一种具有大线性复杂度伪随机序列的构造

刁哲军, 陈嘉兴, 刘志华
(河北师范大学, 河北石家庄 050031)

摘 要: 本文提出了一种具有大线性复杂度、低相关性能和序列数目多的新伪随机序列构造方案. 这种设计的关键之处在于利用移位序列分析法在理论上对相控序列进行改进, 使用交织序列做基础序列代替原来的理想自相关序列, 再利用具有理想自相关性的序列和相应的移位序列一起得到新伪随机序列. 本文对其相关性能进行了分析, 其最大值满足 Welch 界的要求; 新序列的线性复杂度比现有的任意序列都要大; 得到的新序列族中的序列有些是平衡的, 族的数目和每一族中序列的数目都要多于现有的任意序列.

关键词: 交织序列; 相控序列; 线性复杂度; 相关性
中图分类号: TN914 文献标识码: A 文章编号: 0372-2112 (2008) 10-1961-05

A New Design for Pseudorandom Sequences with Large Linear Span

DIAO Zhe-jun, CHEN Jia-xing, LIU Zhi-hua
(*Hebei Normal University, Shijiazhuang, Hebei 050031, China*)

Abstract: A new design method for families of sequences with large linear span, low cross correlation and large sequences number is presented. The key idea of the new design is to use the analytical method of shift sequences to improve phase-controlled sequences in theory and use interleaved sequences to be basic sequences instead of the original sequences with the two-level autocorrelation function to construct a set of long sequences with the desire properties. The correlation property has also been analyzed, and the maximal correlation value is optimal with respect to the Welch bound. The linear span, the number of families and the number of sequences in each family of the new sequence families are all larger than that of any other sequence families, and some new sequences are balanced.

Key words: interleaved sequences; phase-controlled sequences; linear span; correlation value

1 引言

伪随机序列在流密码、信道编码、扩频通信等领域有着广泛的应用. 它的好坏将直接影响整个通信系统性能的优劣, 所以如何构造出好的伪随机序列就成为人们研究的热点[1,2]. 判断一个周期序列的伪随机性可以用一些指标来衡量, 线性复杂度是序列伪随机性的重要度量指标之一, 在保密要求很高的军用通信中, 选用具有大线性复杂度的伪随机序列可以使系统在保密、抗干扰、抗截获等方面表现的更加出色. 因此, 构造具有大线性复杂度的伪随机序列也是当前一个研究焦点[3]. 1995 年 Gong 首先提出了交织序列和相控序列的雏形[4], 交织序列可通过生成理想自相关序列得到所需的移位序列, 再对另一个理想自相关序列依照移位序列来生成. 理想自相关序列指自相关函数值为 2 值的序列. 2002 年她又提出相控序列的进一步构造方法[5], 分别由基础序列 a, b 和移位序列 e 构成, 并且将基础序列扩展到所有理想自相关序列的范围. 相控序列具有周期长、相关性能好、线性复杂度大等优点. 其中线性复杂度可以说是当今所有相近长度伪随机序列中最大的. 正是由于相控序列具有这些优良的性质, 所以引起了部分学者的兴趣, 并对其进行了大量的研究[6,7]. 但是目前的研究仅是局限在基础序列属于理想自相关序列的范围, 基于以上情况, 我们提出将相控序列的基础序列 a 范围再扩大的思想, 将其范围扩大到所有的交织序列, 生成新的伪随机序列, 使得新序列的线性复杂度优于以前的序列, 从而可以更有针对性的应用到有相关要求的通信系统中.

2 新伪随机序列的构造

由于新伪随机序列是在相控序列的基础上进行构造的, 为了方便起见, 在文中统称为广义相控序列.

