一类大集合*p*元低相关序列集的线性复杂度研究

陈 俊[1,2]，陈 运[2]，吴 震[2]

(1. 西南交通大学信息科学与技术学院 成都 610031; 2. 成都信息工程学院信息安全研究所 成都 610225)

【摘要】构造具有大线性复杂度和大集合容量的*p*元低相关序列集对码分多址(CDMA)通信系统具有重要的意义。采用Klapper的方法，利用*d*-型函数，构造了一类具有大集合容量的*p*元低相关序列集 $S^{(r)}$。该序列集的集合容量为 p^{2n}，序列的周期为 p^n-1，相关函数的最大边峰值为 $4p^{\frac{n}{2}}-1$。利用Key的方法，证明了当 $p=3$ 或 $p=5$ 该序列集的最小和最大线性复杂度分别为 $2^{\frac{n}{2}-2}n$ 和 $3^{\frac{n}{2}-1}\times 2^{\frac{n}{2}-2}n$；而当 $p>5$ 时，证明了其线性复杂度的最大和最小值分别大于 $3^{\frac{n}{4}-1}\times 2^{\frac{n}{4}-2}n$ 和 $2^{\frac{n}{4}-2}n$。该序列集能极大地提高CDMA通信系统的安全性。

关 键 词 大集合容量; 大线性复杂度; 低相关性; *p*元序列集

中图分类号 TP914 **文献标识码** A doi:10.3969/j.issn.1001-0548.2011.03.010

Research on the Linear Complexity for a Family of Large Size of *p*-ary Sequences with Low Correlation

CHEN Jun[1,2], CHEN Yun[2], and WU Zhen[2]

(1. School of Information Science and Technology, South Jiaotong University Chengdu 610031;

2. Information Security Institute, Chengdu University of Information Technology Chengdu 610225)

Abstract Constructing a large family of *p*-ary sequences with large linear complexity and low correlation is very important for code division multiple access (CDMA) communication systems. By use of Klapper's method and *d*-form function, a large family $S^{(r)}$ of *p*-ary sequences with low correlation is constructed. Such family contains p^{2n} sequences of period p^n-1 with maximal nontrivial correlation value $4p^{\frac{n}{2}}-1$. The minimal and maximal linear complexity of the sequences family are proven to be $2^{\frac{n}{2}-2}n$ and $3^{\frac{n}{2}-1}\times 2^{\frac{n}{2}-2}n$ for $p>5$ and $r=(p^{m-1}-1)/(p-1)$, respectively. It is also proven that the maximal and minimal linearcomplexity of the sequences set are larger than $3^{\frac{n}{4}-1}\times 2^{\frac{n}{4}-2}n$ and $2^{\frac{n}{4}-2}n$ for $p=3$, 5 and $r=(p^{m-1}-1)/(p-1)$, respectively. This sequences family can greatly improve the security of CDMA communication systems.

Key words large family size; large linear complexity; low correlation; *p*-ary sequences family

具有大线性复杂、大集合容量(family size)和低相关特性的伪随机序列被广泛应用于码分多址通信系统[1]。在码分多址通信系统中，序列之间较低的相关特性可以降低来自同一信道其他用户的干扰；较多的序列数目可以增加系统的容量；而较大的线性复杂度可以抵抗基于Berlekamp-Massey算法进行的攻击，从而提高系统的安全性。因此，构造同时具有低相关性特、大线性复杂和大集合容量的伪随机序列集成为一个重要的研究课题。

人们已经构造出许多具有低相关特性的 p (p 是奇素数)元序列集，如文献[2-10]中的序列集，但这些序列的线性复杂度都很低。

最近，文献[11]和文献[12]分别构造了具有低相关特性和大集合容量的 p 元序列集 $S^{(r)}$，但未给出序列的线性复杂度。本文中，证明了当参数 r 选取适当的值时，该序列集中的序列的线性复杂度远大于几类已知的非二元序列集的线性复杂度，并给出了线性复杂度的精确值或下界。

