一类具有极低相关性的CDMA序列

孙霓刚[1,2],胡 磊[2]
(1.华东理工大学计算机科学与工程系,上海 200237;2.中国科学院研究生院信息安全国家重点实验室,北京 100049)

摘 要: 本文利用环$\mathbb{Z}_{p^l}$上线性递归序列的最高坐标构造了一类序列数目众多的p元序列族,这里p为奇素数且整数l不小于2.对具体可用序列的条数进行了估计.同时利用Galois环上的指数和估计以及$\mathbb{Z}_{p^l}$的加法群上的谱分析对该序列族的相关性进行了详细分析,得到了其非同步自相关性及互相关性的估计.结果表明,所构造的序列具有极低的相关性,其相关性的模值具有与Welch下界相同的数量级,可以作为CDMA通信系统中的码序列.

关键词: 相关性;Galois环;最高坐标;Welch下界
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2010) 07-1525-06

A New CDMA Sequence Family with Low Correlation

SUN Ni-gang[1,2], HU Lei[2]
(1. *Department of Computer Science and Engineering, East China University of Science and Technology, Shanghai 200237, China;*
2. *State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing 100049, China*)

Abstract: A new family of p-phase sequences with large family size is constructed, where p is an odd prime. The technique employed uses the highest coordinate of some linear recurrence sequences over the ring $\mathbb{Z}_{p^l}$, for any integer l which is greater than or equal to 2. The size of the family is estimated. Based on Galois ring theory (the local Weil bound) and spectral analysis over the additive group of $\mathbb{Z}_{p^l}$, we analyze the correlation properties of the sequences in detail and derive an estimate of the nontrivial autocorrelation and crosscorrelation of the sequences. The result shows that these sequences have low correlation, which makes it possible as code sequences in CDMA communication systems.

Key words: correlation; Galois ring; highest coordinate; Welch's lower bound

1 引言

码分多址(CDMA)通信系统是一种利用扩频技术所形成的不同码序列实现多址通信的方式.在该系统中,码序列通过公共信道同时分配给不同的用户[1].为了达到区分不同用户以及降低相互之间干扰的目的,不同的码序列之间必须具有低的互相关性.同时,同一码序列不同相位之间的自相关性也必须非常低以保证能够准确地获得用户的相位信息.此外,码序列的数量也必须足够大以满足系统中不断增加的用户数量.因此,序列数目众多且具有低相关性的码序列族在CDMA通信系统中有着十分重要的作用.

1974年,Welch在文献[2]中证明了序列的最大非同步自相关性和最大互相关性模值的下界为$\sqrt{T}$(Welch下界),这里T是序列的周期.追求序列族的Welch下界是码序列设计的一个重要环节.文献[3~10]构造了一些适合CDMA通信信道上传输的具有最佳相关性(相关性的模值达到Welch下界)或极小相关(相关性模值接近Welch下界)的二元序列族.而文献[11~16]则给出了几类相关性模值达到或接近Welch下界的四元序列族.本文利用最高坐标映射构造了一类序列周期为$q-1$($q=p^m$,p为奇素数,m为正整数),序列数目众多的p元序列族.并利用Kumar等人[17]以及Helleseth等人[18]给出的Galois环上指数和估计以及傅立叶变换对该序列族的非同步自相关性和互相关性进行了估计,证明该序列族的相关性模值具有与Welch下界相同的数量级$\sqrt{q}$.

2 基本概念

假设p为素数,$l\geqslant 2$和m为正整数.$R=GR(p^l,m)$表示具有特征p^l及阶p^{lm}的Galois环.任取$\zeta\in R$满足$\zeta^{p^m}=\zeta$并且令Γ为R的一个Teichmüller集,即

$$\Gamma=\{0,1,\zeta,\zeta^2,\cdots,\zeta^{p^m-2}\}$$

收稿日期:2008-01-04;修回日期:2010-04-08
基金项目:信息安全国家重点实验室开放课题;国家科技支撑计划(No.2009BAH46B03)

R 中任意元素 x 均可表示为 $x = x_0 + px_1 + \cdots + p^{l-1}x_{l-1}$，其中 $x_0, x_1, \cdots, x_{l-1} \in \Gamma$. 我们称之为 x 的 p-adic 展开. 对上述 x，如下定义 Frobenius 算子 F：

$$F(x_0 + px_1 + \cdots + p^{l-1}x_{l-1}) = x_0^p + px_1^p + \cdots + p^{l-1}x_{l-1}^p$$

以及从 R 到 $\mathbb{Z}_{p^l}$ 的迹函数 Tr：

$$\mathrm{Tr}(x) = \sum_{j=0}^{m-1} F^j(x)$$

类似于最显著比特映射(most-significant-bit map)[8]，定义最高坐标映射 $HC: \mathbb{Z}_{p^l} \to \mathbb{Z}_p$ 满足

$$HC(x_0 + px_1 + \cdots + p^{l-1}x_{l-1}) = x_{l-1}$$

易见，对任意正整数 q，HC 可自然地推广为从 $\mathbb{Z}_p^{q^{l-1}}$ 到 $\mathbb{Z}_p^{q^{l-1}}$ 的映射. 更多 Galois 环的知识请参见文献[19, 20].

