

一类零相关区序列集构造方法的改进

江文峰¹, 曾祥勇^{1,2}, 胡 磊², 刘合国¹

(1. 湖北大学数学与计算机科学学院, 湖北武汉 430062; 2. 中科院研究生院信息安全国家重点实验室, 北京 100039)

摘 要: 最近 Matsufoji 和 Torii 等人分别提出了由酉矩阵和完备序列构造零相关区序列集的方法. 本文不仅推广了 Matsufoji 等人的结论, 而且推广了 Torii 等人的部分结论, 扩大了基于酉矩阵和完备序列构造零相关区序列集的方法的适用范围, 得到了一些新的零相关区序列集.

关键词: 准同步 CDMA 通信系统; 零相关区序列集; 完备序列; 酉矩阵

中图分类号: TN914.53 文献标识码: A 文章编号: 0372-2112 (2005) 08-1476-04

An Improved Method for Constructing ZCZ Sequence Sets

JIANG Wenfeng¹, ZENG Xiangyong^{1,2}, HU Lei², LIU Hefu¹

(1. Faculty of Mathematics and computer science, Hubei University, Wuhan, Hubei 430062, China;

2. State Key Laboratory of Information Security (Graduate School of the Chinese Academy of Sciences, Beijing 100039, China)

Abstract: Based on perfect sequences and unitary matrices, Matsufoji and Torii et al. propose new methods for constructing ZCZ sequence sets. In this paper, we propose a new method which is an improvement of their methods. The proposed method can be used to construct ZCZ sequence sets with wider range of available periods and width. Furthermore, some new ZCZ sequence sets are obtained by our method.

Key words: QS CDMA system; zero correlation zone (ZCZ) sequence sets; perfect sequences; unitary matrix

1 引言

CDMA 技术已被广泛地应用于移动通信. CDMA 通讯系统的容量大小和通讯质量在很大程度上取决于所采用的扩频序列. 针对准同步 CDMA 系统, 人们提出了零相关区序列集的概念. 在准同步 CDMA 系统中, 采用零相关区序列集作为其扩频序列集, 可以降低或消除系统中如共信道干扰等一些干扰.

描述零相关区的参数主要有序列周期 L , 集合容量 M , 零相关区长度 T 以及相数. 在数学上三个参数满足下面的上界^[10]: $T \leq L/M - 1$ 对于工程上最容易实现的二元和四相序列的情况, 目前发现的最好的序列集的参数分别满足 $T = L/(2M)$ 和 $T = 7L/(8M)$ ^[17].

目前, 针对零相关区序列集的设计, 人们提出了多种构造零相关区序列集的方法. Suchio 在文献^[1]中提出了一种构造二元和多相零相关区序列集的方法. Deng, Fan, Hao, Xu 和 Li 由互补序列对构造出了几类零相关区序列集^[3~5]. 最近, Matsufoji 和 Torii 等人分别提出了另外一种构造思想, 即由完备序列和酉矩阵出发构造零相关区序列集^[6,7]. 本文不仅推广了 Matsufoji 等人的结论, 而且推广了 Torii 等人的部分结论, 扩大了基于酉矩阵和完备序列构造零相关区序列集的方法的适用范围, 得到了一些新的具有较优参数的零相关区序列集. 例如, 利用本文提出的方法可以构造出新的四相 ZCZ- (192, 12, 14) 零相关区序列集, 其参数达到了 $T = 7L/(8M)$.