1 基本概念

令 GF(p^n) 表示含有 p^n 个元素的有限域。设正整数 n,m,e 满足 $n=me$，定义从 GF(p^n) 到 GF(p^m) 的迹函数为：

收稿日期：2010－02－05; 修回日期：2010－11－25

基金项目：国家自然科学基金(60873216)

作者简介：陈 俊(1971－)男，博士生，讲师，主要从事扩频通信序列设计方面的研究.

$$\mathrm{tr}_m^n(x)=\sum_{h=0}^{e-1}x^{p^{hm}}$$

式中，$x\in \mathrm{GF}(p^n)$。迹函数的性质参见文献[13]。

设 $S=\{s_i\mid 0\leqslant i\leqslant M-1\}$ 是由 M 条周期为 N 的 p 元序列组成的序列集，其中序列为 $s_i=\{s_i(t)\}_{t=0}^{N-1}$，$s_i(t)\in \mathrm{GF}(p)$。

序列 s_i 和 s_j 的周期相关函数定义为：

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

式中，$0\leqslant i,j\leqslant M-1$；$t+\tau$ 是模 N 加；ω 是 p 次本原复数单位根。

序列集 S 的周期相关函数的最大边峰值为 $R_{\max}=\max\{|R_{i,j}(\tau)|\,i\neq j$ 或 $\tau\neq 0\}$。

引理 1 设 p，m 为正整数，若 $\gcd(m-1,p-1)=1$，则 $\gcd(p^m-1,(p^{m-1}-1)/(p-1))=1$。

证明 因为：

$$\gcd(p^m-1,(p^{m-1}-1)/(p-1))=$$
$$\gcd((p-1)^2,p^{m-1}-1))/(p-1)=$$
$$\gcd(p-1,p^{m-2}+p^{m-3}+\cdots+p+1)=$$
$$\gcd(p-1,m-1)$$

所以，当 $\gcd(p-1,m-1)=1$ 时，可得 $\gcd(p^m-1,(p^{m-1}-1)/(p-1))=1$。证毕。

2 序列集的构造

定义序列集 $S^{(r)}$ 为：

$$S^{(r)}=\{s_{l_1,l_2}^{(r)}\mid 1\leqslant l_1,l_2\leqslant p^n\}$$

其中：

$$s_{l_1,l_2}^{(r)}=\{s_{l_1,l_2}^{(r)}(t)=tr_1^m\{[\mathrm{tr}_m^n(\alpha^t+\gamma_{l_1}\alpha^{(2p^m-1)t}+\gamma_{l_2}\alpha^{(3p^m-2)t})]^r\}\}_{t=0}^{p^n-2}$$

式中，$\gamma_{l_1},\gamma_{l_2}\in \mathrm{GF}(p^n)$；$\gcd(r,p^m-1)=1$；$\alpha$ 是 $\mathrm{GF}(p^n)$ 的一个本原元；当 $p=3$ 或 $p=5$ 时，取 $n=4m$，而当 $p>5$ 时，取 $n=2m$。

定理 1 [1] 序列集 $S^{(r)}$ 的最大边峰值为 $4p^{\frac{n}{2}}-1$。

定理 2 当 $r=(p^{m-1}-1)/(p-1)$，$\gcd(p-1,m-1)=1$ 时，序列集 $S^{(r)}$ 的最大边峰值为 $4p^{\frac{n}{2}}-1$。

