一类理想自相关序列的伪随机性

胡予濮
(西安电子科技大学 ISN 国家重点实验室,信息安全研究所,陕西西安 710071)

摘 要: 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.线性复杂度及其稳定性是序列伪随机性的重要度量指标. C Ding 等给出了一类具有理想自相关性的周期序列,该序列的 0 - 1 分布是几乎均衡的.本文讨论了此类序列的其它伪随机性.本文的主要结果如下:此类序列具有令人满意的线性复杂度;在一个符号替换之下此类序列的线性复杂度不会退化.

关键词: 伪随机序列; 流密码; 线性复杂度; 稳定性
中图分类号: TN918.1 **文献标识码**: A **文章编号**: 0372-2112 (2003) 02-0245-03

Pseudo-Randomness of a Class of Sequences with Ideal Autocorrelation

HU Yu-pu
(*ISPI, ISN National Key Lab., Xidian University, Xi'an, Shaanxi* 710071, *China*)

Abstract: Pseudo random sequence has broad applications in stream cipher, channel coding, and spread spectrum communication. Linear complexity and its robustness are important features of pseudo randomness. C Ding presented a novel class of sequences with ideal autocorrelation and almost balanced 0 - 1 distribution. This paper discusses other pseudo-randomness of such sequences. The major results are the following: such sequences have quite satisfactory linear complexities; their linear complexities do not degenerate under single symbol substitution.

Key words: pseudo-random sequence; stream cipher; linear complexity; robustness

1 引言

$GF(2)$ 上的伪随机序列具有极为广泛的应用,比如流密码、信道编码、扩频通信等等.评价一个伪随机序列优劣的基本准则是伪随机性.我们用许多指标来描述一个周期序列的伪随机性,比如大的周期、大的线性复杂度、均衡性、良好的自相关性、稳定性等等.所谓良好的自相关性指的是自相关函数的绝对值一致地小.自相关函数定义为

定义 1 设 $GF(2)$ 上的周期序列$\{s(t), t = 0,1,2,\cdots\}$,其最小周期为 N.称

$$C_s(w) = \sum_{t=0}^{N-1}(-1)^{s(t+w)-s(t)},\ w = 1 \sim N-1$$

为序列$\{s(t), t = 0,1,2,\cdots\}$的自相关函数.

希望自相关函数的绝对值普遍较小.令 w 遍取 $1 \sim N-1$,容易得到以下结论:当 $N \equiv -1 \pmod 4$ 时,$C_s(w)$ 的可能取值在$\{-(N-2), -(N-6), \cdots, -1, 3, \cdots, N-4\}$范围内;当 $N \equiv 1 \pmod 4$ 时,$C_s(w)$ 的可能取值在$\{-(N-2), -(N-6), \cdots, -3, 1, \cdots, N-4\}$范围内;当 $N \equiv 2 \pmod 4$ 时,$C_s(w)$ 的可能取值在$\{-N, -(N-4), \cdots, -2, 2, \cdots, N-4\}$范围内;当 $N \equiv 0 \pmod 4$ 时,$C_s(w)$ 的可能取值在$\{-N, -(N-4), \cdots, -4, 0, 4, \cdots, N-4\}$范围内.因此如果出现以下四种情形之一:

(1) $N \equiv -1 \pmod 4$,且恒有 $C_s(w) = -1$; (2) $N \equiv 1 \pmod 4$,且恒有 $C_s(w) = 1$; (3) $N \equiv 2 \pmod 4$,且恒有 $C_s(w) = \pm 2$; (4) $N \equiv 0 \pmod 4$,且 $C_s(w) \in \{-4, 0, 4\}$;

就称周期序列$\{s(t), t = 0,1,2,\cdots\}$为一个具有理想自相关性的序列.寻找具有理想自相关性的序列是理论研究的热点[1~8],但一个重要问题是讨论理想自相关序列的其它伪随机性能,包括线性复杂度、多维分布、游程分布等.在现有的理想自相关序列中有以下事实:最小周期为 $2^n - 1$ 的 m 序列具有良好的多维分布和游程分布,但最小的线性复杂度 n;最小周期为 $2^n - 1$ 的 GMW 序列[9]或广义 GMW 序列[10,11],同样具有良好的多维分布和游程分布,但其线性复杂度也仅仅为 n 的幂;以 Mersenne 素数 p 为最小周期的 Legendre 序列具有很好的多维分布和游程分布[12],且线性复杂度与 p 为同阶大数[13];其它各类理想自相关序列的伪随机性能尚不清楚.

