第 36 卷 第 3 期 计 算 机 工 程 2010 年 2 月
Vol.36 No.3 Computer Engineering February 2010
·博士论文· 文章编号：1000—3428(2010)03—0022—02 文献标识码：A 中图分类号：TP309

大线性复杂度和低相关性的 p 元 CDMA 序列

孙霓刚 [1,2]

(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： 利用环 Z_{p^2} 上广义 Kerdock 码的最高权位生成了一类 p 元最高权位序列，并对其密码特性进行研究。给出序列线性复杂度的准确计算公式，利用 Galois 环上的 Weil 指数和估计对序列的互相关性及非同步自相关性进行刻画。实验结果表明，构造的最高权位序列具有大的线性复杂度和极低的互相关性及非同步自相关性，可作为 CDMA 通信系统中的码序列。

关键词： Galois 环；最高权位序列；线性复杂度；相关性

p-phase CDMA Sequence with Large Linear Complexities and Low Correlation

SUN Ni-gang[1,2]

(1. Department of Computer Science and Engineering, East China University of Science and Technology, Shanghai 200237;
2. State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing 100049)

【Abstract】 A new family of p-phase highest coordinate sequences, is constructed by using the highest coordinate of the generalized Kerdock codes over the ring Z_{p^2}. This paper not only deduces an exact formula on the linear complexities of the sequences, but also derives an estimate of the correlation of the sequences by utilizing the Weil exponential sums over Galois rings. Results shows that these sequences have both large linear complexities and low crosscorrelation and nontrivial autocorrelation, which make it possible to be the code sequences in CDMA communication systems.

【Key words】 Galois ring; highest coordinate sequence; linear complexities; correlation

1 概述

码序列的设计是码分多址(CDMA)通信系统中的核心问题。在该系统中，为了能够区分不同用户以及降低用户之间的干扰，不同的码序列之间必须具有低的互相关性。此外，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。出于安全性方面的考虑，码序列还应该具有大的线性复杂度以满足保密通信的要求。因此，设计和分析具有大线性复杂度、低互相关性和非同步自相关性等良好性质的码序列就为 CDMA 通信系统中的一个关键问题[1]。

1974 年，文献[2]证明了序列的最大非同步自相关性和最大互相关性的模值的下界为 $\sqrt{T}$ (Welch 下界)，这里 T 是序列的周期。追求 Welch 下界以及大线性复杂度是码序列设计中的一个重要环节，目前已经取得了许多结果，如构造了一些相关性模值达到或接近 Welch 下界，并且具有大线性复杂度的二元序列[3-6]。文献[3-4]构造的 Bent 序列及 No 序列的相关性模值均达到了 Welch 下界且具有极大的线性复杂度，但可用序列的数量较少，其序列族的阶的数量级仅为 $\sqrt{T}$ 。文献[5]构造了一类相关性模值达到 Welch 下界的二元序列，并给出了序列线性复杂度的精确值。文献[6]构造了一类相关性模值与 Welch 下界同阶且数量众多的二元最高权位序列，其序列族的阶具有数量级 $T^2/4$，同时对所构造序列的线性复杂度进行了估计，证明了其具有极大的线性复杂度，但没有给出线性复杂度的精确值。文献[7]利用特征为 4 的 Galois 环上的非退化多项式，构造了一类相关性模值与 Welch 下界同阶的二元序列，但没有对序列的线性复杂度进行讨论。随着理论研究和实际应用的不断深入，具有低相关性的多元序列也逐渐成为研究的热点。文献[8-9]构造了 2 类具有极低相关性的四元序列，其相关性的模值与 Welch 下界同阶。在文献[10]中，笔者利用环上的非退化多项式及最高权位映射，构造了一类序列数目众多的 p 元最高权位序列(p 为任意素数)，并利用 Galois 环上的 Weil 指数和估计证明了该序列族具有极低的互相关性和非同步自相关性，其相关性的模值具有与 Welch 下界相同的数量级。上述工作均没有对所构造序列的线性复杂度进行讨论。本文利用环 Z_{p^2} 上广义 Kerdock 码的最高权位生成了一类 p 元最高权位序列，并对序列的密码特性进行了研究，给出了序列线性复杂度的准确计算公式，利用 Galois 环上的 Weil 指数和估计对序列的相关性进行了刻画，最后对可用序列的条数进行了估计。结果表明，所构造的序列不仅具有大的线性复杂度和数量众多的可用序列，而且具有极低的互相关性和非同步自相关性，其相关性的模值具有与 Welch 下界相同的数量级。

设 p 为奇素数，m 为正整数。$R=GR(p^2,m)$ 表示具有特征 p^2 及阶 p^{2m} 的 Galois 环。R^* 表示 R 中所有单位元所组成的单位群。设 α 为 R 中元素并且满足 $\alpha^{p^m}=\alpha$ 。定义 R 中的