下面我们均假设 $q = p^m$. 设

$$f(x) = \sum_{i=0}^{n} c_i x^i$$

是 $R[x]$ 中次数为 n 的多项式. 将 $f(x)$ 的系数 c_i 进行 p-adic 展开，可以得到 $f(x)$ 的 p-adic 展开，即

$$f(x) = F_0(x) + pF_1(x) + \cdots + p^{l-1}F_{l-1}(x), F_j(x) \in \Gamma[x].$$

设 $F_j(x) = \sum_{i=0}^{n_j} F_{j,i}x^i$，其中 n_j 是 $F_j(x)$ 的次数. 我们称多项式 $f(x)$ 是非退化的，如果 $F_j(x)$ 的系数 $F_{j,i}$ 满足

$$F_{j,i} = 0, \text{当 } i = 0 \pmod p, 0 \leqslant i \leqslant n_j, 0 \leqslant j \leqslant l-1$$

$f(x)$ 的非退化性表明当 $i = 0 \pmod p$ 时，$c_i = 0$. $R[x]$ 中任意多项式 f 的权重次数 D_f 定义为

$$D_f = \max\{n_0 p^{l-1}, n_1 p^{l-2}, \cdots, n_{l-1}\}$$

进而，对任意给定的整数 $D \geqslant p$，我们可以定义集合

$$S_D = \{f(x) \in R[x] \mid D_f \leqslant D, f \text{ 是非退化的}\}$$

其中 D_f 是 f 的权重次数. 易见，S_D 是 R 上的线性空间. 关于权重次数，我们有下面的引理.

引理 1 假设 $f(x)$ 是 $R[x]$ 中多项式并且其 p-adic 展开为

$$f(x) = F_0(x) + pF_1(x) + \cdots + p^{l-1}F_{l-1}(x), F_j(x) \in \Gamma(x)$$

令 $f_i(x) = p^i F_i(x)$. 对 R 中的任意单位 α，定义 $g(x) = f(\alpha x)$，$g_i(x) = f_i(\alpha x)$，其中 $i = 0, 1, \cdots, l-1$. 我们有

(1) $D_{g_i} = D_{f_i}$，其中 D_{f_i} 是 $f_i(x)$ 的权重次数，D_{g_i} 是 $g_i(x)$ 的权重次数；

(2) $D_g = D_f$，其中 D_f 是 $f(x)$ 的权重次数，D_g 是 $g(x)$ 的权重次数.

证明 (1)设 $F_i(x) = c_0 + c_1 x + \cdots + c_d x^d$，其中 d 是 $F_i(x)$ 的次数，$c_j \in \Gamma$. 易见，f_i 的权重次数 $D_{f_i} = p^{l-1-i} \cdot d$. 对任意 $0 \leqslant k \leqslant l-1$，设 α^k 的 p-adic 展开为

$$\alpha^k = \sum_{j=0}^{l-1} \alpha_{j,k} p^j$$

将 αx 代入 $F_i(x)$，我们有

$$F_i(\alpha x) = \sum_{k=0}^{d} c_k \alpha^k x^k = \sum_{k=0}^{d} c_k \left(\sum_{j=0}^{l-1} \alpha_{j,k} p^j\right) x^k.$$

交换和号，上式可以表示为

$$F_i(\alpha x) = \sum_{j=0}^{l-1} p^j \sum_{k=0}^{d} c_k \alpha_{j,k} x^k = \sum_{j=0}^{l-1} p^j F_{i,j}(x),$$

其中 $F_{i,j}(x) \in \Gamma[x]$ 且次数最高为 d. 由 α 是 R 中的单位可知，$\alpha_{0,k} \neq 0 (k = 0, \cdots, d)$，因此多项式

$$F_{i,0}(x) = \sum_{k=0}^{d} c_k \alpha_{0,k} x^k$$

的次数等于 d. 从而 $g_i(x) = f_i(\alpha x)$ 的权重次数 $D_{g_i} = p^{l-1-i}d = D_{f_i}$.

