一类相互正交的零相关区序列集的构造

曾祥勇[①②] 程 池[①] 胡 磊[②] 刘合国[①②]
[①](湖北大学数学与计算机科学学院 武汉 430062)
[②](信息安全国家重点实验室 中国科学院研究生院 北京 100049)

摘 要 该文基于完备序列和正交序列集，构造出一类相互正交的零相关区序列集。与 Rathinakumar 和 Chaturvedi 的构造相比，该文提出的方法能生成更多相互正交的零相关区序列集。

关键词 扩频序列，准同步 CDMA 系统，相互正交序列集，零相关区序列
中图分类号：TN914.53 **文献标识码**：A **文章编号**：1009-5896(2006)12-2347-04

Construction of Mutually Orthogonal Sets of Zero Correlation Zone Sequences

Zeng Xiang-yong[①②] Cheng Chi[①] Hu Lei[②] Liu He-guo[①②]
[①](*School of Mathematics & Computer Science, Hubei University, Wuhan* 430062, *China*)
[②](*The State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijin*g 100049, *China*)

Abstract Based on perfect sequences and orthogonal sequence sets, a new class of mutually orthogonal sets of zero correlation zone sequences is presented. Different from the construction given by Rathinakumar and Chaturvedi, the proposed method can generate more mutually orthogonal sets of zero correlation zone sequences.

Key words Spreading sequences, Quasi-synchronous CDMA system, Mutually orthogonal sequence sets, Zero correlation zone sequences

1 引言

近年来，准同步(Quasi-Synchronous, QS)CDMA 系统引起了人们的广泛关注，这是因为在这些系统中的一个或多个码片上不存在共信道干扰[1]。为实现这一优势，人们使用零相关区(Zero Correlation Zone, ZCZ)序列作为扩频序列。Fan 等利用正交非周期互补序列集成功地构造出二相、四相和多相的零相关区序列集，并且序列的相数不会随着周期或序列数目的增大而增加[2-4]。Tang 等人由 Welch 界[5]导出了零相关区序列集的理论界[6]。利用完备序列和 Walsh 序列，Matsufuji 等人构造出了满足理论界的多相零相关区序列，但序列的相数受到了限制[7]。Torii 等构造出了与理论界较为接近的二相和多相零相关区序列集，其中序列的相数没有受到限制，也不会因为周期或序列数目的增大而增加[8]。江文峰等放宽了 Matsufuji 和 Torii 等的构造中的限制条件，得到了一类新的零相关区序列集[9]。此外，徐绍君和李道本构造出了一类接近理论界的零相关窗互补码[10,11]。文献[3]中分析和模拟试验的结果表明，零相关区序列的确比传统的正交序列更适用于多径传输信道。但是随着零相关区长度的增加，能够使用的序列数目减少。最近，Rathinakumar 和 Chaturvedi 引入了相互正交零相关区序列集的概念并指出，对给定的零相关区，构造两个相互正交的零相关区序列集是可能的[12]；通过推广文献[2]中的构造，他们得到了一类相互正交的二相零相关区序列集。

引入相互正交的零相关区序列集概念的目的是为了提供更多能在准同步 CDMA 系统中使用的序列，但文献[12]中的构造方法只能生成两个相互正交的二相零相关区序列集。一个很自然的问题是：能否构造更多相互正交的二相或多相序列集。本文基于完备序列和正交序列集，提出了一个构造更多相互正交的二相或多相零相关区序列集的方法。文中提出的方法是文献[8]中构造方法的推广，但是我们的方法能够生成更多的零相关区序列集，而且任意两个不同集合的序列是相互正交的。文献[12]中构造的序列集合是二相的，而用我们的方法能生成二相或多相序列集合，并且所构造的相互正交的序列集的数目能够大于 2。

