Z_{pq}环上的一类新的2^k阶广义割圆序列的线性复杂度*)

杜小妮[1,2]　肖国镇[1]

(西安电子科技大学综合业务网国家重点实验室　西安 710071)[1]

(西北师范大学 数学与信息科学学院　兰州 730070)[2]

摘　要　线性复杂度是度量序列随机性的一个重要指标。基于W-割圆理论,通过寻找序列特殊的特征集,构造了Z_{pq}环上一类新的2^k($k>1$)阶二元广义割圆序列,给出了该类序列的极小多项式和线性复杂度。其线性复杂度最小为$\frac{(p+1)(q-1)}{2}$,最大为$(q-1)p$。结果表明,该类序列具有良好的线性复杂度性质。

关键词　割圆类,W-割圆序列,线性复杂度,极小多项式

Linear Complexity of a New Class of Generalized Cyclotomic Sequences of Order 2^k over Z_{pq}

DU Xiao-Ni[1,2]　XIAO Guo-Zhen[1]

(The ISN National Key Laboratory, Xidian University, Xi'an 710071)[1]

(College of Mathematic and Information Science, Northwest Normal University, Lanzhou 730070)[2]

Abstract　Linear complexity is the most important index for measuring the randomness properties of sequences. Based on the White-generalized cyclotomy, new binary generalized cyclotomic sequences of order 2^k($k>1$) over Z_{pq} of length pq are constructed by finding out a special characteristic set. The minimal polynomials and linear complexity($L(s^\infty)$) of these new sequences are determined. The minimum of $L(s^\infty)$ is $\frac{(p+1)(q+1)}{2}$ and the maximum$(q-1)p$. It is shown that these sequences have good linear complexity.

Keywords　Cyclotomic class, W-cyclotomic sequence, Linear complexity, Minimal polynomial

1　引言

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。流密码中使用的伪随机序列应具有良好的不可预测性和随机性[1]。度量这些性质的一个重要指标就是它的线性复杂度。如果伪随机序列$s^\infty=(s_0,s_1,\cdots,s_i,\cdots)$满足反馈函数$s_j+c_1s_{j-1}+\cdots+c_Ls_{j-L}=0(j\geqslant L)$,其中$L$为正整数,$c_1,c_2,\cdots,c_L\in GF(N)$,$GF(N)$表示$N$阶有限Galois域,则称$s^\infty$为线性递归序列。定义最小$L$的为序列$s^\infty$的线性复杂度,记作$L(s^\infty)$。为抵抗已知明文攻击,密钥流序列的线性复杂度必须足够大。根据Berlekamp-Massey算法,如果$L(s^\infty)>\frac{p}{2}$(p是s^∞的周期),则认为s^∞具有好的线性复杂度。无穷序列$s^\infty=(s_0,s_1,s_2,\cdots)$和有限序列$s^N=(s_0,s_1,\cdots,s_{N-1})$的生成函数分别定义成$s(x)=\sum_{i=0}^{\infty}s_ix^i$和$s^N(x)=\sum_{i=0}^{N}s_ix^i$。如果$N$为序列$s^\infty$的周期,则

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

称为序列s^∞的极小多项式,并且有:(见文献[2])

$$L(s^\infty)=deg(m(x))=N-deg(gcd(x^N-1,s^N(x))) \tag{2}$$

令$(A,+)$为N阶Abel群,设D为A的子集,定义D的特征序列$s^\infty=(s_0,s_1,s_2,\cdots,s_i,\cdots)$如下

$$s^\infty=\begin{cases}1, & i \bmod N\in D,\\ 0, & \text{其他。}\end{cases}$$

同时称D为序列s^∞的特征集[3]。显然,N为特征序列的一个周期。

令p和q为两个奇素数$p<q$,$N=pq$,$d=gcd(p-1,q-1)$,$e=(p-1)(q-1)/d$,则可得到剩余类环Z_{pq}的一个乘法子群[4]

