

# 广义 Legendre 序列和广义 Jacobi 序列的线性复杂度

胡予濮, 魏仕民, 肖国镇

(西安电子科技大学 ISN 国家重点实验室, 信息保密研究所, 西安 710071)

**摘 要:** 本文讨论广义 Legendre 序列和两类广义 Jacobi 序列的线性复杂度. 对于广义 Legendre 序列, 给出了当  $r^t = 3, 4$  时的线性复杂度和当  $r^t = 8$  及一般奇素数时的部分结果. 对于第一类广义 Jacobi 序列, 给出了当  $r^t = 2, 3, 4$  时的线性复杂度和当  $r^t = 8$  时的部分结果. 对于第二类广义 Jacobi 序列, 给出了当  $r^t = 2, 3$  时的线性复杂度和当  $r^t$  为一般奇素数时的部分结果, 还给出了当  $r^t = 4$  时线性复杂度的一个下界.

**关键词:** 信息安全; 流密码; Legendre 序列; Jacobi 序列; 线性复杂度

**中图分类号:** TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2000) 02-0113-05

## On the Linear Complexity of Generalised Legendre/Jacobi Sequences

HU Yu-pu, WEI Shi-min, Xiao Guo-zhen

(ISN National Key Lab., Information Security Institute, Xidian University, Xi'an 710071, China)

**Abstract:** This article discusses the linear complexities of generalised Legendre sequences and two classes of generalised Jacobi sequences. For generalised Legendre sequences, linear complexities are given for  $r^t = 3$  and 4, with part results for  $r^t = 8$  and  $r^t = r$ , a general prime. For the first class of generalised Jacobi sequences, linear complexities are given for  $r^t = 2, 3, 4$ , with part results for  $r^t = 8$ . For the second class of generalised Jacobi sequences, linear complexities are given for  $r^t = 2, 3$ , with part results for  $r^t = r$  and a lower bound of linear complexities for  $r^t = 4$ .

**Key words:** information security; stream cipher; legendre sequence; Jacobi sequence; linear complexity

### 1 定义、性质和若干引理

设计性能好的密钥序列始终是密码学的一个研究热点, 性能好的主要标志是伪随机性和高线性复杂度. Legendre 序列和 Jacobi 序列的伪随机性良好<sup>[1]</sup>, 文[2]又给出了 Legendre 序列的线性复杂度和反馈多项式. 本文推广了文[2]的结论, 定义并讨论了广义 Legendre 序列和两类广义 Jacobi 序列的线性复杂度. 对于广义 Legendre 序列, 给出了当  $r^t = 3, 4$  时的线性复杂度和当  $r^t = 8$  及一般奇素数时的部分结果. 对第一类广义 Jacobi 序列, 给出了当  $r^t = 2, 3, 4$  时的线性复杂度和当  $r^t = 8$  时的部分结果. 对第二类广义 Jacobi 序列, 给出了当  $r^t = 2, 3$  时的线性复杂度和当  $r^t$  为一般奇素数时的部分结果, 还给出了当  $r^t = 4$  时线性复杂度的一个下界.

**定义 1** 设奇素数  $p, q$ , 素数  $r$ , 正整数  $t$ , 满足  $r^t | \gcd(p-1, q-1)$ ,  $p \neq q$ . 在  $GF(p)$  和  $GF(q)$  上分别取定本原元  $g_1$  和  $g_2$ , 令  $h_1 = g_1^{(p-1)/r^t} \pmod{p}$ ,  $h_2 = g_2^{(q-1)/r^t} \pmod{q}$ . 定义  $\log_p x = j$ , 若  $\gcd(p, x) = 1$ ,  $\left(\frac{x}{p}\right)_{r^t} = h_1^j \pmod{p}$ ;  $j = 0 \sim r^t - 1$ . 其中  $\left(\frac{x}{p}\right)_{r^t}$  为  $x$  关于  $p$  的  $r^t$  阶剩余符号<sup>[3,4]</sup>. 同理当  $\gcd(q, x) = 1$  时可定义  $\log_q x$ . 令  $n = pq$ ,  $\gcd(n, x) = 1$ , 定义  $\log_n x = \log_p x$

$+ \log_q x \pmod{r^t}$ .

以下总记  $r^t = R$ . 任意取定  $GF(R)$  上全体元素的一个排列  $\{b_0, b_1, \dots, b_{R-1}\}$

**定义 2**  $GF(R)$  上周期为  $p$  的序列  $a = a_0 a_1 a_2 \dots$  称为广义 Legendre 序列, 如果  $a_i = 0$ , 当  $p \nmid i$ ;  $a_i = b_j$ , 当  $\gcd(p, i) = 1$  且  $\log_p i = j$  (注: 当  $R = 2$  时  $a$  为 Legendre 序列<sup>[1]</sup>, 其线性复杂度已由文[2]给出).

**定义 3**  $GF(R)$  上的序列  $a = a_0 a_1 a_2 \dots$  称为第一类广义 Jacobi 序列, 如果

$a_i = 0$ , 当  $\gcd(n, i) > 1$ ;  $a_i = b_j$ , 当  $\gcd(n, i) = 1$  且  $\log_n i = j$ ; 取定  $j_1, j_2, 0 \leq j_1 \leq R-1, 0 \leq j_2 \leq R-1$ . 补充定义  $\log_p x = j_1$ , 当  $p \nmid x$ ;  $\log_q x = j_2$ , 当  $q \nmid x$ .  $GF(R)$  上的序列  $a = a_0 a_1 a_2 \dots$  称为第二类广义 Jacobi 序列, 如果  $a_i = b_j$ , 当  $\log_n i = j$ .

