New families of $p$-ary sequences with low correlation and large linear span

Abstract This article presents a new family of $p$-ary sequences. The proposed sequences are proved to have not only low correlation property, but also large linear span and large family size. Furthermore, it shows that the new family of sequences contains Tang’s construction as a subset if $m$-sequences are excluded from both constructions.

Keywords $p$-ary sequences, correlation function, family size, linear span, quadratic form

1 Introduction

A family of sequences with low correlation and large linear span has important applications in code division multiple access (CDMA) communications, spread spectrum systems, and broadband satellite communications [1]. The sequences with low correlation used in CDMA communications can successfully combat interference from the other users who share a common channel. Many families of binary sequences of period $2^n-1$ with low correlation have been reported. The Gold sequence [2] achieving the Sidelnikov bound, the large and small families of Kasami sequences [3], as well as the GKW-like sequences in Ref. [4] all have desirable correlation properties. The constructions were extended to the nonbinary case as kumar-moreno (KM) sequences in Ref. [5], Trachtenberg-Helleseth (TH) sequences in Refs. [6, 7] and TH-like sequences in Ref. [8]. However, these sequences have small values of linear span. In Ref. [9], by relaxing correlation, Yu and Gong constructed a family of sequence with larger linear span and family size.

In this article, Tang’s construction in Ref. [8] is generalized at the price of the decrease of maximum linear span and the increase of maximum correlation. A new family of $p$-ary sequences in $S_\rho$ is constructed for $n = me$ with odd $m$ and an integer $1 \leq \rho \leq (m-1)/2$. When $\rho = 1$, $S_\rho$ is the family of the TH-like sequences constructed by Tang [8].
where $\tau \neq 0$ if $i = j$. Clearly, $C_{\text{max}}$ is the maximum magnitude of all nontrivial auto- and cross correlation of the sequence in $S$. The set $S$ is called a $(N, M, C_{\text{max}})$ family of sequences, where $N$ is the period of the sequence, $M$ is the family size, and $C_{\text{max}}$ is the maximum correlation magnitude. The sequence family has low correlation if $C_{\text{max}} \leq c\sqrt{N}$, where $c$ is a constant.

The linear span of a periodic sequence is the length of the shortest linear feedback shift registers that can generate the sequence.

In the following, the relationships between the rank of a quadratic form $p(x)$ over $F_q^m$ and the cross-correlation function of the sequences with the trace representation $p(x)$ are shown.

Let $x = \sum_{i=1}^{m} x_i \alpha_i$, where $x_i \in F_q$ and $\alpha_i$, $i = 1, 2, ..., m$ is a basis for $F_q^m$ over $F_q$. Then the function $p(x)$ is a quadratic form over $F_q$ if it can be expressed as:

$$p(x) = p\left(\sum_{i=1}^{m} x_i \alpha_i\right) = \sum_{i=1}^{m} b_{ij} x_i x_j ; \quad b_{ij} \in F_q$$

That is, $p(x)$ is a homogeneous polynomial of degree 2 in ring $F_q[x_1, x_2, ..., x_m]$.

The rank of the quadratic form $p(x)$ is the minimum number of variables required to represent the function under the nonsingular coordinate transformations. It is related to the dimension of the vector subspace $W$ in $F_q^m$, that is,

$$W = \{ \omega \in F_q^m \mid p(x + \omega) = p(x), \text{ for all } x \in F_q \}$$

More precisely, the rank $r = m - \dim W$.

**Lemma 1** (Hellesteh-Gong [10]) If $p(x) = f(x^2)$ is a quadratic form, then the cross-correlation function $C_{\tau, x\tau}(\tau)$ can be written as:

$$C_{\tau, x\tau}(\tau) = -1 + S(\tau)$$

where $2S(\tau) = \sum_{i=0}^{\lambda} \omega_i^\tau(\lambda) + \sum_{i=0}^{\lambda} \omega_i^\tau(\lambda)$, $\lambda$ is a nonsquare in $F_q$.

