第 36 卷 第 4 期 计 算 机 工 程 2010 年 2 月
Vol.36 No.4 Computer Engineering February 2010
·安全技术· 文章编号：1000—3428(2010)04—0150—02 文献标识码：A 中图分类号：TN918.4

6 阶 W-广义割圆序列的线性复杂度

李淑清[1]，闫统江[2]
(1. 中国石油大学计算机与通信工程学院，东营 257061；2. 中国石油大学数学与计算科学学院，东营 257061)

摘 要：在所有周期为 pq 的 2^k 阶 W-广义割圆序列的线性复杂度都已经得到准确计算的基础上，考虑周期为 pq 的 6 阶 W-广义割圆序列的线性复杂度。结果表明这类序列的线性复杂度的下界是 $(p-1)(q-1)/2$。从密码学的角度看，多数的二元 W-广义割圆序列具有良好的线性复杂度性质，以它们做密钥流序列的密码系统具有很强的抵抗 B-M 算法攻击的能力。
关键词：流密码；割圆类；割圆序列；线性复杂度

Linear Complexity of Sextic Whiteman Generalized Cyclotomic Sequences

LI Shu-qing[1], YAN Tong-jiang[2]
(1. College of Computer and Communication Engineering, China University of Petroleum, Dongying 257061;
2. College of Mathematics and Computational Science, China University of Petroleum, Dongying 257061)

【Abstract】 This paper considers the linear complexity of binary sextic Whiteman generalized cyclotomic sequences with period pq. Results show that the lower bound of their linear complexity is $(p-1)(q-1)/2$. From the viewpoint of stream cipher cryptosystems, almost all these sequences have good linear complexity. They can resist attacks from the application of the Berlekamp-Massey algorithm.
【Key words】 stream cipher; cyclotomic class; cyclotomic sequences; linear complexity

1 概述

具有特定性质的伪随机序列在数字模拟、软件测试、全球定位系统、CDMA，尤其是流密码中有着广泛的应用。度量序列伪随机性的一个重要指标是它的线性复杂度[1]。如果周期为 N 的伪随机序列 $s^N=(s_0,s_1,\cdots,s_{N-1})$ 满足反馈函数

$$s_j=c_1s_{j-1}+c_2s_{j-2}+\cdots+c_Ls_{j-L},\ j>L$$

s^N 称为线性反馈序列，最小的 L 称为 s^N 的线性复杂度，记为 $L(s^N)$，它也是生成 s^N 的最短线性反馈移位寄存器的级数。根据 B-M 算法，如果 $L(s^N)>N/2$，则认为 s^∞ 具有好的线性复杂度性质。所以，考查一簇序列的线性复杂度，重点是考察其线性复杂度的下界。序列 $s^N=(s_0,s_1,\cdots,s_{N-1})$ 的生成函数为 $S^N(x)=\sum_{i=0}^{N-1}s_ix^i$，并且

$$L(s^\infty)=N-\deg(\gcd(x^N-1,\ S^N(x))) \tag{1}$$

本文中 $AB=\{xy|x\in A,y\in B\}$，$xB=\{xy|y\in B\}$，$\mathrm{ord}_N(x)$ 表示 x 模 N 的阶。

2 二元 W-广义割圆序列的定义和性质

令 p 和 q 是 2 个不同的奇素数，$N=pq, 2n=\gcd(p-1,q-1), e=(p-1)(q-1)/2n, p<q$，则剩余类环 Z_N 具有乘法子群[2] $Z_N^*=\{g^sx^i:s=0,1,\cdots,e-1;\ \ i=0,1,\cdots,2n\text{-}1\}$，其中，$g$ 是 p 和 q 共同的本原根；x 是满足条件 $x\equiv g \bmod p,\ \ x\equiv 1 \bmod q$ 的正整数。

定义 1 集合 $D_i=\{g^tx^i:t=0,1,\cdots,e-1\}, i=0,1,\cdots,2n-1$ 称为关于 p 和 q 的 $2n$ 阶W-广义割圆类[3-4]。

