文章编号:1673-5005(2006)01-0142-04

8 阶二元广义割圆序列的线性复杂度

闫统江[1,2], 张卫国[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:为了从剩余类环上的二元广义割圆序列中寻求满足需要的密钥流序列,考虑了双素数积剩余类环 Z_{pq} 上的一类二元广义 8 阶割圆序列,利用有限域理论,给出了该序列在不同情形下的极小多项式,进而得到了它的线性复杂度。结果表明,该序列有很好的复杂度性质,可以通过选取适当的奇素数 p 和 q,使得其线性复杂度足够大。

关键词:流密码; 剩余类环; 广义割圆; 序列; 线性复杂度

中图分类号:TN 918.4 **文献标识码**:A

Linear complexity of binary generalized cyclotomic sequences of order eight

YAN Tong-jiang[1,2], ZHANG Wei-guo[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, *China*)

Abstract: In order to get suitable binary sequences for key streams, binary generalized cyclotomic sequences of order eight on the two-prime residue class ring were considered. By means of the polynomial theory over finite fields, minimal polynomials and linear complexity of these sequences were obtained. The results show that sequences with high linear complexity can be produced if the values of p and q are small enough, where p and q are distinct odd primes.

Key words: stream ciphers; residue class ring; generalized cyclotomy; sequences; linear complexity

1 问题的提出

为了从剩余类环上的二元广义割圆序列中寻求满足需要的密钥流序列,DING Cunsheng 和 BAI Enjian 等分别考虑了剩余类环 Z_{pq} 上的 2 阶和 4 阶二元广义割圆序列的线性复杂度[1,2]。由于在实际应用中,要求奇素数 p 和 q 的取值都比较大,得到满足条件 $2=\gcd(p-1,q-1)$ 或 $4=\gcd(p-1,q-1)$ 的 p 和 q 是不容易的。这就需要研究更多种类的广义割圆序列。

如果序列 $s^\infty=(s_0,s_1,s_2,\cdots)$ 满足递归关系式

$$s_j+c_1s_{j-1}+\cdots+c_Ls_{j-L}=0, j\geqslant L, \quad (1)$$

其中 L 是正整数,则称 s^∞ 是一个线性递归序列,满足式(1)的最小的正整数 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为足够大。

序列 $s^\infty=(s_0,s_1,s_2,\cdots)$ 的生成函数定义为

$$S(x)=s_0+s_1x+s_2x^2+\cdots=\sum_{i=1}^{\infty}s_ix^i.$$

有限序列 $s^N=(s_0,s_1,s_2,\cdots,s_{N-1})$ 的生成函数定义为

$$S^N(x)=s_0+s_1x+s_2x^2+\cdots+s_{N-1}x^{N-1}.$$

如果 N 是 s^∞ 的周期,则

$$m(x)=(1-x^N)/\gcd(s^N(x),1-x^N)$$

是 s^∞ 的极小多项式,且

$$L(s^\infty)=\deg(m(x)).$$

令 p 和 q 是两个不同的奇素数,$d=\gcd(p-1,$

收稿日期:2005-06-15

基金项目:国家自然科学基金项目(60473028)

作者简介:闫统江(1973-),男(汉族),山东郓城人,讲师,博士研究生,研究方向为序列密码设计。

$q-1)$,$e=(p-1)(q-1)/d$,则剩余类环 Z_{pq} 具有关于乘法的子群 $Z_{pq}^*=\{g^s x^i \mid s=0,1,\cdots,e-1;i=0,1,\cdots,d-1\}$,这里 g 是 p 和 q 共同的本原根,x 是满足条件 $x\equiv g(\mathrm{mod}p)$,$x\equiv 1(\mathrm{mod}q)$ 的整数。称 $D_i=\{g^s x^i \mid s=0,1,\cdots,e-1\}$,$i=0,1,\cdots,d-1$ 为关于 p 和 q 的 d 阶广义割圆类。显然存在同构 $\psi: Z_{pq}\to Z_p\oplus Z_q$,$\psi(z)=(z(\mathrm{mod}p),z(\mathrm{mod}q))$,且 $Z_p\oplus Z_q=(Z_p^*,Z_q^*)\cup(Z_p^*,0)\cup(0,Z_q^*)\cup\{(0,0)\}$。Whiteman[3] 已证明 $\psi^{-1}((Z_p^*,Z_q^*))=Z_{pq}^*$。