理想自相关序列的另一个重要问题是稳定性,比如在有传输差错时其各种伪随机性能不应退化.最近文献[6]给出了一类具有理想自相关性的周期序列,且该序列的 0 - 1 分布是几乎均衡的.此类序列是 Legendre 序列和对数序列[14]的变形.本文讨论了此类序列的其它伪随机性和稳定性.主要结果:此类序列的线性复杂度令人满意,为最小周期的同阶大数;在一个符号替换之下此类序列的线性复杂度不会退化.

2 一类理想自相关序列及其线性复杂度

定义 2[6] 设素数 p 满足 $p = 4f + 1 = x^2 + 4y^2$,其中 $x \equiv 1 \pmod 4$.取定 $GF(p)$ 上的本原元 α,记乘法子群 $D_0 = (\alpha^4)$;记陪集 $D_j = \alpha^j D_0, j \in \{0,1,2,3\}$.取定三个整数 i, j, l,它们互不相同,且均取值于$\{0,1,2,3\}$.定义序列$\{s(t), t = 0,1,2,\cdots\}$如下:在以下四种情形 $s(t) = 1$,否则 $s(t) = 0$: t 偶且 $t \pmod p \in D_i$; t 偶且 $t \pmod p \in D_j$; t 奇且 $t \pmod p \in D_l$; t 奇且 $t \pmod p \in D_j$.

定理 1[6]

收稿日期:2001-08-17;修回日期:2002-08-25
基金项目:ISN 国家重点实验室开放课题基金(No. 5 - 03);武器装备预研基金(No. 51436010201DZ0104)

(1) 定义 2 给出的序列$\{s(t)\}$最小周期为 $2p$,且$|\{t|s(t)=1, t=0\sim 2p-1\}|=p-1$;

(2) 设 $y=1$,f 奇,$(i,j,l)=(0,1,3)$ 或 $(0,2,1)$,则$\{s(t)\}$是理想自相关序列;

(3) 设 $x=1$,f 奇,$(i,j,l)=(1,0,3)$ 或 $(0,1,2)$,则$\{s(t)\}$是理想自相关序列.

引理 1 记 $D_{(0,1)}=\{t|\ t=1\sim 2p-1, t$ 奇, $t(\mathrm{mod}\,p)\in D_0\}$,则 ① $|D_{(0,1)}|=(p-1)/4$; ②对任何 t,任何 $n\in D_{(0,1)}$,$s(nt)=1$ 当且仅当 $s(t)=1$.

证明 ①显然. 为证 ②,只须注意到: $nt\equiv t(\mathrm{mod}2)$, $nt\equiv t(\mathrm{mod}\,p)$. 引理 1 得证.

引理 2 设 β 为 2 特征域上的一个 p 阶元. 记 X 的多项式 $S(X)=\sum_{t=0}^{2p-1}s(t)X^t$. 则对任何整数 m,任何 $k\in D_{(0,1)}$,$S(\beta^n)=S(\beta^{nk})$.

证明 首先对于固定的 $k\in D_{(0,1)}$,存在唯一的 n,$1\le n\le 2p-1$,使得 $kn\equiv 1(\mathrm{mod}2p)$. 其次有 $n\in D_{(0,1)}$. 因此由引理 1 得

$$S(\beta^{nk})=\sum_{t=0\sim 2p-1;\,s(t)=1}\beta^{nkt}=\sum_{t=0\sim 2p-1;\,s(nt)=1}\beta^{nt}=\sum_{t=0\sim 2p-1;\,s(t)=1}\beta^{nt}=S(\beta^n)$$

引理 2 得证.