定义 2 定义集合表示

$$P=\{p,2p,\cdots,(q-1)p\}, Q=\{q,2q,\cdots,(p-1)q\},\ R=\{0\},$$

$$B_0=\bigcup_{i=0}^{\frac{n}{2}-1}D_i,\ B_1=\bigcup_{i=\frac{n}{2}}^{n-1}D_i,\ C_0=R\cup Q\cup B_0,\ C_1=P\cup B_1$$

阶为 $2n$ 的第 1 类二元 W-广义割圆序列 $s^\infty=(s_0,s_1,\cdots,s_i,\cdots)$ 定义为 $s_i=\begin{cases}0 & i\in C_0\\ 1 & i\in C_1\end{cases}$。文献[2-3]给出了第 1 类 2 阶 W-广义割圆序列的线性复杂度和自相关值。文献[4-5]给出了 4 阶情形的线性复杂度和自相关函数值的分布。文献[6]讨论了 8 阶情形的线性复杂度，给出了所有 $2^k(k>1)$ 阶情形的线性复杂度。目前给出的所有结果都表明，这类序列拥有比较好的密码学指标，例如它们的线性复杂度都大于半个周期，而相关函数值的分布也比较平坦。下面将讨论 6 阶(即 $2n=6$)情形的线性复杂度。

如果将第 1 类二元 W-广义割圆序列的定义中的 $B_0=\bigcup_{i=0}^{\frac{n}{2}-1}D_i$，$B_1=\bigcup_{i=\frac{n}{2}}^{n-1}D_i$ 改为 $B_0=\bigcup_{i=0}^{n-1}D_{2i}$，$B_1=\bigcup_{i=0}^{n-1}D_{2i+1}$，其他不做任何改变，则得到第 2 类二元 W-广义割圆序列。目前已经证明这类序列就是修改的 Jacobi 序列，这类序列的密码学性质已经讨论得比较清楚，见文献[7]。值得注意的是这类序列包含了著名的孪生素数序列。只在 p 和 q 是孪生素数时，这 2 类序列才能达到符号平衡。为了在一般情形下也能够满足符号平衡性质，文献[8-9]对第 1 类 2 阶 W-广义割圆序列的定义作了修改，得到了一类新的二元 W-广义割圆序列。本文给出的新的研究思路对研究这类广义割圆序列也非常有用。

为了讨论第 1 类 6 阶 W-广义割圆序列的线性复杂度，需

基金项目：国家自然科学基金资助项目(60503009)；中国石油大学(华东)博士科研基金资助项目(y080806)；青年教师基础科研基金资助项目(Y080803)
作者简介：李淑清(1973－)，女，硕士研究生，主研方向：通信安全；闫统江，副教授、博士
收稿日期：2009-08-09 **E-mail：**yantoji@163.com

要下面的引理 1~引理 5。

首先，由 P,Q 和 R 的定义可得

引理 1 在剩余类环 Z_N 中，$P^2=P,\ PQ=QP=R,\ D_jP=P,\ D_jQ=Q,\ D_jD_i=D_{i+j},\ i,j=0,1,\cdots,5$。

假设二元域 GF(2) 上的多项式 x^N-1 的分裂域是 GF(2^m)，$m=\mathrm{ord}_N(2)$。令 α 表示有限域 GF(2^m) 的 N 次本原单位根。于是，1，α，$\alpha^2,\cdots,\alpha^{N-1}$ 就是多项式 x^N-1 在 GF(2^m) 内的 N 个不同的根，根据式(1)可知，线性复杂度 $L(s^N)=N-\left|\{k\,|\,S^N(\alpha^k)=0,k\in Z_N\}\right|$，也就是说，使 $S^N(\alpha^k)=0$ 的 k 越少，序列的线性复杂度 $L(s^N)$ 就越大。

引理 2 在有限域 GF(2^m) 中，对于选定的 α ：

(1) $\sum_{j\in P}\alpha^j=\sum_{j\in Q}\alpha^j=\sum_{j\in Z_N/R}\alpha^j=1$

(2) $\sum_{j\in Z_N^*}\alpha^j=1$

证明：引理 2 的(1)可由以下事实证明：

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

而由(1)可得 $\sum_{j\in Z_N^*}\alpha^j=\sum_{j\in Z_N/R}\alpha^j-\sum_{j\in P}\alpha^j-\sum_{j\in Q}\alpha^j=1$。所以，(2)得证。

