

一类新的性能优异的伪随机序列——GMW 相控序列

康 凯, 郭 伟, 吴诗其

(电子科技大学通信抗干扰国防重点实验室, 成都 610054)

摘 要: 基于交错方法构造出了一类新的伪随机序列, 称为 GMW 相控序列. 给出了 GMW 相控序列的生成算法, 证明了 GMW 相控序列均满足平衡性, 具有优良的相关特性和极大的线性复杂度, 可适用于 CDMA 扩频通信和保密通信系统中.

关键词: GMW 相控序列; 交错方法; 伪随机序列

中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2000) 11A-0073-03

A New Family of Pseudorandom Sequences with Good Properties ——GMW Phase Controlled Sequences

KANG Kai, GUO Wei, WU Shi-qi

(National Communication Lab., UESTC, Chengdu 610054, China)

Abstract: Based on the interleave method, a new class of binary pseudorandom sequences is constructed, which is called GMW Phase Controlled sequence (or GMW PC sequence). The generating algorithm is derived. It is verified that the GMW PC sequences have balance, optimal auto/cross correlation functions, and very large linear spans and can be used in the CDMA spread spectrum communication and cryptography.

Key words: GMW PC sequences; interleave method; pseudorandom sequences

1 引言

具有优良伪随机特性和较大线性复杂度的伪随机序列广泛应用于 CDMA 扩频通信和密码学中, 并对其通信系统传输性能和安全性都具有决定性的作用. 伪随机序列的设计已成为 CDMA 扩频通信和密码学中最关键的问题之一. 近年来所提出的交错方法作为一种有效的伪随机序列设计的新方法, 受到普遍的重视. 本文基于交错方法, 构造出了一类新的伪随机序列, 称为 GMW 相控序列. 证明了 GMW 相控序列具有优良的伪随机特性和极大的线性复杂度, 适用于 CDMA 扩频通信和保密通信系统中.

2 GMW 交错序列的基本概念

交错方法^[1]是一类基于有限域上迹函数^[2]的伪随机序列设计方法, 由此构造出的序列称为交错序列. 定义如下一类有用的交错序列, 称为 GMW 交错序列.

定义 1 设 α 是 $GF(q^n)$ 的本原元, $u_0 = \{tr_1^e[tr_0^n(\alpha^{-i})]^{r_1}\}$ 是 $GF(q)$ 上周期为 $q^n - 1$ 的 GMW 序列^[3], m 为非负整数, 对于 $GF(q)$ 上的序列 $u = \{u_k\} (k = im + j, i \geq 0, 0 \leq j < m)$, 若对每个 $u(j) = \{u_{im+j}\} (0 \leq j < m)$ 均与 u_0 平移等价, 则定义 u 为 GMW 交错序列, 称 u_0 为 u 的基准序列, $\{u(j)\}$ 为分量序列.

定义 $e(u) = \{e_0, e_1, \dots, e_{m-1}\}$ 为 u 的移位数列, 表征分量序列相对于基准序列 u_0 的不同相移:

$$e = \begin{cases} u(j) \text{ is zero-sequence} \\ e_j, u(j) = L^{e_j}(u_0), 0 \leq j < q^n - 1, \end{cases} \quad 0 \leq j < m \quad (1)$$

并定义 $e \pm = \pm =$, 有:

$$u_k = u_{im+j} = tr_1^e[tr_0^n(\alpha^{-i+e_j})]^{r_1}, i \geq 0, 0 \leq j < m \quad (2)$$

对于 GMW 交错序列, 定义如下两个集合 $S_0(s), S_1(s)$:

$$S_0(s) = \{e_j - e_{j+s} \bmod (q^n - 1) \mid 0 \leq j < m - s\} \quad (3)$$

$$S_1(s) = \{e_j - e_{j+s} \bmod (q^n - 1) \mid m - s \leq j < m\} \quad (4)$$

以 $G(u_0, m)$ 表示与 u_0 和 m 相关的 GMW 交错序列全体的集合.

