具有几乎最优自相关幅度二元序列的构造

张 璇*① 温巧燕② 秦 静③
①(山东财政学院统计与数理学院 济南 250014)
②(北京邮电大学网络与交换技术国家重点实验室 北京 100876)
③(山东大学数学院 济南 250100)

摘 要：该文提出具有几乎最优自相关幅度二元序列的 5 种构造方案。第 1 种构造是利用任意理想 2-值自相关序列来构造的，其余 4 种构造是基于某些序列及其修正版序列，且给出新序列周期自相关函数值的分布。利用 $2N\times2$ 交织序列构造的二元序列，其周期自相关函数值除了一个点外均达到最优。这将为 CDMA 通信系统及其他应用提供更多的选择。

关键词：二元序列；交织序列；几乎最优自相关幅度
中图分类号：TN918.1 **文献标识码**： A **文章编号**：1009-5896(2011)08-1908-05
DOI: 10.3724/SP.J.1146.2011.00158

Constructions of Binary Sequences with Almost Optimal Autocorrelation Magnitude

Zhang Xuan① Wen Qiao-yan② Qin Jing③
①(*School of Statistic and Mathematics*, *Shandong University of Finance*, *Jinan* 250014, *China*)
②(*State key laboratory of Networking and Switching Technology*,
Beijing University of Posts and Telecommunications, *Beijing* 100876, *China*)
③(*School of Mathematics*, *Shandong University*, *Jinan* 250100, *China*)

Abstract: In this paper, five constructions of binary sequences with almost optimal autocorrelation magnitude are proposed. The first construction is to use an arbitrary ideal 2-level autocorrelation sequence. The other four constructions are based on some sequences and their modified versions. $2N\times2$ interleaved sequences are used to get the sequences whose values of the autocorrelations are optimal except one points. And the distributions of the periodic autocorrelation functions of the resultant sequences are given. The results provide more choices for CDMA system and other applications.

Key words: Binary sequences; Interleaved sequences; Almost optimal autocorrelation magnitude

1 引言

在雷达测距、码分多址(CDMA)通信系统、全球定位系统、软件测试、雷达导航硬件检测和流密码加密系统的生成流密钥中，具有良好周期自相关性质的伪随机序列有许多的应用，尤其是具有良好自相关性质的二元或四元序列[1]。

若周期 N=0 (mod 4)的二元序列 a，其非平凡周期自相关值为 0 时称之为完备序列，但事实上，除了序列(0, 1, 1, 1)外，对于周期 N<548964900 的二元序列不存在完备的序列了[2]。对于非完备序列，若其非平凡周期自相关值在{0; −4}或{0; 4}中时，则称为最优自相关值二元序列[3]。2001 年 No 等人[4]给出周期是 $N=p^n-1$ 的最优自相关值二元序列的构造。若其非平凡周期自相关值在{0; 4; −4}之中时，则称为最优自相关幅度二元序列，这种序列与最优自相关值二元序列在实际应用中具有相同的最优性质[3]。Gong[5,6]首先提出一种构造序列重要方法——交织序列构造方法，该方法对理解已有序列的结构及对构造新序列都是很好的方法，也可为准同步码分多址构造所需的低(零)相关区序列集[6−8]。2008 年，文献[9]利用完备序列与交织技术构造出周期为 $N=4(2^{2k}-1)$且具有最优自相关幅度与其他良好性质的二元序列。2009 年，Jang 等人[10]利用 Gray 映射构造具有良好自相关值四元序列。2010 年，Chung 等人[11]给出偶周期且具有 3 周期自相关值的四元序列的构造方案；文献[3]利用 $N\times4$ 交织序列构造 3 类周期为 $4N$ 且具有最优自相关值/幅度的二元序

2011-02-28 收到，2011-05-18 改回
国家自然科学基金(60873191, 60903152, 60821001, 60873041)资助课题
*通信作者：张璇 zhxx100@163.com

