文章编号:1673-5005(2006)02-0147-04

修改的Jacobi序列的线性复杂度

闫统江[1,2], 张 宁[1], 肖国镇[1]

(1.西安电子科技大学 综合业务网国家重点实验室,陕西 西安 710071;
2.中国石油大学 数学与计算科学学院,山东 东营 257061)

摘要:利用剩余类环 Z_{pq} 上的广义割圆理论,给出了周期为 pq 的修改的Jacobi序列的一个新定义,并得到了修改的Jacobi序列的线性复杂度和极小多项式,从而证明了Green猜想的正确性。分析结果表明,多数修改的Jacobi序列具有良好的线性复杂度。

关键词:Jacobi序列; 割圆理论; 线性复杂度; 极小多项式

中图分类号:TN 918.4 **文献标识码**:A

Linear complexity of modified Jacobi sequences

YAN Tong-jiang[1,2], ZHANG Ning[1], XIAO Guo-zhen[1]

(1. ISN *National Key Laboratory*, *Xidian University*, *Xi'an* 710071, *China*;
2. *College of Mathematics and Computational Science in China University of Petroleum*, *Dongying* 257061, *Shandong Province*, *China*)

Abstract: According to the theory of generalized cyclotomy on two-prime residue class ring Z_{pq}, a new definition of modified Jacobi sequences (MJSs) with the period of pq was presented. Based on the new definition, linear complexity and minimal polynomials of MJSs were calculated. The obtained results can guarantee the correctness of Green conjecture and show that most of MJSs possess good linear complexity.

Key words: Jacobi sequence; cyclotomy theory; linear complexity; minimal polynomial

1 预备知识

如果序列 $s^\infty=(s_0,s_1,s_2,\cdots)$ 满足 $s_j=c_1s_{j-1}+c_2s_{j-2}+\cdots+c_Ls_{j-L}(j>L$,其中 L 是正整数),则称 s^∞ 是一个线性递归序列,满足上式的最小的 L 称为该递归序列的线性复杂度,记为 $L(s^\infty)$。线性复杂度是衡量密钥流序列的不可测性的重要指标,只要知道它的任意 $2L(s^\infty)$ 个连续比特就可预测整个序列。因此,为抗已知明文攻击,密钥流序列的线性复杂度应不小于 $N/2$,这里 N 是 s^∞ 的最小正周期。无穷序列 $s^\infty=(s_0,s_1,s_2,\cdots)$ 和有限序列 $s^N=(s_0,s_1,\cdots,s_{N-1})$ 的反馈函数分别为 $S(x)=\sum_{i=0}^{\infty}s_ix^i$ 和 $S^N(x)=\sum_{i=0}^{N-1}s_ix^i$。$s^\infty$ 的极小多项式是

$$m(x)=\frac{1-x^N}{\gcd(S^N(x),1-x^N)},\text{且}$$

$$L(s^\infty)=N-\deg(\gcd(x^N-1,S^N(x)).\quad(1)$$

2 Whiteman广义割圆类

令 p 和 q 为两个奇素数,$N=pq,p>q,2n=\gcd(p-1,q-1),e=\frac{(p-1)(q-1)}{2n}$,则剩余类环 Z_{pq} 存在关于乘法的子群 $Z_{pq}^*=\{g^sx^i:s=0,1,\cdots,e-1;i=0,1,\cdots,2n-1\}$,这里 g 是 p 和 q 共同的本原根,x 是满足条件 $x\equiv g\bmod p$ 和 $x\equiv 1\bmod q$ 的正整数。称 $D_i=\{g^sx^i:s=0,1,\cdots,e-1\},i=0,1,\cdots,2n-1$ 为关于 p 和 q 的 $2n$ 阶Whiteman广义割圆类(简记为W-GC)。定义 $P=\{p,2p,\cdots,(q-1)p\},Q=\{q,2q,\cdots,(p-1)q\},B_0=\bigcup_{i=0}^{n-1}D_{2i}$,

收稿日期:2005-08-13
基金项目:国家自然科学基金资助项目(60473028)
作者简介:闫统江(1973-),男(汉族),山东郓城人,讲师,博士研究生,研究方向为流密码和序列密码设计。

万方数据

$B_1 = \bigcup_{i=0}^{n-1} D_{2i+1}, R = \{0\}, C_0 = R \cup Q \cup B_0, C_1 = P \cup B_1$,则如下等式显然成立:

$$C_0 \cup C_1 = Z_N, \quad C_0 \cap C_1 = \emptyset,$$
$$B_0 \cup B_1 = Z_N^*, \quad B_0 \cap B_1 = \emptyset.$$

