A FAMILY OF NONBINARY SEQUENCES WITH OPTIMAL CORRELATION PROPERTY

Xinjiao Chen

School of Computer Science
Key Laboratory of Aerospace Information Security
and Trusted Computing of Ministry of Education
Wuhan University
Wuhan, 430079
P.R. China
e-mail: xinjiaochen@hotmail.com

Abstract. In this paper, we first present a family of p-ary sequences with ideal two-level autocorrelation property, which could be regarded as a generalization of the well-known nonbinary sequences introduced by Helleseth and Gong. Utilizing the proposed sequences and m-sequences, we later construct a family of p-ary sequences of which the correlation property is optimal in terms of the Welch lower bound.

Keywords: p-ary sequences, correlations, autocorrelations, Welch bound.

1. Introduction

Pseudorandom sequences with good correlation properties have many applications in modern communication systems and cryptography, such as radar, CDMA communication systems, and stream cipher cryptosystems [2], [3], [9]. The design of sequences with two-level ideal autocorrelation, which play important roles in synchronization applications and also have close connection to different sets, has been an interesting research topic for decades in [3] and [6]. In recent years, there have been numerous researches on binary sequences with two-level autocorrelation property, see [3] for details. However, for p-ary sequences with two-level autocorrelation, without using a subfield constructions, there is only one general construction for any arbitrary odd prime p, which is the m-sequences. Helleseth and Gong [5] presented a construction of p-ary sequences with ideal two-level autocorrelation for any odd p, which generalized the ternary family by Helleseth, Kumar and Martinsen [4]. This is another general construction for p-ary sequences with ideal autocorrelation property and we refer it as HG sequence in the sequel.

In the present paper, we generalize certain parameters of the HG sequences and deduce a family of p-ary sequences with two-level ideal autocorrelation. With the proposed sequences and p-ary m-sequences, a family of p-ary sequences with period $p^n - 1$, size p^n and the maximal nontrivial correlation value $R_{\max}$ not exceeding $p^{n/2} + 1$ are given.

2. Prelimilaries

First, we fix some notations throughout the paper.

- n is a positive integer with $n = (2m+1)e$;
- k is a positive integer such that $\gcd(k, n) = e$;
- p is an odd prime and $q = p^e$;
- $\mathbb{F}_q$ is the finite field with $q = p^e$ elements and $\mathbb{F}_{p^n} = \mathbb{F}_{q^{2m+1}}$;
- $\mathrm{Tr}_n(x)$ (resp. $\mathrm{Tr}_e(x)$) is the absolute trace function from $\mathbb{F}_{p^n}$ (resp. $\mathbb{F}_{p^e}$) to $\mathbb{F}_p$, and $\mathrm{Tr}_e^n(x)$ is the trace function from $\mathbb{F}_{p^n}$ to the subfield $\mathbb{F}_{p^e}$;

2.1. Quadratic forms over finite fields

Let $x = \sum_{i=0}^{2m} x_i\alpha_i$ where $x_i \in \mathbb{F}_q$ and α_i, $i = 0, 1, ..., 2m$ is a basis for $\mathbb{F}_{q^{2m+1}}$ over $\mathbb{F}_q$. Then the function $Q(x)$ in $\mathbb{F}_{q^{2m+1}}$ is a quadratic form over $\mathbb{F}_q$ if it can be expressed as

$$Q(x) = Q\left(\sum_{i=0}^{2m} x_i\alpha_i\right) = \sum_{i=0}^{2m}\sum_{j=0}^{2m} b_{i,j}x_ix_j$$

where $b_{i,j} \in \mathbb{F}_q$. The quadratic form in odd characteristic has been well analyzed in [8]. The rank of a quadratic form is the minimum number of variables required to represent the function under the nonsingular coordinate transformations, which is related to the dimension of the vector space $\mathcal{W}$ in $\mathbb{F}_{q^{2m+1}}$, i.e.,

$$\mathcal{W} = \{y \in \mathbb{F}_{q^{2m+1}} \mid Q(x+y) = Q(x) \text{ for all } x \in \mathbb{F}_{q^{2m+1}}\}.$$

More precisely, $\rho = 2m + 1 - \dim(\mathcal{W})$.

The main result depends on the following lemma which is an extension and consequence of results from Trachtenberg [10] and Helleseth and Gong [5].