2 相互正交零相关区序列集的构造

首先回顾一些基本概念：

定义 1 设 $S=\{s_i\}_{i=0}^{M-1}$ 为 M 个周期是 L 的序列组成的集合，其中 $s_i=(s_{i,0},s_{i,1},\cdots,s_{i,L-1})$ $(0\le i<M)$，$s_{i,k}$ $(0\le k<L)$ 为复数。S 被称作一个 ZCZ $-(L,M,\mathrm{Zcz})$ 集，如果对任意的 $0\le i,j<M$ 满足

$$R_{s_i,s_j}(\tau)=\sum_{k=0}^{L-1}s_{i,k}s_{j,(k+\tau)\bmod L}^{*}=\begin{cases}\sum_{k=0}^{L-1}|s_{i,k}|^2, & i=j,\quad \tau=0\\ 0, & i\ne j,\quad \tau=0\\ 0, & 1\le|\tau|\le \mathrm{Zcz}\end{cases}$$

2005-05-12 收到, 2006-02-08 改回
国家自然科学基金项目(60373041, 60573053,10371032), 信息安全国家重点实验室和高校博士点基金项目(20050512002)资助课题

其中 $R_{s_i,s_j}(\tau)$ 表示 s_i 和 s_j 之间的周期互相关函数，符号*表示共轭运算，符号 $|s_{i,k}|$ 表示 $s_{i,k}$ 的绝对值。当 $\mathrm{Zcz}=0$ 时，S 被称作正交序列集。N 个不同的序列集 $S^0,S^1,\cdots,S^{N-1}$ 被称作是相互正交的，如果对任意的两个集合 S^{n_1},S^{n_2} 和任意的 $s_i^{n_1}\in S^{n_1}$，$s_j^{n_2}\in S^{n_2}$，$0\le i,j<M$，满足 $R_{s_i^{n_1},s_j^{n_2}}(0)=0$。

下面给出我们的构造方法：

设 $a=(a_0,a_1,\cdots,a_{m-1})$ 是周期为 m 的完备序列，即序列 a 的自相关函数具有如下性质：

$$R_a(\tau)=\sum_{i=0}^{m-1}a_i a^*_{(i+\tau)\bmod m}=\begin{cases}\sum_{i=0}^{m-1}|a_i|^2, & \tau=0\\ 0, & \text{其它}\end{cases}$$

设 $0\le k<n$，$e^k=(e_0^k,e_1^k,\cdots,e_{n-1}^k)$ 是整数序列，对 $0\le i<n$ 有 $e_i^k\in Z_m$。利用序列 a 和 e^k，我们构造序列集 $B^k=\{b_i^k\}_{i=0}^{m-1}$，其中

$$b_i^k=(b_{i,0}^k,b_{i,1}^k,\cdots,b_{i,n-1}^k),\quad b_{i,j}^k=a_{(e_j^k+i)\bmod m}$$

又设 $C=\{c_i\}_{i=0}^{n-1}$ 是一个正交序列集，$c_i=(c_{i,0},\ c_{i,1},\cdots,c_{i,n-1})$。我们可以构造 n 个序列集合 $S^k=\{s_j^k\}_{j=0}^{n-1}$，$s_j^k=(s_{j,0}^k,s_{j,1}^k,\cdots,s_{j,mn-1}^k)$，其中

$$s_{j,i}^k=b^k_{\left\lfloor\frac{i}{n}\right\rfloor,i\bmod n}c_{j,i\bmod n}\tag{1}$$

$0\le i<mn$，$\left\lfloor\dfrac{i}{n}\right\rfloor$ 表示不超过 $\dfrac{i}{n}$ 的最大整数。

这 n 个序列集中任意两条序列的相关值由下面引理给出：

引理 1 设序列 $s_i^{k_1}\in S^{k_1}$，$s_j^{k_2}\in S^{k_2}$ $(0\le i,j\le n-1)$，$l=l_2n+l_1$，以及 $\tau=\tau_2n+\tau_1$ 其中 $0\le l_1\le n-1$，$0\le l_2\le m-1$，则它们相关值为

$$R_{s_i^{k_1},s_j^{k_2}}(\tau)=\sum_{l_1=0}^{n-1}R_a\left(\left(e^{k_2}_{(l_1+\tau_1)\bmod n}+\tau_2+\left\lfloor\frac{l_1+\tau_1}{n}\right\rfloor-e^{k_1}_{l_1}\right)\bmod m\right)c_{i,l_1}(c_{j,(l_1+\tau_1)\bmod n})^*\tag{2}$$