如果定义 $\psi^{-1}((Z_p^*,0))=Q$,$\psi^{-1}((0,Z_q^*))=P$,$\psi^{-1}((0,0))=R$,则 $P=\{p,2p,\cdots,(q-1)p\}$,$Q=\{q,2q,\cdots,(p-1)q\}$,$R=\{0\}$。

引理 1[3]　(1)$a\in Z_{pq}^*\Leftrightarrow\gcd(a,pq)=1\Leftrightarrow\gcd(a,p)=\gcd(a,q)=1$;

(2)$a\in Z_{pq}^*\Leftrightarrow aP=P,aQ=Q$;

(3)$a\in P\Leftrightarrow aP=P,aQ=\{0\},a\in Q\Leftrightarrow aP=\{0\},aQ=Q$;

(4)$a\in R\Leftrightarrow aP=aQ=\{0\}$。

令 $N=pq$,则 $Z_N^*=\bigcup_{i=0}^{d-1}D_i$,$D_i\cap D_j=\varnothing$,$|D_i|=|D_j|=e$,这里 $i\neq j$,$\varnothing$ 表示空集。

令 $C_0=D_0\cup D_1\cup\cdots\cup D_{(d-2)/2}$,$C_1=D_{d/2}\cup D_{(d+2)/2}\cup\cdots\cup D_{d-1}$,$B_0=R\cup Q\cup C_0$,$B_1=P\cup C_1$,则 $B_0\cup B_1=Z_N$,$B_0\cap B_1=\varnothing$。

以 B_1 为特征集的二元序列称为 d 阶二元广义割圆序列。例如选取 $p=17$,$q=41$,则 $d=\gcd(p-1,q-1)=8$,$e=80$。由中国剩余定理可得 $g=88$ 和满足定义的 $x=411$,则

$D_i=\{411^i 88^s \mid s=0,1,\cdots,79\}$,$i=0,1,\cdots,7$.

$P=\{17,34,\cdots,680\}$, $Q=\{41,82,\cdots,656\}$.

$B_1=\{409\times 88^s,122\times 88^s,655\times 88^s,163\times 88^s;s=0,1,\cdots,79\}\cup\{17,34,\cdots,680\}$.

定义序列 $s^\infty=(s_0,s_1,\cdots,s_i,\cdots)$,$s_i$ 为

$$s_i=\begin{cases}1, & \text{如果 } i\mathrm{mod}(697)\in B_1,\\ 0, & \text{其他},\end{cases}$$

则 s^∞ 为 8 阶二元广义割圆序列。

2　引　理

本文中考虑 8 阶的情形。为了使序列易于达到平衡,应考虑分别以 B_1 和 B_0 为特征集的序列。这里先考虑前者,关于后者的结果可对称地得到。

引理 2[1]　(1)$\mathrm{ord}_N(g)=e$,这里 $\mathrm{ord}_N(g)$ 表示 g 在 Z_N 中的阶数;

(2)D_0 是 Z_N 的一个乘法子群。

引理 3[4] 如果 $a\in D_i$,则 $aD_j=D_{i+j}$。

引理 4　如果定义 $J_i=\bigcup_{4+i}^{(7+i)}D_j$,则 $J_0=C_1$,$J_4=C_0$,$aJ_i=J_{i+j}$,$\forall a\in D_j$。

证明　由引理 3 可得。

假设 $S_i(x)=\sum_{j\in J_i\cup P}x^j$,$i=0,1,\cdots,7$,则 $S_0(x)=\sum_{i\in B_1}x^i$ 是二元序列 s^∞ 的生成多项式。

假设 α 是有限域 $GF(2^m)$ 的 N 次本原根,这里 $m=\mathrm{ord}_N(2)$,$GF(2^m)$ 是多项式 x^N-1 的分裂域。

引理 5　(1)$\sum_{j\in P}\alpha^j=\sum_{j\in Q}\alpha^j=1$;

(2)$S_i(\alpha)+S_{4+i}(\alpha)=1$。

证明　(1) 由 α 的定义可知,

$0=\alpha^N-1=(\alpha^p)^q-1=(\alpha^p-1)(1+\alpha^p+\alpha^{2p}+\cdots+\alpha^{(q-1)p})$.