引理 3 设 β 为 2 特征域上的一个 p 阶元,多项式 $S(X)$ 如引理 2 所示. 则集合

$$\{S(\beta^n)|\ m=0\sim p-1\}$$

中的非 0 元的个数是 $(p-1)/4$ 的非 0 倍数.

证明 首先由定理 1,$S(\beta^0)=|\{t|\ s(t)=1, t=0\sim 2p-1\}|(\mathrm{mod}2)=0$. 其次集合$\{S(\beta^n)|\ m=0\sim p-1\}$中的元素不全为 0 元,否则有

$$\sum_{t=0}^{p-1}(s(t)+s(t+p))\beta^{nt}=0,\ m=0\sim p-1$$

即 X 的多项式 $\sum_{t=0}^{p-1}(s(t)+s(t+p))X^t$ 的系数全为 0;换句话说,序列$\{s(t)\}$最小周期为 p,与定理 1 矛盾. 最后注意到 $D_{(0,1)}$ 中的数关于 mod p 互不同余,故由引理 1 和引理 2,集合$\{S(\beta^n)|\ m=0\sim p-1\}$中的非 0 元的个数是$|D(0,1)|$的非 0 倍数. 引理 3 得证.

定理 2 由定义 2 给出的序列$\{s(t)\}$线性复杂度不小于 $(p-1)/2$.

证明 设 β 为一个 p 阶元,我们知道序列$\{s(t)\}$的极小多项式为

$$g(X)=\frac{1-X^{2p}}{\gcd(1-X^{2p},S(X))}=\frac{(1-X^p)^2}{\gcd((1-X^p)^2,S(X))}$$

而 $(1-X^p)^2=(\prod_{m=0}^{p-1}(X-\beta^n))^2$. 当 $S(\beta^n)\ne 0$ 时,$(X-\beta^n)^2|\ g(X)$. 由引理 3,$g(X)$ 的次数不小于 $(p-1)/2$. 定理 2 得证.

定理 3 如果素数 $p=4f+1$,f 奇,则由定义 2 给出的序列$\{s(t)\}$线性复杂度不小于 $2(p-1)$.

证明 我们知道此时 2 不是模 p 的二次剩余,因此 1、2、4、8 分别属于 D_0 的不同陪集(见定义 2). 取定一个 m 使得 $S(\beta^n)\ne 0$,则由引理 2 和引理 3 有

$$S(\beta^{nk})\ne 0,\ k\in D_{(0,1)};$$
$$S(\beta^{2mu})=S(\beta^{nu})^2\ne 0,\ u\in D_{(0,1)};$$
$$S(\beta^{4mv})=S(\beta^{nv})^4\ne 0,\ v\in D_{(0,1)};$$
$$S(\beta^{8mw})=S(\beta^{nw})^8\ne 0,\ w\in D_{(0,1)}.$$

注意到$\{mk|\ k\in D_{(0,1)}\}$、$\{2mu|\ u\in D_{(0,1)}\}$、$\{4mv|\ v\in D_{(0,1)}\}$、$\{8mw|\ w\in D_{(0,1)}\}$关于模 p 互不同余,因此$\{S(\beta^n)|\ m=0\sim p-1\}$中非 0 元的个数是 $4|D_{(0,1)}|$ 的非 0 倍数. 类似于定理 2 的证明过程,序列$\{s(t)\}$的极小多项式 $g(X)$ 的次数不小于 $8|D_{(0,1)}|=2(p-1)$. 定理 3 得证.

推论 如果 2 是模 p 的二次剩余但非四次剩余(注意到此时 f 是偶数),则由定义 2 给出的序列$\{s(t)\}$线性复杂度不小于 $(p-1)$.

证明 从上知道,此时因 1、2 分别属于 D_0 的不同陪集. 取定 m 使得 $S(\beta^n)\ne 0$,则由引理 2 和引理 3 有: $S(\beta^{nk})\ne 0$, $k\in D_{(0,1)}$; $S(\beta^{2mu})=S(\beta^{nu})^2\ne 0$, $u\in D_{(0,1)}$.

