Journal of Theoretical and Applied Information Technology
10th June 2013. Vol. 52 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

GENERALIZED *P*-ARY SEQUENCES WITH TWO-LEVEL AUTOCORRELATION

[1] XINJIAO CHEN, [2] HUANGUO ZHANG

[1]Affiliation, School of Computer Science Wuhan University, P.R. CHINA

[2]Affiliation, School of Computer Science Wuhan University, P.R. CHINA

E-mail: [1]xinjiaochen@hotmail.com, [2]liss@whu.edu.cn

ABSTRACT

In this paper, we find a family of p-ary sequences with ideal two-level autocorrelation with symbols in the finite field $\mathbb{F}_p$. The proposed family may be considered as a generalization of the well-known nonbinary sequences introduced by Helleseth and Gong. Using the constructed sequences and m-sequences, we present a family of p-ary sequences of which the correlation property is optimal in terms of the Welch lower bound.

Keywords: *Communication Systems, Pseudorandom Sequences, Correlation, Ideal Two-Level Autocorrelation*

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 [1-5]. 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 [2] and [4]. In recent years, there have been numerous researches on binary sequences with two-level autocorrelation property, see [2] 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 [4] 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 [5]. This is another general construction for p-ary sequences with ideal autocorrelation property and we refer it as HG sequence in the sequel. Using p-ary HG sequences, Jang, *et al* presented a family of nonbinary sequences having optimal auto- and cross-correlation property with respect to the well-known Welch bound [6].

In the present paper, we give a class of p-ary sequence with two-level ideal autocorrelation which shall be referred as a generalization of the HG sequence. With the proposed construction, a family of p-ary sequence with period p^n-1, size p^n and the maximal nontrivial correlation value $R_{\max}$ not exceeding $p^{n/2}+1$ is proposed.

2. PRELIMILARIES

Let $n=(2m+1)e$ and p an odd prime. Throughout we denote the finite field of order p^n by $\mathbb{F}_{p^n}$ and its nonzero elements by $\mathbb{F}_{p^n}^*$, and we assume α is a primitive element of $\mathbb{F}_{p^n}$. Let $q=p^e$. We denote $\mathbb{F}_{p^e}$ as $\mathbb{F}_q$ and $\mathbb{F}_{p^n}$ as $\mathbb{F}_{q^{2m+1}}$ when convenient. Let $\mathrm{Tr}_e^n(x)$ (and, respectively, $\mathrm{Tr}_1^e(x)$) be the trace mapping from $\mathbb{F}_{p^n}$ into the subfield $\mathbb{F}_q$ (and, respectively, from $\mathbb{F}_q$ into $\mathbb{F}_p$). They are given by

$$\mathrm{Tr}_e^n(x)=\sum_{i=0}^{2m}x^{p^{ie}},\quad \mathrm{Tr}_1^e(x)=\sum_{i=0}^{e-1}x^{p^i}.$$

For simplicity, we denote $\mathrm{Tr}_1^n(x)$ (and, respectively, $\mathrm{Tr}_1^e(x)$) as $\mathrm{Tr}_n(x)$ (and respectively, $\mathrm{Tr}_e(x)$).

Given two sequences $a=\{a_0,a_1,\cdots,a_{N-1}\}$ and $b=\{b_0,b_1,\cdots,b_{N-1}\}$ 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 the p-th root of unity given by $\omega=e^{\frac{2\pi\sqrt{-1}}{p}}$. In particular, we denote the cross

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

correlation of a with itself at shift τ by $A_a(\tau)$, which is the autocorrelation of a. A sequence a of period N is called an ideal two-level autocorrelation sequence if $A_a(\tau) = -1$ for any $\tau \neq 0 \pmod N$.

Let $x = \sum_{i=0}^{2m} x_i\alpha_i$ where $x_i \in \mathbb{F}_q$ and α_i, $i = 0, 1, \cdots, 2m$ 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

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

where $b_{i,j} \in \mathbb{F}_q$. The quadratic form in odd characteristic has been well analyzed in [7]. 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.,

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

for all $x \in \mathbb{F}_{q^{2m+1}}$. More precisely,

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

It is well known that any quadratic form of rank ρ can be transferred to one of the following three canonical form [7].