构造 **1** 构造周期是 $V^4(V$ 为自然数$)$的广义相控序列族. (对于 2 元情况, 所构造的广义相控序列的周

收稿日期: 2007-06-06; 修回日期: 2008-06-11
基金项目: 河北省科技厅基金(No. 07407234SD); 河北省教育厅基金(No. 2007472); 河北师范大学基金 (No. L2005B27, L2007Z10)

期为$(2^{2n}-1)^2$);

(1)选择 $\bar{a}=(\bar{a}_0, \bar{a}_1, \cdots, \bar{a}_{V-1})$ 为 $GF(p)$ 上的一个理想自相关序列. (对于 2 元情况, 设 $\bar{a}$ 的周期为 2^n-1);

(2)选择 $e^0=(e'_0, e'_1, \cdots, e'_{V-1})$ 为一个元素选自 Z_V (模 V 的一个整数冗余环)的一个整数序列, 且满足 $|\{e'_j-e'_{j+s}\,|\,0\leqslant j<V-s'\}|=V-s'$, 其中 $1\leqslant s'<V$. (设 e^0 的周期为 2^n+1, 相应的 V 处均为 2^n+1);

(3)基于理想自相关序列 $\bar{a}$ 和移位序列 e^0 构建一个 V 行 V 列(或 2^n-1 行 2^n+1 列的交织序列 $a=(a_0, a_1, \cdots, a_{V^2-1})$. a 的周期为 $2^{2n}-1$);

(4)选择 $b=(b_0, b_1, \cdots b_{V^2-1})$ 为 $GF(p)$ 上的一个理想自相关序列. (b 的周期为 $2^{2n}-1$);

(5)选择 $e=(e_0, e_1, \cdots, e_{V^2-1})$ 为选自 Z_{V^2} (V^2 模的一个整数冗余环)的一个整数序列, 且满足 $|\{e_j-e_{j+s}\,|\,0\leqslant j<V^2-s\}|=V^2-s$ 其中 $1\leqslant s<V^2$. (e 的周期为 $2^{2n}-1$, 相应的 V^2 处均为 $2^{2n}-1$);

(6)基于 a 和 e 构建一个 V^2 行 V^2 列(或 $(2^{2n}-1)$ 行 $(2^{2n}-1)$ 列)的扩展交织序列 $u=(u_0, u_1, \cdots u_{V^4-1})$, 其第 j 项列序列以 $L^{e_j}(a)$, $j=0, 1, \cdots, V^2-1$ 所给出. (u 的周期为 $(2^{2n}-1)^2$, 相应的 V^2 处均为 $2^{2n}-1$);

(7)设序列 $s_j=(s_{j,0}, s_{j,1}, \cdots, s_{j,V^4-1})$, 序列 s_j 的元素满足 $s_{j,i}=u_i+b_{j+i}$, 或等价的, $s_j=u+L^j(b)$, $0\leqslant i\leqslant V^4$ $(0\leqslant i<(2^{2n}-1)^2)$, $0\leqslant j<V^2$ $(0\leqslant j<2^{2n}-1)$;

(8)广义相控序列族 $S=s(a, b, e)$ 构造如下: $S=\{s_j: j=0, 1, \cdots, V^2-1\}$(或 $S=\{s_j: j=0, 1, \cdots, 2^{2n}-1\}$). 这里称 a 和 b 分别为 S 的前基础序列和后基础序列, e 为 S 的一个移位序列.

3 新伪随机序列的性能分析

3.1 序列的相关性能分析:

下面我们以周期是 V^4 的广义相控序列族为例进行相关性能的分析, 对于 2 元情况的分析是类似的, 在此不再赘述.

定理1 设 S 为周期是 V^4 的广义相控序列族, 如上文所构造, 则 s 中的广义相控序列之间的互相关值(或异相自相关值)为 16 值, 属于集合 $\{-2V^2+V+2, V^2-2V-4, V^2-2, V^2+2V, -V^3, 2V^2-3V-6, -V-2, -2V^2-V, V, -V^2, -2V^2+1, -1, 2V^2+3V, 2V^2-3, V^2, V^3+2V^2\}$, 且最大值 V^3+2V^2 满足 Welch 界的要求.

