THE JOURNAL OF CHINA UNIVERSITIES OF POSTS AND TELECOMMUNICATIONS
Volume 14, Issue 4, December 2007

TONG Xin, WEN Qiao-yan

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

**CLC number** TN918.1 **Document** A **Article ID** 1005-8885 (2007) 04-0053-04

**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 $S_e(\rho)$ is constructed for $n = me$ with odd $m$ and an integer $1\leqslant\rho\leqslant(m-1)/2$. When $\rho=1$, $S_e(1)$ is the family of the TH-like sequences constructed by Tang [8].

## 2 Preliminaries

Assume that $p$ is an odd prime, and $n = me$, where $m$ is odd. Let $F_{p^n}$ be the finite field with $p^n$ elements, let $q = p^e$, for simplicity, denote $F_{p^e}$ as $F_q$ and $F_{p^n}$ as $F_{q^m}$. Then the trace function $\mathrm{tr}_e^n(\cdot)$, from $F_{q^m}$ to the subfield $F_q$, is defined by

$$\mathrm{tr}_e^n(x)=\sum_{i=1}^{m-1}x^{p^{ei}}$$

The trace function has the following properties:

1) $\mathrm{tr}_e^n(ax+by)=a\mathrm{tr}_e^n(x)+b\mathrm{tr}_e^n(y)$; for $a,b\in F_q$, $x,y\in F_{q^m}$;

2) $\mathrm{tr}_e^n(x^{p^e})=\mathrm{tr}_e^n(x)$; for $x\in F_{q^m}$.

Any sequence $\{s_t(t)\}$ over $F_p$ of period $n$ has a trace representation, that is, there exists a function $g(x)$ from $F_{p^n}$ to $F_p$, satisfies the following condition

$$g(x)=\sum_{k\in\Gamma(n)}\mathrm{tr}_1^{n_k}(A_kx^k);\quad A_k\in F_{p^{n_k}},x\in F_{p^n}$$

Such that $s(t)=g(\alpha^t)$, $t=0,1,...,p^n-2$. Here $\Gamma(n)$ is the set comprising of all coset leaders modulo $p^{n_k}-1$, $n_k\mid n$ is the size of the cyclotomic coset, $\alpha$ is a primitive element of $F_{p^n}$.

Let $S$ be a family of $M$ $p$-ary sequences of period $N=p^n-1$, given by $S=\{s_i(t)\mid 0\leqslant i\leqslant M-1,\ 0\leqslant t\leqslant N-1\}$. Then, the correlation function between two sequences $\{s_i(t)\}$ and $\{s_j(t)\}$ is defined as

$$C_{s_i,s_j}(\tau)=\sum_{t=0}^{N-1}\omega^{s_i(t)+s_j(t+\tau)};\quad 0\leqslant i,j\leqslant M-1,\ 0\leqslant\tau\leqslant N-1 \qquad (1)$$

where $\omega$ is the complex $p$th root of unity given by $\omega=e^{2\pi i/p}$, $i=\sqrt{-1}$. The maximum magnitude $C_{\max}$ of the correlation values is defined by

$$C_{\max}=\max|C_{s_i,s_j}(\tau)|;\quad 0\leqslant i,j\leqslant M-1,\ 0\leqslant\tau\leqslant N-1$$

where $\tau\neq 0$ if $i=j$. Clearly, $C_{\max}$ is the maximum magnitude

Received date: 2006-09-27
TONG Xin (童), WEN Qiao-yan
State key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
E-mail: tongxin2030@sina.com

of all nontrivial auto- and cross correlation of the sequence in $S$. The set $S$ is called a $(N, M, C_{\max})$ family of sequences, where $N$ is the period of the sequence, $M$ is the family size, and $C_{\max}$ is the maximum correlation magnitude. The sequence family has low correlation if $C_{\max} \leqslant c\sqrt{N}$, 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 $F_q$ 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:

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

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 $\mathcal{W}$ in $F_{q^m}$, that is,

$$\mathcal{W} = \{ \omega \in F_q \mid p(x+\omega) = p(x), \text{ for all } x \in F_q \} \tag{2}$$

More precisely, the rank $r = m$ –dim $\mathcal{W}$.