证明 由引理1知，此时 $\gcd(r,p^m-1)=1$，再根据定理1可证。证毕。

定理 3[1] 序列集 $S^{(r)}$ 的集合容量为 p^{2n}。

3 序列的线性复杂度

由文献[15]知，如果将序列 $s_{l_1,l_2}^{(r)}(t)$ 表示为 α^t 的多项式，则该多项式中所包含的关于 α^t 的单项式的数目就是序列的线性复杂度。因此，若令 $x=\alpha^t$，则 $s_{l_1,l_2}^{(r)}(x)=\mathrm{tr}_1^m\{[\mathrm{tr}_m^n(x+\gamma_{l_1}x^{2p^m-1}+\gamma_{l_2}x^{3p^m-2})]^r\}$ 的展开式中关于变量 x 的单项式的数目就是序列的线性复杂度。用 $\mathrm{LS}(s_{l_1,l_2}^{(r)})$ 表示序列 $s_{l_1,l_2}^{(r)}$ 的线性复杂度。

下面分别讨论当 $p>5$ 和 $p=3$ 或 $p=5$ 时，序列集 $S^{(r)}$ 中序列的线性复杂度。

1) 首先讨论 $p>5$ 的情况。

因为当 $p>5$ 时，取 $n=2m$，所以如果令 $y=x^{p^m-1}$，则有：

$$s_{l_1,l_2}^{(r)}(x)=\mathrm{tr}_1^m\{[\mathrm{tr}_m^n(x+\gamma_{l_1}x^{2p^m-1}+\gamma_{l_2}x^{3p^m-2})]^r\}=$$
$$\sum_{i=0}^{m-1}[xy^{-2}(\gamma_{l_2}^{p^m}+\gamma_{l_1}^{p^m}y+y^2+y^3+\gamma_{l_1}y^4+\gamma_{l_2}y^5)]^{p^ir}$$

令：

$$\Delta_i(x)=[xy^{-2}(\gamma_{l_2}^{p^m}+\gamma_{l_1}^{p^m}y+y^2+y^3+\gamma_{l_1}y^4+\gamma_{l_2}y^5)]^{p^ir}\tag{1}$$

则有如下的引理成立。

引理 2 如果 $i\neq i'$，则 $\Delta_i(x)$ 与 $\Delta_{i'}(x)$ 中不存在指数相同的 x 的单项式。

证明 因为 $y=x^{p^m-1}$，所以 $\Delta_i(x)$ 的展开式中，变量 x 的指数模 p^m-1 同余 p^ir。

若存在 i,i'，使得 $p^ir\equiv p^{i'}r \bmod p^m-1$，则由于 $\gcd(r,p^m-1)=1$，因此有 $p^i\equiv p^{i'} \bmod p^m-1$，从而 $i=i'$。证毕。

用 $|\Delta_i(x)|$ 表示 $\Delta_i(x)$ 的展开式中关于变量 x 的单项式的数目，根据引理2可知：

$$\mathrm{LS}(s_{l_1,l_2}^{(r)})=m|\Delta_i(x)|\tag{2}$$

若令 $\Gamma(y)=(\gamma_{l_2}^{p^m}+\gamma_{l_1}^{p^m}y+y^2+y^3+\gamma_{l_1}y^4+\gamma_{l_2}y^5)^r$，则有：

$$\mathrm{LS}(s_{l_1,l_2}^{(r)})=m|\Gamma(y)|\tag{3}$$

因而只需要计算 $\Gamma(y)$ 中关于 y 的单项式的数目。

定理 4 当 $p>5$，$n=2m$，$\gcd(p-1,m-1)=1$，并且 $r=(p^{m-1}-1)/(p-1)$ 时，序列 $s_{l_1,l_2}^{(r)}$ 的线性复杂度 $\mathrm{LS}(s_{l_1,l_2}^{(r)})=3^{\frac{n}{2}-1}\times 2^{\frac{n}{2}-2}n$ 或 $2^{\frac{n}{2}-2}n$ 或 $2^{n-3}n$。