列; 文献[12]利用采样序列也得到具有最优自相关值的二元序列。

具有良好自相关性质的二元序列在通信系统和密码学中有着广泛应用, 因而需要大量这样的序列。本文利用 $2N\times 2$ 交织序列构造出具有几乎最优自相关幅度的几类二元序列方案。第 1 种方案是基于任意理想 2-值自相关序列, 其余 4 种方案基于文献[3]提出的周期是 $N=2^{2k}-1$ 的扩展 GMW 序列及其修正版, 周期是 $p(p+2)$的孪生素数序列及其修正版, 以及两种类型的 Legendre 序列来构造。本文提出的方案具有以下优点: (1)第 1 种方案是基于任意 2-值自相关序列。这使得对预选序列有更多的选择, 且可得到更多的具有几乎最优自相关峰值序列。(2)新构造的序列非平凡周期自相关函数值除一点外都在{0; 4; −4}之中, 即为几乎最优自相关幅度二元序列。(3)给出这些具有良好自相关性质二元序列的周期自相关函数值具体分布。这些在 CDMA, 流密码加密系统等领域会有更多的应用。

2　预备知识

若序列每一分量值只是0或1(相应地 +1 或 −1), 则称之为二元序列, 记符号 $\hat{a}_n$ 代表由0或1表示的二元序列, 符号 a_n 代表由+1或者-1表示的二元序列, 显然有 $a_n=(-1)^{\hat{a}_n}$。给定两个周期为 N 的二元序列 $a=(a_0,\cdots,a_{n-1})$ 和 $b=(b_0,\cdots,b_{n-1})$, 则其周期互相关函数定义为 $R_{a,b}(\tau)=\sum_{t=0}^{n-1}a_t b_{t+\tau}$ 。相应地, 对于二元序列 $\hat{a}$ 和 $\hat{b}$, 其周期互相关函数定义为 $R_{\hat{a},\hat{b}}(\tau)=\sum_{t=0}^{n-1}(-1)^{\hat{a}_t+\hat{b}_{t+\tau}}$, 其中 $0\le\tau<N$ 。这两种定义等价, 且 $R_{a,b}(-\tau)=R_{b,a}(\tau)$。当 $a=b$ 时, $R_{b,a}(\tau)$ 简记为 $R_a(\tau)$, 称为序列 a 的周期自相关函数。

定义1　周期为 $N=0\ (\mathrm{mod}\,4)$ 的二元序列 a, 如果对移位 τ, $0<\tau<N$, 除一点外, 其余非平凡周期自相关函数值都在{0; 4; −4}中, 则称为具有几乎最优自相关幅度二元序列。

定义 2[1, 13]　周期为 N 的二元序列 a, 如果满足 $R_a(\tau)=-1,\ 0<\tau<N$, 则该序列称为(理想)2-值自相关序列。

例如, m-序列是2-值自相关序列。而任意周期是非素数的m-序列都可以用交织方法表示出来[1]。令 $\{\alpha_0,\cdots,\alpha_{M-1}\}$ 是 M 个 N 长复值序列集合, 其中 $\alpha_i=(a_{i,0},a_{i,1},\cdots,a_{i,N-1})$, 若定义 $N\times M$ 矩阵 $\boldsymbol{U}$ 的第 i 列为 $\alpha_i, 0\le i<M$, 即 $\boldsymbol{U}=[\alpha_0,\alpha_1,\cdots,\alpha_{M-1}]$, 串联矩阵 $\boldsymbol{U}$ 的每一行得一长 MN 的交织序列 u, 则 u 称为由 $\boldsymbol{U}$ 生成, 此即交织方法, 记作 $I(\alpha_0,\cdots,\alpha_{M-1})$ [1]。2010年, 文献[3]给出了扩展的GMW序列, 一型、二型Legendre序列, 孪生素数序列及其修正版序列的交织技术表示。

定义 3[1,13]　令 α 是素数 N 的本原根, 其中 N=1 (mod4), 则周期为 N 的 Legendre 序列(也称为二次剩余序列) $\hat{l}=(\hat{l}(0),\hat{l}(1),\cdots,\hat{l}(N-1))$ 定义为

$$\hat{l}(i)=\begin{cases}1\text{或者}0, & i=0\\ 1, & i\text{是}\bmod N\text{二次剩余}\\ 0, & i\text{是}\bmod N\text{二次非剩余}\end{cases}\qquad(1)$$