基金项目： 信息安全国家重点实验室开放课题基金资助项目
作者简介： 孙霓刚(1978－)，男，讲师、博士，主研方向：密码学与信息安全
收稿日期： 2009-10-30 **E-mail：** nigsun@ecust.edu.cn

Teichmüller 系 $\Gamma=\{0,1,\alpha,\alpha^2,\cdots,\alpha^{p^m-2}\}$。$Tr$ 表示 R 到环 Z_{p^2} 的迹函数。

对 R 中任意元素 x 均可进行 p-adic 展开，即 $x=x_0+px_1$，其中，$x_0,x_1\in\Gamma$。类似于最显著比特映射，定义最高权位映射 $HC:Z_{p^2}\to Z_p$ 满足 $HC(x_0+px_1)=x_1$。令 $q=p^m$，易见，HC 可以扩展为从 $Z_{p^2}^{q-1}$ 到 Z_p^{q-1} 的映射。

定义 Z_{p^2} 上长度为 $q-1$ 的循环码 C_m，即

$$C_m=\{\underline{x}=(x_0,x_1,\cdots,x_{q-2})\in Z_{p^2}^{q-1}\mid x_t=Tr(\lambda\alpha^t),\ \lambda\in R^*\}$$

令 $C(m)=HC(C_m)$，则 $C(m)$ 是 Z_p 上长度为 $q-1$ 的循环码。将 $C(m)$ 中的每个码字按其长度进行周期性重复，均可得到一条周期为 $q-1$ 的 p 元序列，并将所有这些序列组成的集合记为 S_m。

2 线性复杂度

利用文献[11]中的定理 1，可以得到如下关于 S_m 中序列线性复杂度的结果。

定理 1 对 S_m 中任意序列 $s=\{s_t\}_{t\geqslant 0}$，设 $s_t=HC(Tr(\lambda\alpha^t))$，其中，$\lambda=\lambda_0+p\lambda_1\in R^*$，$\lambda_0,\lambda_1\in\Gamma$，则 s 的线性复杂度为

$$LC(s)=(u-1)m+\binom{m+p-1}{p}$$

其中，$u=\begin{cases}1 & \lambda_1\neq 0\\ 0 & \lambda_1=0\end{cases}$。

由定理 1 可以看出，S_m 中序列的线性复杂度随着 m 的增大而增大，并且当 m 充分大时具有数量级 $m^p/p!$。

3 相关性

本节讨论 S_m 中序列的互相关性和非同步自相关性。

令 $\omega=\mathrm{e}^{\frac{2\pi i}{p^2}}$ 表示复数域中的 p^2 次本原单位根以及 $\theta=\omega^p$。易见 θ 是复数域中的 p 次本原单位根。定义 Z_{p^2} 上的加法特征 φ_k 满足 $\varphi_k(x)=\omega^{kx}$。对于 Z_{p^2} 中的任意元素 a，均有唯一分解 $a=a_0+pa_1$，其中，$a_0,a_1\in Z_p$。进而可以定义映射 $\mu:Z_{p^2}\to\{1,\theta,\theta^2,\cdots,\theta^{p-1}\}$ 满足 $\mu(a)=\theta^{a_1}$。利用 Z_{p^2} 上的傅立叶变换，可得

$$\mu(x)=\sum_{j=0}^{p^2-1}\mu_j\varphi_j(x)$$

其中，$\mu_j=\frac{1}{p^2}\sum_{x=0}^{p^2-1}\mu(x)\varphi_j(-x)$。

令 $C=\frac{4}{p}\ln(p)+2$。由文献[10]中的引理 4.1 和推论 4.4 可知，μ_j 具有以下性质：

引理 1 对任意 $0\leqslant j\leqslant p^2-1$，$\mu_j$ 满足：

(1) $\mu_j=\begin{cases}0 & j\neq 1\ (\mathrm{mod}\ p)\\ \frac{1}{p}\frac{1-\theta^{-j}}{1-\omega^{-j}} & j=1\ (\mathrm{mod}\ p)\end{cases}$。

(2) $\sum_{j=0}^{p^2-1}|\mu_j|<C$。

用 G 表示 Z_{p^2} 中所有使得 $\mu_j\neq 0$ 的 j 所组成的乘法群。对 R 中任意元素 λ，定义特征 $\psi_\lambda:R\to\mathrm{C}^*$ 满足 $\psi_\lambda(x)=\omega^{Tr(\lambda x)}$。易见，$\varphi_k$ 和 ψ_λ 满足关系：