**Lemma 2** (Hellesteh-Gong [10]) Let $p(x)$ be a quadratic form over $F_q$ of odd rank $r$, and $\lambda$ is a nonsquare in $F_q$, then

$$2S(\tau) = \sum_{i=0}^{r} \omega_i^\tau(p(x)) + \sum_{i=0}^{r} \omega_i^\tau(p(x)) = 0$$

**Lemma 3** (Tang [8]) Let $p(x)$ be a quadratic form over $F_q$ of even rank $r$, and $\lambda$ is a nonsquare in $F_q$, then

$$S(\tau) = \frac{1}{2} \left( \sum_{i=0}^{r} \omega_i^\tau(p(x)) + \sum_{i=0}^{r} \omega_i^\tau(p(x)) \right) = \pm p^{\tau r / 2}$$

**Theorem 1** Let $e = \gcd(n, k)$ and $n/e$ be an odd integer. If $d = (p^{2k} + 1)/2$, where $d \neq p^i (\text{mod } p^n - 1)$ for any $0 \leq i < n$, then the cross-correlation functions take the following three values:

$$-1 + p^{(n/e)/2}, \quad p^{n/e} + p^{(n/e)/2} \text{ times}$$

$$-1, \quad p^n + p^{n/e} \text{ times}$$

$$-1 - p^{(n/e)/2}, \quad p^{n/e} - p^{(n/e)/2} \text{ times}$$

### 3 New family of $p$-ary sequences with large size

**Construction** For $n = \text{me}$ with an odd $m$ and an integer $1 \leq p \leq (m - 1)/2$, let $s_i(t) = \{ s_i(t) \mid 0 \leq i \leq p^n - 1 \}$, a family of $p$-ary sequences $s_i(\rho)$ is defined by

$$s_i(t) = s_i(t + 1) = \sum_{\rho} t_i(v_j \alpha_{ij}^\tau) = \sum_{\rho} t_i(v_j \alpha_{ij}^\tau) + \sum_{\rho} t_i(\alpha_{ij}^\tau)$$

**Lemma 4** All sequences in $s_i(\rho)$ are cyclically distinct. Thus, the family size of $s_i(\rho)$ is $p^{\rho n}$.

**Proof** A time-shifted version of a sequence in $s_i(\rho)$ is represented as

$$s_{i}(t + 1) = t_i(v_j \alpha_{ij}^\tau) + \sum_{\rho} t_i(v_j \alpha_{ij}^\tau) + \sum_{\rho} t_i(\alpha_{ij}^\tau)$$

For all $0 \leq t \leq p^n - 1$, it is identical to the sequence of Eq. (3), if and only if

$$v_{i} = v_{i}^{\rho \alpha_{ij}^\tau}, \quad v_{i} = v_{i}^{\rho \alpha_{ij}^\tau}, \quad 1 \leq j < \rho$$

and

$$\alpha_{ij}^\tau = 1; \quad \rho \leq j < \frac{m - 1}{2}$$

For odd $m$, since $\gcd(p^n - 1, + p^{2k} = 2, \quad 0 \leq i \leq m$, and $4 | 1 + p^{2k}$, then $\gcd(p^n - 1, (1 + p^{2k})/2 = 1$, thus $\alpha_{i}^\tau = 1$ is the unique solution in Eq. (5), which only gives a trivial solution of $v_{i} = v_{i}^{\rho \alpha_{ij}^\tau}$ for $0 \leq i < \rho$. Thus, the sequences in $s_i(\rho)$ for any $v_{i}^{\alpha_{ij}^\tau}$ with $0 \leq i < \rho$ are cyclically distinct.

In the following, the main theorem of this article is provided.

**Theorem 2** For $n = \text{me}$ with an odd $m$ and an integer $1 \leq p \leq (m - 1)/2$, the family $s_i(\rho)$ has cyclically distinct $p$-ary sequences of period $p^n - 1$. The correlation function of sequences is $(2\rho + 2)$-valued and maximum correlation is

$$1 + p^{(n/e)(4\rho - 2)}$$

Therefore, $s_i(\rho)$ constitutes a $(p^n - 1, p^{\rho n}, 1 + p^{(n/e)(4\rho - 2)})$ family of sequences.

**Proof** The computation of the correlation function $C_{\tau, x\tau}(\tau)$ between two sequences $s_i(t)$ and $s_j(t)$ can be divided into four cases depending on different values of $\tau$, $i$ and $j$.

**Case 1** $\tau = 0, i = j$. 


In this trivial case, \( C_{a,b}(t) = p^s - 1 \).

**Case 2** \( t \neq 0 \) and \( i = j = p^n \).

It is straightforward that \( C_{a,b}(t) = -1 \) since the sequence \( \{a(t)\} \) is just an m-sequence over \( F_p \).

**Case 3** \( i \neq p^n, \ j = p^n \) or \( i = p^n, \ j \neq p^n \).

The cross correlation between the sequence is investigated. \( a = tr^n(v_0a^n) + \sum_{x=1}^{m} tr^n(v_0') (\alpha^{(x^2+1)/2}) + \sum_{x=1}^{m} tr^n(\alpha^{(x^2+1)/2}) \) and the m-sequence \( b = tr^n(\alpha'^n) \).