证明 因为此时 $r=1+p+p^2+\cdots+p^{m-2}$，所以 $\Gamma(y)$ 的展开式中 y 的指数为：

$$b=\sum_{i=0}^{m-2}t_ip^i\qquad t_i\in\{0,1,2,3,4,5\}\tag{4}$$

容易知道 $b<p^m+1$ 以及式(4)是某个正整数的 $p\,(p>5)$ 进制表示，从而，当向量 $(t_0,t_1,t_2,\cdots,t_{m-2})\neq(t'_0,t'_1,t'_2,\cdots,t'_{m-2})$ 时，一定有 $\sum_{i=0}^{m-2}t_ip^i\neq\sum_{i=0}^{m-2}t'_ip^i$，即 $\Gamma(y)$ 的展开式中 y 的指数互不相同。因此，当

$\gamma_{l_1}\gamma_{l_2}\neq 0$时，$\Gamma(y)$的展开式中共有$6^{m-1}$个指数互不相同的$y$的单项式，从而根据式(3)有$\mathrm{LS}(s^{(r)}_{l_1,l_2})=3^{\frac{n}{2}-1}\times 2^{\frac{n}{2}-2}n$。而当$\gamma_{l_1}=\gamma_{l_2}=0$时，同理可得$\mathrm{LS}(s^{(r)}_{l_1,l_2})=2^{\frac{n}{2}-2}n$。其他情况下，有$\mathrm{LS}(s^{(r)}_{l_1,l_2})=2^{n-3}n$。证毕。

2) 其次讨论当$p=3$或$p=5$时，序列$s^{(r)}_{l_1,l_2}$的线性复杂度。

根据序列集$S^{(r)}$的定义可知，此时$n=4m$，所以令$y=x^{p^{2m}-1}$，从而可以得到：

$$s^{(r)}_{l_1,l_2}(x)=\mathrm{tr}^m_1\{[\mathrm{tr}^n_m(x+\gamma_{l_1}x^{2p^m-1}+\gamma_{l_2}x^{3p^m-2})]^r\}=\sum_{i=0}^{m-1}\{\sum_{j=0}^{1}[xy^{-2}(\gamma_{l_2}^{p^{2m}}+\gamma_{l_1}^{p^{2m}}y+y^2+y^3+\gamma_{l_1}y^4+\gamma_{l_2}y^5)]^{p^{mj}}\}^{p^i r}$$

令：

$$\Delta_i(x)=\{\sum_{j=0}^{1}[xy^{-2}(\gamma_{l_2}^{p^{2m}}+\gamma_{l_1}^{p^{2m}}y+y^2+y^3+\gamma_{l_1}y^4+\gamma_{l_2}y^5)]^{p^{mj}}\}^{p^i r}$$

采用与文献[14]中定理1相同的证明方法，可得如下的引理。

引理 3　对$i\neq i'$，$\Delta_i(x)$和$\Delta_{i'}(x)$中不存在指数相同的x的单项式。

根据引理3，只需要计算$\Delta_0(x)=\left\{\sum_{j=0}^{1}[xy^{-2}(\gamma_{l_2}^{p^{2m}}+\gamma_{l_1}^{p^{2m}}y+y^2+y^3+\gamma_{l_1}y^4+\gamma_{l_2}y^5)]^{p^{mj}}\right\}^r$中关于变量$x$的单项式的数目。

令$u=xy^{-2}(\gamma_{l_2}^{p^{2m}}+\gamma_{l_1}^{p^{2m}}y+y^2+y^3+\gamma_{l_1}y^4+\gamma_{l_2}y^5)$，则有：

$$\Delta_0(x)=(u+u^{p^m})^r=\sum_{\boldsymbol{a}=(a_0,a_1)}u^{a_0+a_1p^m}$$

式中，$a_0=\sum_{k=0}^{m-2}a_{0,k}p^k$；$a_1=\sum_{k=0}^{m-2}a_{1,k}p^k$；$a_{0,k}+a_{1,k}=1$；并且$a_{j,k}\in\{0,1\}$；$j\in\{0,1\}$；$a_0+a_1=r$。从而有：

$$\Delta_0(x)=\sum_{\boldsymbol{a}=(a_0,a_1)}[xy^{-2}(\gamma_{l_2}^{p^{2m}}+\gamma_{l_1}^{p^{2m}}y+y^2+y^3+\gamma_{l_1}y^4+\gamma_{l_2}y^5)]^{a_0+a_1p^m}.$$