证明 $R_{s_i^{k_1},s_j^{k_2}}(\tau)=\sum_{l=0}^{mn-1}s_{i,l}^{k_1}s_{j,(l+\tau)\bmod mn}^{k_2*}$

$$=\sum_{l=0}^{mn-1}b^{k_1}_{\left\lfloor\frac{l}{n}\right\rfloor,l\bmod n}c_{i,l\bmod n}\left(b^{k_2}_{\left\lfloor\frac{(l+\tau)\bmod mn}{n}\right\rfloor,(l+\tau)\bmod n}c_{j,(l+\tau)\bmod n}\right)^*$$

$$=\sum_{l=0}^{mn-1}b^{k_1}_{\left\lfloor\frac{l}{n}\right\rfloor,l\bmod n}\left(b^{k_2}_{\left\lfloor\frac{(l+\tau)\bmod mn}{n}\right\rfloor,(l+\tau)\bmod n}\right)^*c_{i,l\bmod n}\left(c_{j,(l+\tau)\bmod n}\right)^*$$

$$=\sum_{l_1=0}^{n-1}\sum_{l_2=0}^{m-1}b^{k_1}_{l_2,l_1}\left(b^{k_2}_{\left(l_2+\tau_2+\left\lfloor\frac{l_1+\tau_1}{n}\right\rfloor\right)\bmod m,(l_1+\tau_1)\bmod n}\right)^*\cdot c_{i,l_1}(c_{j,(l_1+\tau_1)\bmod n})^*$$

$$=\sum_{l_1=0}^{n-1}\left(\sum_{l_2=0}^{m-1}a_{(e^{k_1}_{l_1}+l_2)\bmod m}\left(a_{(e^{k_2}_{(l_1+\tau_1)\bmod n}+l_2+\tau_2+\left\lfloor\frac{l_1+\tau_1}{n}\right\rfloor)\bmod m}\right)^*\right)\cdot c_{i,l_1}(c_{j,(l_1+\tau_1)\bmod n})^*$$

$$=\sum_{l_1=0}^{n-1}R_a\left(\left(e^{k_2}_{(l_1+\tau_1)\bmod n}+\tau_2+\left\lfloor\frac{l_1+\tau_1}{n}\right\rfloor-e^{k_1}_{l_1}\right)\bmod m\right)\cdot c_{i,l_1}(c_{j,(l_1+\tau_1)\bmod n})^*$$

由式(2)可知，构造零相关区序列的关键在于找到满足适当条件的序列 e^k，为此定义：对任意的 $0\le j<n$，

$$e_j^k=\begin{cases}\left(\dfrac{jm}{n}+k\right)\bmod m, & j<n-k\\ \left(\dfrac{jm}{n}+k+1\right)\bmod m, & j\ge n-k\end{cases}\tag{3}$$

其中 $n\,|\,m$ 且 $e^k=(e_0^k,e_1^k,\cdots,e_{n-1}^k)$。

引理 2 对任意的 $0\le k<n$，设整数序列如式(3)。那么按照式(1)构造的每个序列集 S^k 都是 ZCZ $-(mn,n,m-2)$ 序列集。

证明 设序列 $s_i^k,s_j^k\in S^k$ $(0\le i,j\le n-1)$，由式(2)，它们的相关值为

$$R_{s_i^k,s_j^k}(\tau)=\sum_{l_1=0}^{n-1}R_a\left(\left(e^k_{(l_1+\tau_1)\bmod n}+\tau_2+\left\lfloor\frac{l_1+\tau_1}{n}\right\rfloor-e^k_{l_1}\right)\bmod m\right)\cdot c_{i,l_1}(c_{j,(l_1+\tau_1)\bmod n})^*$$

无论 $l_1+\tau_1<n$ 或者 $l_1+\tau_1\ge n$ 均有

$\left(e^k_{(l_1+\tau_1)\bmod n}+\tau_2+\left\lfloor\dfrac{l_1+\tau_1}{n}\right\rfloor-e^k_{l_1}\right)\bmod m=\dfrac{m}{n}\tau_1+\tau_2$ 或 $\dfrac{m}{n}\tau_1+\tau_2+1$。