显然两类广义 Jacobi 序列的最小周期均为  $n = pq$ , 但第二类的分布对称性稍优于第一类. 具体地说, 记  $n_j$  为周期内取值  $b_j$  的次数, 则第一类广义 Jacobi 序列有

$$n_j = \begin{cases} (n)/r^t, & \text{当 } b_j = 0 \\ (n)/r^t + p + q - 1, & \text{当 } b_j \neq 0 \end{cases}$$

第二类广义 Jacobi 序列有

$$n_j = \begin{cases} (n-1)/r^l, & \text{当 } j = j_1 + j_2 \pmod{r^l} \\ (n-1)/r^l + 1, & \text{当 } j = j_1 + j_2 \pmod{r^l} \end{cases}$$

以下总记序列  $a$  的线性复杂度为  $L(a)$ .

引理 1<sup>[2,5]</sup> 设  $a$  为  $GF(R)$  上最小周期为  $m$  的序列, 则

$$m - L(a) = |\{i: S_a(r^i) = 0, 0 \leq i \leq m-1\}|$$

其中  $r$  为  $r$  特征域上的  $m$  阶元,  $S_a(x) = \sum_{i=0}^{m-1} a_i x^i$ .

引理 2 设  $a$  为  $GF(R)$  上周期为  $p$  的广义 Legendre 序列, 则

$$S_a(x) = \sum_{j=0}^{R-1} b_j f_j(x), f_j(x) = \begin{cases} 1, & 0 < i < p, \gcd(p, i) = 1, \log_p i = j \\ 0, & \text{其他} \end{cases}$$

当  $\gcd(p, R) = 1, \log_p R = k$  时有  $f_j(r^l) = f_{j+k}(r^l), j+k$  取为  $j+k \pmod{R}$ . 因此, 有

$$S_a(r^l) = \{b_0, b_1, \dots, b_{R-1}\} * (k) \{f_0(r^l), f_1(r^l), \dots, f_{R-1}(r^l)\} = k \{b_0, b_1, \dots, b_{R-1}\} * \{f_0(r^l), f_1(r^l), \dots, f_{R-1}(r^l)\}$$

其中  $(k)\{ \cdot \}$  和  $k\{ \cdot \}$  分别表示对向量的  $k$  位右轮转变换和  $k$  位左轮转变换:

$$f_k(r^l) = r^{-1}, \quad b_j = \begin{cases} 1, & \text{当 } R=2 \\ 0, & \text{当 } R=2^2 \end{cases}$$

因此若有  $k_j, \gcd(p, k_j) = 1, \log_p k_j = j, j = 0 \sim R-1$ , 则

$$S_a(r^{k_j}) = \begin{cases} 1, & \text{当 } R=2 \\ 0, & \text{当 } R=2^2 \end{cases}$$

若  $\log_p r = 0$ , 则  $f_j(r) = GF(r)$ , 且  $\{f_0(r), f_1(r), \dots, f_{R-1}(r)\}$  中至少有两个不同值.

证明只须注意: 当  $\log_p r = 0$  时,  $f_j(r) = f_j(r^r) = f_j(r)$ .

推论 设  $a$  为  $GF(R)$  上周期为  $n$  的第一类广义 Jacobi 序列. 将引理 2 中的  $p$  改为  $n$ , 则除了  $\sum_{k=0}^{R-1} f_k(r) = r-1$  不成立外 (此时  $\sum_{k=0}^{R-1} f_k(r) = 1$ ), 引理 2 全部结论成立.

证明只须注意: 当  $n$  是  $n$  阶元时,  $\sum_{j=1}^{p-1} j^q = \sum_{j=1}^{q-1} j^p = r-1$ . 推论得证.

引理 3 设  $a$  为  $GF(R)$  上周期为  $p$  的广义 Legendre 序列. 则当  $R=2$  且  $(p-1)/2$  为奇数时  $S_a(1) = 1$ , 其他情形  $S_a(1) = 0$ .

## 2 广义 Legendre 序列的线性复杂度

### 2.1 $R=4$ 的情况

对  $R=4$ , 即  $p=8u+1$  或  $p=8u+5$ . 当  $p=8u+1$  时  $\left(\frac{2}{p}\right)_4 = \pm 1^{[4]}$  (两个值都可能取得, 如  $\left(\frac{2}{73}\right)_4 = -1; \left(\frac{2}{89}\right)_4 = 1$ ). 当  $p=8u+5$  时  $\left(\frac{2}{p}\right)_4 = \pm 1$ .

定理 1 对  $GF(2^2)$  上元素的任意排列  $\{b_0, b_1, b_2, b_3\}$ ,  $p=8u+1$  时恒有  $L(a) = 3(p-1)/4$ ;  $p=8u+5$  时恒有  $L(a) = p-1$ .

证明 情形 1  $p=8u+1$  且  $\left(\frac{2}{p}\right)_4 = 1$ . 由引理 2,  $\{f_0(r), f_1(r), f_2(r), f_3(r)\}$  中恰有一个 0 三个 1, 或三个 0 一个

1. 无论如何,  $\{f_0(r), f_1(r), f_2(r), f_3(r)\}; k=0 \sim 3$  恰好取遍  $GF(2^2)$ .