令：

$$\Gamma_{\boldsymbol{a}}(x)=[xy^{-2}(\gamma_{l_2}^{p^{2m}}+\gamma_{l_1}^{p^{2m}}y+y^2+y^3+\gamma_{l_1}y^4+\gamma_{l_2}y^5)]^{a_0+a_1p^m}$$

则有引理4成立。

引理 4　如果向量$\boldsymbol{a}=(a_0,a_1)\neq\boldsymbol{a}'=(a'_0,a'_1)$，则$\Gamma_{\boldsymbol{a}}(x)$与$\Gamma_{\boldsymbol{a}'}(x)$的展开式中，变量$x$的指数互不相同。

证明　因为$a_j,a'_j<p^m$，$j=0,1$，所以当$\boldsymbol{a}\neq\boldsymbol{a}'$时，$a_0+a_1p^m\neq a'_0+a'_1p^m$。又由于$y=x^{p^{2m}-1}$，因此在$\Gamma_{\boldsymbol{a}}(x)$的展开式中，变量$x$的指数模$p^{2m}-1$同余$a_0+a_1p^m$。从而若$a_0+a_1p^m\equiv a'_0+a'_1p^m \bmod p^{2m}-1$，则有$(a_0,a_1)=(a'_0,a'_1)$。证毕。

若用$|\Delta_0(x)|$表示$\Delta_0(x)$的展开式中指数互不相同的x的单项式的数目，则有：

$$|\Delta_0(x)|=\sum_{\boldsymbol{a}}|\Gamma_{\boldsymbol{a}}(x)| \tag{5}$$

令：

$$\Phi_{\boldsymbol{a}}(y)=(\gamma_{l_2}^{p^{2m}}+\gamma_{l_1}^{p^{2m}}y+y^2+y^3+\gamma_{l_1}y^4+\gamma_{l_2}y^5)^{a_0+a_1p^m} \tag{6}$$

则有$|\Delta_0(x)|=\sum_{\boldsymbol{a}}|\Phi_{\boldsymbol{a}}(y)|$。

根据引理3、引理4及式(5)、式(6)，可得命题1。

命题 1　序列$s^{(r)}_{l_1,l_2}$的线性复杂度为：

$$\mathrm{LS}(s^{(r)}_{l_1,l_2})=m\sum_{\boldsymbol{a}}|\Phi_{\boldsymbol{a}}(y)| \tag{7}$$

因为当$a_0+a_1p^m$为一般值时，很难精确计算式(6)的展开式中指数互不相同的y的单项式的个数，所以只考虑$a_0+a_1p^m$取两个特殊值时，$\Phi_{\boldsymbol{a}}(y)$的展开式中单项式y的数目。

1) 当$a_0=(p^{m-1}-p)/(p^2-1)$，$a_1=(p^m-1)/(p^2-1)$时，显然满足$a_0+a_1=(p^{m-1}-1)/(p-1)=r$，且有：

$$5(a_0+a_1p^m)=5(p^{2m}-(p-1)p^{m-1}-p)/(p^2-1)<p^{2m}+1$$

令b表示$\Phi_{\boldsymbol{a}}(y)$的展开式中变量y的指数，则有：

$$b=p\sum_{j=0}^{(m-4)/2}t_jp^{2j}+p^m\sum_{i=0}^{(m-2)/2}k_ip^{2i}$$

$$t_j,k_i\in\{0,1,2,3,4,5\}.$$

因为$y^{p^{2m}+1}=1$，而$b\leqslant 5(a_0+a_1p^m)<p^{2m}+1$，并且$t_j,k_i<p^2$，$p\sum_{j=0}^{(m-4)/2}t_jp^{2j}<p^m$，$\sum_{i=0}^{(m-2)/2}k_ip^{2i}<p^m$，所以$y$的指数$b$的表示是唯一的，因而此时$\Phi_{\boldsymbol{a}}(y)$的展开式中$y$的指数互不相同，且共有$6^{m-1}$或$4^{m-1}$或$2^{m-1}$个指数互不相同的$y$的单项式。