证明: 设广义相控序列 s_i 和 s_j 为 S 中的任意两个序列, 周期都为 V^4, 又设 A_i, A_j 分别为 s_i 和 s_j 对应的矩阵. 设 τ 为 s_i 的一个相位移位, $\tau=rV^2+s$; τ' 为序列 s_j 的一个相位移位, 且设 $\tau'=r'V^2+s'$. 设 r 和 s 各为一常量, 已知当 $e_j-e_{j+s}\equiv r \bmod V^2$, 其中 $0\leqslant j<V^2$ 时, 我们称 e_j 和 e_{j+s} 是相一致的. 另外设 $N'=|\{0\leqslant j<V^2|\, e_j-e_{j+s}\equiv r \bmod V^2\}|$ 由文献[5]知, 当 e 为与相控序列相伴的移位序列时, N' 的取值有三种情况, $N'\in\{0, 1, 2\}$. 分别写出 s_i, $s_{i+\tau}$ 和 $s_{j+\tau'}$ 的矩阵形式

$$A_i=\begin{bmatrix} a_{e_0}+b_i & a_{e_1}+b_{i+1} & \cdots & a_{e_{V^2-1}}+b_0 & \cdots & a_{e_{V^2-1}}+b_{i-1} \\ a_{e_0+1}+b_i & a_{e_1+1}+b_{i+1} & \cdots & a_{e_{V^2-1}+1}+b_0 & \cdots & a_{e_{V^2-1}+1}+b_{i-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{e_0+V^2-1}+b_i & a_{e_1+V^2-1}+b_{i+1} & \cdots & a_{e_{V^2-1}+V^2-1}+b_0 & \cdots & a_{e_{V^2-1}+V^2-1}+b_{i-1} \end{bmatrix} \tag{1}$$

$$A_{i+\tau}=\begin{bmatrix} a_{e_s+t}+b_{i+s} & \cdots & a_{e_{V^2-1}+t}+b_0 & \cdots & a_{e_{s-1}+t}+b_{i+s-1} \\ a_{e_s+t+1}+b_{i+s} & \cdots & a_{e_{V^2-1}+t+1}+b_0 & \cdots & a_{e_{s-1}+t+1}+b_{i+s-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{e_s+t-1}+b_{i+s} & \cdots & a_{e_{V^2-1}+t-1}+b_0 & \cdots & a_{e_{s-1}+t-1}+b_{i+s-1} \end{bmatrix} \tag{2}$$

$$A_{j+\tau'}=\begin{bmatrix} a_{e'_s+t'}+b_{j+s'} & \cdots & a_{e_{V^2-j}+t'}+b_0 & \cdots & a_{e'_{s-1}+t'}+b_{j+s'-1} \\ a_{e'_s+t'+1}+b_{j+s'} & \cdots & a_{e_{V^2-j}+t'+1}+b_0 & \cdots & a_{e'_{s-1}+t'+1}+b_{j+s'-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{e'_s+t'-1}+b_{j+s'} & \cdots & a_{e_{V^2-j}+t'-1}+b_0 & \cdots & a_{e'_{s-1}+t'-1}+b_{j+s'-1} \end{bmatrix} \tag{3}$$

当 $e_s+t=e'_s+t'$ 且 $i+s=j+s'$ 时, s_i 的异相自相关值与 s_i 和 s_j 的互相关值相同, 可见讨论两者是等价的. 则我们以讨论广义相控序列 s_i 的异相自相关函数值为例, 由式(1)和式(2)可得

$$C_{s_i, s_i}(\tau)=\sum_{j=0}^{V^2-1}(-1)^{b_{i+j}+b_{i+s+j}}\sum_{f=0}^{V^2-1}(-1)^{a_{e+f}+a_{e_{s+j}+t+f}} \tag{4}$$

