一类新的 *pqr* 长 2 阶广义分圆序列的线性复杂度

常祖领[1],周玉倩[2],柯品惠[3]
(1.郑州大学数学与统计学院,河南郑州 450001;2.北京邮电大学网络与交换技术研究院,北京 100876;
3.福建师范大学网络安全与密码技术重点实验室,福建福州 350007)

摘 要: 具有良好随机性质的伪随机序列在流密码和通信领域中有着广泛的应用.本文构造出一类新的长为 *pqr* 的 2 阶广义分圆序列,并且计算其线性复杂度和极小多项式.结果显示这种序列具有高线性复杂度.

关键词: 广义分圆序列; 线性复杂度; 极小多项式
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2015)01-0166-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.01.026

Linear Complexity of New Generalized Cyclotomic Sequences of Order Two and Length *pqr*

CHANG Zu-ling[1], ZHOU Yu-qian[2], KE Pin-hui[3]
(1. *Department of Mathematics and Statistics, Zhengzhou University, Zhengzhou, Henan* 450001, *China*;
2. *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*;
3. *Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou, Fujian* 350007, *China*)

Abstract: Pseudorandom sequences with good randomness properties are widely used in stream ciphers and communications. This paper introduces one new class of generalized cyclotomic sequences of order two and length *pqr*, then calculates the linear complexity and the minimal polynomial of these sequences. The results show that the new cyclotomic sequences have high linear complexity.

Key words: generalized cyclotomic sequences; linear complexity; minimal polynomial

1 引言

伪随机序列可广泛地应用于扩频通信系统、码分多址系统、全球定位系统和软件测试等.具有良好相关特性的伪随机序列可用做雷达测距、同步和线性系统测量的信号.具有高线性复杂度的伪随机序列也有多方面的应用,如用于加密系统等.从线性复杂度的角度考虑,根据 Berlekamp-Massey 算法,对于一个周期为 N 的序列,若其线性复杂度大于 $N/2$,则该序列可称为一个好的序列或称具有高线性复杂度[1].

由于具有良好的随机特性及代数结构,分圆序列得到人们的深入研究.丁存生首先构造得到周期为 pq 的二阶二元分圆序列,该序列具有高线性复杂度和好的自相关性[2,3];白等人提出周期为 pq 的四阶二元分圆序列,其线性复杂度在特定的情况下亦可达到 $pq-p$[4,5];文献[6]给出周期为 pq 的二元序列分圆序列的另一种构造方法,该序列亦可同样达到 $pq-p$;进一步地讲,Yan 等人研究周期为 p^m 的二元分圆序列,并计算得到其线性复杂度[7];另一方面,V A Edemskiy 以周期为 p 的经典分圆序列为基础对分圆序列的周期进行推广,提出周期为 p^{n+1} 的另一种构造和其线性复杂度[8];鉴于之前的研究工作多是奇数长分圆序列,2012 年,偶数周期为 $2p^m$ 的分圆序列被首次提出,并研究得到其相关性和线性复杂度[9,10];Hu 等人进一步极大地扩充奇数周期范围,给出了周期为 $p^{m+1}q^{n+1}$ 的广义分圆序列的一般构造方法,并给出其线性复杂度的计算公式[11].

需要注意的是,已有结果都是针对一个或两个素数幂长度的分圆序列,关于超过三个的素数幂长度的分圆序列的研究则基本没有.我们对这个问题进行了深入研究,以丁存生和 Helleseth 提出的长为 $p_1^{e_1}\cdots p_t^{e_t}$ 的分圆

收稿日期:2013-09-27;修回日期:2013-12-09;责任编辑:孙瑶
基金项目:国家自然科学基金联合基金(No.U1304604);国家自然科学基金青年基金(No.61102093);河南省教育厅科学技术研究重点项目(No.14A110022)

码[12]为理论基础,首次构造得到周期长为 pqr 的二阶广义分圆序列,并且计算得到其线性复杂度和极小多项式.本文得到该序列在特定情况下,其线性复杂度可以达到 $pqr-pr+r-1$.本文中采用的分析方法可用来分析更一般长度的分圆序列,为进一步工作奠定基础.