Lemma 1. For any quadratic form $Q(x)$ in $\mathbb{F}_q$, if the rank of $Q(x)$ is ρ, then $Q(x)$ is equivalent to the following

Type I: $B_\rho(x)$;
Type II: $B_{\rho-1}(x) + \mu x_\rho^2$;
Type III: $B_{\rho-2}(x) + x_{\rho-1} - \lambda x_\rho^2$;

where $B_\rho = x_1x_2 + \cdots + x_{\rho-1}x_\rho$, $\mu \in \{1, \lambda\}$ and λ is a fixed nonsquare in $\mathbb{F}_q$. For any element $\xi \in \mathbb{F}_q$, the number of solutions to the equation $Q(x) = \zeta$ is as follows:

Type I: $q^{2m} + v(\zeta)q^{2m-\rho/2}$;
Type II: $q^{2m} + \eta(\zeta\mu)q^{2m+1-(\rho+1)/2}$;
Type III: $q^{2m} - v(\zeta)q^{2m-\rho/2}$;

where $v(x)$ and $\eta(x)$ are functions in $\mathbb{F}_q$, respectively, given by

$$v(x) = \begin{cases} -1 & \text{if } x \neq 0, \\ q-1 & \text{otherwise.} \end{cases}$$

and

$$\eta(x) = \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x \text{ is a squre} \\ -1 & \text{otherwise.} \end{cases}$$

Let $p(x)$ be a polynomial with coefficients in $\mathbb{F}_{p^n}$ such that $p(\lambda x) = \lambda p(x)$ for any $\lambda \in \mathbb{F}_{p^e}$. Let d be a positive integer such that $\gcd(d, p^n - 1) = 2$ and $d \equiv 2 \pmod{p^e - 1}$. Then,

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

where $Q(x) = \mathrm{Tr}_e^n(p(x^d))$ is a quadratic form over $\mathbb{F}_q$ and r is a nonsquare in $\mathbb{F}_q$.

The main result depends on the following lemma which is an extension and consequence of results from Trachtenberg [9] and Helleseth and Gong [4].

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

$$S = \frac{1}{2}\Big(\sum_{x\in\mathbb{F}_{q^{2m+1}}} \omega^{\mathrm{Tr}_k(Q(x))} + \sum_{x\in\mathbb{F}_{q^{2m+1}}} \omega^{\mathrm{Tr}_k(rQ(x))}\Big).$$

Then

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

Helleseth and Gong in [4] introduced a family of p-ary sequences with ideal two-level autocorrelation.

Theorem 1. ([4]) 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 $i = 1, 2, \cdots, m$, 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 $i = 1, 2, \cdots, m$. Define

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

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

Using the above Helleseth-Gong sequences, a family of p-ary sequences of period $p^n - 1$ with size p^n, which has the optimal correlation property, was constructed in [8]. That is, 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 lower bound [6].

3. NONBINARY SEQUENCES WITH IDEAL AUTOCORRELATION

Similar to the idea adopted by Helleseth and Gong, we present a family of nonbinary sequences with two-level autocorrelation in this paper.

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 $i = 1, 2, \cdots, m$, where indices of b_{is} are taken

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

modulo $2m+1$. Let $u_0 = b_0/2 = (p+1)/2$ and $u_i = b_{2i}$ for $i = 1, 2, \cdots, m$. Define

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

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

Remark 1. For the special case of $k = e$, the function $f(x)$ defined in Theorem 2 turns to be the function f_0 in Theorem 1. Then the sequences $\{a(t)\}$ and $\{b(t)\}$ are the same. In general, we will show in Proposition 2 and Example 1 that there exist integers k such that the sequences $\{a(t)\}$ and $\{b(t)\}$ are cyclically inequivalent. Hence we regard the sequences obtained in Theorem 2 as generalized Hellseth-Gong sequences.

We firstly give an interesting result which will be used in the proof of Theorem 2.

Define a vector

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

and the right circular shift operator σ over ε as

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

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

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

$$M_{i,j} = \beta_{j-i}(tz_i z_j - 1), \quad (3)$$

where

$$\beta = \sigma^r(\varepsilon) = (\varepsilon_{2m+1-r}, \cdots, \varepsilon_{2m}, \varepsilon_0, \cdots, \varepsilon_{2m-r}) \quad (4)$$

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 $t_{i,j} = tz_i z_j - 1$ 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 (3) 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

$$det(M) = 2^{2m-1}\Big(\prod_{i=0}^{2m}(tz_i z_{i+r}-1) + \prod_{i=0}^{2m}(tz_i z_{i+r-1}-1)\Big).$$

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

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

For $i = 0, 1, \cdots, 2m$, 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 entity

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

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

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

We repeat the process above for the matrix R, i.e., for $i = 0, 1, \cdots, 2m$ we replace the i-th row the sum of the i-th and $(i+1)$-th row (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 nonzero elements in the resulting matrix S are

$$S_{i,i+r} = \beta_{r-1} + (tz_{i+r}(z_i + z_{i+1}) - 2)/tz_{i+r}(z_i - z_{i+1})$$
$$= 2(tz_i z_{i+r} - 1)/tz_{i+r}(z_i - z_{i+1})$$

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

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

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 $i = 0, 1, \cdots, 2m$. That is to say, the determinant

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

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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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

The proof is ended. ■

We can now complete 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 $i = 0, 1, \cdots, m$.