$$Z_N=\{g^tx^i:s=0,1,\cdots,e-1;i=0,1,\cdots,d-1\}$$

此处g为p和q公共的本原元,x是同时满足$x\equiv g \bmod p$和$x\equiv 1 \bmod q$的整数。定义

$$D_i=\{g^tx^i:t=0,1,\cdots e-1\},i=0,1\cdots,d-1 \tag{3}$$

为关于p和q的d阶广义W-割圆类($W\text{-}GC_d$)[4]。

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

当阶$d=gcd(p-1,q-1)=2^k$,$k>1$时,存在2^k个$W\text{-}GC_{2^k}$,即$D_0,D_1,\cdots,D_{2^k-1}$。令$B_0=\bigcup_{i=0}^{2^{k-1}-1}D_{2i}$,$B_1=\bigcup_{i=0}^{2^{k-1}-1}D_{2i+1}$,$C_0=R\cup Q\cup B_0$,$C_1=P\cup B_1$,则$C_0\cup C_1=Z_N$,$C_0\cap C_1=\emptyset$,$B_0\cup B_1=Z_N^*$,$B_0\cap B_1=\emptyset$。$\emptyset$表示空集。设$B\subseteq Z_N$,$a\in Z_N$,定义$aB=\{ab,b\in B\}$。

定义$W\text{-}GCS_{2^k}$为C_1关于p和q特征序列。显然C_1为该类序列的特征集。当p和q的取值接近时,该序列几乎为平衡序列。序列$W\text{-}GCS_2$的自相关值和线性复杂度由Ding在文献[5,6]中给出。本文的主要结果在下面给出。

下文中所采用的符号如上所定义,不再赘述。

2　2^k阶二元广义W-割圆序列的线性复杂度和极小多项式

由P,Q和R的定义有如下的结论。

*)基金项目:国家自然科学基金项目(60473028)和973项目(G1999035804)。**杜小妮**　博士研究生,主要研究方向为密码学和信息安全;**肖国镇**　教授,博士生导师。

引理 2.1 (1) 若 $a\in P$，则 $aP=P,aQ=R$。

(2)若 $a\in Q$，则 $aP=R,aQ=Q$。

(3) 若 $k\in D_j$，则 $kP=P,kQ=Q,j=0,1,\cdots,2^k-1$。

假设 α 是有限域 $GF(2^m)$ 上的一个 N 次单位本原根，$GF(2^m)$ 为 x^N-1 的分裂域，其中 $m=ord_N(2)$。

引理 2.2 $\sum_{j\in P}\alpha^j=\sum_{j\in Q}\alpha^j=\sum_{i\in Z_N^*}\alpha^i=1$。

证明：由 α 的定义有

$$\begin{aligned}0=\alpha^N-1&=(\alpha^p-1)(1+\alpha^p+\alpha^{2p}+\cdots+\alpha^{(q-1)p})\\&=(\alpha^q-1)(1+\alpha^q+\alpha^{2q}+\cdots+\alpha^{(p-1)q})\\&=(\alpha-1)(1+\alpha+\alpha^2+\cdots+\alpha^{pq-1})\end{aligned}$$

由以上事实即可证明该引理。

引理 2.3 和 2.4 均引自文[6]。

引理 2.3 如果 $a\in D_i$，则 $aD_j=D_{i+j},i,j=0,1,\cdots,2^k-1$。

引理 2.4 $ord_N(g)=e$，其中 $ord_N(g)$ 表示 g 模 N 的阶。

引理 2.5
$$\sum_{i\in D_j}\alpha^{ki}=\begin{cases}\dfrac{p-1}{2^k}\bmod 2, & \text{若 } k\in P,\\ \dfrac{q-1}{2^k}\bmod 2, & \text{若 } k\in Q.\end{cases}$$