2 零相关区序列集的构造

定义 1 设 $C = \{C^0, C^1, \dots, C^i, \dots, C^{M-1}\}$ 是由 M 个周期为 L 的等能量 E 的序列构成的序列集, 其中

$$C^i = (c_0^i, c_1^i, \dots, c_j^i, \dots, c_{L-1}^i)$$

$0 \leq i \leq M-1, 0 \leq j \leq L-1$. T 是非负整数, 如果对任意的 $C^{i_1}, C^{i_2} \in C$, 它们的周期相关函数满足:

$$R_{C^{i_1}, C^{i_2}}(\tau) = \sum_{j=0}^{L-1} c_j^{i_1} c_{j+\tau}^{i_2*} \bmod L = \begin{cases} E, & (i_1 = i_2, \tau = 0) \\ 0, & (i_1 = i_2, 0 < |\tau| \leq T) \\ 0, & (i_1 \neq i_2, 0 \leq |\tau| \leq T) \end{cases}$$

其中 $*$ 表示复共轭, 那么称 C 为一个 ZCZ- (L, M, T) 零相关区序列集.

2.1 序列集的生成

由序列 $a = (a_0, a_1, \dots, a_{N_1-1})$ 和 N_2 阶方阵 $B = \frac{1}{\sqrt{N_2}}$ $(b_{ij})_{N_2 \times N_2}$ 定义序列集

$$C = \{C^0, C^1, \dots, C^{N_2-1}\},$$

其中

$$C^i = (c_0^i, c_1^i, \dots, c_{N_1-1}^i, c_{N_1}^i, \dots, c_{N_1+N_2-1}^i),$$

$c_j^i = a_{((N_1/d) \cdot j + \lfloor j/d \rfloor) \bmod N_1} b_{i, j \bmod N_2}, 0 \leq i \leq N_2-1, 0 \leq j \leq N_1+N_2-1$, $d = (N_1, N_2)$ 表示 N_1 和 N_2 的最大公约数, $\lfloor j/d \rfloor$ 表示取 j/d 的整数部分. 则 C 中序列 C^{i_1} 与 C^{i_2} 的周期相关函数可表示为

收稿日期: 2004-12-12; 修回日期: 2005-04-19

基金项目: 国家自然科学基金 (No. 60373041, No. 90104034)

$$\begin{aligned}
R_{C^1 C^2}(\tau) &= \sum_{j=0}^{N_1 N_2 - 1} c_j^1 c_{j+\tau}^{2*} \bmod N_1 N_2 \\
&= \sum_{j=0}^{N_1 N_2 - 1} a((N_1/d) \cdot j + \lfloor j/d \rfloor) \bmod N_1 b_{i_1, j \bmod N_2}^* \\
&\quad \cdot a((N_1/d) \cdot (j + \tau) + \lfloor (j + \tau)/d \rfloor) \bmod N_1 b_{i_2, (j + \tau) \bmod N_2}^* \\
&= \sum_{k=0}^{N_1 - 1} \sum_{r=0}^{N_2 - 1} b_{i_1, (kN_2 + r) \bmod N_2}^* b_{i_2, (kN_2 + r + \tau_0 d + \tau_1) \bmod N_2}^* \\
&\quad \cdot a((N_1/d) \cdot (kN_2 + r) + \lfloor (kN_2 + r)/d \rfloor) \bmod N_1 \\
&\quad \cdot a((N_1/d) \cdot (kN_2 + r + \tau_0 d + \tau_1) + \lfloor (kN_2 + r + \tau_0 d + \tau_1)/d \rfloor) \bmod N_1 \\
&= \sum_{r=0}^{N_2 - 1} b_{i_1, r}^* b_{i_2, (r + \tau_0 d + \tau_1) \bmod N_2}^* \\
&\quad \cdot \sum_{k=0}^{N_1 - 1} a((N_1/d) \cdot r + kN_2/d + \lfloor r/d \rfloor) \bmod N_1 \\
&\quad \cdot a((N_1/d) \cdot (r + \tau_1) + kN_2/d + \tau_0 + \lfloor r + \tau_1 \rfloor/d) \bmod N_1
\end{aligned}$$