所以,$1+\alpha^p+\alpha^{2p}+\cdots+\alpha^{(q-1)p}=0$。对称地可得到 $1+\alpha^p+\alpha^{2q}+\cdots+\alpha^{(p-1)q}=0$,从而(1)得证。

(2) 由 α 的定义可知,

$0=\alpha^N-1=\alpha^{pq}-1=(\alpha-1)(1+\alpha+\alpha^2+\cdots+\alpha^{pq-1})$.

所以有

$$0=1+\alpha+\alpha^2+\cdots+\alpha^{pq-1}=\sum_{j\in Z_{pq}}\alpha^j=\sum_{j\in Z_{pq}^*}\alpha^j+\sum_{j\in P}\alpha^j+\sum_{j\in Q}\alpha^j+\sum_{j\in R}\alpha^j=\sum_{j\in Z_{pq}^*}\alpha^j+1.$$

这样 $\sum_{j\in Z_{pq}^*}\alpha^j=1$,则

$$S_i(\alpha)=S_{4+i}(\alpha)=\sum_{j\in P}\alpha^j+\sum_{j\in J_i}\alpha^j+\sum_{j\in P}\alpha_j+\sum_{j\in J_{4+i}}\alpha^j=\sum_{j\in Z_{pq}^*}\alpha^j=1.$$

引理 6

$$\sum_{i\in D_j}\alpha^{ai}=\begin{cases}\dfrac{p-1}{8}(\mathrm{mod}2), & \text{如果 } a\in P;\\ \dfrac{q-1}{8}(\mathrm{mod}2), & \text{如果 } a\in Q.\end{cases}$$

其中 $j=0,1,\cdots,7$。

证明　类似于文献[1]中引理 2 的证明。

引理 7　如果 $a\in P\cup Q$,那么

$$\sum_{i\in C_j}\alpha^{ai}=4\Big(\sum_{i\in D_j}\alpha^{ai}\Big)=0.$$

证明　注意到 $\alpha\in GF(2^m)$,由引理 6 可证。

引理 8

$$S_0(\alpha^a)=\begin{cases}S_0(\alpha), \text{如果 } a\in D_0;\\ S_1(\alpha), \text{如果 } a\in D_1;\\ S_2(\alpha), \text{如果 } a\in D_2;\\ S_3(\alpha), \text{如果 } a\in D_3;\\ 1+S_0(\alpha), \text{如果 } a\in D_4;\\ 1+S_1(\alpha), \text{如果 } a\in D_5;\\ 1+S_2(\alpha), \text{如果 } a\in D_6;\\ 1+S_3(\alpha), \text{如果 } a\in D_7;\\ 0, \text{如果 } a\in Q;\\ 1, \text{如果 } a\in P.\end{cases}$$

证明 由引理 3 和引理 4 可知,对于任意的 $a\in Z_N^*$,$aP=P$。如果 $a\in D_0$,则 $aJ_0=J_0$,

$$S_0(\alpha^a)=\sum_{i\in P}\alpha^{ai}+\sum_{i\in J_0}\alpha^{ai}=\sum_{i\in aP}\alpha^i+\sum_{i\in aJ_0}\alpha^i=\sum_{i\in P}\alpha^i+\sum_{i\in J_0}\alpha^i=S_0(\alpha).$$

如果 $a\in D_1$,则 $aJ_0=J_1$,

$$S_0(\alpha^a)=\sum_{i\in P}\alpha^{ai}+\sum_{i\in J_0}\alpha^{ai}=\sum_{i\in aP}\alpha^i+\sum_{i\in aJ_0}\alpha^i=\sum_{i\in P}\alpha^i+\sum_{i\in J_1}\alpha^i=S_1(\alpha).$$

同理可证,如果 $a\in D_i$,则 $S_0(\alpha^a)=S_i(\alpha)$,$i=2,3,4,5,6,7$,并且由引理 5 可知,$S_i(\alpha)=S_{4+i}(\alpha)$。

如果 $a\in P$,由引理 1 可知 $aP=P$。由引理 7 可得,$\sum_{i\in C_1}\alpha^{ai}=0$,则

$$S_0(\alpha^a)=\sum_{i\in P}\alpha^{ai}+\sum_{i\in J_0}\alpha^{ai}=\sum_{i\in aP}\alpha^i+\sum_{i\in C_1}\alpha^{ai}=\sum_{i\in P}\alpha^i=1.$$