其中,$\emptyset$ 表示空集。

割圆理论是代数学的重要内容。Store T 和 Whiteman 等人的工作主要是利用广义割圆类来构造差集[1,2],但密码构造学家很快发现,利用差集构造的序列具有最优的自相关性质,如果作为密钥流,则具有很强的抗相关攻击的能力。DING Cunsheng 等直接用广义割圆类来构造序列,并研究这些序列的密码学性质[3-5]。研究证明,利用 W-GC 构造的很多序列都具有良好的密码学性质。修改的 Jacobi 序列(简记为 MJS)是常见的伪随机序列。它被证明具有很好的相关性质。Green 在大量的计算机搜索数据基础上给出了关于修改的 Jacobi 序列的线性复杂度的猜想[6]。笔者认为修改的 Jacobi 序列可以由 W-GC 构造得到,并利用割圆理论给出它的线性复杂度和极小多项式,以证明 Green 猜想的正确性。

3 MJS 的线性复杂度和极小多项式

周期为 N 的 MJS 定义为

$$s_i = \begin{cases} (\frac{i}{p}) \oplus (\frac{i}{q}), \ \gcd(i,N) = 1, \\ 0, \ i \equiv 0 \bmod q, \\ 1, \ 其他. \end{cases}$$

MJS 也可以定义为 C_1 的特征序列,即

$$s_i = \begin{cases} 0, \ i \in C_0, \\ 1, \ i \in C_1. \end{cases}$$

事实上,由 x 的定义得

$$g^s x^j \bmod p = g^{s+j} \bmod p,$$
$$g^s x^j \bmod q = g^s \bmod q.$$

如果 $i \in B_0$,则 $j \equiv 0 \bmod 2$。从而 i 同时为 p 和 q 的剩余类或非剩余类。于是 $(\frac{i}{p}) \oplus (\frac{i}{q}) = 0$。

如果 $i \in B_1$,则 $j \equiv 1 \bmod 2$。从而 i 不能同时为 p 和 q 的剩余类或非剩余类。于是 $(\frac{i}{p}) \oplus (\frac{i}{q}) = 1$。

引理 1[7] P, Q 和 R 如前面的定义,

(1) 如果 $a \in P$,则 $aP = P, aQ = R$;

(2) 如果 $a \in Q$,则 $aP = R, aQ = Q$;

(3) 如果 $a \in D_j$,则 $aP = P, aQ = Q, aD_i = D_{i+j}$。这里,$i, j = 0,1,\cdots,2n-1$。

设 m 为 2 的模 N 阶,即 $2^m \equiv 1 \bmod N$。由于 $\gcd(N,2) = 1$,故在 $x^N - 1 \in GF(2)[x]$ 的分裂域 $GF(2^m)$ 上存在 N 次单位原根 α。由式(1)可得

$$L(s^\infty) = N - |\{j : S(\alpha^k) = 0, 0 \leqslant k \leqslant N-1\}|. \tag{2}$$

显然,MJS 的反馈函数是 $S(x) = \sum_{i \in C_1} x^i$,且 $S(x) \in GF(2)[x]$,

$$S(1) = (q-1) + (p-1)(q-1)/2 \equiv 0 \bmod 2. \tag{3}$$

引理 2[3] 若 P, Q 和 Z_N^* 如前面的定义,则 $\sum_{j \in P} \alpha^j = \sum_{j \in Q} \alpha^j = \sum_{j \in Z_N^*} \alpha^j = 1$.

引理 3[3] $\mathrm{ord}_N(g) = e$,这里 $\mathrm{ord}_N(g)$ 表示 g 的模 N 阶。

引理 4

$$\sum_{i \in D_j} \alpha^{ki} = \begin{cases} \frac{p-1}{2n} \bmod 2, k \in P, \\ \frac{q-1}{2n} \bmod 2, k \in Q, \end{cases}$$

$j = 0,1,\cdots,2n-1$.

证明 令 $k \in Q$,由引理 3 和 D_j 的定义得 $D_j \bmod p = \{g^s x^j \bmod p : s = 0,1,\cdots,e-1\} = \{g^{s+j} \bmod p : s = 0,1,\cdots,e-1\}$,当 s 跑遍 $\{0,1,\cdots,e-1\}$ 一次,$g^s x^j \bmod p$ 取集合 $\{1,\cdots,p-1\}$ 每个元素 $\frac{q-1}{2n}$ 次。所以由引理 2 可得

$$\sum_{i \in D_j} \alpha^{ki} = [\frac{q-1}{2n} \bmod 2] \sum_{i \in Q} \alpha^i = \frac{q-1}{2n} \bmod 2.$$

