第41卷第7期 中国科学技术大学学报 Vol. 41, No. 7
2011年7月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Jul. 2011

文章编号:0253-2778(2011)07-0636-06

一类新的具有大集合容量的 p 元低相关序列集

夏永波

(中南民族大学数学与统计学学院,湖北武汉 430074)

摘要:设 p 是奇素数,正整数 $n\geqslant 3$,$\gcd(k,n)=1$,利用有限域 F_{p^n} 上的一类二次型,构造了一类新的周期为 p^n-1 的 p 元序列集 $\mathscr{F}_{n,k}$. 新构造的序列集的容量为 p^{2n},最大非平凡相关值为 $p^{n/2+1}+1$,其相关值分布也被确定. 同其他低相关序列集相比,所得的序列集 $\mathscr{F}_{n,k}$ 不仅具有低的相关特性,同时还具有更大的集合容量.

关键词:二次型;指数和;p 元序列;有限域

中图分类号:TN918.1 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2011.07.011

A new family of p-ary low correlation sequences with large family size

XIA Yongbo

(*School of Mathematics and Statistics, South-Central University for Nationalities, Wuhan* 430074, *China*)

Abstract: Let p be an odd prime and $n\geqslant 3$, and k be positive integers with $\gcd(k,n)=1$. Utilizing a class of quadratic forms over F_{p^n}, a new family of p-ary sequences with period p^n-1 was proposed. The proposed family has family size p^{2n} and maximum correlation $p^{n/2+1}+1$. The correlation distribution of the family was completely determined. Compared with the known sequence families, the proposed family has larger family size, while still maintaining low correlation.

Key words: quadratic form; exponential sum; p-ary sequences; finite fields

0 引言

低相关序列集在通信系统与密码系统中具有重要的应用[1]. 在某些应用环境如在码分多址(CDMA)通信系统中,序列集的低相关特性和序列集的容量是决定系统性能的重要参数,因此设计具有低相关特性和大集合容量的序列集具有重要的意义. 二元序列集、四相序列集[2]以及一般的 p 元序列集(p 是一奇素数)是通信系统中常用的序列集. 人们在二元序列集的构造中,经常通过挑选线性码中循环移位不等价的一些码字来构造具有低相关特性的序列集[3-7],其中典型的代表是周期为 2^n-1 的大集合 Kasami 序列集[3,7],其集合容量为 $2^{3n/2}+2^n$ 或 $2^{3n/2}+2^n-1$. 对于奇素数 p,人们也构造出了一些具有周期 p^n-1 的 p 元低相关序列集[8-13],但是这些集合的容量都不超过 $p^{3n/2}$.

设 p 是一奇素数,正整数 $n\geqslant 3$,$\gcd(k,n)=1$,最近,Feng 等在文献[14]中研究了由有限域 F_{p^n} 上二次型

$$Q_{\gamma,\delta}(x)=Tr_1^n(\gamma x^{p^k+1}+\delta x^2),\gamma,\delta\in F_{p^n}$$

所定义的一类指数和

$$S(\gamma,\delta,\lambda)=\sum_{x\in F_{p^n}}\omega^{Q_{\gamma,\delta}(x)+Tr_1^n(\lambda x)},\gamma,\delta,\lambda\in F_{p^n}$$

确定了该指数和的取值分布,其中 $Tr(\cdot)$ 表示从有

收稿日期:2011-04-28;**修回日期**:2011-06-21

基金项目:中南民族大学校自然科学基金(YZY10008)资助.

作者简介:夏永波,男,1979年生,博士/讲师. 研究方向:编码与密码学. E-mail: xiaybm@126.com

限域 F_{p^n} 到其子域 F_p 的迹函数[15]，$\omega=e^{\frac{2\pi\sqrt{-1}}{p}}$ 为 p 次本原单位根.

本文利用前述二次型构造了一类新的周期为 p^n-1 的 p 元低相关序列集，并在文献[14]的研究基础上进一步研究了指数和 $S(\gamma,\delta,\lambda)$ 的性质，进而确定了新序列集的相关值分布. 这类新序列集的集合容量为 p^{2n}，最大非平凡相关值为 $p^{n/2+1}+1$，同其他已知的具有低相关性的序列集相比，新构造出的序列集在保持低相关特性的同时，还具有更大的集合容量.