(2)由 $D_g = D_{g_0 + g_1 + \cdots + g_{l-1}} = \max\{D_{g_0}, D_{g_1}, \cdots, D_{g_{l-1}}\}$ 以及结论(1)可知：$D_g = \max\{D_{f_0}, D_{f_1}, \cdots, D_{f_{l-1}}\} = D_f$

证毕. □

利用权重次数和非退化多项式，Kumar 等人给出了下面的不等式.

引理 2[17, Theorem 1] 沿用前面的记号. 设 $f(x)$ 是 $R[x]$ 中的非退化多项式，其权重次数记为 D_f. 令 $\chi: R \to \mathbb{C}$ 为 R 上的加法特征，则

$$\left|\sum_{x \in \Gamma} \chi(f(x))\right| \leqslant (D_f - 1)\sqrt{q}$$

3 新的 p 元序列族

定义 1 对任意整数 $D \geqslant p$，定义码长为 $q-1$ 的 $\mathbb{Z}_{p^l}$ 线性码 $C_{l,m}(D) = \{\underline{x} = (x_0, \cdots, x_{q-2}) \in \mathbb{Z}_p^{q^{l-1}} \mid x_j = \mathrm{Tr}(f(\zeta^j)), f \in S_D\}$. 考虑到 ζ 的阶为 $q-1$，我们可以得到下面的引理.

引理 3 令 $C(l, m, D)$ 表示 $C_{l,m}(D)$ 在最高坐标映射 HC 下的像，即 $C(l, m, D) = HC(C_{l,m}(D))$，则 $C(l, m, D)$ 是码长为 $q-1$ 的 p 元循环码.

由引理 3 可知，如果把 $C(l, m, D)$ 中任意码字进行周期性的重复，均可得到一条周期为 $q-1$ 的 p 元序列. 我们给出下面的定义.

定义 2 对任意 $f \in S_D$，定义 $\mathbb{Z}_p$ 上具有周期 $q-1$ 的序列 $(c_t)_{t=0}^{\infty}$，其中 $c_t = HC(\mathrm{Tr}(f(\zeta^t)))$. 进而定义集合 $S(l, m, D) = \{(c_t)_{t=0}^{\infty} \mid f \in S_D\}$.

易见，$S(l, m, D)$ 为 p 元序列族，其中的每条序列均具有周期 $q-1$. 在文献[17]中，Kumar, Helleseth 和 Calderbank 指出序列族 $S(l, m, D)$ 中序列的条数至少为

$$\frac{1}{q-1}\sum_{d \mid q-1} (q^{\lfloor D/d \rfloor - \lfloor D/(dp^l) \rfloor} - 1)u(d)$$

其中 $\lfloor x \rfloor$ 表示不超过 x 的最大整数，u 为 Möbius 函数：

$$u(d) = \begin{cases} 1, \text{当 } d = 1 \\ (-1)^r, \text{当 } d \text{ 是 } r \text{ 个不同素数的乘积} \\ 0, \text{其他情况.} \end{cases}$$

表 1 给出了对 $S(l, m, D)$ 在某些选定参数情况下的序

列数目的估计.

表 1　$S(l,m,D)$中的序列数目

参数 p,l	权重次数 D	序列的条数
2,2	2	$q+1$
2,2	3	$\frac{q^3-1}{q-1}$, m 为奇数 $\frac{q^3-1}{q-1}-1$, m 为偶数
2,3	4	$\frac{q^4-1}{q-1}$, m 为奇数 $\frac{q^4-1}{q-1}-1$, m 为偶数
2,3	5	$\geqslant q^4$
2,3	6	$\geqslant q^5$
2,3	7	$\geqslant q^6$
3,2	8	$\geqslant q^7$
3,3	9	$\geqslant q^8$
3,3	10	$\geqslant q^9$
3,3	11	$\geqslant q^{10}$