注意到$\{mk|\ k\in D_{(0,1)}\}$、$\{2mu|\ u\in D_{(0,1)}\}$关于模 p 互不同余,因此集合$\{S(\beta^n)|\ m=0\sim p-1\}$中的非 0 元的个数是 $2|D_{(0,1)}|$ 的非 0 倍数. 类似于定理 2 的证明过程,序列$\{s(t)\}$的极小多项式 $g(X)$ 的次数不小于 $4|D_{(0,1)}|=(p-1)$. 推论得证.

3 线性复杂度的稳定性

以下总设 β 为 2 特征域上的一个 p 阶元,多项式 $S(X)$ 如引理 2 所示.

引理 4 集合$\{S(\beta^n)|\ m=0\sim p-1\}$中的所有元素均满足 $S(\beta^n)^{16}=S(\beta^n)$.

证明 当 $S(\beta^n)=0$ 时结论正确,以下设 $S(\beta^n)\ne 0$,我们知道此时 $m\ne 0(\mathrm{mod}\,p)$. 当 $S(\beta^n)^2=S(\beta^n)$,或 $S(\beta^n)^4=S(\beta^n)$,或 $S(\beta^n)^8=S(\beta^n)$ 时结论正确. 以下设 m 使得 $S(\beta^n)$、$S(\beta^n)^2$、$S(\beta^n)^4$、$S(\beta^n)^8$ 互不相等. 注意到以下事实:

$$S(\beta^{nk})=S(\beta^n),\ k\in D_{(0,1)};$$
$$S(\beta^{2mu})=S(\beta^{nu})^2=S(\beta^{2m}),\ u\in D_{(0,1)};$$
$$S(\beta^{4mv})=S(\beta^{nv})^4=S(\beta^{4m}),\ v\in D_{(0,1)};$$
$$S(\beta^{8mw})=S(\beta^{nw})^8=S(\beta^{8m}),\ w\in D_{(0,1)}.$$

因此四个集合$\{mk(\mathrm{mod}\,p)|\ k\in D_{(0,1)}\}$;$\{2mu(\mathrm{mod}\,p)|\ u\in D_{(0,1)}\}$;$\{4mv(\mathrm{mod}\,p)|\ v\in D_{(0,1)}\}$;$\{8mw(\mathrm{mod}\,p)|\ w\in D_{(0,1)}\}$必须互不相交. 又因为其中每个集合的元素个数为 $(p-1)/4$,故

$$\{mk(\mathrm{mod}\,p)|\ k\in D_{(0,1)}\}\cup\{2mu(\mathrm{mod}\,p)|\ u\in D_{(0,1)}\}\cup\{4mv(\mathrm{mod}\,p)|\ v\in D_{(0,1)}\}\cup\{8mw(\mathrm{mod}\,p)|\ w\in D_{(0,1)}\}=\{1,2,\cdots,p-1\}$$

综合以上事实,$S(\beta^n)^{16}$ 必须等于 $S(\beta^n)$、$S(\beta^{2m})$、$S(\beta^{4m})$、$S(\beta^{8m})$ 中的一个. 又因为 2 与 $S(\beta^n)$ 的阶互素,故只能有 $S(\beta^n)^{16}=S(\beta^n)$. 引理 4 得证.

定理 4 设 $p>15$,$S^*(X)=S(X)+X^d$,$0\le d\le 2p-1$,且 $d\ne 0$,$d\ne p$. 则$\{S^*(\beta^n)|\ m=0\sim p-1\}$中都是非 0 元,因此有 $\frac{1-X^{2p}}{\gcd(1-X^{2p},S^*(X))}=1-X^{2p}$.

证明 当 $m=0$ 时,$S^*(\beta^n)=1$;当 $m=1\sim p-1$ 时,

$S^*(\beta^n) = S(\beta^n) + \beta^{nd}$,其中 $S(\beta^n)$ 的阶是 15 的因子(见引理 4),β^{nd} 的阶为 p,故 $S^*(\beta^n) \neq 0$. 定理 4 得证.

引理 5　取定多项式 $h(X) = \sum_{t \in D_i \cup D_l} X^t$. 则 $S(\beta^n) = h(\beta^n)$, $m = 0 \sim p-1$.