引理 3[3] $\mathrm{ord}_N(g)=e$

引理 4 $\sum_{i\in D_j}\alpha^{ki}=\begin{cases}\frac{p-1}{6}\bmod 2 & k\in P\\ \frac{q-1}{6}\bmod 2 & k\in Q\end{cases}\quad j=0,1,\cdots,5$

证明：对于 $k\in Q$，由引理 3 和 g 与 D_j 的定义可得

$$D_j \bmod p=\{g^tx^j \bmod p:t=0,1,\cdots,e-1\}=$$
$$\{g^{t+j} \bmod p:t=0,1,\cdots,e-1\}$$

当 t 跑遍集合 $\{0,1,\cdots,e-1\}$ 一次，$g^tx^j \bmod p$ 取集合 $\{1,2,\cdots,p-1\}$ 每个元素 $\frac{q-1}{6}$ 次。由引理 2 可得：$\sum_{i\in D_j}\alpha^{ki}=[\frac{q-1}{6}\bmod 2]\sum_{i\in Q}\alpha^i=\frac{q-1}{6}\bmod 2$。其余部分同理可证。

令 $S_j(\mathrm{x})=\sum_{i\in D_j\cup D_{j+1}\cup D_{j+2}}x^i,\ j=0,1,\cdots,5$，则 $S_j(x)\in \mathrm{GF}(2)[x]$，$S_0(x)$ 是 s^N 的生成函数，并且它满足方程

$$S_0(\alpha^0)=S_0(1)=(q-1+\frac{(p-1)(q-1)}{2})1=0 \qquad (2)$$

引理 5 $S_0(\alpha^k)=\begin{cases}S_0(\alpha) & k\in D_0\\ S_1(\alpha) & k\in D_1\\ S_2(\alpha) & k\in D_2\\ 1+S_0(\alpha) & k\in D_3\\ 1+S_1(\alpha) & k\in D_4\\ 1+S_2(\alpha) & k\in D_5\\ 1+\frac{p-1}{6}\bmod 2 & k\in P\\ \frac{q-1}{6}\bmod 2 & k\in Q\end{cases}$

证明：由引理1和引理2可知，如果 $k\in D_0$，$S_0(\alpha^k)=\sum_{i\in P}\alpha^{ki}+\sum_{i\in D_0\cup D_1\cup D_2}\alpha^{ki}=\sum_{i\in P}\alpha^i+\sum_{i\in k(D_0\cup D_1\cup D_2)}\alpha^i=S_0(\alpha)$。

如果 $k\in D_1$，$S_0(\alpha^k)=\sum_{i\in P}\alpha^{ki}+\sum_{i\in D_0\cup D_1\cup D_2}\alpha^{ki}=\sum_{i\in kP}\alpha^i+\sum_{i\in k(D_0\cup D_1\cup D_2)}\alpha^i+\sum_{i\in D_1\cup D_2\cup D_3}\alpha^i=S_1(\alpha)$。

如果 $k\in D_2$，$S_0(\alpha^k)=\sum_{i\in P}\alpha^{ki}+\sum_{i\in D_0\cup D_1\cup D_2}\alpha^{ki}=\sum_{i\in kP}\alpha^i+\sum_{i\in k(D_0\cup D_1\cup D_2)}\alpha^i=\sum_{i\in P}\alpha^i+\sum_{i\in D_2\cup D_3\cup D_4}\alpha^i=S_2(\alpha)$。

如果 $k\in D_3$，$S_0(\alpha^k)=\sum_{i\in P}\alpha^{ki}+\sum_{i\in D_0\cup D_1\cup D_2}\alpha^{ki}=\sum_{i\in kP}\alpha^i+\sum_{i\in k(D_0\cup D_1\cup D_2)}\alpha^i=\sum_{i\in D_3\cup D_4\cup D_5}\alpha^i=1+S_0(\alpha)$。

如果 $k\in D_4$，$S_0(\alpha^k)=\sum_{i\in P}\alpha^{ki}+\sum_{i\in D_0\cup D_1\cup D_2}\alpha^{ki}=\sum_{i\in kP}\alpha^i+\sum_{i\in k(D_0\cup D_1\cup D_2)}\alpha^i=\sum_{i\in P}\alpha^i+\sum_{i\in D_4\cup D_0}\alpha^i=1+S_1(\alpha)$。