4　相关性

我们沿用前面的记号和定义并假设 $p\geqslant 3$. 令 $\omega=e^{2\pi i/p^l}$表示复数域$\mathbb{C}$中的 p^l 次本原单位根以及 $\theta=\omega^{p^{l-1}}$. 易见 θ 为$\mathbb{C}$中的 p 次本原单位根. 定义$\mathbb{Z}_{p^l}$上的加法特征 Ψ_k:

$$\Psi_k(x)=\omega^{kx}$$

考虑到$\mathbb{Z}_{p^l}$中的任意元素 a 均可以唯一地写成如下形式:$a=a_0+pa_1+\cdots+p^{l-1}a_{l-1}$, $a_0,a_1,\cdots,a_{l-1}\in\mathbb{Z}_p$，我们可以定义映射 $\mu:\mathbb{Z}_{p^l}\to\{1,\theta,\theta^2,\cdots,\theta^{p-1}\}$ 满足 $\mu(a)=\theta^{a_{l-1}}$. 利用$\mathbb{Z}_{p^l}$ 上的傅立叶变换[21],我们有

$$\mu(x)=\sum_{j=0}^{p^l-1}\mu_j\Psi_j(x),\text{其中 }\mu_j=\frac{1}{p^l}\sum_{x=0}^{p^l-1}\mu(x)\Psi_j(-x) \tag{1}$$

我们给出下述引理.

引理 4　对任意 $0\leqslant j\leqslant p^l-1$,我们有

$$\mu_j=\begin{cases}0, & j\neq 1\pmod p\\ \dfrac{1}{p^{l-1}}\dfrac{1-\theta^{-j}}{1-\omega^{-j}}, & j=1\pmod p\end{cases}$$

证明　由 ω 和 θ 的定义可知,

$$\Psi_j(x-ip^{l-1})=\Psi_j(x)\theta^{-ji}$$

考虑到映射 $\mu(x)$满足 $\mu(x+p^{l-1})=\mu(x)\theta$,我们可以推出 $\mu(x+ip^{l-1})=\mu(x)\theta^i$,

进而
$$\begin{aligned}\mu_j&=\frac{1}{p^l}\sum_{x=0}^{p^l-1}\mu(x)\Psi_j(-x)\\&=\frac{1}{p^l}\sum_{x=0}^{p^{l-1}-1}\sum_{i=0}^{p-1}\mu(x+ip^{l-1})\Psi_j(-x-ip^{l-1})\\&=\frac{1}{p^l}\sum_{x=0}^{p^{l-1}-1}\mu(x)\Psi_j(-x)\sum_{i=0}^{p-1}\theta^{(1-j)i}\end{aligned}$$

因此对任意 $j\neq 1\pmod p$,我们有 $\mu_j=0$. 另一方面,由于当 $x=0,1,\cdots,p^{l-1}-1$ 时,$\mu(x)=1$. 因此对任意 $j=1\pmod p$,我们有

$$\mu_j=\frac{1}{p^{l-1}}\sum_{x=0}^{p^{l-1}-1}\Psi_j(-x)=\frac{1}{p^{l-1}}\frac{1-\theta^{-j}}{1-\omega^{-j}}$$

证毕. □

推论 1　对任意 $0\leqslant j\leqslant p^l-1$,当 $j=1\pmod p$时,我们有

$$|\mu_j|=\frac{1}{p^{l-1}}\frac{\sin(\frac{\pi}{p})}{\sin(\frac{\pi j}{p^l})}$$

证明　令 $i=\sqrt{-1}$. 考虑到

$$\sin(\frac{\pi j}{p})=\frac{e^{\frac{\pi ij}{p}}-e^{-\frac{\pi ij}{p}}}{2i}=\frac{e^{\frac{2\pi ij}{2p}}-e^{\frac{2\pi i(-j)}{2p}}}{2i}=\frac{\theta^{\frac{j}{2}}-\theta^{-\frac{j}{2}}}{2i},$$

我们可以推出

$$1-\theta^{-j}=\theta^{-\frac{j}{2}}(\theta^{\frac{j}{2}}-\theta^{-\frac{j}{2}})=2i\theta^{-\frac{j}{2}}\sin(\frac{\pi j}{p})$$

类似地,我们可以得到

$$1-\omega^{-j}=2i\omega^{-\frac{j}{2}}\sin(\frac{\pi j}{p^l})$$

从而对任意整数 j 满足 $0\leqslant j\leqslant p^l-1$ 以及 $j=1\pmod p$,利用引理 4,我们有

$$|\mu_j|=\frac{1}{p^{l-1}}\frac{|1-\theta^{-j}|}{|1-\omega^{-j}|}=\frac{1}{p^{l-1}}\frac{\sin(\frac{\pi}{p})}{\sin(\frac{\pi j}{p^l})}$$

证毕.

假设 $T=\dfrac{p^{l-1}-1}{2}$,并且令

$$A=\ln(\tan(\frac{\pi}{4}-\frac{p-2}{4p^l}\pi))+\ln(\cot(\frac{\pi}{2p^l})),$$

$$B=\ln(\cot(\frac{p-1}{2p^l}\pi))+\ln(\cot(\frac{\pi}{4}+\frac{p+2}{4p^l}\pi)).$$

利用 A 和 B,我们给出如下估计.