同理可证引理的其余部分。

引理 5

$$S(\alpha^k) = \begin{cases} S(\alpha), \ k \in B_0, \\ 1 + S(\alpha), \ k \in B_1. \end{cases}$$

证明 如果 $k \in B_0$,由引理 1 得

$$S(\alpha^k) = \sum_{i \in P} \alpha^{ki} + \sum_{i \in B_1} \alpha^{ki} = \sum_{i \in kP} \alpha^i + \sum_{i \in kB_1} \alpha^i = \sum_{i \in P} \alpha^i + \sum_{i \in B_1} \alpha^i = S(\alpha).$$

如果 $k \in B_1$,由引理 1 和 2 得,

$$S(\alpha^k) = \sum_{i \in P} \alpha^{ki} + \sum_{i \in B_1} \alpha^{ki} = \sum_{i \in P} \alpha^i + \sum_{i \in B_0} \alpha^i = \sum_{i \in P} \alpha^i + 1 + \sum_{i \in B_1} \alpha^i = 1 + S(\alpha).$$

引理 6 $S(\alpha) \in \{0,1\}$ 当且仅当 $2 \in B_0$。

证明 因为 $S(x) \in GF(2)[x]$,由引理 5,如果 $2 \in B_0$,则 $S(\alpha)^2 = S(\alpha^2) = S(\alpha)$。从而 $S(\alpha) \in \{0,1\}$。如果 $2 \in B_1$,$S(\alpha)^2 = S(\alpha^2) = 1 + S(\alpha)$。于是 $S(\alpha) \notin \{0,1\}$。

万方数据

引理 7　$2\in B_0$ 当且仅当 $p\equiv\pm 1 \bmod 8, q\equiv\pm 1 \bmod 8$,或者 $p\equiv\pm 3 \bmod 8, q\equiv\pm 3 \bmod 8$。

证明　假设 $2\in B_0$,由 B_0 的定义,存在一个整数 s 和一个偶数 i 使得 $2=g^s x^i, 0\leqslant s\leqslant e-1, 0\leqslant i\leqslant 2n-1$。由 p,q 和 x 的定义,有

$$2 \bmod p = g^s x^i \bmod p = g^{s+i} \bmod p,$$
$$2 \bmod q = g^s x^i \bmod q = g^s \bmod q.$$

如果 s 是偶数,则 2 是模 p 和 q 的一个二次剩余,由二次剩余定理,$p\equiv\pm 1 \bmod 8, q=\pm 1 \bmod 8$;如果 s 是奇数,则 2 是 p 和 q 的一个二次非剩余,所以,$p\equiv\pm 3 \bmod 8, q=\pm 3 \bmod 8$。假设 $2\notin B_0$,则 $2\in B_1$,由 B_1 的定义,存在一个整数 s 和一个奇数 $j, 0\leqslant s\leqslant e-1, 0\leqslant j\leqslant 2n-1$ 使得 $2=g^s x^j \bmod (pq)$,则

$$2 \bmod p = g^s x^j \bmod p = g^{s+j} \bmod p,$$
$$2 \bmod q = g^s x^j \bmod q = g^s \bmod q.$$

如果 s 是偶数,则 2 是模 p 的一个二次非剩余,是模 q 的一个二次剩余。所以,由二次剩余定理,$p\equiv\pm 3 \bmod 8, q=\pm 1 \bmod 8$。如果 s 是奇数,则 2 是模 p 的一个二次剩余,是模 q 一个二次非剩余。所以 $p\equiv\pm 1 \bmod 8, q=\pm 3 \bmod 8$。

引理 8

$$S(\alpha^k)=\begin{cases}1+n\dfrac{p-1}{2n} \bmod 2, & k\in P,\\ n\dfrac{q-1}{2n} \bmod 2, & k\in Q.\end{cases}$$

证明　如果 $k\in Q$,由引理 1,4 和 2 得

$$S(\alpha^k)=\sum_{i\in P}\alpha^{ki}+\sum_{i\in B_1}\alpha^{ki}=\sum_{i\in P}1+\sum_{i\in B_1}\alpha^{ki}=n\frac{p-1}{2n} \bmod 2.$$

如果 $k\in P$,由引理 1,2 和 4,得

$$S(\alpha^k)=\sum_{i\in P}\alpha^{ki}+\sum_{i\in B_1}\alpha^{ki}=\sum_{i\in P}\alpha^{i}+\sum_{i\in B_1}\alpha^{ki}=1+n\frac{p-1}{2n} \bmod 2.$$