Lemma 1 *Let $Q(x)$ be a quadratic form over $\mathbb{F}_q$ in $2m+1$ variables of rank ρ. Let r be a non-square in $\mathbb{F}_q$ and define*

$$S = \frac{1}{2}\left(\sum_{x\in\mathbb{F}_{q^{2m+1}}} \omega^{Tr_e(Q(x))} + \sum_{x\in\mathbb{F}_{q^{2m+1}}} \omega^{Tr_e(rQ(x))}\right).$$

Then

$$S = \begin{cases} 0, & \text{if } \rho \text{ is odd,} \\ \pm q^{(2m+1)-\rho/2}, & \text{if } \rho \text{ is even.} \end{cases}$$

2.2. Sequences with two-level ideal autocorrelation function

Given two sequences $a = \{a_0, a_1, ..., a_{N-1}\}$ and $b = \{b_0, b_1, ..., b_{N-1}\}$ of period N, we define the periodic cross correlation between a and b at shift τ as

$$C_{a,b}(\tau) = \sum_{t=0}^{N-1} \omega^{a_t - b_{t+\tau}},$$

where ω is a p-th primitive root of unity given by

$$\omega = e^{\frac{2\pi\sqrt{-1}}{p}}.$$

Sequences with ideal autocorrelation properties are of considerable interest because of their applications in spread spectrum communication systems, cryptography and their close connections with difference sets. A number of ideal two-level autocorrelation sequences of period $p^n - 1$ have been discovered during the past few decades [1]. For p-ary sequences with two-level autocorrelation, without using a subfield constructions, there are only two general constructions for any arbitrary odd prime p, which are the well-known m-sequences and the sequences introduced by Helleseth and Gong [5].

Theorem 1 ([5]) *Let s, $1 \le s \le 2m$ be an integer such that $\gcd(s, 2m+1) = 1$. Define $b_0 = 1$, $b_i = b_{2m+1-i}$ and $b_{is} = (-1)^i$ for $i = 1, 2, ..., m$, where indices of b_{is} are taken modulo $2m+1$. Let $u_0 = b_0/2 = (p+1)/2$ and $u_i = b_{2i}$ for $i = 1, 2, ..., m$. Define*

$$f_0(x) = \sum_{i=0}^{m} u_i x^{(p^{2ie}+1)/2}. \tag{1}$$

Then the sequence over $\mathbb{F}_p$ defined by $a(t) = Tr_n(f_0(\alpha^t))$ has an ideal two-level autocorrelation.

Let $\mathcal{F}$ be a family of sequences, $C_{i,j}(\tau)$ denote the crosscorrelation between the i-th and j-th sequences at shift τ, i.e.,

$$C_{i,j}(\tau) = \sum_{t=0}^{p^n-2} \omega^{s_i(t+\tau) - s_j(t)}, \quad 0 \le \tau \le p^n - 2.$$

The maximum correlation value $C_{\max}$ of $\mathcal{F}$ is defined by

$$C_{\max} = \max\{|C_{i,j}(\tau)| : \text{either } i \ne j \text{ or } \tau \ne 0\ \}. \tag{2}$$

The crosscorrelation function is important in code-division multiple-access (CDMA) communication systems. Here each user is assigned a distinct signature sequence. To minimize interference due to the other users, it is desirable that the signature sequences have pairwise low values of crosscorrelation function. The classical goal in sequences design for CDMA systems has been minimization of the parameter $C_{\max}$ and maximization of the family size M for a given period, which are conflicting requirements.

3. Nonbinary sequences from difference-balanced functions

In this section we firstly generalize a parameter of the Helleseth-Gong (HG) sequences. Then we will employ the proposed sequences and m-sequences to construct a sequence family $\mathcal{F}$, which is optimal in the sense that it attains the Welch lower bound [11].

Theorem 2 *Let k be an positive integer such that $\gcd(n,k)=e$. Let $s, 1 \le s \le 2m$ be an integer such that $\gcd(s, 2m+1)=1$. Define $b_0=1$, $b_i=b_{2m+1-i}$ and $b_{is}=(-1)^i$ for $i=1,2,...,m$, where indices of b_{is} are taken modulo $2m+1$. Let $u_0=b_0/2=(p+1)/2$ and $u_i=b_{2i}$ for $i=1,2,...,m$. Define*

$$f(x)=\sum_{i=0}^{m} u_i x^{(p^{2ik}+1)/2}. \tag{3}$$

Then the sequence over $\mathbb{F}_p$ defined by $b(t)=Tr_n(f(\alpha^t))$ has an ideal two-level autocorrelation.

