二元 W-广义割圆序列的线性复杂度

闫统江[1,2]，范 凯[1]，杜小妮[1,3]，肖国镇[1]

(1. 西安电子科技大学 综合业务网理论与关键技术国家重点实验室，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；3. 西北师范大学 数学与信息科学学院，甘肃 兰州 730070)

摘要：周期为 pq 上的 2 阶 W- 广义割圆序列的线性复杂度和极小多项式是丁存生于 1998 年给出的. 采用有限域上的多项式理论，考虑了任意的 W- 广义割圆序列的线性复杂度和极小多项式，并完全解决了这一问题. 结果表明这类序列的线性复杂度的上界和下界分别是 $pq-1$ 和 $(p-1)(q-1)/2$. 从密码学的角度看，多数的二元 W- 广义割圆序列具有很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；极小多项式

中图分类号：TN918.4 **文献标识码**：A **文章编号**：1001-2400(2006)04-0617-05

Linear complexity of binary whiteman generalized cyclotomic sequences

YAN Tong-jiang[1,2], *FAN Kai*[1], *DU Xiao-ni*[1,3], *XIAO Guo-zhen*[1]

(1. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China; 2. College of Mathematics and Computer Science, China Univ. of Petroleum, Dongying 257061, China; 3. Math. and Inform. Sci., Northwest Normal Univ., Lanzhou 730070, China)

Abstract: Based on the polynomial theory on a Galois field, the author presents linear complexity and minimal polynomials of all binary Whiteman generalized cyclotomic sequences with the period pq. The results obtained show that the upper bound and the lower bound of their linear complexity are $pq-1$ and $(p-1)(q-1)/2$ respectively. From the viewpoint of stream cipher cryptosystems, almost all these sequences have good linear complexity. They can resist the attacks from the application of the Berlekamp-Massey algorithm.

Key Words: stream cipher; cyclotomic class; cyclotomic sequence; linear complexity; minimal polynomial

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就是它的线性复杂度[1]. 如果序列 $s^\infty=(s_0,s_1,\cdots,s_i,\cdots)$ 满足反馈函数 $s_j=c_1s_{j-1}+c_2s_{j-2}+\cdots+c_Ls_{j-L}, j>L$，则 s^∞ 就称为线性反馈序列，最小的 L 称为 s^∞ 的线性复杂度，记为 $L(s^\infty)$，它也是生成 s^∞ 的最短线性反馈移位寄存器的级数. 根据 B-M 算法，如果 $L(s^\infty)>N/2$(N 是 s^∞ 的周期)，则认为 s^∞ 具有好的线性复杂度性质. 序列 s^∞ 和 $s^N=(s_0,s_1,\cdots,s_{N-1})$ 的生成函数分别为 $S(x)=\sum_{i=0}^{\infty}s_ix^i$ 和 $S^N(x)=\sum_{i=0}^{N-1}s_ix^i$. $m(x)=(1-x^N)/\gcd(S^N(x),1-x^N)$ 称为 s^∞ 的极小多项式，并且

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

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

收稿日期：2005-10-31

基金项目：973 项目(G1999035804)

作者简介：闫统江(1973-)，男，中国石油大学讲师，西安电子科技大学博士研究生.

1 二元 W-广义割圆序列的定义和性质

令 p 和 q 是两个不同的奇素数,$N=pq$,$2n=\gcd(p-1,q-1)$,$e=(p-1)(q-1)/(2n)$,$p<q$. 则剩余类环 Z_N 具有乘法子群 $Z_N^*=\{g^s x^i: s=0,1,\cdots,e-1; i=0,1,\cdots,2n-1\}$,这里 g 是 p 和 q 共同的本原根,x 是满足条件 $x\equiv g \bmod p$,$x\equiv 1 \bmod q$ 的正整数.

$$D_i=\{g^t x^i: t=0,1,\cdots,e-1\}\quad,\quad i=0,1,\cdots,2n-1\quad,$$

D_i 称为关于 p 和 q 的 $2n$ 阶 W- 广义割圆类[2]. 令

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

$$B_0=\bigcup_{i=0}^{n-1} D_{2i}\quad,\quad B_1=\bigcup_{i=0}^{n-1} D_{2i+1}\quad,\quad C_0=R\cup Q\cup B_0\quad,\quad C_1=P\cup B_1\quad.$$

二元 W- 广义割圆序列 $s^\infty=(s_0,s_1,\cdots,s_i,\cdots)$ 定义为 $s_i=\begin{cases}0 & i\in C_0\\ 1 & i\in C_1\end{cases}$.