其中 $j = kN_2 + r$, $\tau = \tau_0 d + \tau_1$, $0 \leq k \leq N_1 - 1$, $0 \leq r \leq N_2 - 1$, $0 \leq \tau_1 \leq d - 1$. 记

$$\begin{aligned}
T_{k, r} &= ((N_1/d) \cdot r + k \cdot (N_2/d) + \lfloor r/d \rfloor) \bmod N_1, \text{ 则 } T_{k, r} + \tau - \\
&T_{k, r} \text{ 与 } k \text{ 无关, 所以我们可记} \\
t_r, \tau &= T_{k, r} + \tau - T_{k, r} \\
&= ((N_1/d) \cdot \tau_1 + \tau_0 + \lfloor (r + \tau_1)/d \rfloor - \lfloor r/d \rfloor) \bmod N_1
\end{aligned} \quad (1)$$

显然, 若 N_2/d 与 N_1 互素, 则

$$\{T_{k, r} | k = 0, 1, \dots, N_1 - 1\} = \{0, 1, \dots, N_1 - 1\},$$

此时 C^{i_1}, C^{i_2} 的周期相关函数可简化为

$$R_{C^{i_1} C^{i_2}}(\tau) = \sum_{r=0}^{N_2 - 1} b_{i_1, r}^* b_{i_2, (r + \tau_0 d + \tau_1) \bmod N_2}^* R_{a, a}(t_r, \tau) \quad (2)$$

根据上述分析可得以下定理:

定理 1 设 $a = (a_0, a_1, \dots, a_{N_1 - 1})$ 是一个完备序列, $B = \frac{1}{\sqrt{N_2}}(b_{ij})_{N_2 \times N_2}$ 为 N_2 阶酉矩阵, $d = (N_1, N_2)$. 如果 N_2/d 与 N_1 互素, 那么

(1) 当 $d = 1$ 时, C 是一个 $ZCZ - (N_1 N_2, N_2, N_1 - 1)$ 零相关区序列集.

(2) 当 $d > 1$ 时, C 是一个 $ZCZ - (N_1 N_2, N_2, N_1 - 2)$ 零相关区序列集.

证明 (1) 因为 $\tau = \tau_0 d + \tau_1$, $0 \leq \tau_1 \leq d - 1$, 所以当 $d = 1$ 时, $\tau_1 = 0$, $t_r, \tau = \tau$. 则由式(2)可得 $R_{C^{i_1} C^{i_2}}(\tau) = \sum_{r=0}^{N_2 - 1} b_{i_1, r}^* b_{i_2, (r + \tau_0 d + \tau_1) \bmod N_2}^* R_{a, a}(\tau)$. 又因为 a 是完备序列, 所以当 $0 < |\tau| \leq N_1 - 1$ 时, $R_{a, a}(\tau) = 0$, $R_{C^{i_1} C^{i_2}}(\tau) = 0$. 当 $i_1 \neq i_2$ 时, $R_{C^{i_1} C^{i_2}}(0) = R_{a, a}(0) \cdot \sum_{r=0}^{N_2 - 1} b_{i_1, r}^* b_{i_2, r}^* \bmod N_2$, 由 B 是酉矩阵可得 $\sum_{r=0}^{N_2 - 1} b_{i_1, r}^* b_{i_2, r}^* \bmod N_2 = 0$, $R_{C^{i_1} C^{i_2}}(0) = 0$. 因此定理中的(1)成立.

(2) 当 $d > 1$ 时, 若 $\tau_0 \leq N_1/d - 2$, 因为 $0 \leq \tau_1 \leq d - 1$, 则 $((N_1/d) \cdot \tau_1 + \tau_0 + (\lfloor (r + \tau_1)/d \rfloor - \lfloor r/d \rfloor) \leq (N_1/d) \cdot (d - 1) + N_1/d - 2 + 1 = N_1 - 1$

若 $\tau_0 = N_1/d - 1$, $\tau_1 \leq d - 2$, 则

$$((N_1/d) \cdot \tau_1 + \tau_0 + (\lfloor (r + \tau_1)/d \rfloor - \lfloor r/d \rfloor) \leq (N_1/d) \cdot (d - 2) + N_1/d - 1 + 1 = N_1 - N_1/d \leq N_1 - 1$$