其中 $0\le i<N$。若 $\hat{l}(0)=1$, 则 $\hat{l}$ 称为一型 Legendre 序列, 否则称为二型 Legendre 序列。令 $\hat{l}$ 和 $\hat{l}'$ 分别代表一型和二型 Legendre 序列。

引理 1[3]　令 l 和 l' 分别是如上定义的一型和二型 Legendre 序列, 周期 N=1 (mod4), 对 $0\le\tau<N-1$, 则其周期自相关函数值分布如下:

$$R_{l,l}(\tau)=\begin{cases}N, & \tau=0\\ A(\tau), & \text{其他}\end{cases};\quad R_{l',l'}(\tau)=\begin{cases}N, & \tau=0\\ B(\tau), & \text{其他}\end{cases}\qquad(2)$$

其中

$$A(\tau)=\begin{cases}1, & \tau\text{是模}N\text{的二次剩余}\\ -3, & \tau\text{是模}N\text{的二次非剩余}\end{cases}$$

$$B(\tau)=\begin{cases}-3, & \tau\text{是模}N\text{的二次剩余}\\ 1, & \tau\text{是模}N\text{的二次非剩余}\end{cases}$$

引理 2[14]　令 $a=(a_0,\cdots,a_i,\cdots,a_{n_1-1})$ 和 $b=(b_0,\cdots,b_i,\cdots,b_{n_2-1})$ 分别为周期为 n_1 和 n_2 的序列, 其中 n_1 和 n_2 互素, 即 $\gcd(n_1,n_2)=1$。令 z 是长度为 $n=n_1n_2$ 的序列, 定义为 $z=(z_0,\cdots,z_i,\cdots,z_{n-1})$, 其中 $z_i=a_{i\bmod n_1}b_{i\bmod n_2},(0\le i\le n-1)$。则如此构造的两个长度为 n 的序列 z 和 z' 的周期相关函数满足: $R_{zz'}(\tau)=R_{aa'}(\tau\bmod n_1)R_{bb'}(\tau\bmod n_2)$。

引理 3[15]　周期是 $2n$ 的交织序列对 $I(a,b)$ 和 $I(a',b')$ 的周期相关函数满足: $R_{I(a,b),I(a',b')}(2\tau)=R_{a,a'}(\tau)+R_{b,b'}(\tau)$, 且 $R_{I(a,b),I(a',b')}(2\tau+1)=R_{a,b'}(\tau)+R_{b,a'}(\tau+1)$, 其中 $0\le\tau<2n$。

引理 4　对于整数 d, $0\le d<2N$。令 $0\le\tau_1<2N$, 则

(1) τ_1+d 和 τ_1-d+1 的奇偶性是不同的。

(2)若 N 是奇整数且 $d=(N+1)/2$, 则 $\tau_1-d+1=\tau_1+N-(N+1)/2+1=\tau_1+d\ (\mathrm{mod}\,N)$, 因而具有相同二次剩余性, 即, 若 $\tau_1-d+1\ (\mathrm{mod}\,N)$ 是二次剩余, 则 $\tau_1+d\ (\mathrm{mod}\,N)$ 也是; 反之亦然。

(3) 若 $N=2^{2k}-1$ 和 $d=(N+1)/2$, 则有 $\tau_1-d+1\ (\mathrm{mod}\,2^k+1)=\tau_1+N-(N+1)/2+1=\tau_1+d\ (\mathrm{mod}\,2^k+1)$。

3 具有几乎最优自相关幅度二元序列的构造

构造 1

令 $s=(s_0,s_1,\cdots,s_{N-1})$ 是周期为 N 的 2-值自相关二元序列，令 $v=(v_0,v_1)$，其中 $v=(1,-1)$ 或 $v=(-1,1)$。首先构造序列 $u=(u_t)_{t=0}^{2N-1}=(s_{t \bmod N}\cdot v_{t \bmod 2})_{t=0}^{2N-1}$，则定义新交织序列为 $a=I(u,L^d(u))$，其中 d 是任意整数。