1　预备知识

本文总设 p 是一奇素数，n 为一正整数，F_{p^n} 表示含有 p^n 个元素的有限域. 令

$$\mathscr{F}=\{\{s_i(t)\}_{t=0}^{p^n-2}\mid 0\leqslant i<M\}$$

表示含 M 条周期为 p^n-1 的 p 元序列集，即序列集 $\mathscr{F}$ 的集合容量是 M. 序列集 $\mathscr{F}$ 中序列 $\{s_i(t)\}_{t=0}^{p^n-2}$ 与 $\{s_j(t)\}_{t=0}^{p^n-2}$ 的相关函数定义为

$$R_{i,j}(\tau)=\sum_{t=0}^{p^n-2}\omega^{s_i(t)-s_j(t+\tau)},\ 0\leqslant\tau<p^n-1$$

式中，$\omega=e^{\frac{2\pi\sqrt{-1}}{p}}$ 为 p 次本原单位根；$t+\tau$ 是在模 p^n-1 意义下的加法. 当 $0<\tau<p^n-1$ 或 $\tau=0$ 但 $i\neq j$ 时，相关函数 $R_{i,j}(\tau)$ 的值称为序列集 $\mathscr{F}$ 的非平凡相关值. 序列集 $\mathscr{F}$ 的最大非平凡相关值 $R_{\max}$ 定义为

$$R_{\max}=\max\{|R_{i,j}(\tau)|\mid 0\leqslant i,j<M,\ 0<\tau<p^n-1\text{ 或 }\tau=0\text{ 但 }i\neq j\}$$

即 $R_{\max}$ 为序列集 $\mathscr{F}$ 的所有非平凡相关值的模的最大值. 若一个周期为 p^n-1 的 p 元序列集 $\mathscr{F}$ 集合容量为 M，最大非平凡相关值为 $R_{\max}$，就称 $\mathscr{F}$ 是一个具有参数 $(p^n-1,M,R_{\max})$ 的 p 元序列集[1].

设有周期为 p^n-1 的 p 元序列 $\{a(t)\}_{t=0}^{p^n-2}$ 与 $\{b(t)\}_{t=0}^{p^n-2}$，若存在 $0\leqslant\tau<p^n-1$ 使得 $b(t)=a(t+\tau)$，对所有的 $t\in\{0,1,\cdots,p^n-2\}$ 都成立，则称 $\{a(t)\}_{t=0}^{p^n-2}$ 与 $\{b(t)\}_{t=0}^{p^n-2}$ 是循环移位等价的，并称 $\{b(t)\}_{t=0}^{p^n-2}$ 是由 $\{a(t)\}_{t=0}^{p^n-2}$ 循环左移 τ 位生成的.

有限域上的二次型被广泛地用于构造低相关序列集[7,12-13,16]. 本文将利用下面的二次型来构造一类 p 元序列集.

定义 1.1　设 p 是一奇素数，k,n 是正整数，$n\geqslant3$ 且 $\gcd(k,n)=1$. 定义

$$Q_{\gamma,\delta}(x)=Tr_1^n(\gamma x^{p^k+1}+\delta x^2),\ \gamma,\delta\in F_{p^n}\quad(1)$$

定义 1.2　设 $Q_{\gamma,\delta}(x)$ 是定义 1.1 中的二次型. 定义线性码

$$C=\{c(\gamma,\delta,\lambda)\mid\gamma,\delta,\lambda\in F_{p^n}\}\quad(2)$$

式中，

$$c(\gamma,\delta,\lambda)=(Q_{\gamma,\delta}(x)+Tr_1^n(\lambda x),x\in F_{p^n}^*).$$

文献[14]中，Feng 等在研究线性码 C 的权重分布时，确定了如下指数和

$$S(\gamma,\delta,\lambda)=\sum_{x\in F_{p^n}}\omega^{Q_{\gamma,\delta}(x)+Tr_1^n(\lambda x)},\ \gamma,\delta,\lambda\in F_{p^n}\quad(3)$$

的取值分布，其中 $\omega=e^{\frac{2\pi\sqrt{-1}}{p}}$. 下设 η 表示有限域 F_{p^n} 上的二次特征[15].

引理 1.1[14]　设 $n\geqslant3$，$\gcd(k,n)=1$. 则当 (γ,δ) 遍历 $F_{p^n}^2$ 一次，$S(\gamma,\delta,0)$ 的取值分布情况如表 1 所示.