令 $\beta=\alpha^p$ 是 x^q-1 的一个 p 次单位原根,$\lambda=\alpha^q$ 是 x^p-1 的一个 q 次单位原根,则

$$x^p-1=(x-1)\prod_{i\in Q}(x-\alpha^i),$$
$$x^q-1=(x-1)\prod_{i\in P}(x-\alpha^i).$$

定义 $d(x)=\prod_{i\in Z_{pq}^*}(x-\alpha^i)$,因为 $m\mid\varphi(pq)=(p-1)(q-1)$,$\deg(d(x))=\varphi(pq)$,则 $d(x)\in GF(2)[x]$。

定义 $d_j(x)=\prod_{i\in B_j}(x-\alpha^i), j=0,1$,如果 $2\in B_0$,则 $2B_0=B_0, 2B_1=B_1, d_j(x)^2=\prod_{i\in B_j}(x^2-\alpha^{2i})=d_j(x^2)$。所以

$$d_j(x)\in GF(2)[x], d(x)=d_0(x)d_1(x),$$
$$x^N-1=\frac{(x^p-1)(x^q-1)d(x)}{x-1}=\frac{(x^p-1)(x^q-1)d_0(x)d_1(x)}{x-1}.$$

由引理 5,如果 $2\in B_0$,则 $S(\alpha)$ 和 $1+S(\alpha)$ 中有且仅有一个为 0。如果选择一个固定的 α,使得 $S(\alpha)=0$,则有定理 1 ~ 4 成立。

定理 1　(1) 如果 $p\equiv q\equiv 1 \bmod 8$ 或者 $p\equiv q\equiv 5 \bmod 8$,那么

$$L(s^\infty)=\frac{(p+1)(q-1)}{2},$$
$$m(x)=\frac{x^{pq}-1}{(x^p-1)d_0(x)}\text{(由 }\alpha\text{ 的选择)};$$

(2) 如果 $p\equiv 1 \bmod 8, q\equiv 5 \bmod 8$ 或者 $p\equiv 5 \bmod 8, q\equiv 1 \bmod 8$,那么

$$L(s^\infty)=(q-1)p,$$
$$m(x)=\frac{x^{pq}-1}{x^p-1}\text{(由 }\alpha\text{ 的选择)}.$$

证明　由(1) 和(2) 的条件可知 $4\mid 2n$,即 $2\mid n$。由引理 8 得

$$S(\alpha^k)=\begin{cases}1 \bmod 2, & k\in P,\\ 0 \bmod 2, & k\in Q;\end{cases}$$

由引理 5 和 6,若(1) 的条件满足,则 $S(\alpha)\in\{0,1\}$。由式(1) ~ (3) 和引理 4 得

$$L(s^\infty)=N-1-(p-1)-\frac{(p-1)(q-1)}{2}=\frac{(p+1)(q-1)}{2},$$

而且 $\gcd(S(x),x^N-1)=(x^p-1)d_0(x)$,从而 $m(x)=\dfrac{x^{pq}-1}{(x^p-1)d_0(x)}$。

若(2) 的条件满足,$S(\alpha^k), 1+S(\alpha^k)\notin\{0,1\}$,$L(s^\infty)=N-1-(p-1)=p(q-1)$。而且 $\gcd(S(x),x^N-1)=x^p-1$,则 $m(x)=\dfrac{x^{pq}-1}{x^p-1}$。

定理 2　(1) 如果 $p\equiv 1 \bmod 8, q\equiv 7 \bmod 8$ 或者 $p\equiv 5 \bmod 8, q\equiv 3 \bmod 8$ 则

$$L(s^\infty)=\frac{pq+p+q-3}{2},$$
$$m(x)=\frac{x^{pq}-1}{(x-1)d_0(x)}\text{(由 }\alpha\text{ 的选择)};$$

(2) 如果 $p\equiv 1 \bmod 8, q\equiv 3 \bmod 8$,或者 $p\equiv 5 \bmod 8, q\equiv 7 \bmod 8$,则

万方数据

$$L(s^{\infty}) = pq - 1,$$

$$m(x) = \frac{x^{pq}-1}{x-1}(\text{由 } \alpha \text{ 的选择}).$$

证明 由(1)和(2)的条件可知,n 和$\frac{q-1}{2n}$是奇数,$\frac{p-1}{2n}$是偶数,由引理 8 得

$$S(\alpha^k) = \begin{cases} 1\bmod 2, & k \in P, \\ 1\bmod 2, & k \in Q. \end{cases}$$