Remark 1 In the case of $k=e$, the function $f(x)$ defined in Theorem 2 reduces to the function f_0 in Theorem 1. Then the sequences $\{a(t)\}$ and $\{b(t)\}$ are the same. Hence Theorem 2 generalizes the result of Theorem 1. Moreover, it is easy to verify that both $f(x)$ and $f_0(x)$ defined in Theorems 1 and 2 are difference-balanced functions.

First, we give an interesting result which will be later used in the proof of Theorem 2.

Define a vector

$$\varepsilon=(\varepsilon_0,\varepsilon_1,...,\varepsilon_{2m}),\ \varepsilon_i=(-1)^i \text{ for } 0\le i\le 2m$$

and the right circular shift operator σ over ε as

$$\sigma(\varepsilon)=(\varepsilon_{2m},\varepsilon_0,...,\varepsilon_{2m-1}).$$

By iterating the shift operator σ over ε, we can obtain a set $\Gamma=\{\varepsilon,\sigma(\varepsilon),...,\sigma^{2m}(\varepsilon)\}$.

Define a $(2m+1)\times(2m+1)$ matrix M as

$$M_{i,j}=\beta_{j-i}(tz_iz_j-1), \tag{4}$$

where

$$\beta=\sigma^r(\varepsilon)=(\varepsilon_{2m+1-r},...,\varepsilon_{2m},\varepsilon_0,...,\varepsilon_{2m-r}) \tag{5}$$

is an element of Γ and the indices of β_i's and z_i's are taken modulo $2m+1$.

For example, when $m=2$ and $r=1$, denoting $t_{i,j}=tz_iz_j-1$ for $0\le i,j\le 4$ for simplicity, we obtain the matrix M as follows.

$$M = \begin{pmatrix} t_{0,0} & t_{0,1} & -t_{0,2} & t_{0,3} & -t_{0,4} \\ -t_{1,0} & t_{1,1} & t_{1,2} & -t_{1,3} & t_{1,4} \\ t_{2,0} & -t_{2,1} & t_{2,2} & t_{2,3} & -t_{2,4} \\ -t_{3,0} & t_{3,1} & -t_{3,2} & t_{3,3} & t_{3,4} \\ t_{4,0} & -t_{4,1} & t_{4,2} & -t_{4,3} & t_{4,4} \end{pmatrix}.$$

The determinant of the matrix M as defined in (4) is characterized in Proposition 1.

Proposition 1 *Let $\beta = \sigma^r(\varepsilon)$ with $0 \le r \le 2m$. The determinant $det(M)$ is given by*

$$det(M) = 2^{2m-1}\left(\prod_{i=0}^{2m}(tz_iz_{i+r} - 1) + \prod_{i=0}^{2m}(tz_iz_{i+r-1} - 1)\right).$$

Proof. Note that for $i = 0, 1, ..., 2m$,

$$\beta_i + \beta_{i-1} = \begin{cases} 2, & \text{if } i = r, \\ 0, & \text{otherwise.} \end{cases}$$

For $i = 0, 1, ..., 2m$, by replacing the i-th row by the sum of the i-th and $(i+1)$-th row (where indices are taken modulo $2m+1$), we obtain a matrix N with the entity

$$\begin{aligned} N_{i,j} &= \beta_{j-i}(tz_iz_j - 1) + \beta_{j-(i+1)}(tz_{i+1}z_j - 1) \\ &= \begin{cases} tz_j(z_i + z_{i+1}) - 2, & \text{if } j - i = r, \\ \beta_{j-i}tz_j(z_i - z_{i+1}), & \text{otherwise.} \end{cases} \end{aligned}$$

Then dividing the elements in the i-th row by $t(z_i - z_{i+1})$ and the elements in the j-th column by z_j, the determinant of the matrix N becomes

$$det(N) = \prod_{i=0}^{2m}(t(z_i - z_{i+1}))\prod_{j=0}^{2m} z_j \cdot det(R),$$

where R is a $(2m+1) \times (2m+1)$ matrix such that

$$R_{i,j} = \begin{cases} \dfrac{(tz_j(z_i + z_{i+1}) - 2)}{tz_j(z_i - z_{i+1})}, & \text{if } j - i = r, \\ \beta_{j-i}, & \text{otherwise.} \end{cases}$$