表 1　(γ,δ) 遍历 $F_{p^n}^2$ 一次时 $S(\gamma,\delta,0)$ 的取值分布

Tab. 1　**The value distribution of** $S(\gamma,\delta,0)$ **when** (γ,δ) **runs through** $F_{p^n}^2$

n	$S(\gamma,\delta,0)$	出现次数
奇数	p^n	1
	$\pm\sqrt{\eta(-1)}\,p^{n/2}$	$\frac{p^2(p^n-p^{n-1}-p^{n-2}+1)(p^n-1)}{2(p^2-1)}$
	$\pm p^{\frac{n+1}{2}}$	$\frac{p^{\frac{n-1}{2}}(p^{\frac{n-1}{2}}\pm1)(p^n-1)}{2}$
	$\pm\sqrt{\eta(-1)}\,p^{\frac{n}{2}+1}$	$\frac{(p^{n-1}-1)(p^n-1)}{2(p^2-1)}$
偶数	p^n	1
	$\pm p^{\frac{n}{2}}$	$\frac{p^2[p^n-p^{n-1}-p^{n-2}\pm(p^{\frac{n}{2}}-p^{\frac{n}{2}-1})+1](p^n-1)}{2(p^2-1)}$
	$\pm\sqrt{\eta(-1)}\,p^{\frac{n+1}{2}}$	$\frac{p^{n-1}(p^n-1)}{2}$
	$\pm p^{\frac{n}{2}+1}$	$\frac{(p^{\frac{n}{2}}\mp1)(p^{\frac{n}{2}-1}\pm1)(p^n-1)}{2(p^2-1)}$

表 2 (γ,δ,λ) **遍历** $F_{p^n}^3$ **一次时** $S(\gamma,\delta,\lambda)$ **的取值分布**

Tab. 2 The value distribution of $S(\gamma,\delta,\lambda)$ when (γ,δ,λ) runs through $F_{p^n}^3$

n	$S(\gamma,\delta,0)$	出现次数
奇数	p^n	1
	0	$(p^n-1)(p^{2n-1}-p^{2n-2}+p^{2n-3}-p^{n-2}+1)$
	$\pm\sqrt{\eta(-1)}p^{\frac{n}{2}}$	$\frac{p^{n+1}(p^n-p^{n-1}-p^{n-2}+1)(p^n-1)}{2(p^2-1)}$
	$\pm\sqrt{\eta(-1)}p^{\frac{n}{2}}\omega^j, j\in F_p^*$	$\frac{p^{\frac{n+3}{2}}(p^n-p^{n-1}-p^{n-2}+1)(p^n-1)(p^{\frac{n-1}{2}}\pm\eta(-j))}{2(p^2-1)}$
	$\pm p^{\frac{n+1}{2}}$	$\frac{p^{n-2}(p^{n-1}\pm p^{\frac{n+1}{2}}+p-1)(p^n-1)}{2}$
	$\pm p^{\frac{n+1}{2}}\omega^j, j\in F_p^*$	$\frac{p^{n-2}(p^{n-1}-1)(p^n-1)}{2}$
	$\pm\sqrt{\eta(-1)}p^{\frac{n}{2}+1}$	$\frac{p^{n-3}(p^{n-1}-1)(p^n-1)}{2(p^2-1)}$
	$\pm\sqrt{\eta(-1)}p^{\frac{n}{2}+1}\omega^j, j\in F_p^*$	$\frac{p^{\frac{n-3}{2}}(p^{n-1}-1)(p^n-1)(p^{\frac{n-3}{2}}\pm\eta(-j))}{2(p^2-1)}$
偶数	p^n	1
	0	$(p^n-1)(p^{2n-1}-p^{2n-2}+p^{2n-3}-p^{n-2}+1)$
	$\pm p^{\frac{n}{2}}$	$\frac{p^{\frac{n}{2}+1}[p^{\frac{n}{2}}\pm(p-1)][p^n-p^{n-1}-p^{n-2}\pm(p^{\frac{n}{2}}-p^{\frac{n}{2}-1})+1](p^n-1)}{2(p^2-1)}$
	$\pm p^{\frac{n}{2}}\omega^j, j\in F_p^*$	$\frac{p^{\frac{n}{2}+1}(p^{\frac{n}{2}}\mp1)[p^n-p^{n-1}-p^{n-2}\pm(p^{\frac{n}{2}}-p^{\frac{n}{2}-1})+1](p^n-1)}{2(p^2-1)}$
	$\pm\sqrt{\eta(-1)}p^{\frac{n+1}{2}}$	$\frac{p^{2n-3}(p^n-1)}{2}$
	$\pm\sqrt{\eta(-1)}p^{\frac{n+1}{2}}\omega^j, j\in F_p^*$	$\frac{p^{\frac{3n}{2}-2}(p^{\frac{n}{2}-1}\pm\eta(-j))(p^n-1)}{2}$
	$\pm p^{\frac{n}{2}+1}$	$\frac{p^{\frac{n}{2}-2}(p^{\frac{n}{2}-1}\pm1)(p^{\frac{n}{2}}\mp1)[p^{\frac{n}{2}-1}\pm(p-1)](p^n-1)}{2(p^2-1)}$
	$\pm p^{\frac{n}{2}+1}\omega^j, j\in F_p^*$	$\frac{p^{\frac{n}{2}-2}(p^{\frac{n}{2}}\mp1)(p^{n-2}-1)(p^n-1)}{2(p^2-1)}$

引理 1.2[14] 设 $n\geqslant3$, $\gcd(k,n)=1$. 则当 (γ,δ,λ) 遍历 $F_{p^n}^3$ 一次时, $S(\gamma,\delta,\lambda)$ 的取值分布情况如表 2 所示.