若 $0\le\tau_1\le n-2,\tau_2=\dfrac{m}{n}-1$，则

$0\le\dfrac{m}{n}-1\le\dfrac{m}{n}\tau_1+\tau_2\le m-\dfrac{m}{n}-1$ 或者 $\dfrac{m}{n}\le\dfrac{m}{n}\tau_1+\tau_2+1\le m-\dfrac{m}{n}$。

若 $0\le\tau_1\le n-1$，$0\le\tau_2\le\dfrac{m}{n}-2$，则

$0\le\dfrac{m}{n}\tau_1+\tau_2\le m-2$ 或者 $1\le\dfrac{m}{n}\tau_1+\tau_2+1\le m-1$。

其中 $\dfrac{m}{n}\tau_1+\tau_2=0$ 当且仅当 $\tau_1=\tau_2=0$，此时若 $i\ne j$ 则 $\sum_{l_1=0}^{n-1}c_{i,l_1}(c_{j,l_1})^*=0$。而对其它情况总有

$$R_a\left(\left(e^k_{(l_1+\tau_1)\bmod n}+\tau_2+\left\lfloor\frac{l_1+\tau_1}{n}\right\rfloor-e^k_{l_1}\right)\cdot\bmod m\right)=0$$

故

$$R_{s_i^k,s_j^k}(\tau)=\begin{cases}\sum_{l=0}^{mn-1}|s_{i,l}^k|^2, & i=j,\tau=0\\ 0, & i\ne j,\tau=0\\ 0, & 1\le\tau\le m-2\end{cases}$$

而由 $R_{s_i^k,s_j^k}(-\tau)=R^*_{s_j^k,s_i^k}(\tau)$ 知 $R_{s_i^k,s_j^k}(\tau)=0$ 对 $-(m-2)\le\tau\le-1$ 也成立。这就证明了 S^k 是一个 ZCZ $-(mn,n,m-2)$ 序列集。

当 $k=0$ 和 $e^k=\left(0,\dfrac{m}{n},\dfrac{2m}{n}\bmod m,\cdots,\dfrac{(n-1)m}{n}\bmod m\right)$ 时，本文构造的序列集 S^0 就是 Torri 等人在文献[8]中构造出的 ZCZ $-(mn,n,m-2)$ 集。与 Torri 等的构造相比，本文的方法能够提供更多的零相关区序列集，并且任意两个不同集合中的序列是正交的。

引理 3　(1) 当 $m=n$ 时，式(1)中构造的序列集合 S^0, $S^1,\cdots,S^{n-2}$ 是相互正交的。

(2) 当 $m>n$ 时，式(1)中构造的序列集合 $S^0,S^1,\cdots,S^{n-1}$ 是相互正交的。

证明　设序列 $s_i^{k_1}\in S^{k_1}$ 以及 $s_j^{k_2}\in S^{k_2}$　$(0\le i,j\le n-1)$，由式(2)，它们在零点的相关值为

$$R_{s_i^{k_1},s_j^{k_2}}(0)=\sum_{l_1=0}^{n-1}R_a((e_{l_1}^{k_2}-e_{l_1}^{k_1})\bmod m)c_{i,l_1}(c_{j,l_1})^* \tag{4}$$

(1) 当 $m=n$ 时，对任意的 $0\le k_1\ne k_2\le n-2$，有

$$e_{l_1}^{k_2}-e_{l_1}^{k_1}=\begin{cases}k_2-k_1 & \text{或}\quad k_2-k_1+1-m & \text{若}\quad k_2>k_1\\ k_2-k_1 & \text{或}\quad k_2-k_1-1+m & \text{若}\quad k_2<k_1\end{cases}\text{成立。}$$

因此，　$1\le e_{l_1}^{k_2}-e_{l_1}^{k_1}\le m-1$ 和 $-m+1\le e_{l_1}^{k_2}-e_{l_1}^{k_1}\le -1$ 中必有一式成立，故当 $0\le l_1\le n-1$ 时有 $R_a((e_{l_1}^{k_2}-e_{l_1}^{k_1})\bmod m)=0$。由式(4)，有 $R_{s_i^{k_1},s_j^{k_2}}(0)=0$。因此集合 $S^0,S^1,\cdots,S^{n-2}$ 是相互正交的。