3 GMW 相控序列的构造及其性质

定义 2 设 α 是 $GF(2^n)$ 的本原元, n 为非负整数, $m = 2^n - 1$, $u_0 = \{tr_1^e[tr_0^n(\alpha^{-i})]^{r_1}\}$ 是 $GF(2)$ 上周期为 m 的 GMW 序列, $u = G(u_0, m)$ 且 $e(u) = \{e_0, e_1, \dots, e_{m-1}\}$ 满足条件:

$$\begin{cases} e_j \\ |S_0(s)| = m - s, 0 \leq j < m \end{cases} \quad (5)$$

设 $b = \{tr_1^d[tr_0^n(\alpha^{-k})]^{r_2}\}$ 是周期为 m 的 GMW 序列, 为 $GF(2^n)$

的本原元. 称如下式定义的序列 $z = \{z_k\}$ 为 GMW 相控序列:

$$z_k = u_k + b_k \quad (6)$$

由 b 的 $2^n - 1$ 个循环移位, 可得到一族 $2^n - 1$ 个 GMW 相控序列. 满足条件式 (5) 的移位数列可以通过对用 m 序列构造的声纳数列^[4]做进一步截短^[1]来构造.

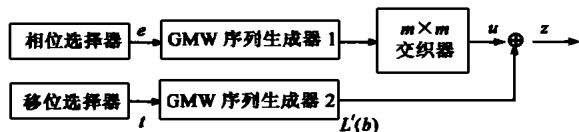


图 1 GMW 相控序列生成框图

GMW 相控序列生成如图 1 所示. 由相位选择器产生移位数列 $e = \{e_0, e_1, \dots, e_{m-1}\}$, 并作为 GMW 序列生成器 1 的初始相位. GMW 序列生成器 1 生成不同初相位下的 u_0 , 经过交织后输出, 即得到 GMW 交错序列 u . 在移位选择器的控制下, GMW 序列生成器 2 产生 GMW 序列 b 的平移等价类 $L^t(b)$ ($0 \leq t < m$). 取不同的移位 t , 即可得到同族的不同 GMW 相控序列. 变换不同的 GMW 序列 u_0 、 b 和移位数列 e , 均可得到不同的 GMW 相控序列族.

定理 1 按式 (6) 所定义的 GMW 相控序列 z 具有如下性质:

1. 序列周期: $\text{per}(z) = (2^n - 1)^2$;
2. 最大线性复杂度为 $mc \cdot 2^{H(r_1)} + d2^{H(r_2)}$, $H(r_1)$ 、 $H(r_2)$ 分别为 r_1 和 r_2 的汉明重量;
3. 码平衡性: GMW 相控序列均是码平衡的, 在一个周期内, 0 码元比 1 码元多一个;
4. 相关特性: 同相自相关函数为 $(2^n - 1)^2$, 异相自相关函数和同族序列间的互相关函数取自五值集合 $\{1, 1 \pm 2^n, 1 \pm 2^{n+1}\}$, 并以 $1 + 2^{n+1}$ 为界;
5. 序列数量: 同族 $2^n - 1$ 个 GMW 相控序列都是平移互异的.

证: (1) z 可以看作是 GMW 交错序列 u 和 GMW 序列 b 的模 2 和. u 的周期为 $(2^n - 1)^2$, 最小多项式为 $f(x^m)^{[1]}$, 设 b 的最小多项式为 $v(x)$, 则由 [5] 可知, z 的周期为:

$$\text{per}(z) = [\text{per}(u), \text{per}(b)] = (2^n - 1)^2 \quad (7)$$

设 z 的最小多项式为 $h(x)$, 由 [5] 可知, 当 $f(x^m)$ 与 $v(x)$ 互素时, 可得到 z 的最大线性复杂度:

$$h(x) = f(x^m) v(x) \quad (8)$$

$$LS(z) = \deg(h) = mc \cdot 2^{H(r_1)} + d2^{H(r_2)} \quad (9)$$

(2) GMW 相控序列 z 的一个周期内的分量序列 $\{z(j)\}$ ($0 \leq j < m$) 中包含有 $2^{n-1} - 1$ 个 GMW 序列和 2^{n-1} 个 GMW 序列的补序列. 因此可知 z 的一个周期内有 $2^{2n} - 2^n + 1$ 个 0 码元和 $2^{2n} - 2^n$ 个 1 码元, 即 z 满足码平衡性.

(3) 设 $z = u + b$, $w = u + L^t(b)$, $1 \leq t < m$, 讨论 z, w 的相关性:

$$\begin{aligned} z_k + w_k &= u_k + u_{k+l} + b_k + b_{k+l+t}, k = im + j, l = mm + s, 0 \leq j, s < m \\ &= tr_1^c [tr_c^n(i + e_j)] r_1 + tr_1^c [tr_c^n(i + r + e_{j+s})] r_1 + b_j + b_{j+s+t} \\ &= tr_1^c [tr_c^n(i + e_j)] r_1 + tr_1^c [tr_c^n(i + r + e_{j+s})] r_1 + d_j \end{aligned} \quad (10)$$