情形 2  $p=8u+1$  且  $\left(\frac{2}{p}\right)_4 = -1$ . 由引理 2 有  $f_j(r)^2 = f_{j+2}(r), j=0, 1, 2, 3$ . 又由定理 1<sup>[2]</sup> 的证明可知, 不妨取使

$$f_0(r) + f_2(r) = 1, f_1(r) + f_3(r) = 0$$

故  $f_0(r)^3 = f_0(r)(1+f_0(r)) = f_0(r) + f_2(r) = 1$ , 即  $f_0(r)$  是三阶元, 记为  $f_0(r) = e, f_2(r) = e^2$ . 又  $f_1(r) + f_3(r) = f_1(r)(1+f_1(r)) = 0$ , 即  $f_1(r)$  和  $f_3(r)$  同时为 0 或同时为 1.

对  $GF(2^2)$  上元素的任意排列  $\{b_0, b_1, b_2, b_3\}, b_0 e + b_2 e^2 + b_2 e + b_0 e^2, b_0 e + b_2 e^2 - b_1 e + b_3 e^2$ . 故  $\{f_0(r), f_1(r), f_2(r), f_3(r)\}; k=0 \sim 3$  恰好取遍  $GF(2^2)$ .

情形 3  $p=8u+5$ . 首先由  $\left(\frac{16}{p}\right)_4 = 1$  得  $f_0(r)^{16} = f_0(r)$ ; 其次由  $\left(\frac{2}{p}\right)_4 = \pm 1$  得

$$1 = f_0(r) + f_1(r) + f_2(r) + f_3(r) = f_0(r) + f_0(r)^2 + f_0(r)^4 + f_0(r)^8$$

因此  $f_0(r)^{15} = 1$ . 又  $f_0(r)$  不是 3 阶元, 否则由上式  $f_0(r) + f_1(r) + f_2(r) + f_3(r) = 0$ . 以上事实说明  $f_0(r)$  是 15 阶元或 5 阶元, 且  $\{f_0(r), f_1(r), f_2(r), f_3(r)\}$  为一个 2-共轭元素系<sup>[6]</sup>.

设  $f_0(r)$  是 15 阶元. 记  $f_0(r) = x$ . 由定理 1<sup>[2]</sup> 的证明知  $x^4 + x + 1 = f_2(r) + f_0(r) + 1 = 0$ , 故  $x$  只能是  $GF(2)$  上 4 次本原多项式  $x^4 + x^3 + 1$  根<sup>[6]</sup>. 于是

$$\{f_0(r), f_1(r), f_2(r), f_3(r)\} = \{x, x^2, x^3 + 1, x^3 + x^2 + x\}$$

$$GF(2^2) = \{0, 1, x^5, x^{10}\} = \{0, 1, x^3 + x + 1, x^3 + x\}$$

不妨置  $b_0 = 0$ , 则排列  $\{b_0, b_1, b_2, b_3\}$  共有 6 种. 计算结果为

$$\{b_0, b_1, b_2, b_3\} * (k) \{f_0(r) \sim f_3(r)\} = 0, k=0 \sim 3$$

设  $f_0(r)$  是 5 阶元, 且  $f_0(r) = x^3, x$  是  $GF(2)$  上本原多项式  $x^4 + x^3 + 1$  的根. 于是

$$\{f_0(r) \sim f_3(r)\} = \{x^3, x^6, x^{12}, x^9\}$$

$$= \{x^3, x^3 + x^2 + x + 1, x + 1, x^2 + 1\}$$

$$GF(2^2) = \{0, 1, x^5, x^{10}\} = \{0, 1, x^3 + x + 1, x^3 + x\}$$

对每种排列  $\{b_0, b_1, b_2, b_3\}$ , 计算结果为

$$\{b_0, b_1, b_2, b_3\} * (k) \{f_0(r) \sim f_3(r)\} = 0, k=0 \sim 3$$

设  $f_0(r)$  是 5 阶元, 且  $f_0(r) = x^3, x$  是  $GF(2)$  上本原多项式  $x^4 + x + 1$  的根. 于是

$$\{f_0(r) \sim f_3(r)\} = \{x^3, x^6, x^{12}, x^9\}$$

$$= \{x^3, x^3 + x^2, x^3 + x^2 + x + 1, x^3 + x\}$$

$$GF(2^2) = \{0, 1, x^5, x^{10}\} = \{0, 1, x^2 + x, x^2 + x + 1\}$$

对每种排列  $\{b_0, b_1, b_2, b_3\}$ , 计算结果为

$$\{b_0, b_1, b_2, b_3\} * (k) \{f_0(r) \sim f_3(r)\} = 0, k=0 \sim 3$$

综合以上三种情形及引理 3, 定理 1 得证.

### 2.2 $R=3$ 的情况

定理 2 对  $GF(3)$  元素任意排列  $\{b_0, b_1, b_2\}, \log_p 3 = 0$ , 则  $L(a) = 2(p-1)/3; \log_p 3 \neq 0$  则  $L(a) = p-1$ .

证明 若  $\log_p 3 = 0$ , 由引理 2 和引理 3,  $f_j(\cdot) \in GF(3)$ , 且  $\{f_0(\cdot), f_1(\cdot), f_2(\cdot)\}$  中恰有两个不同值. 故  $\{f_0(\cdot), f_1(\cdot), f_2(\cdot)\}^* \cdot (k) \{f_0(\cdot), f_1(\cdot), f_2(\cdot)\}, k=0, 1, 2\}$  恰好取遍  $GF(3)$ .