丁存生给出的 2 阶 W- 广义割圆序列的线性复杂度[3] 和自相关值[4] 表明,这类序列具有很好的密码学性质. 现在考虑任意的大于 2 阶的 W- 广义割圆序列.

由 P,Q 和 R 的定义可得以下引理.

引理 1 在剩余类环 Z_N 中,$P^2=P$,$PQ=QP=R$,$D_jP=P$,$D_jQ=Q$,$D_j D_i=D_{i+j}$,这里 $i,j=0,1,\cdots,2n-1$.

令 α 表示有限域 $\mathrm{GF}(2^m)$ 的 N 次本原单位根,这里 $\mathrm{GF}(2^m)$ 是 x^N-1 的分裂域,$m=\mathrm{ord}_N(2)$.

引理 2 在有限域 $\mathrm{GF}(2^m)$ 中,对于选定的 α,$\sum_{j\in P}\alpha^j=\sum_{j\in Q}\alpha^j=\sum_{j\in Z_N/R}\alpha^j=1$.

证明 可由以下事实证明

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

引理 3 $\mathrm{ord}_N(g)=e$.[3]

引理 4 $\sum_{i\in D_j}\alpha^{ki}=\begin{cases}((p-1)/(2n)) \bmod 2 & k\in P\\ ((q-1)/(2n)) \bmod 2 & k\in Q\end{cases}$, $j=0,1,\cdots,2n-1$.

证明 对于 $k\in Q$,由引理 3 和 g 与 D_j 的定义,

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

当 t 跑遍集合 $\{0,1,\cdots,e-1\}$ 一次,$g^t x^j \bmod p$ 取集合 $\{1,\cdots,p-1\}$ 每个元素 $(q-1)/(2n)$ 次. 由引理 2 得,$\sum_{i\in D_j}\alpha^{ki}=\left[\frac{q-1}{2n} \bmod 2\right]\sum_{i\in Q}\alpha^i=\frac{q-1}{2n} \bmod 2$. 其余部分同理可证.

令 $S(x)=\sum_{i\in C_1}x^i$,则 $S(x)$ 是 s^∞ 的生成多项式.

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

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 由引理 1 和引理 2,如果 $k\in B_0$,

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

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

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

证明 既然 $S(x)\in \mathrm{GF}(2)[x]$,由引理 6,如果 $2\in B_0$,$S(\alpha)^2=S(\alpha^2)=S(\alpha)$,则 $S(\alpha)\in\{0,1\}$. 如果 $2\notin B_0$,即 $2\in B_1$,$S(\alpha)^2=S(\alpha^2)=1+S(\alpha)$. 于是 $S(\alpha)\notin\{0,1\}$.

引理 7　$S(\alpha^k)=\begin{cases}1+n(p-1)/(2n) \bmod 2 & , \quad k\in P \\ n(q-1)/(2n) \bmod 2 & , \quad k\in Q\end{cases}$.

证明　由引理 1,引理 2 和引理 4,如果 $k\in P$,

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

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

2　主要结论

α^p 和 α^q 分别是多项式 x^q-1 和 x^p-1 的本原 p 次和 q 次单位根,并且

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

定义 $d(x)=\prod_{i\in Z_N^*}(x-\alpha^i)$,由于 $m\mid\varphi(N)=(p-1)(q-1)$,$\deg(d(x))=\varphi(N)$,则 $d(x)\in \mathrm{GF}(2)[x]$. 定义 $d_j(x)=\prod_{i\in B_j}(x-\alpha^i)$,$j=0,1$. 如果 $2\in B_0$,则 $2B_0=B_0$,$2B_1=B_1$. 于是

$$d_j(x)^2=\prod_{i\in B_j}(x^2-\alpha^{2i})=\prod_{i\in B_j}(x^2-\alpha^i)=d_j(x^2) .$$

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

根据引理 6,如果 $2\in B_0$,$S(\alpha)$ 和 $1+S(\alpha)$ 二者有且仅有一个为 0. 选择适当的 α 使得 $S(\alpha)=0$,则有下列的定理.