2 新序列的构造

本节将用式(1)中的函数 $Q_{\gamma,\delta}(x)$ 来构造一类新的 p 元序列, 并利用式(3)中的指数和来研究新序列的相关性.

定义 2.1 设 α 为有限域 F_{p^n} 的本原元. 定义序列集

$$\mathscr{F}_{n,k}=\{\{s_{\gamma,\delta}(t)\}_{t=0}^{p^n-2}\mid\gamma,\delta\in F_{p^n}\}\tag{4}$$

式中, $s_{\gamma,\delta}(t)=Q_{\gamma,\delta}(\alpha^t)+Tr_1^n(\alpha^t)$.

约定 x 以 $x=\alpha^t, t=0,1,2,\cdots,p^n-2$ 的方式遍历 $F_{p^n}^*$, 则式(2)中线性码 C 的一个码字 $c(\gamma,\delta,\lambda)$ 可看作一条序列, 于是有下面的引理.

引理 2.1 $\mathscr{F}_{n,k}=\{c(\gamma,\delta,1)\mid\gamma,\delta\in F_{p^n}\}$. 进一步有, 任取 $c(\gamma,\delta,\lambda)\in C$, 若 $\lambda=\alpha^\tau$, 则 $c(\gamma,\delta,\lambda)$ 是由 $\mathscr{F}_{n,k}$ 中序列 $c(\gamma\alpha^{-(p^k+1)\tau},\delta\alpha^{-2\tau},1)$ 循环左移 τ 位生成的.

证明 由前述约定及序列集 $\mathscr{F}_{n,k}$ 的定义, 可知

$$\mathscr{F}_{n,k}=\{c(\gamma,\delta,1)\mid\gamma,\delta\in F_{p^n}\}.$$

序列 $c(\gamma\alpha^{-(p^k+1)\tau},\delta\alpha^{-2\tau},1)$ 循环左移 τ 位的表达为

$$\{Tr_1^n(\gamma\alpha^{-(p^k+1)\tau}\alpha^{(p^k+1)(t+\tau)}+\delta\alpha^{-2\tau}\alpha^{2(t+\tau)})+Tr_1^n(\alpha^{t+\tau})\}_{t=0}^{p^n-2}=$$
$$\{Tr_1^n(\gamma\alpha^{(p^k+1)t}+\delta\alpha^{2t})+Tr_1^n(\lambda\alpha^t)\}_{t=0}^{p^n-2}=$$
$$c(\gamma,\delta,\lambda).$$

证毕.

下面的引理确定了序列集 $\mathscr{F}_{n,k}$ 的集合容量, 所得结论表明新构造的序列集具有较大的集合容量.

引理 2.2 序列集 $\mathscr{F}_{n,k}$ 中任意两条序列都是循环移位不等价的, 即序列集 $\mathscr{F}_{n,k}$ 的集合容量 $|\mathscr{F}_{n,k}|=p^{2n}$.

证明 取 $\{s_{\gamma_1,\delta_1}(t)\}_{t=0}^{p^n-2}\in\mathscr{F}_{n,k}$, $\{s_{\gamma_2,\delta_2}(t)\}_{t=0}^{p^n-2}\in$

$\mathscr{F}_{n,k}$，假设它们是循环移位等价的，即存在 $0<\tau\leqslant p^n-2$ 使得

$$Q_{\gamma_2,\delta_2}(x)+Tr_1^n(x)=Q_{\gamma_1,\delta_1}(\alpha^\tau x)+Tr_1^n(\alpha^\tau x),\quad \text{任意的 } x\in F_{p^n}^* \tag{5}$$

式(5)成立当且仅当

$$\gamma_2=\gamma_1\alpha^{(p^k+1)\tau},\delta_2=\delta_1\alpha^{2\tau},\alpha^\tau=1 \tag{6}$$

当 $0<\tau\leqslant p^n-2$ 时，因 $\alpha^\tau\neq 1$，故式(6)不可能成立，从而序列集 $\mathscr{F}_{n,k}$ 中任意两条序列都是循环移位不等价的. 由 $\gamma,\delta\in F_{p^n}$，知(γ,δ)不同选取方式有 p^{2n} 种，即 $\mathscr{F}_{n,k}$ 的集合容量为 p^{2n}. 证毕.