由引理 5 和引理 6,若(1)的条件满足,则 $S(\alpha) \in \{0,1\}$。由式(1)~(3)和引理 4 可得,

$$L(s^{\infty}) = pq - 1 - \frac{(q-1)(p-1)}{2} = \frac{pq+p+q-3}{2},$$

而且 $\gcd(S(x), x^N - 1) = (x-1)d_0(x)$,则

$$m(x) = \frac{x^{pq}-1}{(x-1)d_0(x)}.$$

若(2)的条件满足,$S(\alpha), 1 + S(\alpha) \notin \{0,1\}$,$L(s^{\infty}) = pq - 1$,而且 $\gcd(S(x), x^N - 1) = x - 1$,则 $m(x) = \frac{x^{pq}-1}{x-1}$。

定理 3 (1)如果 $p \equiv 3\bmod 8, q \equiv 1\bmod 8$,或者 $p \equiv 7\bmod 8, q \equiv 5\bmod 8$,则

$$L(s^{\infty}) = \frac{(p-1)(q-1)}{2},$$

$$m(x) = \frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)d_0(x)} \text{ (由 } \alpha \text{ 的选择)};$$

(2)如果 $p \equiv 3\bmod 8, q \equiv 5\bmod 8$ 或 $p \equiv 7\bmod 8, q \equiv 1\bmod 8$,则

$$L(s^{\infty}) = (p-1)(q-1),$$

$$m(x) = \frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)} \text{ (由 } \alpha \text{ 的选择)}.$$

证明 由(1)和(2)的条件可知,n 和$\frac{p-1}{2n}$是奇数,$\frac{q-1}{2n}$是偶数,由引理 8 得

$$S(\alpha^k) = \begin{cases} 0\bmod 2, & k \in P, \\ 0\bmod 2, & k \in Q. \end{cases}$$

由引理 5 和引理 6,若(1)的条件满足,则 $S(\alpha) \in \{0,1\}$。由式(1)~(3)和引理 4 得 $L(s^{\infty}) = \frac{(p-1)(q-1)}{2}$,而且

$$\gcd(S(x), x^N - 1) = \frac{d_0(x)(x^p-1)(x^q-1)}{x-1},$$

则

$$m(x) = \frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)d_0(x)}.$$

若(2)的条件满足,则 $S(\alpha), 1 + S(\alpha) \notin \{0, 1\}$,从而 $L(s^{\infty}) = (p-1)(q-1)$,而且

$$\gcd(S(x), x^N - 1) = \frac{(x^p-1)(x^q-1)}{x-1},$$

则

$$m(x) = \frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)}.$$

定理 4 (1)如果 $p \equiv q \equiv 3\bmod 8$,或者 $p \equiv q \equiv 7\bmod 8$,则

$$L(s^{\infty}) = \frac{(p-1)(q+1)}{2},$$

$$m(x) = \frac{x^{pq}-1}{(x^q-1)d_0(x)} \text{(由 } \alpha \text{ 的选择)};$$

(2)如果 $p \equiv 1\bmod 8, q \equiv 5\bmod 8$,或者 $p \equiv 5\bmod 8, q \equiv 1\bmod 8$,则

$$L(s^{\infty}) = (p-1)q,$$

$$m(x) = \frac{x^{pq}-1}{(x^q-1)} \text{(由 } \alpha \text{ 的选择)}.$$

本定理的证明可类似地由定理 3 的证明得到。

4 结束语

给出了 MJS 的 Whiteman 广义割圆定义,并利用割圆理论给出了其线性复杂度和极小多项式,从而证明了 Green 的猜想。分析结果表明,多数 MJS 具有满足密码学需要的线性复杂度。

参考文献:

[1] STORER T. Cyclotomiy and difference set[M]. Chicago: Markham, 1967.

[2] WHITEMAN A L. A family of difference sets[J]. Illinois J Math, 1962, 6: 107-121.

[3] DING Cunsheng. Linear complexity of generalized cyclotomic binary sequence of order 2[J]. Finite Fields and Their Applications, 1997, 3: 159-174.

[4] DING C. Autocorrelation values of generalized cyclotomic sequences of order two[J]. IEEE Transactions on Information Theory, 1998, 44(5): 1699-1702.

[5] BAI Enjian, FU Xiaòtong, XIAO Guozhen. On the linear complexity of generalized cyclotomic sequences of order four over Z_{pq}[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2005, E88-A(1): 392-395.

[6] GREEN D H, CHOI J. The linear complexity of modified Jacobi sequences[J]. IEE Proc Comput Digit Tech, 2002, 149(3): 97-101.

[7] DING Cunsheng. New generalized cyclotomy and its applications[J]. Finite Fields and Their Applications, 1998, 4: 140-166.

(编辑 修荣荣)

万方数据