命题 1　和式 $\sum_{j=0}^{p^l-1}|\mu_j|$的值满足下列不等式

$$\sum_{j=0}^{p^l-1}|\mu_j|<\frac{\sin(\frac{\pi}{p})}{\pi}(A+B)+\frac{\sin(\frac{\pi}{p})}{p^{l-1}\sin(\frac{\pi}{p^l})}+\frac{\sin(\frac{\pi}{p})}{p^{l-1}\sin(\frac{p-1}{p^l}\pi)},$$

$$\sum_{j=0}^{p^l-1}|\mu_j|>\frac{\sin(\frac{\pi}{p})}{\pi}(A+B)+\frac{\sin(\frac{\pi}{p})}{p^{l-1}\cos(\frac{p-2}{2p^l}\pi)}+\frac{\sin(\frac{\pi}{p})}{p^{l-1}\cos(\frac{p+2}{2p^l}\pi)}. \tag{2}$$

证明　利用引理 4 和推论 1,我们有

$$\sum_{j=0}^{p^l-1}|\mu_j|=\sum_{n=0}^{T}|\mu_{np+1}|+\sum_{n=1}^{T}|\mu_{(n+T)p+1}|$$

$$= \frac{\sin(\frac{\pi}{p})}{p^{l-1}}\left(\sum_{n=0}^{r}\frac{1}{\sin(\frac{np+1}{p^l}\pi)} + \sum_{n=1}^{r}\frac{1}{\sin(\frac{np+Tp+1}{p^l}\pi)}\right)$$

$$= \frac{\sin(\frac{\pi}{p})}{p^{l-1}}\left(\sum_{n=0}^{r}\frac{1}{\sin(\frac{np+1}{p^l}\pi)} + \sum_{n=1}^{r}\frac{1}{\cos(\frac{np-\frac{p-2}{2}}{p^l}\pi)}\right) \quad (3)$$

令 $g_1(x)=\frac{1}{\sin(\pi x/p^l)}$,则

$$\sum_{n=0}^{r}\frac{1}{\sin(\frac{np+1}{p^l}\pi)} = \sum_{n=0}^{r} g_1(np+1) \quad (4)$$

由于 $g_1(x)$在区间$[1, Tp+1]$上恒正并且为严格递减函数,我们可以得到如下不等式

$$pg_1((n+1)p+1) < \int_{np+1}^{(n+1)p+1} g_1(x)\mathrm{d}x < pg_1(np+1)$$

其中 $n=0,1,\cdots,T-1$. 对 n 从0到 $T-1$ 进行求和,可得

$$p\sum_{n=1}^{r} g_1(np+1) < \int_{1}^{Tp+1} g_1(x)\mathrm{d}x < p\sum_{n=0}^{r-1} g_1(np+1)$$

进而,我们有

$$\sum_{n=0}^{r} g_1(np+1) < \frac{1}{p}\int_{1}^{Tp+1} g_1(x)\mathrm{d}x + g_1(1) \quad (5)$$

$$\sum_{n=0}^{r} g_1(np+1) > \frac{1}{p}\int_{1}^{Tp+1} g_1(x)\mathrm{d}x + g_1(Tp+1) \quad (6)$$

从而,利用式(4),(5),(6)以及等式

$$\int_{1}^{Tp+1} g_1(x)\mathrm{d}x = \frac{p^l}{\pi}\int_{\frac{\pi}{p^l}}^{\frac{\pi}{2}-\frac{p-2}{p^l}\pi}\frac{\mathrm{d}y}{\sin(y)} = \frac{p^l}{\pi}A$$

我们可以推出

$$\sum_{n=0}^{r}\frac{1}{\sin(\frac{np+1}{p^l}\pi)} < \frac{p^{l-1}}{\pi}A + \frac{1}{\sin(\frac{\pi}{p^l})} \quad (7)$$

$$\sum_{n=0}^{r}\frac{1}{\sin(\frac{np+1}{p^l}\pi)} > \frac{p^{l-1}}{\pi}A + \frac{1}{\cos(\frac{p-2}{2p^l}\pi)} \quad (8)$$

令 $g_2(x)=\frac{1}{\cos(\pi x/p^l)}$,则

$$\sum_{n=1}^{r}\frac{1}{\cos(\frac{np-\frac{p-2}{2}}{p^l}\pi)} = \sum_{n=1}^{r} g_2(np-\frac{p-2}{2}) \quad (9)$$