注意码字 $c(\gamma,\delta,0)$作为序列，其周期为$\dfrac{p^n-1}{2}$，因此不可能将 $c(\gamma,\delta,0)$添加到序列集 $\mathscr{F}_{n,k}$ 中来增加其集合容量. 综合引理 2.1～2.2 可知：

①新定义的序列集 $\mathscr{F}_{n,k}$ 中任意两条序列是循环移位不等价的，并且不可能再通过添加 C 中的码字来增大 $\mathscr{F}_{n,k}$ 的集合容量. 即 $\mathscr{F}_{n,k}$ 是循环码 C 的一个具有两两码字循环移位不等价性质的最大子集.

②任取 $\lambda\in F_{p^n}^*\backslash\{1\}$，可定义序列集

$$\mathscr{F}_{n,k}(\lambda)=\{c(\gamma,\delta,\lambda)\mid \gamma,\delta\in F_{p^n}\}.$$

若 $\lambda=\alpha^\tau$，则 $\mathscr{F}_{n,k}(\lambda)$是由 $\mathscr{F}_{n,k}$ 中的序列循环左移 τ 位生成的. 所以序列集 $\mathscr{F}_{n,k}(\lambda)$的相关性质和 $\mathscr{F}_{n,k}$ 的相关性质完全相同.

下面研究新序列集 $\mathscr{F}_{n,k}$ 的相关性质. 取 $\{s_{\gamma_1,\delta_1}(t)\}_{t=0}^{p^n-2}\in\mathscr{F}_{n,k}$，$\{s_{\gamma_2,\delta_2}(t)\}_{t=0}^{p^n-2}\in\mathscr{F}_{n,k}$，令它们的周期相关函数为

$$R_{\gamma_1\delta_1,\gamma_2\delta_2}(\tau)=\sum_{t=0}^{p^n-2}\omega^{s_{\gamma_1,\delta_1}(t)-s_{\gamma_2,\delta_2}(t+\tau)}$$

为了确定当(γ_1,δ_1)，(γ_2,δ_2)遍历 $F_{p^n}^2$，τ 遍历$\{0,1,\cdots,p^n-2\}$时，周期相关函数 $R_{\gamma_1\delta_1,\gamma_2\delta_2}(\tau)$的取值以及各个取值出现的次数，即为了确定序列集 $\mathscr{F}_{n,k}$的相关值分布，需要用到指数和 $S(\gamma,\delta,\lambda)$的如下的一个性质.

引理 2.3　任意取定 $\lambda\in F_{p^n}^*$，则当(γ,δ)遍历 $F_{p^n}^2$ 一次时，$S(\gamma,\delta,\lambda)$同 $S(\gamma,\delta,1)$具有相同的值分布.

证明

$$S(\gamma,\delta,\lambda)=\sum_{x\in F_{p^n}}\omega^{Tr_1^n(\gamma x^{p^k+1}+\delta x^2+\lambda x)}=\sum_{y\in F_{p^n}}\omega^{Tr_1^n(\gamma\lambda^{-(p^k+1)}y^{p^k+1}+\delta\lambda^{-2}y^2+y)}=S(\lambda^{-(p^k+1)}\gamma,\lambda^{-2}\delta,1)$$

由于 $\lambda\in F_{p^n}^*$ 取定，所以当(γ,δ)遍历 $F_{p^n}^2$ 一次时$(\lambda^{-(p^k+1)}\gamma,\lambda^{-2}\delta)$也遍历 $F_{p^n}^2$一次，所以当(γ,δ)遍历 $F_{p^n}^2$一次时，$S(\gamma,\delta,\lambda)$同 $S(\gamma,\delta,1)$具有相同的值分布. 证毕.

定理 2.1　设 $\mathscr{F}_{n,k}$是定义 2.1 中所构造的序列集. 则当 n 为奇数时，$\mathscr{F}_{n,k}$的相关分布如表 3；当 n 为偶数时，$\mathscr{F}_{n,k}$的相关分布如表 4. 表中 ω 为 p 次本原单位根，η是有限域 F_{p^n}上的二次特征[15].