如果 $a\in Q$,由引理 1 可知,$aP=R=\{0\}$。

$$S_0(\alpha^a)=\sum_{i\in P}\alpha^{ai}+\sum_{i\in J_0}\alpha^{ai}=\sum_{i\in aP}\alpha^i+\sum_{i\in C_1}\alpha^{ai}=(q-1)(\mathrm{mod}2)=0.$$

引理 9 如果 $2\in D_0$,则 $S_0(\alpha)\in\{0,1\}$。

证明 因为

$$S_0(\alpha^a)=\sum_{i\in P}\alpha^i+\sum_{i\in J_0}\alpha^i=1+\sum_{i\in J_0}\alpha^i,$$

如果 $2\in D_0$,

$$S_0^2(\alpha)=S_0(\alpha^2)=1+\sum_{i\in 2J_0}\alpha^i=1+\sum_{i\in J_0}\alpha^i=S_0(\alpha).$$

所以,$S_0(\alpha)\in\{0,1\}$。

如果 $2\in D_1$,则

$$S_0^2(\alpha)=S_0(\alpha^2)=1+\sum_{i\in 2J_0}\alpha^i=1+\sum_{i\in J_1}\alpha^i=S_1(\alpha).$$

$$S_1^2(\alpha)=S_1(\alpha^2)=1+\sum_{i\in 2J_1}\alpha^i=1+\sum_{i\in J_2}\alpha^i=S_2(\alpha).$$

$$S_2^2(\alpha)=S_2(\alpha^2)=1+\sum_{i\in 2J_2}\alpha^i=1+\sum_{i\in J_3}\alpha^i=S_3(\alpha).$$

$$S_3^2(\alpha)=S_3(\alpha^2)=1+\sum_{i\in 2J_3}\alpha^i=1+\sum_{i\in J_4}\alpha^i=S_4(\alpha)=1+S_0(\alpha).$$

由以上关于 $S_i(\alpha)$ 的方程组知,$S_i(\alpha)\notin\{0,1\}$,$i=0,1,2,3$。

由 α,P,Q 和 R 的定义可得

$$x^p-1=\prod_{i\in Q\cup R}(x-\alpha^i),$$

$$x^q-1=\prod_{i\in P\cup R}(x-\alpha^i).$$

如果定义 $d(x)=\prod_{i\in J_0}(x-\alpha^i)$,则

$$x^{pq}-1=\prod_{i=0}^{pq-1}(x-\alpha^i)=\frac{(x^p-1)(x^q-1)}{x-1}d(x),$$

其中 $d(x)\in GF(2)[x]$。

3 主要结果

因为 $\gcd\left(\frac{p-1}{8},\frac{q-1}{8}\right)=1$,所以 $\frac{p-1}{8}$ 和 $\frac{q-1}{8}$ 不能同时为偶数。如果 $g^s=2(\mathrm{mod}pq)$,则 $2\in D_0$。否则,$2\notin D_0$。

定理 1 如果 $g^s\neq 2(\mathrm{mod}pq)$,

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

证明 由引理 8 和引理 9 可得

$$S(\alpha^a)=\begin{cases}0, \text{如果 } a=0;\\ \neq 0, \text{如果 } a\in Z_{pq}^*;\\ 0, \text{如果 } a\in Q;\\ 1, \text{如果 } a\in P.\end{cases}$$

那么

$$\gcd(x^{pq}-1,S_0(x))=x^p-1,$$

$$m(x)=\frac{x^{pq}-1}{\gcd(x^{pq}-1,S_0(x))}=\frac{x^{pq}-1}{x^p-1},$$

$$L(s^\infty)=\deg(m(x))=pq-p=(q-1)p.$$

定义 $d_j(x)=\prod_{i\in D_j}(x-\alpha^i)$,$j=0,1,\cdots,7$。若 $2\in D_0$,由引理 3 可得 $2D_0=D_0$,

$d_0^2(x)=\prod_{i\in D_0}(x^2-\alpha^{2i})=\prod_{j\in D_0}(x^2-\alpha^j)=d_0(x^2)$.