由于 $g_2(x)$在区间$[\frac{p+2}{2}, Tp-\frac{p-2}{2}]$上恒正并且为严格递增函数,因此与前面的讨论类似,我们可以得到

$$\sum_{n=1}^{r} g_2(np-\frac{p-2}{2}) < \frac{1}{p}\int_{\frac{p+2}{2}}^{Tp-\frac{p-2}{2}} g_2(x)\mathrm{d}x + g_2(Tp-\frac{p-2}{2}) \quad (10)$$

$$\sum_{n=1}^{r} g_2(np-\frac{p-2}{2}) > \frac{1}{p}\int_{\frac{p+2}{2}}^{Tp-\frac{p-2}{2}} g_2(x)\mathrm{d}x + g_2(\frac{p+2}{2}) \quad (11)$$

从而,利用式(9),(10),(11)以及等式

$$\int_{\frac{p+2}{2}}^{Tp-\frac{p-2}{2}} g_2(x)\mathrm{d}x = \frac{p^l}{\pi}\int_{\frac{p+2}{2p^l}\pi}^{\frac{\pi}{2}-\frac{p-1}{p^l}\pi}\frac{\mathrm{d}y}{\cos(y)} = \frac{p^l}{\pi}B$$

我们可以推出

$$\sum_{n=1}^{r}\frac{1}{\cos(\frac{np-\frac{p-2}{2}}{p^l}\pi)} < \frac{p^{l-1}}{\pi}B + \frac{1}{\sin(\frac{p-1}{p^l}\pi)} \quad (12)$$

$$\sum_{n=1}^{r}\frac{1}{\cos(\frac{np-\frac{p-2}{2}}{p^l}\pi)} > \frac{p^{l-1}}{\pi}B + \frac{1}{\cos(\frac{p+2}{2p^l}\pi)} \quad (13)$$

最后,将式(7),(8),(12),(13)应用到式(3),我们便可以得到对 $\sum_{j=0}^{p^l-1}|\mu_j|$ 的估计. 证毕.

特别地,我们有下面的推论.

推论2 $\sum_{j=0}^{p^l-1}|\mu_j| < \frac{2l}{p}\ln(p)+2$

证明 由 A 和 B 的定义可知,

$$A=\int_{\frac{\pi}{p^l}}^{\frac{\pi}{2}-\frac{p-2}{2p^l}\pi}\frac{\mathrm{d}y}{\sin(y)},\quad B=\int_{\frac{p+2}{2p^l}\pi}^{\frac{\pi}{2}-\frac{p-1}{p^l}\pi}\frac{\mathrm{d}y}{\cos(y)}$$

考虑到 $\sin(y)$在区间$[\frac{\pi}{p^l},\frac{\pi}{2}]$上恒正以及 $\cos(y)$在区间$[0,\frac{\pi}{2}-\frac{p-1}{p^l}\pi]$上恒正,我们可以推出

$$A<\int_{\frac{\pi}{p^l}}^{\frac{\pi}{2}}\frac{\mathrm{d}y}{\sin(y)} = \ln(\cot(\frac{\pi}{2p^l})),$$

$$B<\int_{0}^{\frac{\pi}{2}-\frac{p-1}{p^l}\pi}\frac{\mathrm{d}y}{\cos(y)} = \ln(\cot(\frac{p-1}{2p^l}\pi))$$

由于当 $0<x<\pi/4$ 时,$\tan(x)>x$. 因此我们有

$$\ln(\cot(x)) = -\ln(\tan(x)) < -\ln(x)$$

从而

$$A<\ln(\cot(\frac{\pi}{2p^l})) < l\ln(p)-\ln(\frac{\pi}{2})$$

$$B<\ln(\cot(\frac{p-1}{2p^l}\pi)) < l\ln(p)-\ln(\frac{\pi}{2})$$

进而,利用不等式 $\sin(\pi/p)<\pi/p$,我们得到

$$\frac{\sin(\frac{\pi}{p})}{\pi}(A+B)<\frac{2l}{p}\ln(p)-\frac{2}{p}\ln(\frac{\pi}{2}) \quad (14)$$

利用不等式 $\sin(\frac{\pi}{p^l})>\frac{\pi}{p^l}(1-\frac{1}{6}(\frac{\pi}{p^l})^2)$

可得

$$\frac{\sin(\frac{\pi}{p})}{p^{l-1}\sin(\frac{\pi}{p^l})}<\frac{\frac{\pi}{p}}{p^{l-1}\frac{\pi}{p}(1-\frac{1}{6}(\frac{\pi}{p^l})^2)}<1.021 \quad (15)$$

类似地,由不等式

$$\sin(\frac{p-1}{p^l}\pi)>\frac{p-1}{p^l}\pi(1-\frac{1}{6}(\frac{p-1}{p^l}\pi)^2)$$

可推出

$$\frac{\sin(\frac{\pi}{p})}{p^{l-1}\sin(\frac{p-1}{p^l}\pi)}<0.545 \quad (16)$$

最后,将式(14),(15),(16)应用到式(2),我们得到

$$\sum_{j=0}^{p^l-1}|\mu_j|<\frac{2l}{p}\ln(p)-\frac{2}{p}\ln(\frac{\pi}{2})+1.021+0.545$$
$$<\frac{2l}{p}\ln(p)+2$$

证毕.