证明　取$\{s_{\gamma_1,\delta_1}(t)\}_{t=0}^{p^n-2}\in\mathscr{F}_{n,k}$，$\{s_{\gamma_2,\delta_2}(t)\}_{t=0}^{p^n-2}\in\mathscr{F}_{n,k}$，则它们的周期相关函数

$$R_{\gamma_1\delta_1,\gamma_2\delta_2}(\tau)=\sum_{t=0}^{p^n-2}\omega^{s_{\gamma_1,\delta_1}(t)-s_{\gamma_2,\delta_2}(t+\tau)}=\sum_{x\in F_{p^n}}\omega^{Q_{\lambda_1,\lambda_2}(x)+Tr_1^n(\lambda_3 x)}-1=S(\lambda_1,\lambda_2,\lambda_3)-1$$

表 3　n 为奇数时序列集 $\mathscr{F}_{n,k}$ 的相关值分布

Tab. 3　The correlation distribution of $\mathscr{F}_{n,k}$ when n is odd

$R_{\gamma_1\delta_1,\gamma_2\delta_2}(\tau)$	出现次数
p^n-1	p^{2n}
-1	$p^{2n}(p^n-2)(p^{2n-1}-p^{2n-2}+p^{2n-3}-p^{n-2}+1)$
$\pm\sqrt{\eta(-1)}p^{\frac{n}{2}}-1$	$\dfrac{p^{2n}(p^n-p^{n-1}-p^{n-2}+1)(p^{2n+1}-2p^{n+1}+p^2)}{2(p^2-1)}$
$\pm\sqrt{\eta(-1)}p^{\frac{n}{2}}\omega^j-1,j\in F_p^*$	$\dfrac{p^{\frac{5n+3}{2}}(p^n-2)(p^n-p^{n-1}-p^{n-2}+1)(p^{\frac{n-1}{2}}\pm\eta(-j))}{2(p^2-1)}$
$\pm p^{\frac{n+1}{2}}-1$	$\dfrac{p^{2n}(p^{\frac{n-1}{2}}\pm1)[(p^n-2)p^{n-2}(p^{\frac{n-1}{2}}\pm(p-1))+p^{\frac{n-1}{2}}]}{2}$
$\pm p^{\frac{n+1}{2}}\omega^j-1,j\in F_p^*$	$\dfrac{p^{2n}(p^n-2)p^{n-2}(p^{n-1}-1)}{2}$
$\pm\sqrt{\eta(-1)}p^{\frac{n}{2}+1}-1$	$\dfrac{p^{2n}(p^{n-1}-1)[(p^n-2)p^{n-3}+1]}{2(p^2-1)}$
$\pm\sqrt{\eta(-1)}p^{\frac{n}{2}+1}\omega^j-1,j\in F_p^*$	$\dfrac{p^{2n}(p^n-2)p^{\frac{n-3}{2}}(p^{n-1}-1)(p^{\frac{n-3}{2}}\pm\eta(-j))}{2(p^2-1)}$

表 4 n 为偶数时序列集 $\mathscr{F}_{n,k}$ 的相关值分布

Tab. 4 The correlation distribution of $\mathscr{F}_{n,k}$ when n is even

$R_{\gamma_1\delta_1,\gamma_2\delta_2}(\tau)$	出现次数
p^n-1	p^{2n}
-1	$p^{2n}(p^n-2)(p^{2n-1}-p^{2n-2}+p^{2n-3}-p^{n-2}+1)$
$\pm p^{\frac{n}{2}}-1$	$\frac{p^{2n+2}[p^n-p^{n-1}-p^{n-2}\pm(p^{\frac{n}{2}}-p^{\frac{n}{2}-1})+1][(p^n-2)(p^{n-1}\pm(p-1)p^{\frac{n}{2}-1})+1]}{2(p^2-1)}$
$\pm p^{\frac{n}{2}}\omega^j-1, j\in F_p^*$	$\frac{p^{\frac{5n}{2}+1}(p^n-2)(p^{\frac{n}{2}}\mp1)[p^n-p^{n-1}-p^{n-2}\pm(p^{\frac{n}{2}}-p^{\frac{n}{2}-1})+1]}{2(p^2-1)}$
$\pm\sqrt{\eta(-1)}p^{\frac{n+1}{2}}-1$	$\frac{p^{3n-3}(p^n+p^2-2)}{2}$
$\pm\sqrt{\eta(-1)}p^{\frac{n+1}{2}}\omega^j-1, j\in F_p^*$	$\frac{p^{\frac{7n}{2}-2}(p^n-2)(p^{\frac{n}{2}-1}\pm\eta(-j))}{2}$
$\pm p^{\frac{n}{2}+1}-1$	$\frac{p^{2n}(p^{\frac{n}{2}-1}\pm1)(p^{\frac{n}{2}}\mp1)[(p^n-2)p^{\frac{n}{2}-2}(p^{\frac{n}{2}-1}\pm(p-1))+1]}{2(p^2-1)}$
$\pm p^{\frac{n}{2}+1}\omega^j-1, j\in F_p^*$	$\frac{p^{\frac{5n}{2}-2}(p^n-2)(p^{\frac{n}{2}}\mp1)(p^{n-2}-1)}{2(p^2-1)}$