其中的加法都模 V^2 计算而得, 设 $C_{s_i, s_i}(\tau)=C(\tau)$, $T_f^j=\sum_{f=0}^{V^2-1}(-1)^{a_{e+f}+a_{e_{s+j}+t+f}}$, 当 $s=0$ 时, 表示 $A_{i+\tau}$ 相对于 A_i 来说只有水平位移, 因为由相控序列的定义和移位序列的求法可知, $\{a_i\}$ 为相位不同的交织序列, 所以当 $s=0$ 时, $A_{i+\tau}$ 和 A_i 各自的移位序列相应位不会出现相一致的情

$$A_i=\begin{bmatrix} a_{e_0} & a_{e_0+1} & \cdots & a_{e_0+V-1} & a_{e_{V^2-1}} & a_{e_{V^2-1}+1} & \cdots & a_{e_{V^2-1}} \\ a_{e_0+V} & a_{e_0+V+1} & \cdots & a_{e_0+2V-1} & a_{e_{V^2-1}+V} & a_{e_{V^2-1}+V+1} & \cdots & a_{e_{V^2-1}+2V-1} \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ a_{e_0+V(V-1)} & a_{e_0+V(V-1)+1} & \cdots & a_{e_0+V^2-1} & a_{e_{V^2-1}+V(V-1)} & a_{e_{V^2-1}+V(V-1)+1} & \cdots & a_{e_{V^2-1}+V^2-1} \end{bmatrix}+\begin{bmatrix} b_i & \cdots & b_{i-1} \end{bmatrix} \tag{5}$$

$$A_{i+\tau}=\begin{bmatrix} a_{e_s+t} & a_{e_s+t+1} & \cdots & a_{e_s+t+V-1} & a_{e_{s-1}+t} & a_{e_{s-1}+t+1} & \cdots & a_{e_{s-1}+t+V-1} \\ a_{e_s+t+V} & a_{e_s+t+V+1} & \cdots & a_{e_s+t+2V-1} & a_{e_{s-1}+t+V} & a_{e_{s-1}+t+V+1} & \cdots & a_{e_{s-1}+t+2V-1} \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ a_{e_s+t+V(V-1)} & a_{e_s+t+V(V-1)+1} & \cdots & a_{e_s+t+V^2-1} & a_{e_{s-1}+t+V(V-1)} & a_{e_{s-1}+t+V(V-1)+1} & \cdots & a_{e_{s-1}+t+V^2-1} \end{bmatrix} + \begin{bmatrix} b_{i+s} & \cdots & b_{i+s-1} \end{bmatrix} \tag{6}$$

况, 因此当 $N'=1,2$ 时, 不必讨论 $s=0$ 的情况. 另外, 因为构造相控序列的前基础序列 $\{a_i\}$ 为交织序列, 所以我们将式(1)和式(2)的每一列都写为矩阵的形式, 具体列出第一列和最后一列如式(5)、(6)

这样每一个子矩阵都为同一个交织序列的移位序列, 我们用 $e=\{e_0, e_1, \cdots, e_{V^2-1}\}$ 来表示这种移位; 并且每一个子矩阵的列都为同一个短周期理想自相关序列的移位序列, 这种移位我们分别用移位序列 $e^i=\{e_0^i, e_1^i, \cdots, e_{V^2-1}^i\}(i=0,1,\cdots,V^2-1)$ 来表示, 由文献[5]知当 e 的第 i 位和第 j 位分别与其移位后对应位的移位序列值不一致的时候, e^i 和 e^j 的相应位相一致的个数是相同的, 设当大矩阵移 τ 位时, 相应的第 i 列对应的子矩阵移 $\bar{\tau}=\bar{r}V^2+\bar{s}$ 位, $N''=|\{0\leqslant j<V^2 \mid e'^i_j-e'^i_{j+s}\equiv \bar{r} \bmod V^2\}|$, 所以

(一)当 $N'=0$ 时,

(1)若 $N''=0$, $T_f^j=-V$,

$$C(\tau)=(-V)\sum_{j=0}^{V^2-1}(-1)^{b_{i+j}+b_{i+s+j}};$$

(a)若 $s=0$, $C(\tau)=(-V)(V^2)=-V^3$;

(b)若 $s\neq 0$, $C(\tau)=V$.