From Lemma 1
\[
C_{a,b}(t) = \sum_{x=0}^{m-1} \omega \left[ \sum_{x=1}^{m} v_0^x \alpha^{(x^2+1)/2} + \sum_{x=1}^{m} v_0^x (\omega^{(x^2+1)/2} - \alpha'^n) x^2 \right] - 1
\]

where \( \lambda \) is a nonsquare in \( F_p \) and the quadratic form
\[
p(x) = tr^n \left( \sum_{x=1}^{m} v_0^x x^{(x^2+1)/2} + \sum_{x=1}^{m} x^{(x^2+1)/2} - (\alpha'^n - \lambda^2) x^2 \right)
\]

For odd \( m \), \( \gcd(2, m) = 1 \), hence, it is immediate that the set \( \{p^{2n+1}, p^{2n+1}, \ldots, p^{(m-1)n} + 1\} \) modulo \( p^s \) is equivalent to the set \( \{p^{2n+1}, p^{2n+1}, \ldots, p^{(m-1)n} + 1\} \).

Since \( ei \neq ej \pmod{n} \), for \( 0 \leq i < j < (m-1)/2 \) and \( tr^n(x^{x^2+1}) = tr^n(x^{x^2+1}) \), then Eq. (6) can be rewritten as
\[
p(x) = tr^n \left( \sum_{x=1}^{m} v_0^x x^{(x^2+1)/2} + \sum_{x=1}^{m} x^{(x^2+1)/2} - (\alpha'^n - \lambda^2) x^2 \right)
\]

To compute the rank of \( p(x) \), it is sufficient to find the number of the elements in the vector subspace \( W \) which is defined by Eq. (2), thus it is equivalent to finding solutions to the following equation
\[
tr^n \left( \sum_{x=1}^{m} (v_0 - 1) (\omega^{x^{(x^2+1)/2}} + \alpha'^n - \lambda^2) x^2 \right) + tr^n \left( \omega \sum_{x=1}^{m} (v_0 - 1) (\omega^{x^{(x^2+1)/2}} + \alpha'^n - \lambda^2) x^2 \right) = 0
\]

In fact,
\[
2tr^n \left( \sum_{x=1}^{m} (v_0 - 1) \omega^{x^{(x^2+1)/2}} + \sum_{x=1}^{m} \omega^{x^{(x^2+1)/2}} - (\alpha'^n - \lambda^2) \omega^2 \right) = tr^n \left( \omega \sum_{x=1}^{m} (v_0 - 1) (\omega^{x^{(x^2+1)/2}} + \alpha'^n - \lambda^2) \omega^2 \right) + tr^n \left( \omega \sum_{x=1}^{m} (v_0 - 1) (\omega^{x^{(x^2+1)/2}} + \alpha'^n - \lambda^2) \omega^2 \right)
\]

Thus,
\[
A = \sum_{x=1}^{m} (v_0 - 1) (\omega^{x^{(x^2+1)/2}} + \alpha'^n - \lambda^2) + tr^n (\omega) (2(\alpha'^n - \lambda^2) + 1) = 0
\]

Obviously,
\[
A^{x^{(x^2+1)/2}} = 0 \iff A = 0
\]

Since the maximum degree of \( A^{x^{(x^2+1)/2}} = 0 \) is \( p^{4(p-1)} \), then it has at most \( p^{4(p-1)} \) solutions. For \( tr^n(\omega) \in F_{p^n} \), the total number of solutions of Eq. (8) is at most \( p'r^{(2(p-1)} = p^{4(p-1)} \) due to Lemma 3. The rank of quadratic form \( p(x) \) is \( m - (4p - 3) \). From Lemmas 3, the maximum correlation takes the value \( 1 + p^{4((4p-3)/2)} \).