定理 1 由构造 1 得到序列 a 的周期自相关函数值分布为：对 $0\le\tau<4N$，且 $d\ne(N+1)/2$，

$$R_a(\tau)=\begin{cases}0, & 2N-4\ 次\\ 4, & N-1\ 次\\ -4, & N-1\ 次\\ -4N, & 1\ 次\\ -2-2N, & 2\ 次\\ 2+2N, & 2\ 次\\ 4N, & 1\ 次\end{cases}\tag{3}$$

证明 记 $\tau=2\tau_1+\tau_2$，$(0\le\tau_1<2N$ 且 $\tau_2=1)$ 或者 $(0<\tau_1<2N$ 且 $\tau_2=0)$，故从两种情况讨论 s 的周期自相关函数。

第 1 种情况：当 $\tau_2=0$ 时，则由引理 2、引理 3 得 $R_a(\tau)=R_{u,u}(\tau_1)+R_{L^du,L^du}(\tau_1)=R_{s,s}(\tau_1 \bmod N)R_{v,v}\cdot(\tau_1 \bmod 2)+R_{s,s}(\tau_1 \bmod N)R_{v,v}(\tau_1 \bmod 2)$。

(1.1-1) $\tau_1=0\ (\bmod 2)$：则 $R_{v,v}(\tau_1 \bmod 2)=2$ 并且 $R_{s,s}(\tau_1 \bmod N)=-1$，故 $R_a(\tau)=-4$。即当 $\tau=0\ (\bmod 4)$ 时，$R_a(\tau)=-4$，共出现 $N-1$ 次。

(1.1-2) τ_1=1$(\bmod 2)$ 且 $\tau_1\ne N$：则 $R_{v,v}(\tau_1 \bmod 2)=-2$ 且 $R_{s,s}(\tau_1 \bmod N)=-1$，故 $R_a(\tau)=4$。即当 $\tau\ne0\ (\bmod 4)$ 且 $\tau=0\ (\bmod 2)$ 时，$R_a(\tau)=4$，共出现 $N-1$ 次。

(1.1-3) $\tau_1=N$：则 $R_{v,v}(\tau_1 \bmod 2)=-2$ 且 $R_{s,s}\cdot(\tau_1 \bmod N)=N$，故 $R_a(\tau)=-4N$。即当 $\tau=2N$ 时，$R_a(\tau)=-4N$，只发生 1 次。

第 2 种情况：当 $\tau_2=1$ 时，则由引理 2，引理 3 得

$$\begin{aligned}R_a(\tau)&=R_{u,L^du}(\tau_1)+R_{L^du,u}(\tau_1+1)\\&=R_{u,u}(\tau_1+d)+R_{u,u}(\tau_1-d+1)\\&=R_{s,s}(\tau_1+d \bmod N)R_{v,v}(\tau_1+d \bmod 2)\\&\quad+R_{s,s}(\tau_1-d+1 \bmod N)R_{v,v}(\tau_1-d+1 \bmod 2)\end{aligned}\tag{4}$$

(1.2-1) τ_1+d=0$(\bmod N)$ 或 τ_1-d+1=0$(\bmod N)$：当 $\tau_1+d=0\ (\bmod N)$ 时，$R_{s,s}(\tau_1+d \bmod N)=N$。当 $d\ne(N+1)/2$ 时，$R_{s,s}(\tau_1-d+1 \bmod N)=-1$，由引理 4，当 $\tau_1+d=1\ (\bmod 2)$ 时，$R_a(\tau)$=$-2-2N$；当 $\tau_1+d=0\ (\bmod 2)$ 时，$R_a(\tau)=2+2N$。同理可证另一种情况。即当 $\tau=2N-2d+1$ 或 $\tau=2d-1$ 时，$R_a(\tau)$=$-2-2N$；当 $\tau=4N-2d$+1 或 $\tau=2N+2d-1$ 时，$R_a(\tau)=2+2N$。