$j=0,1,\cdots,2^k-1$。

证明：令 $k\in Q$，由引理 2.4 和 (3)。

$$\begin{aligned}D_j \bmod p&=\{g^tx^j \bmod p: t=0,1,\cdots,e-1\}\\&=\{g^{t+j} \bmod p: t=0,1,\cdots,e-1\}\\&=\{1,2,\cdots,p-1\}\end{aligned}$$

当 t 遍历 $(0,1,\cdots,e-1\}$ 一次时，$g^tx^j \bmod p$ 取集合 $\{1,2,\cdots,p-1\}$ 中的每个元素 $\frac{q-1}{2^k}$ 次。因此，由引理 2.2 有

$$\sum_{i\in D_j}\alpha^{ki}=\left[\frac{q-1}{2^k}\bmod 2\right]\cdot\sum_{i\in Q}\alpha^i=\frac{q-1}{2^k}\bmod 2$$

其余部分同理可证。

由于 $s(x)=\sum_{i\in C_1}x^i$ 是二元序列 W-GCS$_{2^k}$ 的生成多项式，因而

$$s(1)=\sum_{i\in C_1}1=(q-1)+\frac{(p-1)(q-1)}{2}\equiv 0 \bmod 2 \qquad (4)$$

引理 2.6
$$s(\alpha^k)=\begin{cases}s(\alpha), & \text{如果 } k\in B_0,\\ s(\alpha)+1, & \text{如果 } k\in B_1,\\ 1 \bmod 2, & \text{如果 } k\in P,\\ 0 \bmod 2, & \text{如果 } k\in Q。\end{cases}$$

证明：根据引理 2.3 和引理 2.2，有

如果 $k\in B_0$，则

$$\begin{aligned}s(\alpha^k)&=\sum_{i\in P}\alpha^{ki}+\sum_{i\in B_1}\alpha^{ki}=\sum_{i\in kP}\alpha^i+\sum_{i\in kB_1}\alpha^i\\&=\sum_{i\in P}\alpha^i+\sum_{i\in B_1}\alpha^i=s(\alpha)\end{aligned}$$

如果 $k\in B_1$，则有

$$\begin{aligned}s(\alpha^k)&=\sum_{i\in P}\alpha^{ki}+\sum_{i\in B_1}\alpha^{ki}=\sum_{i\in kP}\alpha^i+\sum_{i\in B_0}\alpha^i\\&=\sum_{i\in P}\alpha^i+\sum_{i\in B_1}\alpha^i=1+s(\alpha)\end{aligned}$$

如果 $k\in P$，又由引理 2.5，

$$\begin{aligned}s(\alpha^k)&=\sum_{i\in P}\alpha^{ki}+\sum_{i\in B_1}\alpha^{ki}=\sum_{i\in P}\alpha^i+\sum_{i\in B_1}\alpha^{ki}\\&=1+2^{k-1}\cdot\frac{p-1}{2^k}\equiv 1 \bmod 2\end{aligned}$$

如果 $k\in Q$，再由引理 2.5，

$$\begin{aligned}s(\alpha^k)&=\sum_{i\in P}\alpha^{ki}+\sum_{i\in B_1}\alpha^{ki}=\sum_{i\in P}1+\sum_{i\in B_1}\alpha^{ki}\\&=q-1+2^{k-1}\cdot\frac{p-1}{2^k}\equiv 0 \bmod 2\end{aligned}$$

定理 2.7
$$L(s^\infty)=\begin{cases}\dfrac{(p+1)(q-1)}{2} & \text{若 } 2\in B_0,\\ (q-1)p & \text{若 } 2\in B_1。\end{cases}$$

证明：如果 $2\in B_0$，因为 $s(x)\in GF(2)[x]$，由引理 2.6，有 $s(\alpha)^2=s(\alpha^2)=s(\alpha)$，因此 $s(\alpha)\in\{0,1\},1+s(\alpha)\in\{0,1\}$。因为 $s(\alpha)$ 和 $s(\alpha)+1$ 分别取 0 和 1，由引理 2.6 和(4)，有

$$\begin{aligned}L(s^\infty)&=N-1-(p-1)-\frac{(p-1)(q-1)}{2}\\&=\frac{(p+1)(q-1)}{2}.\end{aligned}$$