Denote $p(x) = f(\alpha^\tau x) - f(x)$. It follows from Lemmas 2 and 3 that

$$\begin{aligned}A_b(\tau) + 1 &= \frac{1}{2}\Big(\sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_e(Q(x))} + \sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_e(rQ(x))}\Big)\\ &= \begin{cases}0, & \text{if } \rho \text{ is odd},\\ \pm q^{2m+1-\rho/2}, & \text{otherwise},\end{cases}\end{aligned}$$

where

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

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, 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

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

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

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

i.e.,

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

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

$$\begin{aligned}&\mathrm{Tr}_e^n\Big(\sum_{i=0}^{m} v_i(x^{p^{2ik}}y + xy^{p^{2ik}})\Big)\\ =&\mathrm{Tr}_e^n\Big(x\Big(\sum_{i=0}^{m}(v_i^{p^{-2ik}}y^{p^{-2ik}} + v_i y^{p^{2ik}})\Big)\Big)\\ =&0\end{aligned}$$

and

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

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

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

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

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

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

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

where $f = k/e$. Raising the linearized equations $L(y) = 0$ to the q^{isf} power for $i = 0, 1, \cdots, 2m$, we can obtain a linear equation system with $2m+1$ equations in the $2m+1$ unknowns $y^{q^{jsf}}$ for $j = 0, 1, \cdots, 2m$. 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 $i = 1, \cdots, m$. Thus the vector $b = (b_0, b_s, \cdots, b_{2ms})$ becomes

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$b=(1,-1,\cdots,(-1)^m,(-1)^m,\cdots,-1)$$
$$=(-1)^m((-1)^m,\cdots,(-1)^{2m},(-1)^0,\cdots,(-1)^{m-1})$$
$$=(-1)^m\sigma^{m+1}(\varepsilon)$$

where $\sigma^{m+1}(\varepsilon)$ is as given in (4). Denote the variables $z_i=\gamma^{q^{isf}}$ for $i=0,1,\cdots,2m$. Then it follows from Proposition 1 that the determinant of the coefficient matrix M is

$$\Delta=(-1)^m2^{2m-1}\Big(\prod_{i=0}^{2m}(tz_iz_{i+m+1}-1)+\prod_{i=0}^{2m}(tz_iz_{i+m}-1)\Big)$$
$$=(-1)^m2^{2m}\prod_{i=0}^{2m}(tz_iz_{i+m}-1).$$

Note that $z_iz_{i+m}=\gamma^{q^{isf}+q^{(i+m)sf}}$ is a square. Thus, if t is a non-square, $tz_iz_{i+m}-1\neq 0$ for $i=0,1,\cdots,2m$, 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 $i=0,1,\cdots,2m$ 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 is nonzero. ■

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

Proposition 2. Let $f=k/e$. 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 $0\le i\le 2m$, $b_i=b_{\sigma(i)}$, where $\sigma(i)\equiv i\cdot f^{-1}\pmod{2m+1}$.

Proof. As discussed in the proof of Theorem 2,

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

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

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

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

$$\sum_{i=0}^{2m}b_iy^{q^i}=\sum_{i=0}^{2m}b_ic^{\frac{q^{if}+1}{2}}y^{q^{if}}=\sum_{i=0}^{2m}b_{if^{-1}}c^{\frac{q^i+1}{2}}y^{q^i}.$$

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 $i=0,1,\cdots,2m$. It is easily obtained that $c=\alpha^\tau=1$ for $i=0$ and $b_i=b_{if^{-1}}$ for $i=0,1,\cdots,2m$. ■

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 $i=0,1,\cdots,2m$ is not fulfilled, which is independent of the value of p and e. We give two such examples in the following.

Example 1. (i) For $m=2$ and $s=2$, it follows from the definition that $B=(b_0,b_1,b_2,b_3,b_4)=(1,-1,-1,1,1)$ and $(u_0,u_1,u_2)=(1,-1,1)$.Denote

$$B'=(b_{\sigma(0)},b_{\sigma(1)},b_{\sigma(2)},b_{\sigma(3)},b_{\sigma(4)}).$$

If $f=2$, then the inverse of f modulo $2m+1$ is 3. This implies

$$B'=(b_0,b_3,b_1,b_4,b_2)=(1,1,-1,1,-1)\neq B.$$

Then for any odd prime q and positive integer e, the two sequences

$$a(t)=\mathrm{Tr}_n(\alpha^t-\alpha^{t(q^2+1)/2}+\alpha^{t(q^4+1)/2})$$

and

$$b(t)=\mathrm{Tr}_n(\alpha^t-\alpha^{t(q^4+1)/2}+\alpha^{t(q^8+1)/2})$$

are cyclically inequivalent.