式中，

$$\lambda_1=\gamma_1-\gamma_2\alpha^{(p^k+1)\tau},\gamma_2=\delta_1-\delta_2\alpha^{2\tau},\gamma_3=1-\alpha^{\tau} \tag{7}$$

显然$(\lambda_1,\lambda_2,\lambda_3)=(0,0,0)$当且仅当 $\gamma_1=\gamma_2,\delta_1=\delta_2,\tau=0$. 若给定 γ_2,δ_2，由式(7)知：当(γ_1,δ_1)遍历 $F_{p^n}^2,\tau$遍历$\{0,1,\cdots,p^n-2\}$时，$(\lambda_1,\lambda_2,\lambda_3)$遍历 $F_{p^n}\times F_{p^n}\times\{F_{p^n}\backslash\{1\}\}$. 所以相关函数的值分布是当$(\lambda_1,\lambda_2,\lambda_3)$遍历 $F_{p^n}\times F_{p^n}\times\{F_{p^n}\backslash\{1\}\}$时 $S(\lambda_1,\lambda_2,\lambda_3)$的相应值分布的 p^{2n}倍. 由引理 1.1～1.2 和引理 2.3，可计算出当(γ,δ)遍历 $F_{p^n}^2$时 $S(\gamma,\delta,1)$的值分布，进而可求得当$(\lambda_1,\lambda_2,\lambda_3)$遍历 $F_{p^n}\times F_{p^n}\times\{F_{p^n}\backslash\{1\}\}$时，$S(\lambda_1,\lambda_2,\lambda_3)$的值分布. 根据以上分析，通过计算即可得到表 3 和表 4. 证毕.

由表 3 和表 4 知：序列集 $\mathscr{F}_{n,k}$的最大非平凡相关值为 $p^{\frac{n}{2}+1}+1$. 结合引理 2.2 可知序列集 $\mathscr{F}_{n,k}$的集合容量比其周期的平方还要大.

表 5 列出了本文所构造的新序列集与其他几类已知的具有大集合容量的低相关序列集，其中 * 表示 n 可取为奇数或者偶数. 从表中可看出 $\mathscr{F}_{n,k}$在具有低相关性的同时，还具有更大的集合容量. 此外，序列集 $\mathscr{F}_{n,k}$的参数 n 可以为任意≥3 的偶数或奇数.

表 5 具有大集合容量和低相关性的序列集

Tab. 5 Some sequence families with low correlation and large family size

序列集	周期	集合容量	$R_{\max}$	n
Largesetofgeneralized Kasamisequences[3,7]	2^n-1	$2^{\frac{n}{2}}(2^n+1)-1$ or $2^{\frac{n}{2}}(2^n+1)$	$2^{\frac{n}{2}+1}+1$	偶数
Rothaus[5]	2^n-1	$2^{2n}+2^n+1$	$2^{\frac{n+3}{2}}+1$	奇数
Yu-Gong[6]	2^n-1	$2^{\rho n},1<\rho\leqslant\frac{n-1}{2}$	$2^{\frac{n+2\rho-1}{2}}+1$	奇数
Yu-Gong[6]	2^n-1	$2^{\rho n},1<\rho<\frac{n}{2}$	$2^{\frac{n}{2}+\rho}+1$	偶数
Trachtenberg[8]	p^n-1	p^n+1	$p^{\frac{n+1}{2}}+1$	奇数
Helleseth[9]	$p^n-1, p^{\frac{n}{2}}\neq2(\mathrm{mod}\ 3)$	p^n+1	$2p^{\frac{n}{2}}+1$	偶数
Kumar-Moreno[10]	p^n-1	p^n	$p^{\frac{n}{2}}+1$	*
Sidelnikov[11]	p^n-1	p^n	$p^{\frac{n}{2}}+1$	*
Largeset of p-ary Kasamisequences[13]	p^n-1	$p^{\frac{3n}{2}}$	$p^{\frac{n}{2}+1}+1$	偶数
新序列 $\mathscr{F}_{n,k}$	p^n-1	p^{2n}	$p^{\frac{n}{2}+1}+1$	*