(1.2-2) 其他：当 $\tau_1+d\ne0(\bmod N)$ 且 $\tau_1-d+1\ne0(\bmod N)$ 时，$R_{s,s}(\tau_1+d \bmod N)=R_{s,s}(\tau_1-d+1 \bmod N)=-1$，故 $R_a(\tau)$=0。即当 $\tau\equiv3\ (\bmod 4)$ 或 $\tau\equiv1\ (\bmod 4)$，且 τ 不为 (1.2-1) 中的四值时，$R_a(\tau)=0$，共发生出现 $2N-4$ 次。 证毕

推论 1 令 $d=(N+1)/2$，由构造 1 得到序列 a 是周期为 $4N$ 且具有几乎最优自相关幅度的二元序列，即对 $0\le\tau<4N$，

$$R_a(\tau)=\begin{cases}0, & 2N\ 次\\ 4, & N-1\ 次\\ -4, & N-1\ 次\\ -4N, & 1\ 次\\ 4N, & 1\ 次\end{cases}\tag{5}$$

推论 1 的证明类似于定理 1，在(1.2-1)中，当 $d=(N+1)/2$ 时，由引理 4，得 $\tau_1+d=\tau_1-d+1=0\ (\bmod N)$，故 $R_{s,s}(\tau_1+d \bmod N)=R_{s,s}(\tau_1-d+1 \bmod N)=N$，又 τ_1+d 和 τ_1-d+1 的奇偶性是不同的，所以 $R_a(\tau)=0$。因而其非平凡周期自相关函数值只有一个点不在{0; 4; -4}之中，即为几乎最优自相关幅度二元序列。构造 1 基于任意 2-值自相关序列，故对预选序列有更多的选择，如可选择 m-序列、WG 变换序列等及其部分采样序列。

例 取周期为 7 的 m-序列 $s=(-1,-1,-1,1,1,-1,1)$, $v=(1,-1)$。按构造 1 首先构造序列 $u=(-1,1,-1,-1,1,1,1,1,-1,1,1,-1,-1,-1)$，令 $d=4$，定义新交织序列 $a=(-1,1,1,1,-1,1,-1,1,1,-1,1,1,1,1,1,-1,-1,-1,1,-1,1,-1,-1,1,-1,-1,-1,-1)$，计算其周期自相关值为 $R_a(\tau)=(28,0,4,0,-4,0,4,0,-4,0,4,0,-4,0,-28,0,-4,0,4,0,-4,0,4,0,-4,0,4,0)$，其中 $0\le\tau<28$，则 a 是几乎最优自相关幅度二元序列。

构造 2

令 l 和 l' 分别是一型和二型 Legendre 序列，其周期均为奇素数 N，且 N=1 (mod4)。首先构造两个新序列 $u=(u_c)_{c=0}^{2N-1}=(l_{c \bmod N}v_{c \bmod 2})_{c=0}^{2N-1}$，$u'=(u'_c)_{c=0}^{2N-1}=(l'_{c \bmod N}v_{c \bmod 2})_{c=0}^{2N-1}$，则定义新交织序列 $a=I(u,L^d(u'))$。

定理 2 由构造 2 得到序列 a 的周期自相关函数值分布为：对 $0\le\tau<4N$ 且 $d\ne(N+1)/2$，

$$R_a(\tau)=\begin{cases}0, & 2N-4\ 次\\ 4, & N-1\ 次\\ -4, & N-1\ 次\\ -4N, & 1\ 次\\ 2-2N, & 2\ 次\\ 2N-2, & 2\ 次\\ 4N, & 1\ 次\end{cases}\tag{6}$$

证明　记 $\tau=2\tau_1+\tau_2$，类似于定理 1 从两种情况讨论 s 的周期自相关函数值分布。

第 1 种情况：当 $\tau_2=0$ 时，则由引理 2，引理 3 得 $R_a(\tau)=R_{u,u}(\tau_1)+R_{L^du',L^du'}(\tau_1)=R_{l,l}(\tau_1 \bmod N)R_{v,v}(\tau_1 \bmod 2)+R_{l',l'}(\tau_1 \bmod N)R_{v,v}(\tau_1 \bmod 2)$。