We repeat the process above for the matrix R, i.e., for $i = 0, 1, ..., 2m$ we replace the i-th row with the sum of the i-th and $(i+1)$-th rows (where indices are taken modulo $2m+1$). Performing these row operations on R leads to a matrix where all elements are zeros except for only two nonzero elements in each row. The only two nonzero elements in the resulting matrix S are

$$\begin{aligned} S_{i,i+r} &= \beta_{r-1} + (tz_{i+r}(z_i + z_{i+1}) - 2)/tz_{i+r}(z_i - z_{i+1}) \\ &= 2(tz_iz_{i+r} - 1)/tz_{i+r}(z_i - z_{i+1}) \end{aligned}$$

and for $j = i + r + 1$,

$$\begin{aligned} S_{i,j} &= \beta_{r+1} + (tz_j(z_{i+1} + z_{i+2}) - 2)/tz_j(z_{i+1} - z_{i+2}) \\ &= 2(tz_{i+2}z_j - 1)/tz_j(z_{i+1} - z_{i+2}). \end{aligned}$$

Thus, the determinant of S is a product of two terms along two "diagonals" corresponding to indices $(i, i + r)$ and $(i, i + r + 1)$ respectively for $i = 0, 1, ..., 2m$. That is to say, the determinant

$$\begin{aligned} det(S) =& \prod_{i=0}^{2m} \frac{2(tz_iz_{i+r} - 1)}{tz_{i+r}(z_i - z_{i+1})} + \prod_{i=0}^{2m} \frac{2(tz_{i+2}z_{i+r+1} - 1)}{tz_{i+r+1}(z_{i+1} - z_{i+2})} \\ =& \prod_{i=0}^{2m} \frac{2(tz_iz_{i+r} - 1)}{tz_{i+r}(z_i - z_{i+1})} + \prod_{i=0}^{2m} \frac{2(tz_{i+1}z_{i+r} - 1)}{tz_{i+r}(z_i - z_{i+1})}. \end{aligned}$$

Note that the determinant of the matrix with rows r_i for $i = 0, 1, ..., 2m$ is one half of the matrix with row $r_i + r_{i+1}$ for $i = 0, 1, ..., 2m$. This implies,

$$\begin{aligned} det(M) &= det(N)/2 \\ &= \prod_{i=0}^{2m}(t(z_i - z_{i+1})) \prod_{j=0}^{2m} z_j \cdot det(R)/2 \\ &= \prod_{i=0}^{2m}(t(z_i - z_{i+1})) \prod_{j=0}^{2m} z_j \cdot det(S)/4 \\ &= 2^{2m-1} \left(\prod_{i=0}^{2m}(tz_iz_{i+r} - 1) + \prod_{i=0}^{2m}(tz_{i+1}z_{i+r} - 1) \right) \\ &= 2^{2m-1} \left(\prod_{i=0}^{2m}(tz_iz_{i+r} - 1) + \prod_{i=0}^{2m}(tz_iz_{i+r-1} - 1) \right). \end{aligned}$$

The proof is ended. ∎

We are now ready for the proof of Theorem 2.

Proof of Theorem 2. The autocorrelation of $\{b(t)\}$ at shift τ is given by

$$\begin{aligned} A_b(\tau) &= \sum_{t=0}^{p^n-2} \omega^{b(t+\tau)-b(t)} \\ &= \sum_{t=0}^{p^n-2} \omega^{\mathrm{Tr}_n(f(\alpha^{t+\tau})-f(\alpha^t))} \\ &= -1 + \sum_{x \in \mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_n(f(\alpha^\tau x)-f(x))}. \end{aligned}$$

In the following, we will investigate the value of $A_b(\tau)$ when τ is nonzero. From the definition, one has $f(\lambda x) = \lambda f(x)$ for any $\lambda \in \mathbb{F}_{p^e}$ since $(p^{2ik}+1)/2 \equiv 1 \pmod{p^e-1}$ for $i = 0, 1, ..., m$. Denote $p(x) = f(\alpha^\tau x) - f(x)$. It follows from Lemma 1 that

$$A_b(\tau) + 1 = \frac{1}{2}\left(\sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_e(Q(x))} + \sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_e(rQ(x))}\right)$$

$$= \begin{cases} 0, & \text{if } \rho \text{ is odd,} \\ \pm q^{2m+1-\rho/2}, & \text{otherwise,} \end{cases}$$