(2)若 $N''=1$, $T_f^j=1$, $C(\tau)=\sum_{j=0}^{V^2-1}(-1)^{b_{i+j}+b_{i+s+j}}$;

(a)若 $s=0$, $C(\tau)=V^2$; (b)若 $s\neq 0$, $C(\tau)=-1$.

(3)若 $N''=2$, $T_f^j=V+2$,

$$C(\tau)=(V+2)\sum_{j=0}^{V^2-1}(-1)^{b_{i+j}+b_{i+s+j}};$$

(a)若 $s=0$, $C(\tau)=V^3+2V^2$;

(b)若 $s\neq 0$, $C(\tau)=-V-2$.

(二)当 $N'=1$ 时,

(1)若 $N''=0$, T_f^j 中有一项取值为 V^2, 其余 (V^2-1) 项取值为 $-V$, 设 $(-1)^{b_k+b_{k+s}}$ 表示取值为 V^2 的那一项对应式(4)等号后前半部分的项, 令 $h=b_k+b_{k+s}$, 因此若 $s\neq 0$

(a)当 h 为偶数时, $C(\tau)(-1)^h\cdot V^2+V(-1)^h+(-V)\sum_{j=0}^{V^2-1}(-1)^{b_{i+j}+b_{i+s+j}}=V^2+2V$;

(b)当 h 为奇数时, $C(\tau)=-V^2-V+V=-V^2$.

(2)若 $N''=1$, T_f^j 中有一项取值为 V^2, 其余 (V^2-1) 项取值为 1, 设 $(-1)^h$ 表示取值为 V^2 的那一项对应式(4)等号后前半部分的项, 因此若 $s\neq 0$

(a)当 h 为偶数时, $C(\tau)=V^2-1-1=V^2-2$; (b)当 h 为奇数时, $C(\tau)=-V^2+1-1=-V^2$.

(3)若 $N''=2$, T_f^j 中有一项取值为 V^2, 其余 (V^2-1) 项取值为 $V+2$, 设 $(-1)^h$ 表示取值为 V^2 的那一项对应式(4)等号后前半部分的项, 因此若 $s\neq 0$

(a)当 h 为偶数时, $C(\tau)=V^2-2V-4$; (b)当 h 为奇数时, $C(\tau)=-V^2$.

(三)当 $N'=2$ 时,

(1)若 $N''=0$, T_f^j 中有两项取值为 V^2, 其余 (V^2-2) 项取值为 $-V$, 设 $(-1)^{b_k+b_{k+s}}$ 和 $(-1)^{b_l+b_{l+s}}$ 表示取值为 V^2 的那两项对应式(4)等号后前半部分的项, 因此, 若 $s\neq 0$

(a)当 b_k+b_{k+s} 和 b_l+b_{l+s} 都为偶数时, $C(\tau)=2V^2+3V$;

(b)当 b_k+b_{k+s} 和 b_l+b_{l+s} 分别为一个偶数和一个奇数时, $C(\tau)=V$;

(c)当 b_k+b_{k+s} 和 b_l+b_{l+s} 都为奇数时, $C(\tau)=-2V^2-V$.