表 6　$p=3, n=3, k=2$ 时序列集 $\mathscr{F}_{3,2}$ 的相关分布

Tab. 6　The correlation distribution of $\mathscr{F}_{3,2}$ when $p=3, n=3, k=2$

相关值	分布	相关值	分布
26	729	-8	56 862
-1	3 408 075	$\pm 9\omega^2-1$	218 700
$\pm 3\sqrt{3}i-1$	1 482 786	$\pm 9\omega-1$	218 700
$3\sqrt{3}\omega^2 i-1$	1 968 300	$\pm 9\sqrt{3}i-1$	9 477
$-3\sqrt{3}\omega^2 i-1$	984 150	$9\sqrt{3}\omega^2 i-1$	18 225
$3\sqrt{3}\omega i-1$	984 150	$-9\sqrt{3}\omega^2 i-1$	0
$-3\sqrt{3}\omega i-1$	1 968 300	$9\sqrt{3}\omega i-1$	0
8	551 124	$-9\sqrt{3}\omega i-1$	18 225

下面提供一个实例. 取 $p=3, n=3, k=2$, 令 α 为 F_{3^3} 的本原元, 其极小多项式为 $1+2x^2+x^3$. 通过 C++ 语言编程可以输出序列集 $\mathscr{F}_{3,2}=\{\{s_{\gamma,\delta}(t)\}_{t=0}^{25} \mid \gamma,\delta\in F_{3^3}\}$ 中的所有序列. 这里限于篇幅不列出 $\mathscr{F}_{3,2}$ 中的序列, 仅给出由计算机计算得到的 $\mathscr{F}_{3,2}$ 的相关值分布, 如表 6 所示, 其中 $\omega=\frac{-1+\sqrt{3}i}{2}$, $i=\sqrt{-1}$. 这与利用表 3 中的公式计算得到的结果是一致的.

参考文献(References)

[1] Golomb S W, Gong G. Signal Designs for Good Correlation: For Wireless Communications, Cryptography, and Radar [M]. Cambridge, UK: Cambridge University Press, 2005.

[2] Xia Yongbo, Zeng Xiangyong, Liu Heguo, et al. A new family of quadriphase sequences with optimal correlation properties [J]. Acta Mathematic Scientia, 2008, 28(4): 735-741.
夏永波, 曾祥勇, 刘合国, 等. 一类新的四相最优序列集[J]. 数学物理学报, 2008, 28(4): 735-741.

[3] Kasami T. Weight enumerators for several classes of subcodes of the 2nd order Reed-Muller codes [J]. Inform Contr, 1971, 18: 369-394.

[4] Chang A, Gaal P, Golomb S W, et al. On a conjectured ideal autocorrelation sequence and a related triple-error correcting cyclic code [J]. IEEE Transactions on Information Theory, 2000, 46(2): 680-687.

[5] Rothaus O S. Modified Gold codes [J]. IEEE Transactions on Information Theory, 1993, 39(2): 654-656.

[6] Yu N Y, Gong G. A new binary sequence family with low correlation and large size [J]. IEEE Transactions on Information Theory, 2006, 52(4): 1 624-1 636.

[7] Zeng X, Liu J Q, Hu L. Generalized Kasami sequences: The large set [J]. IEEE Transactions on Information Theory, 2007, 53(7): 2 587-2 598.

[8] Trachtenberg H M. On the Cross-Correlation Functions of Maximal Recurring Sequences [D]. Log Angeles, CA: University of Southern California, 1970.

[9] Helleseth T. Some results about the cross-correlation function between two maximal linear sequences [J]. Discrete Math, 1976, 16: 209-232.

[10] Kumar P, Moreno O. Prime-phase sequences with periodic correlation properties better than binary sequences [J]. IEEE Transactions on Information Theory, 1991, 37(3): 603-616.

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

[12] Xia Yongbo, Zeng Xiangyong, Hu Lei. Further crosscorrelation properties of sequences with the decimation factor [J]. Appl Algebra Eng Commun Comput, 2010, 21(5): 329-342.

[13] Xia Yongbo, Zeng Xiangyong, Hu Lei. The large set of -ary Kasami sequences [J]. International Journal of Computer Mathematics, 2010, 87(7): 1 436-1 455.

[14] Feng K, Luo J. Weight distribution of some reducible cyclic codes [J]. Finite Fields Appl, 2008, 14: 390-409.

[15] Lidl R, Niederreiter H. Finite Fields[M]. Cambridge, UK: Cambridge University Press, 1983.

[16] Helleseth T, Kumar P V. Sequences with low correlation[M]// Handbook of Coding Theory. The Netherlands: Elsevier Science, 1998: 1 765-1 853.