如果 $k\in D_5$，$S_0(\alpha^k)=\sum_{i\in P}\alpha^{ki}+\sum_{i\in D_0\cup D_1\cup D_2}\alpha^{ki}=\sum_{i\in kP}\alpha^i+\sum_{i\in k(D_0\cup D_1\cup D_2)}\alpha^i=\sum_{i\in P}\alpha^i+\sum_{i\in D_5\cup D_0\cup D_1}\alpha^i=1+S_2(\alpha)$。

由引理1、引理2和引理4知，如果 $k\in P$，$S_0(\alpha^k)=\sum_{i\in P}\alpha^{ki}+\sum_{i\in D_0\cup D_1\cup D_2}\alpha^{ki}=\sum_{i\in P}\alpha^i+\sum_{i\in D_0\cup D_1\cup D_2}\alpha^{ki}=1+\frac{p-1}{6}\bmod 2$。

如果 $k\in Q$，因为 $q-1$ 是 6 的倍数，所以是个偶数，从而 $S_0(\alpha^k)=\sum_{i\in P}\alpha^{ki}+\sum_{i\in D_0\cup D_1\cup D_2}\alpha^{ki}=\sum_{i\in P}1+\sum_{i\in D_0\cup D_1\cup D_2}\alpha^{ki}=\frac{q-1}{6}\bmod 2$。

3 主要结论

定理 1 如果 $\frac{p-1}{6}$ 是偶数，$\frac{q-1}{6}$ 是奇数，则 6 阶 W-广义割圆序列的线性复杂度的下界是 $L(s^\infty)=\frac{pq+p+q-1}{2}$，即这时的 6 阶 W-广义割圆序列总具有不小于半个周期的线性复杂度。

证明：根据引理 5，当 k 跑遍 Z_{pq}^* 时，至多有半数的 $S_0(\alpha^k)$ 为 0，这时 $\left|\{k\,|\,S_0(\alpha^k)=0,k\in Z_{pq}^*\}\right|=\frac{(p-1)(q-1)}{2}$。

如果 $\frac{p-1}{6}$ 是偶数，$\frac{q-1}{6}$ 是奇数，根据引理 5，$S_0(\alpha^k)=1\neq 0,\forall k\in P\cup Q$，即 $\left|\{k\,|\,S_0(\alpha^k)=0,k\in P\cup Q\}\right|=0$。

再考虑式(2)，可得这时线性复杂度的下界为

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

定理 2 当 $\frac{p-1}{6}$ 和 $\frac{q-1}{6}$ 都是奇数时，6 阶 W-广义割圆序列的线性复杂度的下界是 $L(s^\infty)=\frac{pq+p-q+1}{2}$。

证明：根据引理 5，当 k 跑遍 Z_{pq}^* 时，至多有半数的 $S_0(\alpha^k)$ 为 0，这时 $\left|\{k\,|\,S_0(\alpha^k)=0,k\in Z_{pq}^*\}\right|=\frac{(p-1)(q-1)}{2}$。

如果 $\frac{p-1}{6}$ 和 $\frac{q-1}{6}$ 都是奇数，根据引理 5，$S_0(\alpha^k)=0,\ \forall k\in P;S_0(\alpha^k)=1,\forall k\in Q$，即 $\left|\{k\,|\,S_0(\alpha^k)=0,k\in P\cup Q\}\right|=q-1$。

再考虑式(2)，可得这时线性复杂度的下界为

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

定理 3 如果 $\frac{p-1}{6}$ 是奇数，$\frac{q-1}{6}$ 是偶数，6 阶 W-广义割圆序列的线性复杂度的下界为 $L(s^\infty)=\frac{(p-1)(q-1)}{2}$，这也是所有 6 阶 W-广义割圆序列的线性复杂度的下界。

证明：根据引理 5，当 k 跑遍 Z_{pq}^* 时，至多有半数的 $S_0(\alpha^k)$ 为 0，这时 $\left|\{k\,|\,S_0(\alpha^k)=0,k\in Z_{pq}^*\}\right|=\frac{(p-1)(q-1)}{2}$。

(下转第 154 页)