where

$$Q(x) = \mathrm{Tr}_e^n(p(x^2)) = \mathrm{Tr}_e^n(f(\alpha^\tau x^2) - f(x^2)) \tag{6}$$

is a quadratic form over $\mathbb{F}_q$ and ρ is the rank of $Q(x)$. To determine the rank ρ, as stated in Section 2.1, we need to consider the number of solutions $y \in \mathbb{F}_{p^n} (= \mathbb{F}_{q^{2m+1}})$, such that $Q(x+y) = Q(x)$ for all $x \in \mathbb{F}_{p^n}$. In the following we represent each element $c = \alpha^\tau \in \mathbb{F}_{p^n}$ in the form $c = t\gamma^2$ where $t = 1$ or t is a non-square in the subfield $\mathbb{F}_q$. For simplicity, we denote $v_i = u_i(c^{(p^{2ik}+1)/2} - 1) = u_i(t\gamma^{p^{2ik}+1} - 1)$, then

$$Q(x) = \mathrm{Tr}_e^n(f(\alpha^\tau x^2) - f(x^2)) = \mathrm{Tr}_e^n\left(\sum_{i=0}^{m} v_i x^{p^{2ik}+1}\right).$$

Thus, $Q(x+y) = Q(x)$ is equivalent to

$$\mathrm{Tr}_e^n\left(\sum_{i=0}^{m} v_i((x+y)^{p^{2ik}+1}\right) = \mathrm{Tr}_e^n\left(\sum_{i=0}^{m} v_i x^{p^{2ik}+1}\right),$$

i.e.,

$$\mathrm{Tr}_e^n\left(\sum_{i=0}^{m} v_i(x^{p^{2ik}}y + xy^{p^{2ik}}) + \sum_{i=0}^{m} v_i y^{p^{2ik}+1}\right) = 0.$$

If this holds for all $x \in \mathbb{F}_{q^{2m+1}}$, we must have

$$\mathrm{Tr}_e^n\left(\sum_{i=0}^{m} v_i(x^{p^{2ik}}y + xy^{p^{2ik}})\right) = \mathrm{Tr}_e^n\left(x\left(\sum_{i=0}^{m}(v_i^{p^{-2ik}}y^{p^{-2ik}} + v_i y^{p^{2ik}})\right)\right) = 0$$

and

$$\mathrm{Tr}_e^n\left(\sum_{i=0}^{m} v_i y^{p^{2ik}+1}\right) = 0.$$

The first equation holds for all $x \in \mathbb{F}_{q^{2m+1}}$ if and only if

$$L(y) = \sum_{i=0}^{m}\left(v_i^{p^{-2ik}}y^{p^{-2ik}} + v_i y^{p^{2ik}}\right) = 0.$$

The second equation follows directly as a consequence of $L(y) = 0$ by considering $\mathrm{Tr}_e^n(yL(y)) = 0$. Hence, $Q(x+y) = Q(x)$ holds for all $x \in \mathbb{F}_{q^{2m+1}}$ if and only if

$L(y) = 0$. That is to say, in order to show the rank of $Q(x)$ is $2m+1$, it suffices to show that the equation $L(y) = 0$ has only one solution $y = 0$.

From the definition of v_i, we have

$$L(y) = \sum_{i=0}^{m} u_i \left((t\gamma^{p^{-2ik}+1} - 1)y^{p^{-2ik}} + (t\gamma^{p^{2ik}+1} - 1)y^{p^{2ik}} \right).$$

Further, since $u_i = b_{2i}$, $b_i = b_{2m+1-i}$ for $i = 0, 1, ..., m$ and $\gcd(s, 2m + 1) = 1$,

$$\begin{aligned} L(y) &= \sum_{i=0}^{2m} b_i (t\gamma^{p^{ik}+1} - 1)y^{p^{ik}} \\ &= \sum_{i=0}^{2m} b_{is} (t\gamma^{q^{isf}+1} - 1)y^{q^{isf}}, \end{aligned}$$

where $f = k/e$.

Raising the linearized equations $L(y) = 0$ to the q^{isf} power for $i = 0, 1, ..., 2m$, we can obtain a linear equation system with $2m + 1$ equations in the $2m + 1$ unknowns $y^{q^{jsf}}$ for $j = 0, 1, ..., 2m$. The coefficient matrix $M = (m_{i,j})$ of this system is given by

$$m_{i,j} = b_{(j-i)s}(t\gamma^{q^{isf}+q^{jsf}} - 1)$$

where the indices are taken modulo $2m + 1$ and $m_{i,j}$ is the coefficient of $y^{q^{jsf}}$ in the equation $(L(y))^{q^{isf}} = 0$.