若  $\log_p 3 \neq 0$ , 只须证明以下两个事实

$f_0(\cdot)$  是 26 阶元或 13 阶元, 且  $\{f_0(\cdot), f_1(\cdot), f_2(\cdot)\}$  为一个 3-共轭元素系;

$\{f_0(\cdot), f_1(\cdot), f_2(\cdot)\}^* \cdot (k) \{f_0(\cdot), f_1(\cdot), f_2(\cdot)\}, k=0, 1, 2\}$  互不相同且不恒为 0.

此时  $f_j(\cdot)^3 = f_j(\cdot^3) = f_{j+1}(\cdot)$  或  $f_{j+2}(\cdot)$ , 即  $f_0(\cdot)^{27} = f_0(\cdot) \neq 0$ . 又  $f_0(\cdot)$  不是 2 阶元, 否则  $f_0(\cdot) + f_1(\cdot) + f_2(\cdot) = 0$ .

故  $\{f_0(\cdot), f_1(\cdot), f_2(\cdot)\}$  互不相同. 故当  $j \neq k$  时  $f_j(\cdot) + 2f_k(\cdot) \neq 0$ . 故 定理 2 得证.

### 2.3 $R=8$ 时线性复杂度的部分结果

此时  $p=8u+1$ . 设  $y$  为  $GF(2^3)$  的一个本原元, 则

$$GF(2^3) = \{0, 1, y, y^2, y^3, y^4, y^5, y^6\} = \begin{cases} \{0, 1, y, y^2, y+1, y^2+y, y^2+y+1, y^2+1\}, & \text{当 } y^3+y+1=0 \\ \{0, 1, y, y^2, y^2+1, y^2+y+1, y+1, y^2+y\}, & \text{当 } y^3+y^2+1=0 \end{cases} \quad (1)$$

定理 3 若  $\left(\frac{2}{p}\right)_8 = -1$ , 则对  $GF(2^3)$  上元素的任意排列  $\{b_0 \sim b_7\}$ , 都有  $L(a) = p-1$ ;

若  $\left(\frac{2}{p}\right)_8 = 1$ , 且  $\{f_0(\cdot) \sim f_7(\cdot)\}$  中有一个或七个 1,

$$\{b_0 \sim b_7\}^* \cdot (k) \{f_0(\cdot) \sim f_7(\cdot)\}, k=0 \sim 7$$

取遍  $GF(2^3)$ , 因此对任意排列  $\{b_0 \sim b_7\}$ , 当  $\{f_0(\cdot) \sim f_7(\cdot)\}$  中有一个或七个 1 时,  $L(a) = 7(p-1)/8$ ;

若  $\left(\frac{2}{p}\right)_8 = 1$  且  $\{f_0(\cdot) \sim f_7(\cdot)\}$  中有三个或五个 1 时, 考虑排列  $\{b_0 \sim b_7\}$  为式 (1) 所示 (称为自然排列), 则  $L(a) = (p-1)/2$ .

这里, 只给出 的证明. 此时  $f_j(\cdot)^2 = f_j(\cdot^2) = f_{j+4}(\cdot)$ , 故  $f_j(\cdot) \in GF(2^2)$ . 取定  $GF(2^2)$  的一个本原元  $e$ , 注意到  $e \in GF(2^3)$ . 由引理 2 知, 在四个对

$$\{f_j(\cdot), f_{j+4}(\cdot)\}, j=0, 1, 2, 3$$

之中恰有奇数个对满足

$$\{f_j(\cdot), f_{j+4}(\cdot)\} = \{e, e+1\} \text{ 或 } \{e+1, e\} \quad (2)$$

又  $\{b_0 \sim b_7\}^* \cdot (k) \{f_0(\cdot) \sim f_7(\cdot)\} = eF_1(y) + F_2(y)$

当恰有一个对满足式 (2) 时显然  $F_1(y) = 0$ ; 再由  $b_0 + \dots + b_7 = 0$  时, 当恰有三个对满足式 (2) 时, 有  $F_1(y) \neq 0$ . 综上所述恒有  $\{b_0 \sim b_7\}^* \cdot (k) \{f_0(\cdot) \sim f_7(\cdot)\} \neq 0$ . 得证.

### 2.4 $R=r$ 为一般奇素数时线性复杂度的讨论

定理 4 取  $GF(r)$  元素的排列为  $\{b_0 \sim b_{r-1}\} = \{0, 1, 2, \dots, r-1\}$  (也称为自然排列), 则

$$L(a) = (r-1)(p-1)/r$$

特别当  $\log_p r = 0$  时有  $L(a) = (r-1)(p-1)/r$ .

证明  $\{b_0 \sim b_{r-1}\}^* \cdot (k) \{f_0(\cdot) \sim f_{r-1}(\cdot)\} = \{b_0 \sim b_{r-1}\}$

$$* (f_0(\cdot) \sim f_{r-1}(\cdot)) = k(r-1) \pmod{r};$$

特别当  $\log_p r = 0$  时,  $\{b_0 \sim b_{r-1}\}^* \cdot (k) \{f_0(\cdot) \sim f_{r-1}(\cdot)\}, k=0 \sim r-1$  取遍  $GF(r)$ . 定理 4 得证.