其中 $d_j = b_j + b_{j+s+t}$, 或 $d = b + L^{s+t}(b)$. $R_{z,w}(l)$ 可以分为如

下几种情况:

(3.1) $l \equiv 0 \pmod{m^2}$ 时, 有:

$$R_{z,w}(l) = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} (-1)^{b_j + b_{j+l}} = -m \quad (11)$$

(3.2) $l \equiv 0 \pmod{m^2}$, $d = 0$ 时:

$$\begin{aligned} R_{z,w}(l) &= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} (-1)^{tr_1^c [tr_c^n(i + e_j)] r_1 + tr_1^c [tr_c^n(i + r + e_{j+s})] r_1} \\ &= \sum_{j=0}^{m-1} \sum_{e_j = e_{j+s}}^{r \bmod m} (-1)^{tr_1^c [tr_c^n(i + e_j)] r_1 + tr_1^c [tr_c^n(i + r + e_{j+s})] r_1} \\ &\quad + \sum_{j=0}^{m-1} \sum_{e_j \neq e_{j+s}}^{r \bmod m} (-1)^{tr_1^c [tr_c^n(i + e_j)] r_1 + tr_1^c [tr_c^n(i + r + e_{j+s})] r_1} \\ &= N(2^n - 1) - (m - N) = (N - 1)2^n + 1 \end{aligned} \quad (12)$$

N 为 r ($0 \leq r < m$) 在 $S_0(s)$ 、 $S_1(s)$ 中出现的次数, 且 r 在 $S_0(s)$ 或 $S_1(s)$ 中都最多出现 1 次. 因此有 $N \in \{0, 1, 2\}$. 此时有:

$$R_{z,w}(l) \in \{1, 1 \pm 2^n\} \quad (13)$$

(3.3) $l \equiv 0 \pmod{m^2}$, $d \neq 0$ 时: d 可划分为集合: $D_1 = \{j \mid d_j = 0, 0 \leq j < m - 1\}$, $D_2 = \{j \mid d_j = 1, 0 \leq j < m - 1\}$, 且 $|D_1| = (m - 1)/2$, $|D_2| = (m + 1)/2$. 设 N_1, N_2 为 r 在 $S_0(s)$ 、 $S_1(s)$ 中出现的次数, 且此时分别有 $j \in D_1, j \in D_2$, 则:

$$\begin{aligned} R_{z,w}(l) &= \sum_{j \in D_1} \sum_{i=0}^{m-1} (-1)^{tr_1^c [tr_c^n(i + e_j)] r_1 + tr_1^c [tr_c^n(i + r + e_{j+s})] r_1} \\ &\quad - \sum_{j \in D_2} \sum_{i=0}^{m-1} (-1)^{tr_1^c [tr_c^n(i + e_j)] r_1 + tr_1^c [tr_c^n(i + r + e_{j+s})] r_1} \\ &= \sum_{j \in D_1} \sum_{e_j = e_{j+s}}^{r \bmod m} (-1)^{tr_1^c [tr_c^n(i + e_j)] r_1 + tr_1^c [tr_c^n(i + r + e_{j+s})] r_1} \\ &\quad + \sum_{j \in D_1} \sum_{e_j \neq e_{j+s}}^{r \bmod m} (-1)^{tr_1^c [tr_c^n(i + e_j)] r_1 + tr_1^c [tr_c^n(i + r + e_{j+s})] r_1} \\ &\quad - \sum_{j \in D_2} \sum_{i=0}^{m-1} (-1)^{tr_1^c [tr_c^n(i + e_j)] r_1 + tr_1^c [tr_c^n(i + r + e_{j+s})] r_1} \\ &\quad - \sum_{j \in D_2} \sum_{e_j \neq e_{j+s}}^{r \bmod m} (-1)^{tr_1^c [tr_c^n(i + e_j)] r_1 + tr_1^c [tr_c^n(i + r + e_{j+s})] r_1} \\ &= N_1(2^n - 1) - [(m - 1)/2 - N_1] - N_2(2^n - 1) \\ &\quad + [(m + 1)/2 - N_2] \\ &= N_1 2^n - N_2 2^n + 1 \end{aligned} \quad (14)$$

由 $N_1, N_2 \in \{0, 1, 2\}$, $N_1 + N_2 \in \{0, 1, 2\}$, 则有:

$$R_{z,w}(l) \in \{1, 1 \pm 2^n, 1 \pm 2^{n+1}\} \quad (15)$$

(3.4) 特别地, 对于 $z = w$, $l \equiv 0 \pmod{m^2}$ 时, 即为 z 的同相自相关函数: $R_z(0) = m^2$.