定义特征 $\Psi_\beta: R\to\mathbb{C}^*$ 满足 $\Psi_\beta(x)=\omega^{\mathrm{Tr}(\beta x)}$.由 ψ_k 及 Ψ_β 的定义可知

$$\psi_k(\mathrm{Tr}(\beta x))=\Psi_{x\beta}(x)$$

下面给出本节的主要结果.

定理 1　对任意移位 $\tau,0<\tau<q-1$,令

$$\Theta(\tau)=\sum_{t=0}^{q-2}\theta^{c_t-c'_{t+\tau}}$$

其中 $c_t=HC(\mathrm{Tr}(f_1(\zeta^t)))$, $c'_t=HC(\mathrm{Tr}(f_2(\zeta^t)))$且 $f_1,f_2\in S_D$.由我们有

$$|\Theta(\tau)|<(1+(D-1)\sqrt{q})(\frac{2l}{p}\ln(p)+2)^2 \quad (17)$$

证明　由映射 μ 的定义以及式(1),我们有

$$\theta^{c_t}=\mu(Tr(f_1(\zeta^t)))=\sum_{j=0}^{p^l-1}\mu_j\Psi_j(f_1(\zeta^t)).$$

由于对任意 $c\in\mathbb{Z}_{p^l}$ 以及 $d=HC(c)$,有 $\theta^{-d}=\alpha\mu(-c)$成立,其中 $\alpha\in\{1,\theta\}$,因此

$$\theta^{-c'_{t+\tau}}=\alpha\mu(-Tr(f_2(\zeta^{t+\tau})))=\alpha\sum_{j=0}^{p^l-1}\mu_j\Psi_j(-f_2(\zeta^{t+\tau})).$$

交换和号,我们可以得到

$$\Theta(\tau)=\alpha\sum_{j_1=0}^{p^l-1}\sum_{j_2=0}^{p^l-1}\mu_{j_1}\mu_{j_2}\sum_{t=0}^{q-2}\Psi_{j_1}(f_1(\zeta^t))\Psi_{j_2}(-f_2(\zeta^{t+\tau})).$$

由 Ψ 的定义可知,

$$\Psi_{j_1}(f_1(\zeta^t))\Psi_{j_2}(-f_2(\zeta^{t+\tau}))=\Psi(g(\zeta^t))$$

其中 $g(x)=j_1f_1(x)-j_2f_2(x\zeta^\tau)$.引理 1 以及 S_D 是 R 上的线性空间保证了 $g(x)\in S_D$.利用引理 2,我们有

$$|\sum_{t=0}^{q-2}\Psi_{j_1}(f_1(\zeta^t))\Psi_{j_2}(-f_2(\zeta^{t+\tau}))|$$
$$=|\sum_{x\in\Gamma/\{0\}}\Psi(g(x))|\leqslant 1+(D-1)\sqrt{q}.$$

进而,利用推论 2,我们有

$$|\Theta(\tau)|\leqslant|\alpha\sum_{j_1=0}^{p^l-1}\sum_{j_2=0}^{p^l-1}\mu_{j_1}\mu_{j_2}|(1+(D-1)\sqrt{q})$$
$$\leqslant(\sum_{j=0}^{p^l-1}|\mu_j|)^2(1+(D-1)\sqrt{q})$$
$$<(1+(D-1)\sqrt{q})(\frac{2l}{p}\ln(p)+2)^2.$$

证毕. □

5　结论

本文构造了一类序列数目众多,序列周期为 p^m-1 的 p 元 CDMA 序列族 $S(l,m,D)(l\geqslant 2)$,并证明了该序列族具有极小的相关性.证明的关键在于将映射 μ 表示成 R 上的特征的线性组合.下一步的工作可以考虑对这类序列的线性复杂度进行估计.

参考文献:

[1] M K Simon, J K Omura, R Scholtz, B K Levitt. Spread-Spectrum Communications [M]. New York: Computer Science Press, vol.1, 1985.