如果 $2\in B_1$，由引理 2.6，有 $s(\alpha)^2=s(\alpha^2)=s(\alpha)+1$，因而 $s(\alpha)\notin\{0,1\}$。由引理 2.6 和 (4)，有 $L(s^\infty)=N-1-(p-1)=p(q-1)$。

令 $\beta=\alpha^p$ 是 x^q-1 的一个 q 次单位根。$\gamma=\alpha^q$ 是 x^p-1 的一个 p 次单位根，那么

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

定义 $d(x)=\prod_{i\in Z_N^*}(x-\alpha^i)$，因为 $m|\varphi(N)=(p-1)(q-1),deg(d(x))=\varphi(N)$，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 $2B_0=B_0,2B_1=B_1$ ，$d_j(x)^2=\prod_{i\in D_j}(x^2-\alpha^{2i})=d_j(x^2)$

从而 $d_j(x)\in GF(2)[x],d(x)=d_0(x)d_1(x)$。此时

$$\begin{aligned}x^N-1&=(x^p-1)(x^q-1)d(x)/(x-1)\\&=(x^p-1)(x^q-1)d_0(x)d_1(x)/(x-1)\end{aligned}$$

选择恰当的 α 使得 $s(\alpha)=0$，则有

定理 2.8 对于给定的 α，W-GCS$_{2^k}$ 的极小多项式为

$$m(x)=\begin{cases}\dfrac{x^N-1}{(x^p-1)d_0(x)}, & \text{如果 } 2\in B_0,\\ \dfrac{x^N-1}{x^p-1}, & \text{如果 } 2\in B_1。\end{cases}$$

证明：如果 $2\in B_0$，由 α 的选取，$\gcd(x^N-1,s(x))=(x^p-1)d_0(x)$，因而 $m(x)=\frac{x^N-1}{(x^p-1)d_0(x)}$。

如果 $2\in B_1$，由定理 2.7 的证明可知 $\gcd(x^N-1,s(x))=x^p-1$，因此，$m(x)=\frac{x^N-1}{x^p-1}$。

结论 文中构造了 Z_{pq} 环上的一种新的周期为 pq 的 2^k $(k>1)$ 阶二元广义 W-割圆序列，给出了该类序列的线性复杂度和极小多项式。结果表明该类序列的线性复杂度最小为 $\frac{(p+1)(q-1)}{2}$，最大为 $(q-1)p$。根据 Berlekamp-Massey 算法，该类序列有良好的线性复杂度，且当 p 和 q 的取值接近时，该序列几乎为平衡序列，因而是密码学意义上好的序列。

参 考 文 献

1 Blum L, Blum M, Shub M. A Simple Unpredictable Pseudo-random Number Generator, SIAM J. Comput, 1986, 15: 364～383

2 Ding C, Xiao G, Shan W. The Stability Theory of Stream Ciphers, Lect. Notes in Comput. Sci, New York/Berlin: Springer-Verlag, 1991, 561

3 Ding C, Tor Helleseth and Kwok Yan Lam, Several Classes of Binary Sequences with Three-Level Autocorrelation. IEEE Trans. Information Theory, 1999, 45(7): 2606～2612

4 Storer T. Cyclotomiy and Difference Set. Chicago: Markham, 1967

5 Ding Cunsheng. Linear Complexity of Generalized Cyclotomic Binary Sequence of Order 2. Finite Field and Their Application, 1997, 3: 159～174

6 Ding C. Autocorrelation Values of Generalized Cyclotomic Sequences of Order Two. IEEE Transactions on Information Theory, 1998, 44(5): 1699～1702