Note that $b_{is} = (-1)^i$ and $b_i = b_{2m+1-i}$, for $i = 1, ..., m$. Thus, the vector $b = (b_0, b_s, ..., b_{2ms})$ becomes

$$\begin{aligned} b &= (1, -1, ..., (-1)^m, (-1)^m, ..., -1) \\ &= (-1)^m((-1)^m, ..., (-1)^{2m}, (-1)^0, ..., (-1)^{m-1}) \\ &= (-1)^m \sigma^{m+1}(\varepsilon) \end{aligned}$$

where $\sigma^{m+1}(\varepsilon)$ is as given in (5). Denote the variables $z_i = \gamma^{q^{isf}}$ for $i = 0, 1, ..., 2m$. Then it follows from Proposition 1 that the determinant of the coefficient matrix M is

$$\begin{aligned} \Delta &= (-1)^m 2^{2m-1} \left(\prod_{i=0}^{2m} (tz_i z_{i+m+1} - 1) + \prod_{i=0}^{2m} (tz_i z_{i+m} - 1) \right) \\ &= (-1)^m 2^{2m} \prod_{i=0}^{2m} (tz_i z_{i+m} - 1). \end{aligned}$$

Note that $z_i z_{i+m} = \gamma^{q^{isf}+q^{(i+m)sf}}$ is a square. Thus, if t is a non-square, $tz_i z_{i+m} - 1 \neq 0$ for $i = 0, 1, ..., 2m$, which implies $\Delta \neq 0$. When $t = 1$, suppose the determinant $\Delta = 0$, then we have $\gamma^{q^{isf}+q^{(i+m)sf}} = 1$ for some integer i, which is equivalent to $\gamma^{\gcd(q^{msf}+1, q^{2m+1}-1)} = 1$. Since $(q^{msf} + 1, q^{2m+1} - 1) = 2$, we have $\gamma^2 = 1$. This leads to a contradiction $c = t\gamma^2 = 1$. Thus, the linear equation system with $(L(y))^{q^{isf}} = 0$ for $i = 0, 1, ..., 2m$ has $y = 0$ as its only solution. This implies the quadratic form

$Q(x) = \mathrm{Tr}_e^n(f(\alpha^\tau x^2) - f(x^2))$ has rank $2m+1$ when $\tau \neq 0$. Thus, $A_b(\tau) + 1 = 0$ when τ is nonzero. ∎

The following proposition characterizes the sufficient and necessary condition for cyclic equivalence of the sequences given in Theorems 1 and 2.

Proposition 2 *Let $k_1 = k/e$. Let $\{a(t)\}$ and $\{b(t)\}$ be the sequences as defined in Theorems 1 and 2. Then $C_{a,b}(\tau) = p^n - 1$ if and only if $\tau = 0$ and for any $0 \leq i \leq 2m$, $b_i = b_{\sigma(i)}$, where $\sigma(i) \equiv i \cdot k_1^{-1} \pmod{2m+1}$.*

Proof. As discussed in the proof of Theorem 2,

$$C_{a,b}(\tau) + 1 = \frac{1}{2}\left(\sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_e(Q_1(x))} + \sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_e(rQ_1(x))}\right),$$

where $Q_1(x) = \mathrm{Tr}_e^n(f_0(x^2) - f(cx^2))$ is a quadratic form in $\mathbb{F}_{q^{2m+1}}$, $c = \alpha^\tau$ and r is a nonsquare of $\mathbb{F}_q$. Note that $C_{a,b}(\tau) = p^n - 1$ if and only if the rank of the quadratic form $Q_1(x)$ equals to zero. That is to say, $C_{a,b}(\tau) = p^n - 1$ if and only if $Q_1(x+y) = Q_1(x)$ holds for any $x, y \in \mathbb{F}_{q^{2m+1}}$. Similar to the method adopted in Theorem 2, $Q_1(x+y) = Q_1(x)$ holds for any $x, y \in \mathbb{F}_{q^{2m+1}}$ is equivalent to the linearized equation

$$\sum_{i=0}^{m}\left(u_i(y^{q^{2i}} + y^{q^{2m+1-2i}})\right) = \sum_{i=0}^{m}\left(u_i c^{\frac{q^{2if}+1}{2}} y^{q^{2if}} + u_i(c^{\frac{q^{-2if}+1}{2}} y^{q^{-2if}})^{q^{(2m+1)f}}\right)$$