一个值得注意的问题是, 取排列  $\{b_0 \sim b_{r-1}\}$  为任意时广

义 Legendre 序列的线性复杂度怎样? 作为特例, 以下考虑  $r^2 = 5$  且  $\log_p r = 0$ , 即使对这一特例的讨论也使问题陷入穷举. 不过由引理 2 仍不难将问题归结为以下 5 种情形:

情形 1  $\{f_0(\cdot) \sim f_4(\cdot)\}$  中有四个 0, 一个 4; 或有一个 0, 四个 1;

情形 2  $\{f_0(\cdot) \sim f_4(\cdot)\}$  中有三个 0, 两个 2; 或有两个 0, 三个 3;

情形 3  $\{f_0(\cdot) \sim f_4(\cdot)\}$  中有三个 0, 一个 1; 一个 3; 或有一个 0, 一个 2; 三个 4; 或有一个 0, 三个 2, 一个 3;

情形 4  $\{f_0(\cdot) \sim f_4(\cdot)\}$  中有两个 0, 两个 1, 一个 2; 或有两个 0, 一个 2; 两个 4; 或有一个 0, 两个 3, 两个 4;

情形 5  $\{f_0(\cdot) \sim f_4(\cdot)\}$  中有两个 0, 一个 2, 一个 3, 一个 4; 或有一个 0, 一个 1; 一个 2, 两个 3; 或有一个 0, 一个 1, 两个 2, 一个 4; 或有一个 0, 两个 1, 一个 3, 一个 4.

总之, 情形 1 有  $L(a) = 4(p-1)/5$ ; 情形 2 有  $L(a) = 3(p-1)/5$ ; 情形 3 有  $L(a) = 2(p-1)/5$ ; 情形 4 和情形 5 的讨论更加繁琐, 故略去.

## 3 第一类广义 Jacobi 序列的线性复杂度

定理 5 设  $R=2$ . 设  $(m_1, m_2) = (p \pmod{8}, q \pmod{8})$ , 则对任一排列  $\{b_0, b_1\}$  有

当  $(m_1, m_2) = (-1, -1)$  或  $(3, 3)$  时  $L(a) = (p-1)(q-1)/2 + p + q - 2$ ;

当  $(m_1, m_2) = (-1, 1)$  或  $(3, 5)$  时  $L(a) = (p-1)(q-1)/2 + q - 1$ ;

当  $(m_1, m_2) = (-1, 3)$  或  $(3, -1)$  时  $L(a) = n - 1$ ;

当  $(m_1, m_2) = (-1, 5)$  或  $(3, 1)$  时  $L(a) = p(q-1)$ ;

当  $(m_1, m_2) = (1, -1)$  或  $(5, 3)$  时  $L(a) = (p-1)(q-1)/2 + p - 1$ ;

当  $(m_1, m_2) = (1, 1)$  或  $(5, 5)$  时  $L(a) = (p-1)(q-1)/2$ ;

当  $(m_1, m_2) = (1, 3)$  或  $(5, -1)$  时  $L(a) = (p-1)q$ ;

当  $(m_1, m_2) = (1, 5)$  或  $(5, 1)$  时  $L(a) = (p-1)(q-1)$ .

证明 由引理 2 及其推论有

$$f_j(x) = \sum_{i=1}^{p-1} x^{kp+i} \quad (3)$$

$$i=1, k: 0 < k < q, \gcd(q, kp+i)=1, \log_q(kp+i)=j, \log_p i$$

故当  $R=2$  时恒有:  $S_a(1) = 0$ ; 对  $0 < i < n, q \nmid i, (q-1)/2$  为奇数时  $S_a(i) = 1$ , 否则  $S_a(i) = 0$ .

由文 [4], 当  $(m_1, m_2) = (-1, -1), (-1, 1), (1, -1), (1, 1), (3, 3), (3, 5), (5, 3), (5, 5)$  时  $\log_2 2 = 0$ ; 当  $(m_1, m_2) = (-1, 3), (-1, 5), (1, 3), (1, 5), (3, -1), (3, 1), (5, -1), (5, 1)$  时  $\log_2 2 = 1$ .

当  $\log_2 2 = 0$  时,  $\{f_0(\cdot), f_1(\cdot)\} = \{0, 1\}$  或  $\{1, 0\}$ . 而当  $\log_2 2 = 1$  时,

$$\{f_0(\cdot)^2, f_1(\cdot)^2\} = \{f_0(\cdot^2), f_1(\cdot^2)\} = \{f_1(\cdot), f_0(\cdot)\} \quad (2)$$

即  $f_0(\cdot)$  为 2 特征域上的 3 阶元,  $f_1(\cdot) = 1 + f_0(\cdot)$ . 再由引理 2 及其推论、定理 1<sup>[2]</sup> 的证明过程, 定理 5 得证.

由类似的证明过程可得定理 6、定理 7、定理 8.

**定理 6** 设  $R=4$ . 记  $(m_1, m_2) = (p \pmod{8}, q \pmod{8})$ , 则对任一排列  $\{b_0, b_1, b_2, b_3\}$  有

当  $(m_1, m_2) = (1, 1)$  或  $(5, 5)$  时  $L(a) = 3(p-1)(q-1)/4$ ;

当  $(m_1, m_2) = (1, 5)$  或  $(5, 1)$  时  $L(a) = (p-1)(q-1)$ .

**定理 7** 设  $R=3$ . 对任一排列  $\{b_0, b_1, b_2\}$ , 当  $\log_3 0$  时  $L(a) = 2(p-1)(q-1)/3$ ; 当  $\log_3 0$  时  $L(a) = (p-1)(q-1)$ .

**定理 8** 设  $R=8$ .  $\log_2 2=4$ , 对任意排列  $\{b_0 \sim b_7\}$ ,  $L(a) = (p-1)(q-1)$ ;  $\log_2 2=0$  且  $\{f_0(\cdot) \sim f_7(\cdot)\}$  中有一个或七个 1, 对任意排列  $\{b_0 \sim b_7\}$ ,  $L(a) = 7(p-1)(q-1)/8$ ;  $\log_2 2=0$  且  $\{f_0(\cdot) \sim f_7(\cdot)\}$  中有三个或五个 1, 对“自然排列”  $\{b_0 \sim b_7\}$  (如 (1) 式所示),  $L(a) = (p-1)(q-1)$ .