(2)若 $N''=1$, T_f^j 中有两项取值为 V^2, 其余 (V^2-2) 项取值为 1, 设 $(-1)^{b_k+b_{k+s}}$ 和 $(-1)^{b_l+b_{l+s}}$ 表示取值为 V^2 的那两项对应式(4)等号后前半部分的项, 因此, 若 $s\neq 0$

(a)当 b_k+b_{k+s} 和 b_l+b_{l+s} 都为偶数时, $C(\tau)=V^2+V^2-1-1-1=2V^2-3$;

(b)当 b_k+b_{k+s} 和 b_l+b_{l+s} 分别为一个偶数和一个奇数时, $C(\tau)=-1$;

(c)当 b_k+b_{k+s} 和 b_l+b_{l+s} 都为奇数时, $C(\tau)=-2V^2+1$.

(3)若 $N''=2$, T_f^j 中有两项取值为 V^2, 其余 (V^2-2) 项取值为 $V+2$, 设 $(-1)^{b_k+b_{k+s}}$ 和 $(-1)^{b_l+b_{l+s}}$ 表示取值为 V^2 的那两项对应式(4)等号后前半部分的项, 因此, 若 $s\neq 0$

(a)当 b_k+b_{k+s} 和 b_l+b_{l+s} 都为偶数时, $C(\tau)=2V^2-3V-6$;

(b)当 b_k+b_{k+s} 和 b_l+b_{l+s} 分别为一个偶数和一个奇数时, $C(\tau)=-V-2$;

(c)当 b_k+b_{k+s} 和 b_l+b_{l+s} 都为奇数时, $C(\tau)=-2V^2+V+2$

由上面的分析可见, 对相控序列来说, 若其基础序

列 a 为交织序列, 基础序列 b 为理想自相关序列, 则互相关值(或者异相自相关值)为 16 值, 属于{$-2V^2+V+2$, V^2-2V-4, V^2-2, V^2+2V, $-V^3$, $2V^2-3V-6$, $-V-2$, $-2V^2-V$, V, $-V^2$, $-2V^2+1$, -1, $2V^2+3V$, $2V^2-3$, V^2, V^3+2V^2}, 互相关值(或者异相自相关值)的最大值为 V^3+2V^2, 满足

$$V^3+2V^2 \geqslant V^4\sqrt{\frac{V^2-1}{V^4V^2-1}}$$

即满足 Welch 界的要求, 且接近 Welch 界, 因为此理论限是伪随机序列构造和性能判断公认的应用最广泛的标准, 所以本文构造的广义相控序列的相关性是优良的.

3.2 序列的线性复杂度分析:

引理 **1** 设 u 为一个(V, V)交织序列, a 为 u 的基础序列, a 和 b 均为周期是 V 的理想自相关序列, 则如果基于 u 和 b 构造的相控序列满足文献[5]中定理 3 的条件, 那么当 V 为素数时

$$LS(u+b)=VLS(u)+LS(b) \tag{7}$$

当 $V=p^n-1$ 时

$$LS(u+b)>\frac{p^n-1}{2}LS(a)+LS(b) \tag{8}$$

定理 **2** 同周期的广义相控序列的线性复杂度要大于相控序列的线性复杂度.

证明: 由文献[5]可知同周期的交织序列中大部分序列的线性复杂度要远远大于理想自相关序列的线性复杂度, 广义相控序列改变了以往构造相控序列所用交织序列的基础序列为理想自相关序列的情况, 其基础序列变为交织序列, 而又由式(7)可见广义相控序列前半部分的线性复杂度要远远大于相控序列前半部分的线性复杂度, 因此同周期的广义相控序列的线性复杂度是大于相控序列的. 证明完毕.

定理 2 给出了广义相控序列线性复杂度的一个定性分析, 下面再以 2 元情况为例用定理 3 给出广义相控序列线性复杂度的定量分析, 以便和原来的相控序列进行比较.