(2.1-1) $\tau_1=0\ (\bmod 2)$：则 $R_{v,v}(\tau_1 \bmod 2)=2$。又当 τ_1 是 $\bmod N$ 的二次剩余时，$R_{l,l}(\tau_1 \bmod N)=1$ 且 $R_{l',l'}(\tau_1 \bmod N)=-3$，则 $R_a(\tau)=-4$。又当 τ_1 是 $\bmod N$ 的二次非剩余时，$R_{l,l}(\tau_1 \bmod N)=-3$ 且 $R_{l',l'}(\tau_1 \bmod N)=1$，则 $R_a(\tau)=-4$。即无论 $\tau_1 \bmod N$ 是否二次剩余，都有 $R_a(\tau)=-4$。这种情况发生 $N-1$ 次。即当 $\tau\equiv 0(\bmod 4)$ 时，$R_a(\tau)=-4$。

(2.1-2), (2.1-3)及第 2 种情况的证明类似于定理 1。　　证毕

推论 2　当 $d=(N+1)/2$ 时，由构造 2 得出序列 a 是周期是 $4N$ 且具有几乎最优自相关幅度二元序列，即对 $0\le\tau<4N$，

$$R_a(\tau)=\begin{cases}0, & 2N\ 次\\ 4, & N-1\ 次\\ -4, & N-1\ 次\\ -4N, & 1\ 次\\ 4N, & 1\ 次\end{cases}\tag{7}$$

由文献[3]中 III 提到的序列及其性质类似于以上构造方案可得以下 3 种构造方案，并得出新序列周期自相关函数值的具体分布。

构造 3

令 l 和 l' 分别是一型和二型 Legendre 序列，周期均为奇素数 N，且满足 N=3 (mod4)。首先构造两个新序列 $u=(u_c)_{c=0}^{2N-1}=(l_{c \bmod N}v_{c \bmod 2})_{c=0}^{2N-1}$，$u'=(u'_c)_{c=0}^{2N-1}=(l'_{c \bmod N}v_{c \bmod 2})_{c=0}^{2N-1}$，则定义新交织序列 $a=I(u,L^d(u'))$，其中 $d=(N+1)/2$。

定理 3　由构造 3 得到序列 a 是周期为 $4N$ 且具有几乎最优自相关幅度二元序列，其周期自相关函数值分布为：对 $0\le\tau<4N$，

$$R_a(\tau)=\begin{cases}0, & 2N\ 次\\ 4, & N-1\ 次\\ -4, & N-1\ 次\\ -4N, & 1\ 次\\ 4N, & 1\ 次\end{cases}\tag{8}$$

构造 4

s 是周期为 $N=2^{2k}-1$ 的扩展 GMW 二元序列，s' 是 s 的修正版序列。首先构造两个新序列 $u=(u_t)_{t=0}^{2N-1}=(s_{t \bmod N}v_{t \bmod 2})_{t=0}^{2N-1}$，$u'=(u'_t)_{t=0}^{2N-1}=(s'_{t \bmod N}\cdot v_{t \bmod 2})_{t=0}^{2N-1}$，则定义新交织序列 $a=I(u,L^d(u'))$，其中 $d=(N+1)/2$。

定理 4　由构造 4 得到序列 a 是周期为 $4N$ 且具有几乎最优自相关幅度二元序列，其周期自相关函数值分布如下：对 $0\le\tau<4N$，

$$R_a(\tau)=\begin{cases}0, & 2N\ 次\\ 4, & N-1+p\ 次\\ -4, & N-1-p\ 次\\ -4N, & 1\ 次\\ 4N, & 1\ 次\end{cases}\tag{9}$$

构造 5

令 N=$p(p$+2)，其中 p 和 p+2 均为素数。令 t 和 t' 分别是孪生素数序列及其修正版序列，其周期都是 N。首先构造两个新序列：$u=(u_c)_{c=0}^{2N-1}=(t_{c \bmod N}\cdot v_{c \bmod 2})_{c=0}^{2N-1}$，$u'=(u'_c)_{c=0}^{2N-1}=(t'_{c \bmod N}v_{c \bmod 2})_{c=0}^{2N-1}$，则定义新交织序列 $a=I(u,L^d(u'))$，其中 d=$(N+1)/2$。