holds for any $y \in \mathbb{F}_{q^{2m+1}}$. From the definition of $u_i = b_{2i}$ for $i = 0, 1, ..., m$, this equation is rewritten as

$$\begin{aligned}\sum_{i=0}^{2m} b_i y^{q^i} &= \sum_{i=0}^{2m} b_i c^{\frac{q^{if}+1}{2}} y^{q^{if}} \\ &= \sum_{i=0}^{2m} b_{if^{-1}} c^{\frac{q^i+1}{2}} y^{q^i}.\end{aligned}$$

Therefore, $Q_1(x+y) = Q_1(x)$ holds for any $x, y \in \mathbb{F}_{q^{2m+1}}$ if and only if $b_i = b_{if^{-1}} c^{\frac{q^i+1}{2}}$ for $i = 0, 1, ..., 2m$. It is easily obtained that $c = \alpha^\tau = 1$ for $i = 0$ and $b_i = b_{ik_1^{-1}}$ for $i = 0, 1, ..., 2m$. ∎

Due to Proposition 2, the task of finding cyclically inequivalent sequences in Theorems 1 and 2 can be reduced to find parameters m, s, f such that the condition $b_i = b_{\sigma(i)}$ for $i = 0, 1, ..., 2m$ is not fulfilled, which is independent of the value of p and e.

By employing the HG sequences, a family of p-ary sequences of period $p^n - 1$ with size p^n [7]. The maximum nontrivial correlation value $C_{\max}$ of all pairs of distinct sequences in the family does not exceed $p^{n/2} + 1$, which means the family has optimal correlation with respect to Welch's lower bound [11]. Similar to the idea adopted in [7], we define

$$\mathcal{F} = \left\{s_i(t) \,|\, 0 \leq i \leq p^n - 1, 0 \leq t \leq p^n - 2\right\} \tag{7}$$

with

$$s_i(t) = \mathrm{Tr}_n(\alpha^t) + \mathrm{Tr}_n(f(\delta_i \alpha^{2t})), \tag{8}$$

where $f(x)$ is defined as in Theorem 2 and $\{\delta_i \,|\, 0 \le i \le p^n - 1\}$ is an enumeration of elements in the field $\mathbb{F}_{p^n}$. Specially, let $\delta_{p^n-1} = 0$.

The correlation property can be investigated in a similar way as in [7]. We give a brief proof here. By the definition of the cross-correlation function, we have

$$\begin{aligned} C_{i,j}(\tau) &= \sum_{t=0}^{p^n-2} \omega^{s_i(t+\tau)-s_j(t)} \\ &= \sum_{t=0}^{p^n-2} \omega^{\mathrm{Tr}_n(\alpha^{t+\tau}+f(\delta_i\alpha^{2(t+\tau)})-\alpha^t-f(\delta_j\alpha^{2t})} \\ &= -1 + \sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_n(f(\delta_i\varepsilon^2x^2)-f(\delta_jx^2)+(\varepsilon-1)x)}, \end{aligned} \tag{9}$$

where $\varepsilon = \alpha^\tau \in \mathbb{F}_{p^n}^*$. We can divide the computation of the cross-correlation $C_{i,j}(\tau)$ into the following cases depending on different values of t, i and j.

1) $\tau = 0$, $i = j$. In this trivial case, $\varepsilon = 1$ and $\delta_i = \delta_j$. Thus, $C_{i,j}(\tau) = p^n - 1$.

2) $\tau \neq 0$ and $\delta_i\varepsilon^2 = \delta_j$. In this case,

$$C_{i,j}(\tau) = -1 + \sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_n((\varepsilon-1)x)} = -1.$$

3) $\delta_i\varepsilon^2 \neq \delta_j$. Denote $\delta_i = \theta_i\eta_i^2$ for $0 \le i \le p^n - 1$, where θ_i is a non-square in $\mathbb{F}_{p^e}$ if δ is a non-square in $\mathbb{F}_{p^n}$ and $\theta_i = 1$ otherwise. Then,

$$\begin{aligned} C_{i,j}(\tau) &= -1 + \sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_n(f(\theta_i\eta_i^2\varepsilon^2x^2)-f(\theta_j\eta_j^2x^2)+(\varepsilon-1)x)} \\ &= -1 + \sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_n\left(f(\theta_i\frac{\eta_i^2\varepsilon^2}{\eta_j^2}x^2)-f(\theta_jx^2)+\frac{(\varepsilon-1)}{\eta_j}x\right)} \end{aligned} \tag{10}$$