综合 (3.1)、(3.2)、(3.3)、(3.4) 即证明了 z 的相关特性的结论.

(4) 对于 $z = w$, $l \equiv 0 \pmod{m^2}$ 时, $R_{z,w}(l) = m^2$, 可得 z 的 $L^l(w)$, 任意两个同族 GMW 相控序列均是平移互异的.

根据本文所提出的生成算法, 对 GMW 相控序列在计算机上进行了构造实现. 以 GMW 序列生成器 1 产生周期为 63

的基准序列 $u_0 = \{tr_1^3[tr_2^6(i)]^3\}$ (在 $GF(2)$ 上的最小多项式为 $x^6 + x^5 + x^2 + x + 1$), 以相位选择器所产生的移位数列作为其初始相位, 经 63×63 交织器后可得到 GMW 交错序列 u , 进而与 GMW 序列生成器 2 产生的周期为 63 的 GMW 序列 $b = \{tr_1^3[tr_2^6(k)]^3\}$ (在 $GF(2)$ 上的最小多项式为 $x^6 + x^5 + x^4 + x + 1$) 进行模 2 和运算, 即生成周期为 3969 的 GMW 相控序列。由移位选择器控制 b 的不同移位, 可得到同族的 63 个 GMW 相控序列, 其相关函数取自五值集合 $\{1, -63, 65, -127, 129\}$, 线性复杂度可达到 768。

4 结束语

通过性能分析, 可以看到 GMW 相控序列具有以下优点:

1. 具有良好的相关特性, 相关函数接近于 Welch 界^[6], 用作 CDMA 系统中的地址码时, 多址干扰小。
2. 长周期的 GMW 相控序列线性复杂度高于周期相近的 GMW 序列^[3]、No 序列^[7]、Bent 序列^[8]和 PC 序列^[1]等非线性序列, 在加密中具有明显的优势, 以其作为序列密钥具有良好的保密性。
3. 用作扩频码时, 克服了 Gold 码存在的码不平衡的不足。
4. 实现简单灵活, 可基于相同的生成结构, 通过变换不同的 GMW 序列和移位数列而获得非常大量的同周期序列族。

但同时 GMW 相控序列也存在着不足之处, 如在多址应用中同族序列数目较为有限, 这有待于进一步研究探讨。综上所述, GMW 相控序列具有优良的伪随机特性和极大的线性复杂度, 且实现简单灵活, 仍不失为一类新的性能优异的伪随机序列, 在 CDMA 通信扩频系统和密码学中都具有潜在的应用价值。

参考文献:

- [1] Gong Guang. Theory and application of q -ary interleaved sequences [J]. IEEE Trans. on IT, 1995, 41 (2): 400 - 413.
- [2] Niederreiter, Introduction to Finite Fields and their Applications [M]. Cambridge: Cambridge Univ. Press, 1983.
- [3] Golomb, et al. GMW sequences [J]. IEEE Trans. on IT 1984, 30(3): 548 - 553.
- [4] Games. An algebraic construction of sonar sequences using m-sequences, S.J. Alg. Disc [J]. 1985, 8(4): 753 - 761.
- [5] 万哲先. 代数与编码(修订版) [M]. 北京: 科学出版社, 1980.
- [6] Welch. Lower bounds on the maximum cross correlation of signals [J]. IEEE Trans. on IT, 1974, 20(3): 397 - 399.
- [7] No, et al. A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span [J]. IEEE Trans. on IT, 1989, 35(2): 371 - 379.
- [8] Olsen et al. Bent-function sequences [J]. IEEE Trans. on IT, 1982, 28(6): 858 - 864.

作者简介:



康 凯 1973 年生, 1999 年 3 月获电子科技大学密码学硕士学位。现为电子科技大学通信学院博士生, 从事无线通信网研究。



郭 伟 1964 年出生于四川, 1985 年、1988 年分别获得电子科技大学学士、硕士学位, 现为电子科技大学通信与信息工程学院教授、副院长, 中国电子学会和中国通信学会高级会员。获电子部科技进步二等奖两项, 四川省科技进步三等奖一项, 成都市科技进步二等奖一项, 发表学术论文二十多篇, 研究领域为: 网络优化设计及仿真技术, 通信网可靠性, 信号检测与处理技术等。

吴诗其 1938 年生, 1960 年毕业于成都电讯工程学院, 现为电子科技大学教授, 博士生导师。长期从事个人通信和卫星通信技术研究。