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

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

where $2S(\tau) = \sum_{x \in F_{p^n}} \omega^{\mathrm{tr}_1^r(p(x))} + \sum_{x \in F_{p^n}} \omega^{\mathrm{tr}_1^r(\lambda p(x))}$, $\lambda$ is a nonsquare in $F_q$.

**Lemma 2** (Hellesth-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

$$2S(\tau) = \sum_{x \in F_{p^n}} \omega^{\mathrm{tr}_1^r(p(x))} + \sum_{x \in F_{p^n}} \omega^{\mathrm{tr}_1^r(\lambda p(x))} = 0$$

**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

$$S(\tau) = \frac{1}{2}\left( \sum_{x \in F_{p^n}} \omega^{\mathrm{tr}_1^r(p(x))} + \sum_{x \in F_{p^n}} \omega^{\mathrm{tr}_1^r(\lambda p(x))} \right) = \pm p^{n - re/2}$$

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

$$\begin{array}{ll} -1 + p^{(n+e)/2}, & p^{n-e} + p^{(n-e)/2} \quad \text{times} \\ -1, & p^n + p^{n-e} \quad \text{times} \\ -1 - p^{(n+e)/2}, & p^{n-e} - p^{(n-e)/2} \quad \text{times} \end{array}$$

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

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

$$s_i(t) = \mathrm{tr}_1^n(v_{i0}\alpha^t) + \sum_{l=1}^{\rho-1} \mathrm{tr}_1^n(v_{il}\alpha^{t(1+p^{2el})/2}) + \sum_{l=\rho}^{(m-1)/2} \mathrm{tr}_1^n(\alpha^{t(1+p^{2el})/2}) \tag{3}$$

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

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

$$s_j(t+\tau) = \mathrm{tr}_1^n(v_{j0}\alpha^{t+\tau}) + \sum_{l=1}^{\rho-1} \mathrm{tr}_1^n\left(v_{jl}\alpha^{(t+\tau)(1+p^{2el})/2}\right) + \sum_{l=\rho}^{(m-1)/2} \mathrm{tr}_1^n\left(\alpha^{(t+\tau)(1+p^{2el})/2}\right)$$

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

$$v_{i0} = v_{j0}\alpha^t, \; v_{il} = v_{jl}\alpha^{\tau(1+p^{2el})/2}; \quad 1 \leqslant j < \rho \tag{4}$$

and

$$\alpha^{\tau(1+p^{2el})/2} = 1; \quad \rho \leqslant j \leqslant \frac{m-1}{2} \tag{5}$$

For odd $m$, since gcd $(p^n - 1, 1 + p^{2el}) = 2$, $0 \leqslant l \leqslant m$, and $4 \nmid 1 + p^{2el}$, then gcd $(p^n - 1, (1 + p^{2el})/2) = 1$, thus $\alpha^\tau = 1$ is the unique solution in Eq. (5), which only gives a trivial solution of $v_{il} = v_{jl}$ for $0 \leqslant l < \rho$. Thus, the sequences in $S_e(\rho)$ for any $v_{il}$ in $F_{p^n}$ with $0 \leqslant l < \rho$ are cyclically distinct.

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

**Theorem 2** For $n = me$ with an odd $m$ and an integer $1 \leqslant \rho \leqslant (m-1)/2$, the family $S_e(\rho)$ 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 $1 + p^{\lfloor n + (4\rho - 3)e \rfloor / 2}$. Therefore, $S_e(\rho)$ constitutes a $(p^n - 1, p^{n\rho}, 1 + p^{\lfloor n + (4\rho - 3)e \rfloor / 2})$ family of sequences.

**Proof** The computation of the correlation function $C_{s_i, s_j}(\tau)$ 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, $C_{s_i, s_j}(\tau) = p^n - 1$.