(2)当 $m>n$ 时，同上可知对任意的 $0\le k_1\ne k_2\le n-1$，$1\le e_{l_1}^{k_2}-e_{l_1}^{k_1}\le n<m$ 和 $-m<-n\le e_{l_1}^{k_2}-e_{l_1}^{k_1}\le -1$ 中必有一式成立，故当 $0\le l_1\le n-1$ 时有 $R_a((e_{l_1}^{k_2}-e_{l_1}^{k_1})\bmod m)=0$。由式(4)，有 $R_{s_i^{k_1},s_j^{k_2}}(0)=0$。因此集合 $S^0,S^1,\cdots,S^{n-1}$ 是相互正交的。

综合引理 2 和引理 3，有如下的定理：

定理 1　对任意的 $0\le k<n$，设整数序列如式(3)。那么式(1)中构造的每个序列集合 S^k 都是 ZCZ $-(mn,n,m-2)$ 集，而且(1) 当 $m=n$ 时，集合 $S^0,S^1,\cdots,S^{n-2}$ 是相互正交的。(2) 当 $m>n$ 时，集合 $S^0,S^1,\cdots,S^{n-1}$ 是相互正交的。

3　例子和结论

例 1　设 $+,-$ 分别表示 $1,-1$。基于完备序列 $a=(++-+)$，正交序列集合 $C=\{+++-,\ ++-+,\ +-++,\ -+++\}$ 以及 $e^0=(0,1,2,3)$，$e^1=(1,2,3,1)$，$e^2=(2,3,1,2)$，按照定理 1 (1)，我们可以构造如下的 3 个相互正交的 ZCZ $-(16,4,2)$ 集：

(1)　$S^0=(s_0^0,s_1^0,s_2^0,s_3^0)$

$s_0^0=(+\,+-\,-+-+\,-\,+-\,-+\,+-\,-+++)$

$s_1^0=(+++++-\,-+-+-+++-\,-)$

$s_2^0=(+-\,-++++++-\,-+++-+-)$

$s_3^0=(-+-+-\,-++++++-++-)$

(2)　$S^1=(s_0^1,s_1^1,s_2^1,s_3^1)$

$s_0^1=(+-+-\,-++++++-+-+-)$

$s_1^1=(+-\,-+-+-\,-++-+++++)$

$s_2^1=(+++\,+-\,-+-+-+++-+)$

$s_3^1=(-\,-++++++-\,-+++-+-+)$

(3)　$S^2=(s_0^2,s_1^2,s_2^2,s_3^2)$

$s_0^2=(-+++++-\,-+++-+-+-)$

$s_1^2=(-+-\,-++++++-++-\,-+)$

$s_2^2=(-\,-+-+-\,-++-++++++)$

$s_3^2=(+++-\,-+-+-+++-\,-++)$

文献[12]中所用的方法只能生成两个相互正交的二相 ZCZ $-(16,4,2)$ 集合，而本文的方法能生成 3 个相互正交的二相 ZCZ $-(16,4,2)$ 序列集。

例 2　设 $0,1,2,3$ 分别表示 $+1,\sqrt{-1},-1,-\sqrt{-1}$。基于完备序列 $a=(00120210)$，正交序列集 $C=(0000,0123,0202,0321)$ 以及 $e^0=(0,2,4,6)$，$e^1=(1,3,5,0)$，$e^2=(2,4,7,1)$，$e^3=(3,6,0,2)$，按照定理 1 (2)，可以构造如下的 4 个相互正交的 ZCZ $-(32,4,6)$ 集：

(1) $S^0=(s_0^0,s_1^0,s_2^0,s_3^0)$

$s_0^0=(01010220101022000101200210100022)$

$s_1^0=(02200303113323230220212111330101)$

$s_2^0=$ (03030022121220020303220012120220)

$s_3^0=$ (00220101133121210022232313310303)