## 4 第二类广义 Jacobi 序列的线性复杂度

### 4.1 可分序列

**定义 4** 首先将广义 Legendre 序列的概念作以下扩展:  $GF(R)$  上周期为  $p$  的序列  $a$  称为广义 Legendre  $(p, \{b_0, b_1, \dots, b_{R-1}\}, j_0)$  序列, 如果  $a_i = b_j$ , 当  $\log_p i = j$  (若  $p \mid i$  则规定  $\log_p i = j_0$ ), 称对应于排列  $\{b_0, b_1, \dots, b_{R-1}\}$  的第二类广义 Jacobi 序列  $a$  为可分序列, 若满足  $a = a^{(1)} + a^{(2)}$ ; 其中  $a^{(1)}$  是广义 Legendre  $(p, \{c_0, c_1, \dots, c_{R-1}\}, j_1)$  序列;  $a^{(2)}$  是广义 Legendre  $(q, \{d_0, d_1, \dots, d_{R-1}\}, j_2)$  序列,  $\{c_0, c_1, \dots, c_{R-1}\}$  和  $\{d_0, d_1, \dots, d_{R-1}\}$  是某两个排列.

**引理 4** 设  $a$  为第二类广义 Jacobi 序列.

取  $R=2$ , 则  $a$  恒为可分序列;

取  $R=3$ , 则  $a$  恒为可分序列;

取  $R=r$  为一般奇素数,  $\{b_0 \sim b_{r-1}\} = \{0 \sim r-1\}$  为“自然排列”, 则  $a$  为可分序列.

**证明**

对任一排列  $\{b_0, b_1\}$ , 只须取  $\{c_0, c_1\} = \{b_0, b_1\}$ ;  $\{d_0, d_1\} = k \{b_0, b_1\}$ , 若  $b_k = 0$ ;

对任一排列  $\{b_0, b_1, b_2\}$ , 取  $\{c_0, c_1, c_2\} = \{b_0, b_1, b_2\}$ ;  $\{d_0, d_1, d_2\} = k \{b_0, b_1, b_2\}$ , 若  $b_k = 0$ ;

显然, 引理 4 得证.

若  $a = a^{(1)} + a^{(2)}$ , 则

$$S_a(x) = S_{a^{(1)}}(x) \sum_{i=0}^{q-1} x^{ip} + S_{a^{(2)}}(x) \sum_{i=0}^{p-1} x^{iq} \quad (4)$$

由文 [7] 有  $L(a) = L(a^{(1)}) + L(a^{(2)})$ . 特别有

**引理 5** 取  $R=r$  为素数, 且  $a$  是可分序列. 则

$$\begin{cases} r=2 \text{ 时}, L(a) = \\ \begin{cases} L(a^{(1)}) + L(a^{(2)}) - 2, & \text{当 } S_{a^{(1)}}(1) = S_{a^{(2)}}(1) = 1 \\ L(a^{(1)}) + L(a^{(2)}), & \text{其它情形} \end{cases} \\ r>2 \text{ 时}, L(a) = \\ \begin{cases} L(a^{(1)}) + L(a^{(2)}) - 2, & \text{当 } c_{j_1} = 0, d_{j_2} = 0, c_{j_1} + d_{j_2} = 0 \\ L(a^{(1)}) + L(a^{(2)}) - 1, & \text{当 } c_{j_1} = 0, d_{j_2} = 0, c_{j_1} + d_{j_2} = 0 \\ L(a^{(1)}) + L(a^{(2)}), & \text{其他} \end{cases} \end{cases}$$

**证明** 由式 (4) 有

$$\{i: 0 \leq i \leq n-1, S_a(i) = 0\} = \{i: 0 \leq i \leq n-1, \gcd(p, i) = 1, \gcd(q, i) = 1\}$$

$$\{i: 0 \leq i \leq n-1, q \mid i, S_{a^{(1)}}(i) = 0\} = \{i: 0 \leq i \leq n-1, p \mid i, S_{a^{(2)}}(i) = 0\} = A$$

其中当  $S_a(1) = 0$  时  $A = \{0\}$ , 否则  $A$  为空集. 又

$S_a(1) = S_{a^{(1)}}(1)q + S_{a^{(2)}}(1)p = S_{a^{(1)}}(1) + S_{a^{(2)}}(1) \pmod{r}$ ; 再由引理 3 易适当  $r > 2$  时

$S_{a^{(1)}}(1) + S_{a^{(2)}}(1) = c_{j_1} + d_{j_2} \pmod{r}$ . 引理 5 得证.

**定理 9** 取  $R=2$ ,  $\{b_0, b_1\} = \{1, 0\}$ ,  $j_1 = j_2 = 1$ . 令  $(m_1, m_2) = (p \pmod{8}, q \pmod{8})$ , 则

当  $(m_1, m_2) = (-1, -1)$  或  $(1, 1)$  时  $L(a) = (p+q)/2 - 1$ ;

当  $(m_1, m_2) = (-1, 1)$  或  $(1, -1)$  时  $L(a) = (p+q)/2$ ;

当  $(m_1, m_2) = (-1, 3)$  或  $(1, 5)$  时  $L(a) = p/2 + q - 3/2$ ;

当  $(m_1, m_2) = (-1, 5)$  或  $(1, 3)$  时  $L(a) = p/2 + q - 1/2$ ;

当  $(m_1, m_2) = (3, -1)$  或  $(5, 1)$  时  $L(a) = p + q/2 - 3/2$ ;

当  $(m_1, m_2) = (3, 1)$  或  $(5, -1)$  时  $L(a) = p + q/2 - 1/2$ ;

当  $(m_1, m_2) = (3, 3)$  或  $(5, 5)$  时  $L(a) = p + q - 2$ ;

当  $(m_1, m_2) = (3, 5)$  或  $(5, 3)$  时  $L(a) = p + q - 1$ .