因此当 $1 \leq \tau \leq N_1 - 2$ 时, 由式(1)有 $1 \leq t_r, \tau \leq N_1 - 1$, 于是根据式(2)和 a 是完备序列就可得到 $R_{C^{i_1} C^{i_2}}(\tau) = 0$. 同样当 $i_1 \neq i_2$ 时, 由 B 是酉矩阵可知 $R_{C^{i_1} C^{i_2}}(0) = R_{a, a}(0) \cdot$

$$\sum_{r=0}^{N_2 - 1} b_{i_1, r}^* b_{i_2, r}^* \bmod N_2 = 0.$$

容易验证 $R_{C^{i_1} C^{i_2}}(-\tau) = R_{C^{i_1} C^{i_2}}(\tau)^*$, 所以当 $-(N_1 - 2) \leq \tau \leq -1$ 时, 也有 $R_{C^{i_1} C^{i_2}}(\tau) = 0$.

综上所述, 当 $d > 1$ 时, C 是一个 $ZCZ - (N_1 N_2, N_2, N_1 - 2)$ 零相关区序列集.

证毕.

由定理 1, 根据所需的集合容量选择适当阶数的酉矩阵, 可以构造出满足要求的序列集. 下面研究如何扩大已知序列集的零相关区长度.

2.2 零相关区长度的扩大

Torii 在文献[7]中给出了一种由完备序列构造具有较大零相关区长度的方法, 下面将该方法一般化到由一个已知零相关区序列集构造新的具有较大零相关区长度的序列集.

设 $B' = \frac{1}{\sqrt{N_2'}}(b'_{ij})_{N_2' \times N_2'}$ 是 N_2' 阶方阵, $C = \{C^0, C^1, \dots, C^{N_2' - 1}\}$ 是一个 $ZCZ - (N_1', N_2', Z_{C'})$ 零相关区序列集, 序列 $C^i = (c_0^i, c_1^i, \dots, c_{N_2' - 1}^i)$, $0 \leq i \leq N_2' - 1$.

构造序列集 $C' = \{C'^0, C'^1, \dots, C'^{N_2' - 1}\}$, 其中

$$C'^i = (c_0^i, c_1^i, \dots, c_{N_2' - 1}^i), c_j^i = c_{j/N_2'}^{\bmod N_2'} b'_{i, j \bmod N_2'}$$

$$0 \leq i \leq N_2' - 1, 0 \leq j \leq N_1' N_2' - 1.$$

可以得到以下定理:

定理 2 如果是酉矩阵, 那么序列集 C' 是一个 $ZCZ - (N_1' N_2', N_2', Z_{C'} N_2')$ 零相关区序列集.

证明 任取 C' 中序列 C'^{i_1} 和 C'^{i_2} , 则它们的相关函数

$$\begin{aligned}
R_{C'^{i_1} C'^{i_2}}(\tau) &= \sum_{j=0}^{N_1' N_2' - 1} c_j^{i_1} c_{j+\tau}^{i_2*} \bmod N_1' N_2' \\
&= \sum_{j=0}^{N_1' N_2' - 1} c_{j/N_2'}^{\bmod N_2'} b'_{i_1, j \bmod N_2'} c_{(j+\tau)/N_2'}^{\bmod N_2'} b'_{i_2, (j+\tau) \bmod N_2'}^* \\
&= \sum_{k=0}^{N_1' - 1} \sum_{r=0}^{N_2' - 1} c_k^{\tau, (r + \tau) \bmod N_2'} c_{k + \lfloor (r + \tau)/N_2' \rfloor}^{\tau, (r + \tau) \bmod N_2'} b'_{i_1, r}^* b'_{i_2, (r + \tau) \bmod N_2'}^* \\
&= \sum_{r=0}^{N_2' - 1} b'_{i_1, r}^* b'_{i_2, (r + \tau) \bmod N_2'}^* \sum_{k=0}^{N_1' - 1} c_k^{\tau, (r + \tau) \bmod N_2'} c_{k + \lfloor (r + \tau)/N_2' \rfloor}^{\tau, (r + \tau) \bmod N_2'} \\
&= \sum_{r=0}^{N_2' - 1} b'_{i_1, r}^* b'_{i_2, (r + \tau) \bmod N_2'}^* R_{C', C'}^{\tau, (r + \tau) \bmod N_2'}(\lfloor (r + \tau)/N_2' \rfloor)
\end{aligned}$$