(2) $S^1=(s_0^1,s_1^1,s_2^1,s_3^1)$

$s_0^1=$ (02201010220101022000101200210100)

$s_1^1=$ (03031133232002212123113101000223)

$s_2^1=$ (00221212200303002202121002230302)

$s_3^1=$ (01011331212200232321133303020021)

(3) $S^2=(s_0^2,s_1^2,s_2^2,s_3^2)$

$s_0^2=$ (10002201010220101022000101200210)

$s_1^2=$ (11232320022121331101012002030333)

$s_2^2=$ (12022003030022121220020303220012)

$s_3^2=$ (13212122002323311303032200010131)

(4) $S^3=(s_0^3,s_1^3,s_2^3,s_3^3)$

$s_0^3=$ (21010002201010220101022000101200)

$s_1^3=$ (22200121213311010220030301331323)

$s_2^3=$ (23030200221212200303002202121002)

$s_3^3=$ (20220323233113030022010103311121)

在例 2 中，每个集合中的 ZCZ 序列的数目为 4，按照 ZCZ $-(L,M,Zcz)$ 集合所满足的界 $M\le\dfrac{L}{\mathrm{Zcz}+1}=\dfrac{32}{6+1}$，达到了理论的最大数目。

结论　本文利用完备序列和正交序列集构造了一类新的相互正交的零相关区序列集。文献[8]中定理 1 的构造可以看作本文所给方法的一种特殊情况。本文所给的方法不仅能够生成二相和多相序列，而且生成的这些相互正交的序列集的数目能够大于 2。

参 考 文 献

[1] Suehiro N. A signal design without co-channel interference for approximately synchronized CDMA systems. *IEEE Journal on Selected Areas in Communications*, 1994, 12(5): 837−841.

[2] Fan P Z, Suehiro N, Kuroyanagi N, *et al*.. A class of binarysequences with zero correlation zone. *IEE Electronics Letters*, 1999, 35(10): 777−779.

[3] Fan P Z, Hao L. Generalized orthogonal sequences and their

applications in synchronous CDMA systems. *IEICE Transactions on Fundamentals*, 2000, E83-A(11): 2054−2069.

[4] Deng X M, Fan P Z. Spreading sequence sets with zero correlation zone. *IEE Electronics Letters*, 2000, 36(11): 993−994.

[5] Welch L R. Lower bounds on the maximum cross-correlation of signals. *IEEE Transactions on Information Theory*, 1974, 20(3): 397−399.

[6] Tang X H, Fan P Z, Matsufuji S. Lower bounds on the maximum correlation of sequence set with low or zero correlation zone. *IEE Electronics Letters*, 2000, 36(6): 551−552.

[7] Matsufuji S, Suehiro N, Kuroyanagi N, *et al*.. Two types of polyphase sequence sets for approximately synchronized CDMA systems. *IEICE Transactions on Fundamentals*, 2003, E86-A(1): 229−234.

[8] Torii H, Nakamura M, Suehiro N. A new class of zero-correlation zone sequences. *IEEE Transactions on Information Theory*, 2004, 50(3): 559−565.

[9] 江文峰, 曾祥勇, 胡磊等. 一类零相关区序列集构造方法的改进. 电子学报, 2005, 33(8): 1476−1479.

[10] Xu Shaojun, Li Daoben. Ternary complementary orthogonal sequences with zero correlation window. The 14th IEEE 2003 International Symposium on Personal, Indoor and Mobile Radio Communication Proceedings, Beijing, 2003: 1669−1672.

[11] 徐绍君, 李道本. 关于零相关窗互补码理论界的几点讨论. 通信学报, 2004, 25(3): 41−49.

[12] Rathinakumar A, Chaturvedi A K. Mutually orthogonal sets of ZCZ sequences. *IEE Electronics Letters*, 2004, 40(18): 1133−1134.

曾祥勇： 男，1973 年生，博士，副教授，研究方向为序列、编码与密码学.

程 池： 男，1981 年生，硕士生，研究方向为序列设计.

胡 磊： 男，1967年生， 教授，博士生导师，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 年生， 教授，博士生导师，研究方向为代数学和格基密码.