定理 1　如果 $p\equiv q\equiv 1 \bmod 4$,那么

$$L(s^\infty)=\begin{cases}\dfrac{(p+1)(q-1)}{2} & , \quad 2\in B_0 \\ (q-1)\,p & , \quad 2\in B_1\end{cases} , \quad m(x)=\begin{cases}\dfrac{x^{pq}-1}{(x^p-1)\,d_0(x)} & , \quad 2\in B_0 \\ \dfrac{x^{pq}-1}{x^p-1} & , \quad 2\in B_1\end{cases} .$$

证明　如果 $p\equiv q\equiv 1 \bmod 4$,则 $4\mid 2n$,即 $2\mid n$. 根据引理 7,$S(\alpha^k)=\begin{cases}1 \bmod 2 & , \quad k\in P \\ 0 \bmod 2 & , \quad k\in Q\end{cases}$,若 $2\in B_0$,根据(1)和(2),$L(s^\infty)=pq-1-(p-1)-(p-1)(q-1)/2=(p+1)(q-1)/2$. 由 α 的选取,$\gcd(S(x),x^N-1)=(x^p-1)\,d_0(x)$,从而 $m(x)=(x^{pq}-1)/(x^p-1)\,d_0(x)$. 若 $2\in B_1$,根据引理 6,$S(\alpha),1+S(\alpha)\notin\{0,1\}$. 根据(1)和(2),$L(s^\infty)=pq-1-(p-1)=p(q-1)$. 显然 $\gcd(S(x),x^N-1)=x^p-1$,从而 $m(x)=(x^{pq}-1)/(x^p-1)$.

定理 2　如果 $p\equiv 3 \bmod 4$,$q\equiv 1 \bmod 4$,则

$$L(s^\infty)=\begin{cases}\dfrac{(p-1)(q-1)}{2} & , \quad 2\in B_0 \\ (p-1)(q-1) & , \quad 2\in B_1\end{cases} , \quad m(x)=\begin{cases}\dfrac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)\,d_0(x)} & , \quad 2\in B_0 \\ \dfrac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)} & , \quad 2\in B_1\end{cases} .$$

证明　如果 $p\equiv 3 \bmod 4$,$q\equiv 1 \bmod 4$,则 n 和 $(p-1)/(2n)$ 是奇数,$(q-1)/(2n)$ 是偶数. 根据引理 7,$S(\alpha^k)=0$,$k\in P\cup Q$. 若 $2\in B_0$,由(1)和(2)得 $L(s^\infty)=(p-1)(q-1)/2$. 根据 α 的选取,$\gcd(S(x),x^{pq}-1)=(x^p-1)(x^q-1)\,d_0(x)/(x-1)$. 从而 $m(x)=(x^{pq}-1)(x-1)/(x^p-1)(x^q-1)\,d_0(x)$. 倘若 $2\in B_1$,则 $L(s^\infty)=(p-1)(q-1)$. 并且 $\gcd(S(x),x^{pq}-1)=(x^p-1)(x^q-1)/(x-1)$. 从而 $m(x)=(x^{pq}-1)(x-1)/(x^p-1)(x^q-1)$.

定理 3　如果 $p\equiv 1 \bmod 4$,$q=3 \bmod 4$,那么

$$L(s^\infty)=\begin{cases}\dfrac{pq+p+q-3}{2} & , \quad 2\in B_0 \\ pq-1 & , \quad 2\in B_1\end{cases} , \quad m(x)=\begin{cases}\dfrac{x^{pq}-1}{(x-1)\,d_0(x)} & , \quad 2\in B_0 \\ \dfrac{x^{pq}-1}{x-1} & , \quad 2\in B_1\end{cases} .$$

证明 可依照定理 2 的证明过程类似地得到.