$$\varphi_k(Tr(\lambda x))=\psi_{k\lambda}(x)$$

利用文献[12]中定理 1 可以得到下面的引理。

引理 2 对任意 $\lambda\in R$，$\lambda\neq 0$，有

$$|\sum_{x\in\Gamma}\psi_\lambda(x)|\leqslant(p-1)\sqrt{q}$$

定理 2 设 $s=\{s_t\}_{t\geqslant 0}$ 和 $s'=\{s_t'\}_{t\geqslant 0}$ 是 S_m 中任意 2 条序列，其中，$s_t=HC(Tr(\lambda_1\alpha^t))$；$s_t'=HC(Tr(\lambda_2\alpha^t))$。对任意 $0<\tau<q-1$，令 $\Theta(\tau)=\sum_{t=0}^{q-2}\theta^{s_t-s_{t+\tau}'}$，则当 λ_1 和 λ_2 属于 $G\times\Gamma^*$ 在 R^* 中的不同陪集时，有

$$|\Theta(\tau)|<(1+(p-1)\sqrt{q})C^2 \tag{1}$$

证明：由映射 μ 的定义可知：

$$\theta^{s_t}=\mu(Tr(\lambda_1\alpha^t))=\sum_{j=0}^{p^2-1}\mu_j\varphi_j(Tr(\lambda_1\alpha^t))=\sum_{j=0}^{p^2-1}\mu_j\psi_{j\lambda_1}(\alpha^t)$$

注意到 $\theta^{-d}=a\mu(-c)$，其中，$a\in\{1,\theta\}$；$c\in Z_{p^2}$ 且 $d=HC(c)$，进而有

$$\theta^{-s'_{t+\tau}}=a\mu(-Tr(\lambda_2\alpha^{t+\tau}))=$$
$$a\sum_{j=0}^{p^2-1}\mu_j\varphi_j(-Tr(\lambda_2\alpha^{t+\tau}))=a\sum_{j=0}^{p^2-1}\mu_j\psi_{-j\lambda_2\alpha^\tau}(\alpha^t)$$

交换和号，可得

$$\Theta(\tau)=a\sum_{j_1=0}^{p^2-1}\sum_{j_2=0}^{p^2-1}\mu_{j_1}\mu_{j_2}\sum_{t=0}^{q-2}\psi_{j_1\lambda_1}(\alpha^t)\psi_{-j_2\lambda_2\alpha^\tau}(\alpha^t)=$$
$$a\sum_{j_1=0}^{p^2-1}\sum_{j_2=0}^{p^2-1}\mu_{j_1}\mu_{j_2}\sum_{x\in\Gamma^*}\psi_{j_1\lambda_1-j_2\lambda_2\alpha^\tau}(x)$$

只需考虑 $j_1,j_2\in G$ 的情况即可(否则有 $\mu_{j_1}\mu_{j_2}=0$)。由于 λ_1 和 λ_2 属于 $G\times\Gamma^*$ 在 R^* 中不同陪集，因此 $j_1\lambda_1-j_2\lambda_2\alpha^\tau\neq 0$。从而利用引理 1 中的结论(2)以及引理 2，可得

$$|\Theta(\tau)|<(1+(p-1)\sqrt{q})C^2$$

定理 2 表明 S_m 中序列的互相关性和非同步自相关性的模值的数量级为 $\sqrt{T}$，与 Welch 下界相同，这里 $T=p^m-1$ 为序列的周期。

由于 R^* 的阶为 $p^{2m}-p^m$，G 的阶为 p，Γ^* 的阶为 p^m-1，因此 S_m 中的相关性满足式(1)的序列的个数 $N_m=\frac{p^{2m}-p^m}{p(p^m-1)}\sim\frac{T}{p}$。

4 结束语

本文利用最高权位映射构造一类具有周期 p^m-1 的 p 元序列族 S_m，讨论 S_m 中序列的线性复杂度和相关性。分析表明，这类序列的线性复杂度当 m 充分大时具有数量级 $m^p/p!$，同时序列的互相关性和非同步自相关性的模值具有数量级 $\sqrt{T}$，与 Welch 下界相同。此外，序列族中可用序列的条数众多，具有数量级 T/p。由上述结果可知，所构造的序列不仅能够满足 CDMA 通信系统对码序列密码特性的要求，而且能够更好地适应系统中日益增加的用户数量。

参考文献

[1] Simon M K, Omura J K, Scholtz R, et al. Spread-spectrum Communications[M]. [S. 1.]: Computer Science Press, 1985.

[2] Welch L R. Lower Bounds of the Maximum Cross Correlation of Signals[J]. IEEE Trans. on Inform. Theory, 1974, 20(3): 397-399.

[3] Olsen J D, Scholtz R A, Welch L R. Bent Function Sequences[J]. IEEE Trans. on Inform. Theory, 1982, 28(6): 858-864.

[4] No J S, Kumar P V. A New Family of Binary Pseudorandom Sequences Having Optimal Periodic Correlation Properties and Large Linear Span[J]. IEEE Trans. on Inform. Theory, 1989, 35(2): 371-379.

（下转第 27 页）