**Case 4** \( t \neq p^{n-2}, 0 \leq i, j < p^n - 1 \)

From Lemma 1
\[
C_{a,b}(t) = \frac{1}{2} \left[ \sum_{x=1}^{m} \omega^{x^{(x^2+1)/2}} + \sum_{x=1}^{m} \omega^{x^{(x^2+1)/2}} \right] - 1
\]

where \( \lambda \) is a nonsquare in \( F_p \) and the quadratic form
\[
p(x) = tr^n \left( \sum_{x=1}^{m} (v_0 - 1) x^{x^{(x^2+1)/2}} - \gamma \sum_{x=1}^{m} (v_0 - 1) (\gamma x)^{x^{(x^2+1)/2}} + \sum_{x=1}^{m} \gamma \sum_{x=1}^{m} (v_0 - 1) x^{x^{(x^2+1)/2}} + \gamma \sum_{x=1}^{m} (v_0 - 1) x^{x^{(x^2+1)/2}} - \gamma \sum_{x=1}^{m} (v_0 - 1) x^{x^{(x^2+1)/2}} - \gamma \sum_{x=1}^{m} (v_0 - 1) x^{x^{(x^2+1)/2}} - \gamma \sum_{x=1}^{m} (v_0 - 1) x^{x^{(x^2+1)/2}} - \gamma \sum_{x=1}^{m} (v_0 - 1) x^{x^{(x^2+1)/2}} 
\]

Since \( m \) is an odd integer, it is clear that a quadratic nonresidue in \( F_{p^2} \) is also a quadratic nonresidue in \( F_q \). Thus, the element \( \alpha'^n \in F_{p^2} \) could be expressed as \( \alpha'^n = \gamma y^2 \), where \( y \in F_{p^2} \) and \( y \) is \( 1 \) or quadratic nonresidues in \( F_q \). Then similar to case 3, \( p(x) \) can be rewritten as
\[
p(x) = tr^n \left( \sum_{x=1}^{m} (v_0 - 1) x^{x^{(x^2+1)/2}} - \gamma \sum_{x=1}^{m} (v_0 - 1) (\gamma y x)^{x^{(x^2+1)/2}} + \sum_{x=1}^{m} \gamma \sum_{x=1}^{m} (v_0 - 1) x^{x^{(x^2+1)/2}} + \gamma \sum_{x=1}^{m} (v_0 - 1) x^{x^{(x^2+1)/2}} - \gamma \sum_{x=1}^{m} (v_0 - 1) x^{x^{(x^2+1)/2}} + \gamma \sum_{x=1}^{m} (v_0 - 1) x^{x^{(x^2+1)/2}} - \gamma \sum_{x=1}^{m} (v_0 - 1) x^{x^{(x^2+1)/2}} 
\]

To compute the rank of \( p(x) \), it is sufficient to find the number of the elements in the vector subspace \( W \), which is defined by Eq. (2), thus it is equivalent to finding solutions to the following equation
\[
tr^n \left( x \sum_{x=1}^{m} (v_0 - 1) (\omega^{x^{(x^2+1)/2}} + \alpha'^n - \lambda^2) x^2 \right) + \gamma \sum_{x=1}^{m} (v_0 - 1) (x^2)^{x^{(x^2+1)/2}} = 0
\]

Similar to above discussion, only the following need to be considered:
\[
\sum_{x=1}^{m} (v_0 - 1) (\omega^{x^{(x^2+1)/2}} + \alpha'^n - \lambda^2) x^2 + \gamma \sum_{x=1}^{m} (v_0 - 1) x^2 = 0
\]

The left-hand side of Eq. (11) is denoted as \( B \). Then:
\[
B^{x^{(x^2+1)/2}} = 0 \iff B = 0
\]

Since the maximum degree of \( B^{x^{(x^2+1)/2}} = 0 \) is \( p^{4(p-1)} \), then
it has at most $p^{4(p-1)e}$ solutions. If $y \in F_q$, the total number of solutions of Eq.(11) is at most $p^p p^{p^{4(p-1)e}} = q^{4p-3}$, when $t_r^{\nu}(o)$ runs through $F_q$. If $y \notin F_q$, the total number of solutions of Eq. (11) is at most $p^{2e} p^{4(p-1)e} = q^{4p-2}$, when $t_r^{\nu}(o)$ and $t_r^{\nu}(y o)$ run through $F_q$. Therefore, the rank of quadratic form $r(x)$ is $m - (4 \rho - 3)$ and $m - (4 \rho - 2)$. From Lemmas 2 and 3, the maximum correlation takes the value $1 + p^{n/(4(p-3)e)}$.

Remark If $\rho=1$, then $s_i(t) = t_r^{\nu}(v_i \alpha^\nu) + \sum_{j=1}^{(m-1)/2} t_r^{\nu}(\alpha^{(j+3p^2)e})$ (12) which represents the sequences introduced by Tang for $n=me$ with odd $m$ and $k = e$ case in Ref. [8]. From Theorem 2, the sequences given by Eq. (12) have four-valued correlation $\{-1 + p^n, -1 \pm p^{(m+1)/2}, -1\}$, for all $v_i \in F_p$.