定理 **3** 设 $s_j=u+L^j(b)$ 为一个 $2^{2n}-1$ 行 $2^{2n}-1$ 列的广义相控序列, 其中 u 为一个 $2^{2n}-1$ 行 $2^{2n}-1$ 列的扩展交织序列, 设 u 的基础序列为交织序列 a, $\bar{a}$ 为一个理想自相关序列, 为交织序列 a 的基础序列, b 为一个周期是 $2^{2n}-1$ 的理想自相关序列. s_j, u, b, a, $\bar{a}$ 均如上文中所构造. 则广义相控序列 s_j 的线性复杂度 $LS(s_j)$ 为

$$LS(s_j)=(2^{2n}-1)(2^n-1)LS(\bar{a})+LS(b) \tag{9}$$

其中 $LS(\bar{a})$和 $LS(b)$ 分别表示理想自相关序列 $\bar{a}$ 和 b 的线性复杂度.

证明: 由文献[5]可知, 当相控序列的定义为 $s_j=u+L^j(b)$, 设$f(x^m)$为生成 u 的多项式, $t(x)$为生成 b 的多项式, $m=2^{2n}-1$ 则有下式成立

$$LS(s_j)=\deg(f(x^m))+\deg(t(x)) \tag{10}$$

其中 $\deg(\cdot)$表示多项式的阶, 则有

$$\deg(f(x^m))=(2^{2n}-1)\deg(f(x^N)) \tag{11}$$

$f(x^N)$为生成交织序列 a 的多项式, $N=2^n-1$, 有下式成立

$$\deg(f(x^N))=(2^n-1)LS(\bar{a}) \tag{12}$$

而 $\deg(t(x))=LS(b)$, 所以

$$LS(s_j)=(2^{2n}-1)(2^n-1)LS(\bar{a})+LS(b) \tag{13}$$

证明完毕.

从上面两个定理可以看出, 新构造的广义相控序列其线性复杂度要远远大于现有相控序列的线性复杂度.

3.3 广义相控序列的族数和一族内个数:

因为构造广义相控序列的前基础序列为交织序列, 交织序列是范围很广的一类序列族, 包括大量常见的序列, 如 GMW 序列、Kasami 序列、No 序列等等, 而构造相控序列的前基础序列为理想自相关序列, 交织序列的移位不等价序列个数比相同长度的理想自相关序列大很多[4], 所以广义相控序列的族数要远远多于相控序列的族数.

由构造广义相控序列和计算相关值的过程可见, 当 $j\neq 0$ 时(j 为序列 b 向右循环移位的大小), j 共有 V^2(或 $2^{2n}-1$)个取值使一族内的广义相控序列移位不等价, 所以周期为 V^4(或$(2^{2n}-1)^2$)的一族广义相控序列中共有 V^2(或 $2^{2n}-1$)个移位不等价序列.

3.4 广义相控序列和相控序列的性能比较:

通过上文对广义相控序列的性能分析, 再结合文献[5]中对相控序列的性能分析, 我们得出以下结论:

(1)广义相控序列不一定是平衡的, 其平衡性需要依赖于前基础序列的类型, 而相控序列是平衡的;

(2)广义相控序列和相控序列一族内的序列都是移位不同的;

(3)广义相控序列互相关值要依赖于前后基础序列的类型, 最多时有 16 值, 最少时有 5 值, 而相控序列的相关值始终是 5 值的;

(4)同周期的广义相控序列的线性复杂度要远远大于相控序列;

(5)同周期的广义相控序列的族数要远远多于相控序列.

(6)同周期的广义相控序列和相控序列一族内的序列数目是相等的.

4　新伪随机序列实例分析

为了便于理解上面的结论, 我们举一实例进行说明.

实例　生成长为 16769025 的广义相控序列和相控序列, 并对它们的性能进行比较.