定理 4 如果 $p \equiv q \equiv 3 \bmod 4$, 那么

$$L(s^{\infty}) = \begin{cases} \dfrac{(p-1)(q-1)}{2}, & 2 \in B_0, \\ (p-1)q, & 2 \in B_1, \end{cases} \quad m(x) = \begin{cases} \dfrac{x^{pq}-1}{(x^q-1)\,d_0(x)}, & 2 \in B_0, \\ \dfrac{x^{pq}-1}{x^q-1}, & 2 \in B_1. \end{cases}$$

证明 如果 $p \equiv q \equiv 3 \bmod 4$, 则 n, $(p-1)/(2n)$ 和 $(q-1)/(2n)$ 都是奇数. 根据引理 7, $S(\alpha^k) = \begin{cases} 0 \bmod 2, & k \in P, \\ 1 \bmod 2, & k \in Q. \end{cases}$ 于是定理 4 的证明可根据定理 1 的证明对称地得到.

定理 5 $2 \in B_0$ 当且仅当 $p \equiv \pm 1 \bmod 8, q \equiv \pm 1 \bmod 8$; 若 $p \equiv \pm 3 \bmod 8, q \equiv \pm 3 \bmod 8$.

证明 既然 $2 \in Z_{pq}^*$, 则存在整数 t 和 i 使得 $2 = g^t x^i, 0 \leqslant t \leqslant e-1, 0 \leqslant i \leqslant 2n-1$. 同时

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

必要性 倘若 $2 \in B_0$, 则 i 是偶数. 如果 t 是偶数, 则 2 是 p 和 q 的二次剩余, 所以 $p \equiv \pm 1 \bmod 8, q \equiv \pm 1 \bmod 8$. 如果 t 是奇数, 则 2 是 p 和 q 的二次非剩余. 所以 $p \equiv \pm 3 \bmod 8, q \equiv \pm 3 \bmod 8$.

充分性 倘若 $2 \notin B_0$, 即 $2 \in B_1$, 则 i 是奇数. 如果 t 是偶数, 则 2 是 p 的二次非剩余和 q 的二次剩余. 所以, $p \equiv \pm 3 \bmod 8, q \equiv \pm 1 \bmod 8$. 如果 t 是奇数, 则 2 是 p 的二次剩余和 q 的二次非剩余, 所以 $p \equiv \pm 1 \bmod 8, q \equiv \pm 3 \bmod 8$.

定理 6 环 Z_{pq} 上的二元 W- 广义割圆序列的线性复杂度和极小多项式分别如表 1 和表 2 所示.

表 1 线性复杂度

p	q			
	$-3 \bmod 8$	$-1 \bmod 8$	$+1 \bmod 8$	$+3 \bmod 8$
$-3 \bmod 8$	$\dfrac{(p+1)(q-1)}{2}$	$pq-1$	$p(q-1)$	$\dfrac{pq+p+q-3}{2}$
$-1 \bmod 8$	$(p-1)(q-1)$	$\dfrac{(p-1)(q+1)}{2}$	$\dfrac{(p-1)(q-1)}{2}$	$(p-1)q$
$+1 \bmod 8$	$p(q-1)$	$\dfrac{pq+p+q-3}{2}$	$\dfrac{(p+1)(q-1)}{2}$	$pq-1$
$+3 \bmod 8$	$\dfrac{(p-1)(q-1)}{2}$	$(p-1)q$	$(p-1)(q-1)$	$\dfrac{(p-1)(q+1)}{2}$

表 2 极小多项式

p	q			
	$-3 \bmod 8$	$-1 \bmod 8$	$+1 \bmod 8$	$+3 \bmod 8$
$-3 \bmod 8$	$\dfrac{x^{pq}-1}{(x^p-1)\,d_0(x)}$	$\dfrac{x^{pq}-1}{x-1}$	$\dfrac{x^{pq}-1}{x^p-1}$	$\dfrac{x^{pq}-1}{(x^p-1)\,d_0(x)}$
$-1 \bmod 8$	$\dfrac{x^{pq}-1}{(x^p-1)(x^q-1)}$	$\dfrac{x^{pq}-1}{(x^q-1)\,d_0(x)}$	$\dfrac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)\,d_0(x)}$	$\dfrac{x^{pq}-1}{x^q-1}$
$+1 \bmod 8$	$\dfrac{x^{pq}-1}{x^p-1}$	$\dfrac{x^{pq}-1}{(x-1)\,d_0(x)}$	$\dfrac{x^{pq}-1}{(x^p-1)\,d_0(x)}$	$\dfrac{x^{pq}-1}{x-1}$
$+3 \bmod 8$	$\dfrac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)\,d_0(x)}$	$\dfrac{x^{pq}-1}{x^q-1}$	$\dfrac{x^{pq}-1}{(x^p-1)(x^q-1)}$	$\dfrac{x^{pq}-1}{(x^q-1)\,d_0(x)}$