4 Linear span of the new family $S_r(\rho)$

In this section, the linear span of the new proposed family $S_r(\rho)$ is investigated.

The linear span of the sequence $\{s_i(t)\}$ can be determined by expanding the expression of the sequence $s_i(t)$ as a polynomial in $\alpha'$ of degree less than $p^n-1$ and then counting the number of monomials with nonzero coefficients occurring in the expansion. This technique will be applied to determine the linear span of sequences in the family $S_r(\rho)$.

Theorem 3 The maximum and minimum linear span of sequences in $S_r(\rho)$ are $\lceil n(m+1)/2 \rceil$ and $\lceil n(m-2\rho+1)/2 \rceil$, respectively.

Proof From the construction and Eq. (3), which denotes the trace representation of the sequence $s_i(t)$ in $S_r(\rho)$, it is easy to see that Eq. (3) has at most of $(m+1)/2$ nonzero trace terms and each trace term has the linear span of $n$. Therefore, the maximum linear span of sequences in $S_r(\rho)$ is given by $LS_{\text{max}}(\rho) = \frac{n(m+1)}{2}$.

Similarly, Eq. (3) has at least of $(m+1)/2 - \rho$ nonzero trace terms and the linear span of each trace term is $n$. Then the minimum linear span of sequences in $S_r(\rho)$ is given by $LS_{\text{min}}(\rho) = \left(\frac{m+1}{2} - \rho\right)n = \frac{n(m-2\rho+1)}{2}$.

5 Conclusions

For $n = me$ with odd $m$ and an integer $1 \leq \rho \leq (m-1)/2$, a new $p$-ary sequences family $S_r(\rho)$ has been presented in this article. The new family $S_r(\rho)$ consists of $(p^n-1, p^\rho, 1 + p^{n/(4p-3e)})$ family of sequences. Compared with the previous constructions of sequences family with low correlation [5–7], the new methods can generate sequences family that not only have a larger family size but also a larger linear span. When the parameter $\rho=1$, the new methods can be regarded as a subset of the new construction. Table 1 shows the comparison of the sequence families with low correlation.

Furthermore, the new sequences family is flexible in that a proper value of parameters and the corresponding family for a specific application can be chosen. When low correlation is more crucial than large family size, a small value of $\rho$ and $e$ can be chosen. When large family size is more important, a large value of $\rho$ and $e$ can be chosen.

Table 1 Comparison of the sequence families with low correlation

<table>
<thead>
<tr>
<th>Family</th>
<th>$n$</th>
<th>Family size</th>
<th>$C_{\text{max}}$</th>
<th>Linear span</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold [2]</td>
<td>$n = 2m + 1$</td>
<td>$2^n + 1$</td>
<td>$1 + 2^{(m+1)/2}$</td>
<td>$2n$</td>
</tr>
<tr>
<td>Kasami [3]</td>
<td>$n = 2m$</td>
<td>$2^n$</td>
<td>$1 + 2^{(m+1)/2}$</td>
<td>$3n/2$</td>
</tr>
<tr>
<td>GKW-like [4]</td>
<td>$n=me, m$ odd</td>
<td>$2^n + 1$</td>
<td>$1 + 2^{(m+1)/2}$</td>
<td>$n(m+1)/2$</td>
</tr>
<tr>
<td>KM [5]</td>
<td>$n=me, m$ odd</td>
<td>$p^n + 1$</td>
<td>$1 + p^{(m+1)/2}$</td>
<td>$2n$</td>
</tr>
<tr>
<td>TH [6,7]</td>
<td>$n=me, m$ odd</td>
<td>$p^n + 1$</td>
<td>$1 + p^{(m+1)/2}$</td>
<td>$2n$</td>
</tr>
<tr>
<td>TH-like [8]</td>
<td>$n=me, m$ odd</td>
<td>$p^n + 1$</td>
<td>$1 + p^{(m+1)/2}$</td>
<td>$n(m+1)/2$</td>
</tr>
<tr>
<td>New family</td>
<td>$n=me, m$ odd</td>
<td>$p^n$</td>
<td>$1 + p^{(m+1)/2}$</td>
<td>$n(m+1)/2$</td>
</tr>
</tbody>
</table>

Acknowledgements This work is supported by the Major Research plan of the National Natural Science Foundation of China (90604023), the Natural Science Foundation of China (90601023), the National High Technology Research and Development Program of China (2006AA01Z419).

References