解: 根据移位序列的求法求出所需移位序列 $\{e_j\}$, $(j=0,1,\cdots,2^{12}-1)$ 和 $\{e'_j\}$, $(j=0,1,\cdots,2^6-1)$, 并且令广义相控序列的前基础序列为交织序列 $u_j=tr_2^{2^3}(\{tr_{2^3}^{2^6}(\{tr_{2^6}^{2^{12}}(\alpha^{2^j})+r_i\alpha^{k_j}\}^{k_2})\}^{k_1})$, 后基础序列为理想自相关序列 $b_i=tr_2^{2^{12}}(\beta^i)$. 域 $GF(2^{12})$ 的本原多项式为 $x^{12}+x^7+x^4+x^3+1=0$, α, β 为 $GF(2^{12})$ 上的本原元, 为简便使二者相同, 可以算出广义相控序列一族有 4095 个移位不等价的序列, 经验证这些序列的异相自相关和互相关值均为 9 值; 构造的广义相控序列的线性复杂度为 $4095\times63\times6+12=1547922$.

设相控序列的前基础序列为理想自相关序列 $a'_i=tr_2^{2^{12}}(\alpha^i)$, 后基础序列 b 不变, 可以算出相控序列一族有 4095 个移位不等价的序列, 经验证其异相自相关和互相关均为 5 值; 构造的相控序列的线性复杂度为 $4095\times12+12=49152$.

由此可见改进后广义相控序列线性复杂度是改进前的 30 倍左右, 线性复杂度上升很快, 但是序列相关性能却有所下降.

5　结论

通过以上结论和实例分析我们可以看出广义相控序列在线性复杂度和族数特性上是优于其它序列的, 而我们前面提到相近周期长度的伪随机序列中相控序列已经被证明其线性复杂度是最大的[5], 所以说我们构造的新伪随机序列——广义相控序列在所有相近周期长度的伪随机序列中线性复杂度是最大的. 另外它在序列总数目、相关性能等特性方面也具有较理想表现, 因此它在军用抗干扰通信中具有很强的应用前景, 是一种比较理想的伪随机序列.

参考文献:

[1] A Klapper. Spectral method for cross correlations of geometric sequences[J]. IEEE Trans. Inform. Theory. 2004, 50(1): 229–232.

[2] B J Peiris, K R Narayanan, S L Miller. A spectral domain approach to design spreading sequences for CDMA systems in frequency selective fading channels[J]. IEEE Trans. Wire. Commun. 2006, 5(9): 2386–2395.

[3] C P Xing, P V Kumar, C S Ding. Low-correlation, large linear span sequences from function fields[J]. IEEE Trans. Inform. Theory. 2003, 49(6): 1439–1446.

[4] Gong Guang. Theory and applications of q-ary interleaved sequences[J]. IEEE Transaction Information Theory, 1995, 1(3): 400–411.

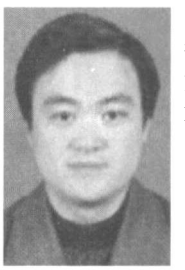
[5] Gong Guang. New designs for signal sets with low cross correlation, balance property and large linear span: GF(p) case[J]. IEEE Transaction Information Theory, 2002, 48(11): 2847–2867.

[6] 康凯, 郭伟, 吴诗其. 一类新的性能优异的伪随机序列—GMW 相控序列[J]. 电子学报, 2000, 28(11A): 73–75.

[7] 严春林, 周亮, 李少谦. 相控序列的改进—采用级连 GMW 序列构造相控序列[J]. 电子学报, 2003, 31(5): 797–800.

作者简介:

刁哲军　男, 1961 年出生于河北辛集, 教授, 1982 年获南京理工大学学士学位, 研究方向为信息处理、智能检测、扩展频谱通信.
E-mail: Diaozhj@hebtu.edu.cn.



陈嘉兴(责任作者)　男, 1977 年出生于安徽阜阳, 哈尔滨工业大学工学博士, 副教授, 研究方向为扩展频谱通信、移动通信、信道编码.
E-mail: xinghuo2815@163.com.

刘志华　女, 1977 年出生于河北沧州, 讲师, 2003 年获燕山大学计算机软件应用专业硕士学位, 研究方向为扩展频谱通信、网络安全.
E-mail: hebtuliuzhihua@163.com.