证明　$S(\beta^0) = h(\beta^0) = 0$. 对于 $m = 1 \sim p-1$,

$$S(\beta^n) = \sum_{t \in D_i \cup D_j} \beta^{nt} + \sum_{t \in D_l \cup D_j} \beta^{nt} = \sum_{t \in D_i \cup D_l} \beta^{nt} = h(\beta^n)$$

引理 5 得证.

引理 6　取定定理 1 的(2)情形. 则$\{S(\beta^n) + S(\beta^n)^2, m = 0 \sim p-1\}$有两种可能的表达方式:$S(\beta^n) + S(\beta^n)^2 = \sum_{t \in D_0 \cup D_2} \beta^{nt}$或$S(\beta^n) + S(\beta^n)^2 = \sum_{t \in D_1 \cup D_3} \beta^{nt}$.

证明　在定理 1 的(2)情形,必有 $2 \in D_1$ 或 $2 \in D_3$. 以下分为四种子情形来分别证明:

①$(i,l) = (0,3)$, $2 \in D_1$. 由引理 5,此时

$$S(\beta^n) + S(\beta^n)^2 = h(\beta^n) + h(\beta^{3n}) = \sum_{t \in D_0 \cup D_3} \beta^{nt} + \sum_{t \in D_1 \cup D_0} \beta^{nt} = \sum_{t \in D_1 \cup D_3} \beta^{nt};$$

②$(i,l) = (0,3)$, $2 \in D_3$. 此时

$$S(\beta^n) + S(\beta^n)^2 = h(\beta^n) + h(\beta^{3n}) = \sum_{t \in D_0 \cup D_3} \beta^{nt} + \sum_{t \in D_3 \cup D_2} \beta^{nt} = \sum_{t \in D_0 \cup D_2} \beta^{nt};$$

③$(i,l) = (0,1)$, $2 \in D_1$. 此时

$$S(\beta^n) + S(\beta^n)^2 = h(\beta^n) + h(\beta^{3n}) = \sum_{t \in D_0 \cup D_1} \beta^{nt} + \sum_{t \in D_1 \cup D_2} \beta^{nt} = \sum_{t \in D_0 \cup D_3} \beta^{nt};$$

④$(i,l) = (0,1)$, $2 \in D_3$. 此时

$$S(\beta^n) + S(\beta^n)^2 = h(\beta^n) + h(\beta^{3n}) = \sum_{t \in D_0 \cup D_1} \beta^{nt} + \sum_{t \in D_3 \cup D_0} \beta^{nt} = \sum_{t \in D_1 \cup D_3} \beta^{nt}.$$

引理 6 得证.

引理 7　取定定理 1 的(2)情形. 则有:

$S(\beta^0) = S(\beta^0)^2$;当 $m = 1 \sim p-1$ 时,$S(\beta^n) \neq S(\beta^n)^2$

证明　$S(\beta^0) = S(\beta^0)^2 = 0$ 是已知的. 由引理 6,当 $m = 1 \sim p-1$ 时无论如何都有

$$S(\beta^n) + S(\beta^n)^2 + (S(\beta^n) + S(\beta^n)^2)^2 = \sum_{t \in D_0 \cup D_2} \beta^{nt} + \sum_{t \in D_1 \cup D_3} \beta^{nt} = \sum_{t=1}^{p-1} \beta^{nt} = 1$$

这说明 $S(\beta^n) + S(\beta^n)^2 \neq 0$. 引理 7 得证.

引理 8　取定定理 1 的(3)情形. 则 $S(\beta^0) = S(\beta^0)^2 = 0$; $S(\beta^n) + S(\beta^n)^2 = 1$, $m = 1 \sim p-1$.

证明　因为$(i,l) = (1,3)$或$(0,2)$,且 $2 \in D_1$ 或 D_3,故由引理 5,

$$S(\beta^n) + S(\beta^n)^2 = \sum_{t \in D_0 \cup D_2} \beta^{nt} + \sum_{t \in D_1 \cup D_3} \beta^{nt} = \sum_{t=1}^{p-1} \beta^{nt} = 1, \quad m = 1 \sim p-1$$

引理 8 得证.