2) 当$a_0=(p^m-1)/(p^2-1)$,$a_1=(p^{m-1}-1)/(p^2-1)$时，显然也有$a_0+a_1=(p^{m-1}-1)/(p-1)=r$，且有：

$$5(a_0+a_1p^m)=5(p^{2m-1}-p^{m+1}+p^{m-1}-1)/(p^2-1)<p^{2m}+1$$

与1)类似，此时$\Phi_{\boldsymbol{a}}(y)$的展开式中y的指数为：

$$b=p\sum_{j=0}^{(m-2)/2}t_jp^{2j}+p^{m+1}\sum_{i=0}^{(m-4)/2}k_ip^{2i}$$

$$t_j,k_i\in\{0,1,2,3,4,5\}$$

同样也因为 $y^{p^{2m}+1}=1$，而 $b<p^{2m}+1, t_j, k_i<p^2$，并且 $\sum_{j=0}^{(m-2)/2} t_j p^{2j} < p^{m+1}$，$\sum_{i=0}^{(m-4)/2} k_i p^{2i} < p^{m+1}$。因此 b 的表示也是唯一的，即 y 的指数互不相同，因而此时 $\Phi_a(y)$ 的展开式中也共有 6^{m-1} 或 4^{m-1} 或 2^{m-1} 个指数互不相同的 y 的单项式。

根据命题1和以上的讨论，有下面的定理成立。

定 理 5 当 $p=3$ 或 $p=5$ 时，$n=4m$，$r=(p^{m-1}-1)/(p-1)$ 时，序列 $s_{l_1,l_2}^{(r)}$ 的线性复杂度 $\mathrm{LS}(s_{l_1,l_2}^{(r)})>2^{\frac{n}{2}-3}n$；或者 $\mathrm{LS}(s_{l_1,l_2}^{(r)})>2^{\frac{n}{4}-2}n$；或者 $\mathrm{LS}(s_{l_1,l_2}^{(r)})>3^{\frac{n}{4}-1}\times 2^{\frac{n}{4}-2}n$。

表1给出了几类周期为 p^n-1 的 p 元序列集的性质比较。

表1 几类周期为p^n-1的p元序列集

序列	n	序列数目	最大边峰值	线性复杂度(最小, 最大)
Sidelnikov序列[7]	偶数或奇数	p^n	$p^{n/2}+1$	$(n,2n)$
Kumar和Moreno序列[4]	$(2m+1)e$	p^n	$p^{n/2}+1$	$(n,2n)$
Liu和Komo序列[5]	偶数	$p^{n/2}$	$p^{n/2}+1$	$(n,3n/2)$
Moriuchi和Imamura序列[6]	偶数	$p^{n/2}$	$p^{n/2}+1$	$(3n,3n)$
Trachtenberg序列[10]	奇数	p^n+1	$p^{(n+1)/2}+1$	$(n,2n)$
Tang等的序列[9]	$2m+1$	p^n+1	$p^{(n+1)/2}+1$	$(n,(m+1)n)$
Jang等的序列[3]	$(2m+1)e$	p^n	$p^{n/2}+1$	$(n,(m+2)n)$
Seo等的序列[8]	偶数	p^n	$p^{n/2+1}+1$	$(n,2n)$
本文序列	$n=4m$，且 m 是偶数	p^{2n}	$4p^{n/2}-1$	$(>2^{\frac{n}{4}-2}n, >3^{\frac{n}{4}-1}\times 2^{\frac{n}{4}-2}n)$ $p=3,5$
本文序列	$n=2m$，且 $\gcd(p-1,m-1)=1$	p^{2n}	$4p^{n/2}-1$	$(2^{\frac{n}{2}-2}n, 3^{\frac{n}{2}-1}\times 2^{\frac{n}{2}-2}n)$ $p>5$