定理 5　由构造 5 得到序列 a 是周期为 $4N$ 且具有几乎最优自相关幅度二元序列，其周期自相关函数值分布如下：对 $0\le\tau<4N$，

$$R_a(\tau)=\begin{cases}0, & 2N次\\ 4, & N-1+p次\\ -4, & N-1-p\ 次\\ -4N, & 1次\\ 4N, & 1\ 次\end{cases}\tag{10}$$

4　结论

本文提出 5 种构造几乎最优自相关幅度二元序列的方案，分别基于理想 2-值序列，一型、二型 Legendre 序列，扩展 GMW 序列及其修正版，孪生素数序列及其修正版构造的几类新二元序列，这些二元序列的周期自相关函数值分布良好，特别是当 $d=(N+1)/2$ 时，周期自相关函数幅度是几乎最优的，即除一个移位外，非平凡周期自相关函数值都

在{0; 4; −4}中。因而新序列将能为 CDMA 通信系统及流密码加密系统提供更多的应用选择。

参 考 文 献

[1] Golomb S W and Gong G. Signal Design for Good Correlation: Wireless Communication, Cryptography and Radar[M]. Cambridge, UK, Cambridge Univ. Press, 2005, Chapter 5.

[2] Mossinghoff M J. Wieferich pairs and Barker sequences[J]. *Designs, Codes and Cryptography*, 2009, 53(3): 149–163.

[3] Tang X H and Gong G. New constructions of binary sequences with optimal autocorrelation value/magnitude[J]. *IEEE Transactions on Information Theory*, 2010, 56(3): 1278–1286.

[4] No J S, Chung H, Song H Y, *et al*.. New construction for binary sequences of period p^m-1 with optimal autocorrelation using $(z+1)^d+az^d+b$[J]. *IEEE Transactions on Information Theory*, 2001, 47(4): 1638–1644.

[5] Gong G. Theory and applications of q-ary interleaved sequences[J]. *IEEE Transactions on Information Theory*, 1995, 41(2): 400–411.

[6] Gong G. New designs for signal sets with low cross correlation, balance property and large linear span: GF(p) case[J]. *IEEE Transactions on Information Theory*, 2002, 48(11): 2847–2867.

[7] Zhang X and Wen Q Y. New constructions of ZCZ sequence sets based on affine transformations[C].The 5th International Conference on Wireless Communications, Networking and Mobile Computing(WiCOM 2009), Beijing, China, Sept. 24-26, 2009: 1–4.

[8] Zhang X, Wen Q Y, and Zhang J. New general constructions of LCZ sequence sets based on interleaving technique and affine transformations[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2010, E93-A(5): 942–949.

[9] Yu N Y and Gong G. New binary sequences with optimal autocorrelation magnitude[J]. *IEEE Transactions on Information Theory*, 2008, 54(10): 4771–4779.

[10] Jang J W and Kim S H. Quaternary sequences with good autocorrelation constructed by Gray mapping[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2009, E92-A(8): 2139–2140.

[11] Chung J H, Han Y K, and Yang K. New quaternary sequences with even period and three-valued autocorrelation[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2010, E93-A(1): 309–315.

[12] Ke P H, Lin F C. New constructions of binary sequences with optimal autocorrelation value[J]. *Electronics Letters*, 2010, 46(20): 1381–1382.

[13] Fan P Z and Darnell M. Sequence Design for Communications Applications[M]. New York: Wiley, 1999: Part II, Chapter 4–6.

[14] Matsufuji S, Kuroyanagi N, Suehiro N, *et al*.. Two types of polyphase sequence sets for approximately synchronized CDMA systems[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2003, E86-A(1): 229–234.

[15] Hayashi T. A generalization of binary Zero-Correlation Zone (ZCZ) sequence sets constructed from Hadamard matrices[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2004, E87-A(1): 286–291.

张 璇： 女，1978 年生，讲师，博士，研究方向为序列设计、密码学.

温巧燕： 女，1959 年生，教授，博士生导师，研究方向为信息安全、密码学.

秦 静： 女，1960 年生，教授，硕士生导师，研究方向为密码学.