Theory*, **52** (2006), 613–627. https://doi.org/10.1109/TIT.2005.862094
6. H. Dobbertin, T. Helleseth, P. V. Kumar, H. Martinsen, Ternary m-sequences with three-valued cross-correlation function: new decimations of Welch and Niho type, *IEEE T. Inform. Theory*, **47** (2001), 1473–1481. https://doi.org/10.1109/18.923728
7. C. Ding, J. Yang, Hamming weights in irreducible cyclic codes, *Discrete Math.*, **313** (2013), 434–446. https://doi.org/10.1016/j.disc.2012.11.009
8. S. W. Golomb, G. Gong, *Signal design for good correlation: for wireless communication, cryptography, and radar*, Cambridge: Cambridge University Press, 2005. https://doi.org/10.1017/CBO9780511546907
9. T. Helleseth, A. Kholosha, Crosscorrelation of m-sequences, exponential sums, bent functions and Jacobsthal sums, *Cryptogr. Commun.*, **3** (2011), 281–291. https://doi.org/10.1007/s12095-011-0048-0
10. Z. Hu, X. Li, D. Mills, E. Müller, W. Sun, W. Willems, et al., On the cross correlation of sequences with the decimation factor, *Appl. Algebr. Eng. Comm.*, **12** (2001), 255–263. https://doi.org/10.1007/s002000100073
11. T. Helleseth, P. Rosendahl, New pairs of m-sequences with 4-level cross-correlation, *Finite Fields Th. App.*, **11** (2005), 674–683. https://doi.org/10.1016/j.ffa.2004.09.001
12. D. J. Katz, Weil sums of binomials, three-level cross-correlation, and a conjecture of Helleseth, *J. Comb. Theory A*, **119** (2012), 1644–1659. https://doi.org/10.1016/j.jcta.2012.05.003
13. E. Lehmer, On the number of solutions of $u^k + D \equiv w^2 \pmod{p}$, *Pacific J. Math.*, **5** (1955), 103–118.
14. J. Luo, Binary sequences with three-valued cross correlations of different lengths, *IEEE T. Inform. Theory*, **62** (2016), 7532–7537. https://doi.org/10.1109/TIT.2016.2620432
15. R. Lidl, H. Niederreiter, *Finite fields*, Cambridge: Cambridge University Press, 1996. https://doi.org/10.1017/CBO9780511525926

16. G. Myerson, Period polynomials and Gauss sums for finite fields, *Acta Arith.*, **39** (1981), 251–264. https://doi.org/10.4064/AA-39-3-251-264

17. E. N. Müller, On the cross correlation of sequences over $GF(p)$ with short periods, *IEEE T. Inform. Theory*, **45** (1999), 289–295. https://doi.org/10.1109/18.746820

18. G. L. Mullen, D. Panario, *Handbook of finite fields*, 1 Eds., New York: Chapman and Hall/CRC, 2013. https://doi.org/10.1201/b15006

19. B. Shcmidt, C. White, All two-weight irreducible cyclic codes, *Finite Fields Th. App.*, **8** (2002), 1–17. https://doi.org/10.1006/ffta.2000.0293

20. Y. Wu, Q. Yue, X. Shi, X. Zhu, Binary and ternary sequences with a few cross correlations, *Cryptogr. Commun.*, **12** (2020), 511–525. https://doi.org/10.1007/s12095-019-00376-4

21. Y. Xia, C. Li, X. Zeng, T. Helleseth, Some results on cross-correlation distribution between a p-ary m-sequence and its decimated sequences, *IEEE T. Inform. Theory*, **60** (2014), 7368–7381. https://doi.org/10.1109/TIT.2014.2350775

22. Y. Xia, X. Zeng, L. Hu, Further cross correlation properties of sequences with the decimation factor, *Appl. Algebr. Eng. Comm.*, **21** (2010), 329–342. https://doi.org/10.1007/s00200-010-0128-y

23. J. Yang, L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, *Sci. China Math.*, **53** (2010), 2525–2542. https://doi.org/10.1007/s11425-010-3155-z

24. T. Zhang, S. Li, T. Feng, G. Ge, Some new results on the cross correlation of m-sequences, *IEEE T. Inform. Theory*, **60** (2014), 3062–3068. https://doi.org/10.1109/TIT.2014.2311113

25. X. Zeng, J. Q. Liu, L. Hu, Generalized Kasami sequences: the large set, *IEEE T. Inform. Theory*, **53** (2007), 2587–2598. https://doi.org/10.1109/TIT.2007.899528