[2] L R Welch. Lower bounds on the maximum correlation of signals[J]. IEEE Trans. Inf. Theory, 1974, 20(3): 397 – 399.

[3] S Boztas, P V Kumar. Near optimal sequences for CDMA[A]. Proc. 1991 IEEE International Symposium on Information Theory[C]. New York: IEEE Press, 1991. 282 – 282.

[4] S H Kim, J S No. New families of binary sequences with low correlation[J]. IEEE Trans. Inf. Theory, 2003, 49(11): 3059—3065.

[5] J Lahtonen, S Ling, P Solé, D Zinoviev. Z_8-Kerdock codes and pseudorandom binary sequences[J]. Journal of Complexity, 2004, 20: 318 – 330.

[6] J S No, S W Golomb, G Gong, H K Lee, P Gaal. Binary pseudorandom sequences of period 2^m-1 with ideal autocorrelation [J]. IEEE Trans. Inf. Theory, 1998, 44(2): 814 – 817.

[7] A G Shanbhag, P V Kumar, T Helleseth. Improved binary codes and sequence families from $\mathbb{Z}_4$- linear codes[J]. IEEE Trans. Inf. Theory, 1996, 42(5): 1582 – 1587.

[8] P solé, D Zinoview. Low-correlation, high – nonlinearity sequences for multiple-code CDMA[J]. IEEE Trans. Inf. Theory, 2006, 52(11): 5158 – 5163.

[9] P Udaya, M U Siddiqi. Optimal biphase sequences with large

* 式(17)表明,序列族 $S(l,m,D)$的相关性模值具有与 Welch 下界相同的数量级$\sqrt{q}$.

linear complexity derived from sequences over $\mathbb{Z}_4$ [J]. IEEE Trans. Inf. Theory, 1996, 42(1): 206 – 216.

[10] N Y Yu, G Gong. A new binary sequence family with low correlation and large size[J]. IEEE Trans. Inf. Theory, 2006, 52(4): 1624 – 1636.

[11] S Boztas, R Hammons, P V Kumar. 4-phase sequences with near-optimum correlation properties [J]. IEEE Trans. Inf. Theory, 1992, 38(3): 1101 – 1113.

[12] P V Kumar, T Helleseth, A R Calderbank, A R Hammons. Large families of quaternary sequences with low correlation [J]. IEEE Tnans. Inf. Theory, 1996, 42(2): 579 – 592.

[13] P Solé. A quaternary cyclic code and a family of quadriphase sequences with low correlation properties [A]. In Lecture Notes in Computer Science[C]. vol. 388, Berlin: Springer, 1989. 193 – 201.

[14] X H Tang, P Udaya. A note on the optimal quadriphase sequences families[J]. IEEE Trans. Inf. Theory, 2007, 53(1): 433 – 436.

[15] P Udaya, M U Siddiqi. Large linear complexity sequences over $\mathbb{Z}_4$ for quadriphase modulated communication systems having good correlation properties[A]. Proc. 1991 IEEE International Symposium on Information Theory [C]. New York: IEEE Press, 1991. 386 – 386.

[16] P Udaya, M U Siddiqi. Optimal and suboptimal quadriphase sequences derived from maximal length sequences over $\mathbb{Z}_4$ [J]. AAECC, 1998, 9: 161 – 191.

[17] P V Kumar, T Helleseth, A R Calderbank. An upper bound for weil exponential sums over Galois rings and applications[J]. IEEE Trans. Inf. Theory, 1995, 41(2): 456 – 468.

[18] T Helleseth, P V Kumar, O Moreno, A G Shanbhag. Improved estimates via exponential sums for the minimum distance of $\mathbb{Z}_4$ linear trace codes[J]. IEEE Trails. Inf. Theory, 1996, 42(4): 1212 – 1216.

[19] B R McDonald. Finite Rings with Identity [M]. New York: Marcel Dekker, 1974.

[20] Z Wan. Finite Fields and Galois Rings [M]. Singapore: World Scientific Publisher, 2003.

[21] S W Golomb, G Gong. Signal Design for Good Correlation—For Wireless Communication, Cryptography and Rader [M]. New York: Cambridge Univ. Press, 2005.

作者简介：

孙霓刚 男，1978 年生于上海市，华东理工大学计算机科学与工程系讲师，主要研究方向为密码学和信息安全.
E-mail: nigsun@ecust.edu.cn

胡 磊 男，1967 年生于湖北麻城，中国科学院研究生院教授，博士生导师，主要研究方向为密码学和信息安全.
E-mail: hu@is.ac.cn