定理 5　取定定理 1 的(2)情形或定理 1 的(3)情形. 设 $S^{**}(X) = S(X) + X^d$, $d = 0$ 或 $d = p$. 则$\{S^{**}(\beta^n) \mid m = 0 \sim p-1\}$中都是非 0 元,因此有 $\frac{1 - X^{2p}}{\gcd(1 - X^{2p}, S^{**}(X))} = 1 - X^{2p}$.

证明　总有 $S^{**}(\beta^0) = 1$. 当 $m = 1 \sim p-1$ 时,由引理 7 和引理 8 知 $S(\beta^n) \neq S(\beta^n)^2$,因此 $S(\beta^n) \neq 1$. 这说明 $S^{**}(\beta^n) \neq 0$. 定理 5 得证.

由定理 4 和定理 5 说明,当有一个符号替换时,序列的线性复杂度增加到 $2p$.

4　一点说明

我们未能证明定义 2 所给出的序列的良好多维分布和良好游程分布. 不过由于此类序列的构造有点像 Legendre 序列,猜想其多维分布和游程分布较好. 以下给出了此类序列似乎具有其它良好伪随机性能的一个证据:将序列进行等间隔采样,间隔长度为 m, m 与 2 和 p 均互素. 则当 $m \in D_0$ 时,采样序列仍然是原来序列的平移序列;当 m 属于其它的 D_k 时,采样序列仍然是形如定义 2 的序列,只不过对应的(i,j,l)改变了.

参考文献:

[1] A Chang, S W Golomb, G Gong, P V Kumar. On ideal autocorrelation sequences arising from hyperovals[A]. in Sequences and Their Applications: Proc. SETA '98[C]. U K: Springer-Verlag, 1999. 17 - 38.

[2] J A Davis. Almost difference sets and reversible difference sets[J]. Arch. Math., 1992, 59: 595 - 602.

[3] C Ding, T Helleseth, K Y Lam. Several classes of binary sequences with three-level autocorrelation[J]. IEEE Trans. IT, 1999, 45: 2601 - 2606.

[4] J - H Kim, H - Y Song. Existence of cyclic Hadamard difference sets and its relation to binary sequences with ideal autocorrelation[J]. J. Commun. And Networks, 1999, 1(1): 14 - 18.

[5] A Lempel, et al. A class of binary sequences with optimal autocorrelation properties[J]. IEEE Trans. IT, 1977, 23(1): 38 - 42.

[6] C Ding, et al. New families of binary sequences with optimal three-level autocorrelation[J]. IEEE Trans. IT, 2001, 47(1): 428 - 433.

[7] J - S No, H Chung, M - S Yun. Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation[J]. IEEE Trans. IT, 1998, 44(2): 814 - 817.

[8] J - S No, H Chung, M - S Yun. Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by polynomial $z^d + (z+1)^d$[J]. IEEE Trans IT, 1998, 44(3): 1278 - 1282.

[9] R A Scholtz, L R Welch. GMW sequences[J]. IEEE Trans IT, 1984, 30(3): 548 - 553.

[10] J - S No. Generalization of GMW sequences and No sequences[J]. IEEE Trans IT, 1996, 42(1): 260 - 262.

[11] Andrew Klapper, A H Chan, Mark Goresky. Cascaded GMW Sequences[J]. IEEE Trans IT, 1993, 39(1): 177 - 183.

[12] I Damgaard. On the randomness of Legendre and Jacobi sequences[A]. Advances in Cryptology-CRYPTO '88[C]. S. Goldwasser, Ed. Berlin, Germany, Springer-Verlag, 1990. 163 - 172.

[13] Cunsheng Ding, Tor Helleseth, Weijuan Shan. On the linear complexity of legendre sequences[J]. IEEE Trans IT, 1998, 44(3): 1276 - 1278.

[14] Yupu Hu, Guoqiang Bai, Guozhen Xiao. On logarithmic sequences[J]. Chinese Journal of Electronics, 2000, 9(4): 479 - 480.