Let $\zeta = \theta_i\frac{\eta_i^2\varepsilon^2}{\eta_j^2}$ and $\lambda = \frac{(\varepsilon-1)}{\eta_j}$. Define

$$Q_2(x) = \mathrm{Tr}_e^n(f(\zeta x^2) - f(\delta_j x^2)). \tag{11}$$

Then we have

$$C_{i,j}(\tau) = -1 + \sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_e(Q_2(x))+\mathrm{Tr}_n(\lambda x)}.$$

It is shown in Theorem 2 that the quadratic form $Q(x) = \mathrm{Tr}_e^n(f(cx^2) - f(x^2)$ has full rank for any nonzero element $c \in \mathbb{F}_{p^n}^*$. By the definition of $f(x)$, it follows that the quadratic form

$$Q_2(x) = \delta_j\mathrm{Tr}_e^n(f(\tfrac{\zeta}{\delta_j}x^2) - f(x^2)) = \delta_jQ(x)$$

with $c = \frac{\zeta}{\delta_j}$ has the full rank. Then

$$\Big|\sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_e(Q_2(x))+\mathrm{Tr}_n(\lambda x)}\Big| = p^{n/2} \text{ for any } \lambda \in \mathbb{F}_{p^n}.$$

Furthermore, one deduces $|C_{i,j}(\tau) + 1| = p^{n/2}$ in this case.

By combining cases 1), 2) and 3), we have the following theorem.

Theorem 3 *The family $\mathcal{F}$ defined in* (7) *has the optimal correlation property with* $C_{max} = p^{n/2} + 1$.

4. Conclusion

In this paper, we generalized the function introduced by Helleseth and Gong [5], which generates sequences over $\mathbb{F}_p$ with two-level ideal autocorrelation. Moreover, by properly choosing the parameter k we can deduce sequences among the proposed sequences that are cyclically inequivalent to the HG sequences. By employing the proposed sequences and m-sequences, a nonbinary sequence family with optimal correlation property was constructed.

Acknowledgements. The author is thankful to the anonymous reviewers for their valuable suggestions. This work was supported by National Natural Science Foundation of China (Grant Nos. 61303212, 61170080), the State Key Program of National Natural Science of China (Grant Nos. 61332019, U1135004).

References

[1] Arasu, K.T., *Sequences and arrays with desirable correlation properties,* Information Security, Coding Theory and Related Combinatorics, 2011, 136-171.

[2] Golomb, S.W., *Shift register sequences*, Aegean Park Press, 1982.

[3] Golomb, S.W.,Gong, G., *Signal design for good correlation for wireless communication, cryptography, and radar*, Cambridge University Press, 2005.

[4] Helleseth, T., *Codes over $Z(4)$*, Computational Discrete Mathematics: Advanced Lectures, 2122 (2011), 47–55.

[5] Helleseth, T., Gong, G., *New nonbinary sequences with ideal two-level autocorrelation*, IEEE Transactions on Information Theory, 48 (11) (2002), 2868–2872.

[6] Helleseth, T., Kumar, P.V., *Sequences with low correlation*, In *Handbook of Coding Theory*, (V.S. Pless and W.C. Huffman, eds.), Elsevier Science, 1998, 1765–1853.

[7] Jang, J.W., Kim, Y.S., No, J.S., Helleseth, T., *New family of p-ary sequences with optimal correlation property and large linear span*, IEEE Transactions on Information Theory, 50 (8) (2002), 1839–1844.

[8] Lidl, R., Niederreiter, H., *Finite fields*, 2nd edition, Cambridge University Press, Cambridge, New York, 1997.

[9] Simon, M.K., Omura, J.K., Scholtz, R.A., Levitt, B.K., *Spread Spectrum Communications*, Electrical Engineering, Telecommunications and Signal Processing Series, Computer Science Press, 1988.

[10] Trachtenberg, H.M., *On the cross-correlation functions of maximal linear sequences*, PhD thesis, University of Southern Califorina, 1970.

[11] Welch, L.R., *Lower bounds on maximum cross-correlation of signals*, IEEE Transactions on Information Theory, 20 (3) (1974), 397–399.

Accepted: 23.10.2015