从表1可以看出，文献[3-7]中的序列具有最优的相关特性，但线性复杂度很小。文献[8-10]中的序列与本文序列都具有次最优的相关特性，但本文序列具有更大的集合容量和线性复杂度。

4 结 论

本文构造了一类具有大线性复杂度、大集合容量的 p 元低相关序列集，该序列集突出的优点是同时具有大线性复杂度、大集合容量和 p 元低相关3个性质，特别是线性复杂度远远大于几类已知 p 元序列的线性复杂度。将该类序列用于码分多址通信系统，可以提高系统的安全性。

参 考 文 献

[1] GOLOMB S W, GONG G. Signal designs with good correlation: for wireless communications, cryptography and radar application[M]. Cambridge, U K: Cambridge University Press, 2005.

[2] HELLESETH T. Some results about the crosscorrelation function between two maximal linear sequences[J]. Discrete Math, 1976, 16: 209-232.

[3] JANG J, KIM Y K, NO J S, et al. New family of p-ary sequences with optimal correlation property and large linear span[J]. IEEE Trans Inform Theory, 2004, 50(8): 1839-1844.

[4] KUMAR P V, MORENO O. Prime-phase sequences with periodic correlation properties better than binary sequences[J]. IEEE Trans Inform Theory, 1991, 37: 603-616.

[5] LIU S C, KOMO J F. Nonbinary kasami sequences over GF (p)[J]. IEEE Trans Inform Theory, 1992, 38: 1049-1412.

[6] MORIUCHI T, IMAMURA K. Balanced nonbinary sequences with good periodic correlation properites obtained from modified kumar-moreno sequences[J]. IEEE Trans Inform Theory, 1995, 41: 572-576.

[7] SIDWLNIKOV V M. On mutual correlation of sequences[J]. Soviet Math Dokl, 1971, 12(1): 197-201.

[8] SEO E Y, KIM Y S, NO J S, et al. Cross-correlation distribution of p-ary m-sequence and its p+1 decimated sequences with shorter period[J]. IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences, 2007, E90-A(11): 2568-2574.

[9] TANG X H, UDAYA P, FAN P Z. A new family of nonbinary sequences with three-level correlation property and large linear span[J]. IEEE Trans Inform Theory, 2005, 51(8): 2906-2914.

[10] TRACHTENBERG H M. On the crosscorrelation functions of maximal linear recurring sequences[D]. Los Angeles: Univ of South Calif, 1970.

[11] ZENG F X. Two classes of large familes of sequences with low correlation[C]//Proceedings of IWSD A'07. Chengdu: IEEE Press, 2007: 56-60.

[12] GOLOMB S W, GONG G. Signal designs with good correlation:for wireless communications,cryptography and radar application[M]. Cambridge, U K: Cambridge University Press, 2005.

[13] ZENG F X. New sequences with low correlation and large family size[J]. IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences, 2008, E91-A(9): 2615-2621.

[14] LIDL R, NIEDERREITER H. Introduction to finite fields and their applications[M]. Cambridge: ambridge University Press, 1994.

[15] KLAPPER A. d-form sequences: families of sequences with low correlation values and large linear spans[J]. IEEE Trans Inform Theory, 1995, 41(2): 423-431.

[16] KEY E L. An analysis of the structure and complexity of nonlinear binary sequence generators[J]. IEEE Trans Inform Theory, 1976, 22(6): 732-736.

编 辑 张 俊