事实上, 还容易得到任意排列  $\{b_0, b_1\}$  及任意  $j_1, j_2$  时  $L(a)$  的值. 只须注意定理 1<sup>[2]</sup> 的证明过程和以下事实: 取序列

$a^{(3)}$  为  $a_i^{(3)} = \begin{cases} a_i^{(1)}, & \gcd(p, i) = 1 \\ a_i^{(1)} + 1, & \gcd(p, i) > 1 \end{cases}$ , 则当  $S_{a^{(1)}}(1) = 1$  时  $L(a^{(3)}) = L(a^{(1)}) - 1$ ; 当  $S_{a^{(1)}}(1) = 0$  时  $L(a^{(3)}) = L(a^{(1)}) + 1$ . 这里省去对众多结果的罗列, 但指出不等式  $L(a) > (p+q)/2 - 3$ .

**引理 6** 取  $R=3$ , 排列  $\{c_0, c_1, c_2\}$  任意. 若  $\log_p 3 = 0$ , 则当  $c_{j_1} = 0$  时  $L(a^{(1)}) = 2(p-1)/3$ , 否则  $L(a^{(1)}) = 2(p-1)/3 + 1$ ; 若  $\log_p 3 \neq 0$ , 则当  $c_{j_1} = 0$  时  $L(a^{(1)}) = p-1$ , 否则  $L(a^{(1)}) = p$ .

$$\text{定理 10 取 } R=3, \text{ 令 } b = \begin{cases} 1, & c_{j_1} + d_{j_2} = 0 \\ 0, & c_{j_1} + d_{j_2} = 0 \end{cases}$$

$\log_p 3 = \log_q 3 = 0$  时  $L(a) = 2(p+q-2)/3 + b$ ;

$\log_p 3 = 0, \log_q 3 \neq 0$  时  $L(a) = 2(p-1)/3 + (q-1) + b$ ;

$\log_p 3 \neq 0, \log_q 3 = 0$  时  $L(a) = (p-1) + 2(q-1)/3 + b$ ;

$\log_p 3 \neq 0, \log_q 3 \neq 0, \log_p 3 \neq \log_q 3$  时  $L(a) = p + q - 2 + b$ .

**定理 11** 取  $R=r$  为奇素数, 则有部分结果: 对自然排列  $\{b_0 \sim b_{r-1}\} = \{0 \sim r-1\}$ ,  $\log_p r = \log_q r = 0$ , 有  $L(a) = (r-1)(p+q-2)/r + b$ , 其中  $b$  为定理 10 所述.

### 4.2 不可分序列

对其它情形的  $R$ , 第二类广义 Jacobi 序列  $a$  未必是可分序列.

设  $f_j(x)$  如式 (3) 所示. 令  $u_j(x) = \sum_{0 < i < n, q \nmid i, \log_q i = j-j_2} x^i, v_j(x) = \sum_{0 < i < n, p \nmid i, \log_p i = j-j_1} x^i$ , 则有

$$S_a(x) = \sum_{j=0}^{R-1} b f_j(x) + \sum_{j=0}^{R-1} b_j u_j(x) + \sum_{j=0}^{R-1} b_j v_j(x) + b_{j_1+j_2} \quad (5)$$

以下总设  $r$  为特征域上  $n$  的阶元. 易知当  $\gcd(p, i) = \gcd(q, i) = 1, \log_p i = k_1, \log_q i = k_2$ , 有

$$S_a(r) = \{b_0 \sim b_{R-1}\} * (k_1 + k_2) \{f_0(\cdot) \sim f_{R-1}(\cdot)\} + \{b_0 \sim b_{R-1}\} * (k_2) \{v_0(\cdot) \sim v_{R-1}(\cdot)\} + b_{j_1+j_2} \quad (6)$$

$$u_j(\cdot) = v_j(\cdot) = r-1 \pmod{r} \quad (7)$$

不难证明,当  $R > 2$  恒有  $L(a) > L(a^{(3)}) + L(a^{(4)}) - 2$ ,其中  $a^{(3)}$ 、 $a^{(4)}$  分别为如下的广义 Legendre 序列:

$$a_i^{(3)} = \begin{cases} b_j, \gcd(p, i) = 1, \log_p i = j - \log_n q \\ b_{j_1+j_2}, \gcd(p, i) > 1 \end{cases}$$

$$a_i^{(4)} = \begin{cases} b_j, \gcd(q, i) = 1, \log_q i = j - \log_n p \\ b_{j_1+j_2}, \gcd(q, i) > 1 \end{cases}$$

不仅如此,对于  $r^i = 4$ ,以下将给出序列  $a$  的线性复杂度的更紧的界.

**引理 7** 取  $r^i = 4$ ,  $m_1 = p \pmod{8}$ ,  $b = \begin{cases} 0, b_{j_1+j_2} = 0 \\ 1, b_{j_1+j_2} = 0 \end{cases}$ , 则  
 $m_1 = 1$  时,  $L(a^{(3)}) = 3(p-1)/4 + b$ ;  $m_1 = 5$  时,  $L(a^{(3)}) = p-1+b$ .