其中

$$j = kN_2' + r, 0 \leq k \leq N_1' - 1, 0 \leq r \leq N_2' - 1.$$

当 $0 < \tau \leq Z_{C'} N_2'$ 时, $0 \leq \lfloor (r + \tau)/N_2' \rfloor \leq Z_{C'}$, $r \neq (r + \tau) \bmod N_2'$, 因为 C 是 $ZCZ - (N_1', N_2', Z_{C'})$ 零相关区序列集, 所

- [2] P Z Fan, N Suehiro, N Kuroyanagi, X M Deng. A class of binary sequences with zero correlation zone[J]. IEE Electron. Lett, May 1999, 35: 777- 779.
- [3] X M Deng, P Z Fan. Spreading sequence sets with zero correlation zone [J]. IEE Electron. Lett, 2000, 36(12): 982- 983.
- [4] P Z Fan, L Hao. Generalized orthogonal sequences and their applications in synchronous CDMA systems[J]. IEICE Trans. Fundamentals, 2000, E83 A: 2054- 2069.
- [5] Shaojun Xu, Daoben Li. Ternary complementary orthogonal sequences with zero correlation window[A]. The 14th IEEE 2003 International Symposium on Personal, Indoor and Mobile Radio Communication Proceedings[C]. Beijing: Publish House of Electronics Industry, IEEE Press, 2003. 1669- 1672.
- [6] S Matsufuji, N Suehiro, N Kuroyanagi, P Z Fan. Two types of polyphase sequence sets for approximately synchronized CDMA systems[J]. IEICE Trans. Fundamentals, Jan. 2003, E86-A(1): 229- 234.
- [7] H Torii, Makoto Nakamura, Naoki Suehiro. A new class of zero correlation zone sequences[J]. IEEE Tran. Inform. Theory, Mar. 2004, 50: 559- 565.
- [8] L R Welch. Lower bounds on the maximum cross correlation of signals [J]. IEEE Trans. Inform. Theory, 1974, IF 20: 397- 399.
- [9] 徐绍君, 李道本. 关于零相关窗互补码理论界的几点讨论[J]. 通信学报, 2004, 25(3): 41- 49.
- [10] X H Tang, P Z Fan, S Matsufuji. Lower bounds on the maximum correlation of sequence set with low or zero correlation zone[J]. IEE Electron. Lett, Mar 2000, 36: 551- 552.

作者简介:



江文峰 男, 1980 年 9 月出生于湖北省黄冈市, 湖北大学数学与计算机科学学院硕士研究生, 主要研究方向为序列设计. E-mail: jiangwf92@sina.com.



曾祥勇 男, 1973 年 11 月出生于湖北省仙桃市, 湖北大学数学与计算机科学学院, 博士, 副教授, 主要研究方向为密码和序列设计.

胡磊 男, 1967 年 3 月出生于湖北省麻城市, 信息安全国家重点实验室(中国科学院研究生院), 教授, 博士生导师, 主要研究方向为序列设计、椭圆曲线公钥密码、理论密码学和密码学在 P2P 网络等新型网络安全中的应用.

刘合国 男, 1967 年 2 月出生于湖北省大冶市, 湖北大学数学与计算机科学学院, 教授, 博士生导师, 主要研究方向为代数学和格基密码.