证明 仅以 $p \equiv q \equiv -3 \bmod 8$ 的情形为例. 根据定理 5, 此时 $2 \in B_0$. 又因为 $p \equiv q \equiv 1 \bmod 4$, 由定理 1 可得 $L(s^{\infty}) = (p+1)(q-1)/2, m(x) = (x^{pq}-1)/(x^p-1)\,d_0(x)$. 其他情形同理可证.

3 结 束 语

笔者考虑了任意的二元 W- 广义割圆序列的线性复杂度. 主要定理表明这类序列的线性复杂度在满足条件 $p \equiv -3 \bmod 8, q \equiv -1 \bmod 8$ 或者 $p \equiv 1 \bmod 8, q \equiv 3 \bmod 8$ 时取得上界 $pq-1$. 其线性复杂度的下界为 $(p-1)(q-1)/2$. 由于用作密钥流的序列通常具有较大的周期, 所以可认为这里大多数的二元 W- 广义割圆序列线性复杂度是好的.

参考文献:

[1] Wei Shimin, Xu Chunxiang, Xiao Guozhen. Distribution of Linear Complexity for Periodic Sequences[J]. Journal of Xidian University, 2001, 28(1): 95-99.

[2] Storer T. Cyclotomiy and Difference Set[M]. Chicago: Markham, 1967.

[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 Trans on Information Theory, 1998, 44(5): 1 699-1 702.

(编辑:郭　华)

(上接第 583 页)

传输时隙调度算法.通过 MIMO 的并行传输可改善时隙调度算法,不仅保证每个节点无冲突广播传输及最小帧长,而且充分利用了 MIMO 的并行数据流传输能力和干扰抑制能力.结果表明该协议可以极大地提高网络容量和减小平均分组时延.

参考文献:

[1] Raleigh G G, Jones V K. Multivariate Modulation and Coding for Wireless Communication[J]. IEEE Journal on Selected Areas in Communications, 1999, 7(5): 851-866.

[2] Narasimhan R. Spatial Multiplexing with Transmit Antenna and Constellation Selection for Correlated MIMO Fading Channels[J]. IEEE Trans on Signal processing, 2003, 51(11): 2 829-2 838.

[3] Wolniansky P W, Foschini G J, Golden G D, et al. V-BLAST: an Architeture for Realizing Very High Data Rates over the Rich-Scattering Wireless Channel[A]. IEEE ISART 1998: Vol 1[C]. Boulder: IEEE, 1998. 9-11.

[4] Zhang Wenzhu, Li Jiandong, Wang Xuan. Effect of the Packet Length on the Performance of Mobile Ad Hoc Networks [J]. Journal of Xidian University, 2003, 30(7): 11-14.

[5] Sundaresan K, Sivalumar R, Ingram M A, et al. Medium Access Control in Ad Hoc Networks with MIMO Links: Optimization Considerations and Algorithms[J]. IEEE Trans on Mobile Computing, 2004, 3(4): 350-365.

[6] Demirkol M F, Ingram M A. Stream Control in Networks with Interfering MIMO Links[A]. IEEE WCNC 2003: Vol 1 [C]. New Orleans: IEEE, 2003. 343-348.

[7] Gaur S, Jiang J S, Ingram M A, et al. Interfering MIMO Links with Stream Control and Optimal Antenna Selection[A]. IEEE GLOBECOM 2004: Vol 5[C]. Dallas: IEEE, 2004. 3 138-3 142.

[8] Hung K W, Yum T S. Fair and Efficient Transmission Scheduling in Multihop Packet Radio Networks[A]. IEEE GLOBECOM 1992: Vol 1[C]. Orlando: IEEE, 1992. 6-10.

[9] Hung K W, Yjm T S. An Efficient Code Assignment Algorithm for Multihop Spread Spectrum Packet Radio Networks [A]. IEEE GLOBECOM 1990: Vol 1[C]. Atlanta: IEEE, 1990. 271-274.

(编辑:高西全)