**证明** 由定理 1 的证明过程稍加推广即得证引理 7.

**引理 8** 取  $r^i = 4$ , 令  $c_k = \{b_0 \sim b_3\} * (k) \{u_0(\cdot) \sim u_3(\cdot)\}$ ,  $k=0 \sim 3$ ; 则  $\{c_0, c_1, c_2, c_3\}$  满足  
 $c_0 + c_1 + c_2 + c_3 = 0$ ,  $c_2 = c_0 + b_0 + b_2$ ,  $c_3 = c_1 + b_0 + b_2$   $c_1$   $(8)$

**引理 9** 固定排列  $\{b_0 \sim b_3\}$ , 设 2 特征域上的两组元素  $\{c_0, c_1, c_2, c_3\}$  和  $\{d_0, d_1, d_2, d_3\}$  各自满足式(8). 记  $B_k = \{c_0 + d_k, c_1 + d_{k-1}, c_2 + d_{k-2}, c_3 + d_{k-3}\}$ , 则  $B_k$  中的元素全部相等或者  $c_0 + d_k = c_2 + d_{k-2}$ ,  $c_1 + d_{k-1} = c_3 + d_{k-3}$ ; 且当  $B_k$  的元素全部相等时  $B_{k+1}$  的元素不全相等.

**证明** 由式(8)知

$$\{c_0 + d_k, c_1 + d_{k-1}, c_2 + d_{k-2}, c_3 + d_{k-3}\} = \{c_0 + d_k, c_1 + d_{k-1}, c_0 + d_k, c_1 + d_{k-1}\}$$

$$\{c_0 + d_{k+1}, c_1 + d_k, c_2 + d_{k-1}, c_3 + d_{k-2}\} = \{c_0 + d_{k+1}, c_1 + d_k, c_0 + d_{k+1}, c_1 + d_k\}$$

引理 9 得证.

**定理 12** 取  $r^i = 4$ . 则  $L(a) \geq (n)/4 + L(a^{(3)}) + L(a^{(4)}) - 1$ ; 记  $(m_1, m_2) = (p \pmod{8}, q \pmod{8})$ ,

$(m_1, m_2) = (1, 1)$  时  $L(a) \geq (n)/4 + 3(p+q-2)/4$ ;

$(m_1, m_2) = (1, 5)$  时  $L(a) \geq (n)/4 + 3(p-1)/4 + (q-1)$ ;

$(m_1, m_2) = (5, 1)$  时  $L(a) \geq (n)/4 + (p-1) + 3(q-1)/4$ ;

$(m_1, m_2) = (5, 5)$  时  $L(a) \geq (n)/4 + (p+q-2)$ .

**证明** 在式(6)中令  $k_1 + k_2$  固定,  $k_1$  变动, 由引理 7~9 即得证定理 12.

## 5 结语

本文的大量结论说明,从线性复杂度角度来说广义 Legendre 序列和广义 Jacobi 序列是非常好的. 广义 Jacobi 序列比广义 Legendre 序列的优越性在于:密藏的分解式而使序列具有更好的伪随机性,且由生成复杂度的少量增加换取线性复杂度的大量增加. 不难证明广义 Legendre 序列和广义 Jacobi 序列的另一个鲜明的优点:在少量符号替换下其线性复杂度很稳健,但其伪随机性仍需进一步研究.

对不可分的第二类广义 Jacobi 序列的线性复杂度所给的界似乎太松. 可以猜想它与  $(n)$  同阶. 定理 12 部分地证实了这一猜想.

## 参考文献

- [1] I. Damgaard. On the randomness of Legendre and Jacobi Sequences. Advances in cryptology: CRYPTO '88, Springer-Verlag, 1990:163~172
- [2] C. Ding, T. Helleseht, W. Shan. On the complexity of Legendre Sequences. IEEE Transactions on IT, May 1998, 44(3):1276~1278
- [3] Scott A. Vanstone, Robert J. Zucchrato. Elliptic Curve Cryptosystems Using Curves of Smooth Order Over Ring  $Z_n$ , IEEE transactions on IT, July 1997, 43(4):1231~1237
- [4] 柯召,孙琦. 数论讲义. 第六章第三节. 161~163. 北京:高等教育出版社,1986
- [5] R. Lidl, H. Niederreiter. Finite Fields. in Encyclopedia of Mathematics and Its Applications, Vol. 20, MA: Addison-Wesley, 1983
- [6] 肖国镇,卿斯汉. 编码理论. 第五章第五节, 188~193. 北京:国防工业出版社, 1993

(上接第 123 页)

## 参考文献

- [1] L. J. Hornbeck. Deformable-mirror spatial light modulators. in Pro. SPIE, 1989, 1150:86~102
- [2] E. Obermeier, J. Lin and V. Schlichting. Design and fabrication of an eletrostatically driven microshutter. in Tech. Dig. 7th Int. Conf. Solid State Sensor and Actuators (Transducers 93), Yokohama, Japan, 1993,

June 7-10:132~135

- [3] J. Mohr, M. Kohl and W. Menz. Micro-optical switching by electrostatic linear actuators with larger displacements. in Tech. Dig. 7th Int. Conf. Solid State Sensors and Auctuators (Transducers 93), Yokohama, Japan, 1993 June 7-10:120~123
- [4] F. P. Beer and E. R. Johnston, Mechanics of Materials. (McGraw-Hill, Ryerson, Toronto 1985)