(ii) For $m=3$ and $s=2$, it follows from the definition that

$$B=(b_0,b_1,b_2,b_3,b_4,b_5,b_6)=(1,1,-1,-1,1,1,-1)$$

and $(u_0,u_1,u_2,u_3)=(1,-1,1,-1)$. Denote $B'=(b_0,b_{\sigma(1)},\cdots,b_{\sigma(6)})$. If $f=3$, then the inverse of f modulo $2m+1$ is 5. This implies

$$B'=(b_0,b_5,b_3,b_1,b_6,b_4,b_2)=(1,1,-1,1,-1,1,-1)\neq B.$$

Then for any odd prime p and positive integer

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

e, the two sequences
$a(t) = \mathrm{Tr}_n(\alpha^t - \alpha^{t(q^2+1)/2} + \alpha^{t(q^4+1)/2}) - \alpha^{t(q^6+1)/2})$
and
$b(t) = \mathrm{Tr}_n(\alpha^t - \alpha^{t(q^{10}+1)/2} + \alpha^{t(q^{20}+1)/2} - \alpha^{t(q^{30}+1)/2})$
$= \mathrm{Tr}_n(\alpha^t - \alpha^{t(q^{10}+1)/2} + \alpha^{t(q^6+1)/2} - \alpha^{t(q^2+1)/2})$
are cyclically inequivalent.

Now we turn to the construction of a sequence family of which the (auto- and cross-) correlation is optimal up to the Welch bound. Similar to the method in [6], an extended family of p -ary sequence with optimal cross correlation property is presented in this paper.

Let $f(x)$ be defined as in Theorem 2. A family of p-ary sequence of period $p^n - 1$ with family size p^n is defined as
$\mathcal{S} = \{s_i(t) \mid 0 \le i \le p^n - 1, 0 \le t \le p^n - 2\}$, (5)
where $s_i(t) = \mathrm{Tr}_n(\alpha^t) + \mathrm{Tr}_n(f(v_i\alpha^{2t}))$ and $\{v_i \mid 0 \le i \le p^n - 1\}$ is an enumeration of elements in the field $\mathbb{F}_{p^n}$. Specially let $v_{p^n-1} = 0$. The following theorem can be similarly proved with the method adopted in the proof of Theorem 7 in [8]. Here we omit the proof.

Theorem 3. The family $\mathcal{S}$ defined in (5) has the optimal correlation property with
$$C_{max} = p^{n/2} + 1.$$

4. CONCLUSION

In this paper, we generalized the function given in [4], which generates sequences over $\mathbb{F}_p$ with two-level ideal autocorrelation. Among the proposed sequences, which is referred as the generalized HG sequences, we have found sequences cyclically inequivalent to the HG sequences. In addition, a nonbinary sequence family with optimal correlation property was constructed.

REFERENCES

[1] S.W. Golomb. Shift register sequences. Aegean Park Press, 1982.
[2] S.W. Golomb and G. Gong. Signal design for good correlation for wireless communication, cryptography, and radar. Cambridge University Press, 2005.
[3] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt. Spread Spectrum Communications. Electrical Engineering, Telecommunications, and Signal Processing Series. Computer Science Press, 1988.
[4] T. Helleseth and G. Gong. New nonbinary sequences with ideal two-level autocorrelation. Ieee Transactions on Information Theory, 48(11):28682872, 2002.
[5] T. Helleseth and P. V. Kumar. Sequences with low correlation. In V. S. Pless and W. C. Human, editors, Handbook of Coding Theory, pages 17651853. Elsevier Science, 1998.
[6] L. R. Welch. Lower bounds on maximum cross-correlation of signals. Ieee Transactions on Information Theory, 20(3):397399, 1974.
[7] Rudolf. Lidl and Harald Niederreiter. Finite fields. Cambridge University Press, Cambridge ; New York :, 2nd ed. edition, 1997.
[8] J. W. Jang, Y. S. Kim, J. S. No, and T. Helleseth. New family of p-ary sequences with optimal correlation property and large linear span. Ieee Transactions on Information Theory, 50(8):1839 1844, 2004.