所以,$d_0(x)\in GF(2)[x]$。类似地,$d_i(x)\in GF(2)[x],i=0,1,\cdots,7$。从而

$$x^{pq}-1=\frac{(x^p-1)(x^q-1)\prod_{i=1}^{7}d_i(x)}{y-1},$$

且 $\deg(d_i(x))=|D_i|=e,i=0,1,\cdots,7$。

显然 $d_i(x)$ 依赖于 α 的定义。由引理 8 可知,正好有 4 个 $S_i(x)$ 为 0。所以选择 α 使得 $S_{i_j}(\alpha)=0$,这里 $i_j\in\Lambda,\Lambda=\{i_j\mid j=0,1,2,3\}\subset\{0,1,\cdots,7\}=I$。

定理 2　如果存在 s 使得 $g^s=2(\mathrm{mod}pq)$,则

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

$$m(x)=\frac{x^{pq}-1}{(x^p-1)\prod_{i\in\Lambda}d_i(x)}(\text{根据 }\alpha\text{ 的选取}).$$

证明　因为 $g^s=2(\mathrm{mod}pq)$ 意味着 $2\in D_0$,由引理 8、引理 9 和 α 的选择可得

$$S(\alpha^a)=\begin{cases}0,\text{ 如果 }a\in\bigcup_{i\in\Lambda}D_i;\\1,\text{ 如果 }a\in\bigcup_{i\in I-\Lambda}D_i;\\0,\text{ 如果 }a\in Q;\\1,\text{ 如果 }a\in P;\end{cases}$$

则

$$\gcd(x^{pq}-1,S_0(x))=(x^p-1)\prod_{i\in\Lambda}d_i(x),$$

$$m(x)=\frac{x^{pq}-1}{\gcd(x^{pq}-1,S_0(x))}=\frac{x^{pq}-1}{(x^p-1)\prod_{i\in\Lambda}d_i(x)},$$

$$L(s^\infty)=\deg(m(x))=pq-p-4e=pq-p-\frac{(q-1)(p-1)}{2}=\frac{(q-1)(p+1)}{2}.$$

4　问题和建议

8 阶广义割圆序列具有和 4 阶类似的线性复杂度表示,它们和 2 阶的一样都可取得足够大的值。本文中的主要结果是在 $2\in D_0$ 和 $2\notin D_0$ 两种情形下给出的,但是没能像文献[1]那样找到进一步刻画这两种情形的方法。另外,若考虑这类序列的密码学应用,还应该讨论它的自相关和互相关性质。

参考文献:

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

[2] BAI Enjian, FU Xiaotong, 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.

[3] STORER T. Cyclotomy and difference set[M]. Chicago:Markham, 1967.

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

(编辑　修荣荣)

中国石油大学(华东)两科研成果达到国际领先水平

近日,由中国石油大学(华东)机电工程学院博士生导师刘永红教授主持完成的"复合型腔割缝筛管及其防砂技术研究"和"非导电工程陶瓷电火花加工技术研究"两科研项目通过教育部鉴定。鉴定委员会一致认为,两科研项目核心技术均达到国际同类技术的领先水平,并填补了国内外空白。

针对目前国内外常用的筛管割缝技术存在加工成本高、加工质量较差以及加工成品容易造成砂粒堵塞,降低抽油效果等问题,刘教授等创造性地提出新型复合缝腔割缝筛管这一构想,并研究开发出了复合型腔割缝筛管及其相应的等离子加工技术。用这种技术研制出的复合型腔割缝筛管具有"自洁"作用好、流阻小、强度高和使用寿命长等优点,技术含量高,创新性明显。目前,经该技术加工出的复合型腔割缝筛管已在国外的哈萨克斯坦油田、国内的胜利、冀东、中原、青海、新疆等油田得到推广应用,取得了良好的社会和经济效益。

针对现有非导电工程陶瓷加工技术存在效率低、成本高,且难以满足高精度和高表面质量的加工要求等缺陷,刘永红教授等科研人员突破了传统的机械磨削和电解电火花机械复合磨削方法,创造性地提出了利用导电复合磨轮与紧贴非导电工程陶瓷工件表面作自动伺服进给运动的薄片电极间的放电作用实现电火花磨削的新技术。该加工技术具有生产率高、精度高、表面质量好、磨削力小和对环境无污染等优点,具备了批量生产的条件,并具有广阔的市场前景。

(摘自中国石油大学(华东)校园网)