2 构造

在本文定义 $N=pqr$, $e=(p-1)(q-1)(r-1)/4$,其中 $p,q,r(p>q>r)$是三个互不相同的奇素数,且满足 $r\equiv 1 \bmod 4$, $\gcd(p-1,q-1)=\gcd(p-1,r-1)=2$ 和 $\gcd(r-1,q-1)=2$.对于环 Z_n, n 是正整数,用 Z_n^* 表示环 Z_n 中所有可逆元构成的集合.由中国剩余定理[13]可知,环 Z_n 中存在唯一模 p,q,r 的公共本原元,将其记为 g,则对应的阶为 $\mathrm{ord}_N(g)=e$[14].

令 y_1 和 y_2 分别是以下两个同余方程组的根:

$$\begin{cases} y_1\equiv g(\bmod p) \\ y_1\equiv 1(\bmod q) \\ y_1\equiv 1(\bmod r) \end{cases}, \begin{cases} y_2\equiv 1(\bmod p) \\ y_2\equiv g(\bmod q) \\ y_2\equiv 1(\bmod r) \end{cases}$$

其中 $0\leqslant y_1,y_2\leqslant N-1$.由中国剩余定理可知, y_1 和 y_2 存在且唯一.

定义 $Y=\{1,y_1\}$.令 g 在 Z_N^* 上生成的群为 $G=(g)$,由定义可得引理 1.

引理 1[12]　$\mathrm{ord}_N(g)=e$ 且 $y_1^2\in G$.

定义　$D_0^{(N)}=\{\, g^s y: s=0,1,\cdots,e-1; y\in Y\,\}$

其中 $D_0^{(N)}$ 是 Z_N^* 的子群且 $|D_0^{(N)}|=2e$,由中国剩余定理可得 $y_2\notin D_0^{(N)}$.则定义

$$D_1^{(N)}=y_2D_0^{(N)}$$

其中乘法定义为环 Z_N 中的乘法.称 $D_0^{(N)}$ 和 $D_1^{(N)}$ 是关于 N 的二阶广义分圆类[12].由引理 1 和 $D_0^{(N)}$ 的定义可得引理 2.

引理 2[12]　$D_0^{(N)}\cap D_1^{(N)}=\varnothing$, $D_0^{(N)}\cup D_1^{(N)}=Z_N^*$,其中 $\varnothing$ 表示空集.

定义　$P=\{p,2p,\cdots,(qr-1)p\}$;

$Q=\{q,2q,\cdots,(pr-1)q\}-\{pq,2pq,\cdots,(r-1)pq\}$;

$R=\{r,2r,\cdots,(pq-1)r\}-\{pr,2pr,\cdots,(q-1)pr\}-\{qr,2qr,\cdots,(p-1)qr\}$;

$O=\{0\}$.

和　$D_0=D_1^{(N)}\cup Q\cup R\cup O$; $D_1=D_0^{(N)}\cup P$,

其中 $A-B(A,B$ 表示集合)表示集合的差.

周期为 N 的二阶广义分圆序列 s^∞ 定义如下:

$$s_i=\begin{cases} 0, \text{if}(i \bmod N)\in D_0 \\ 1, \text{if}(i \bmod N)\in D_1 \end{cases}$$

序列 s^∞ 包含 $[(p-1)(q-1)(r-1)/2]+qr-1$ 个 1 和 $[(p-1)(q+1)(r+1)/2]+2-p$ 个 0,即该序列的不平衡性 I 为:

$$\begin{aligned} I &= |[(p-1)(q+1)(r+1)/2+2-p]| \\ &\quad -[(p-1)(q-1)(r-1)/2+qr-1]| \\ &= |(p-1)(q+r-1)-qr+2| \end{aligned}$$

为了更加快捷地计算得到该序列的线性复杂度和极小多项式,本文将周期为 pqr 的分圆序列 s^∞ 转化为周期为 pq 的分圆序列来考虑,将复杂问题简单化,计算得到序列 s^∞ 的线性复杂度.

3 线性复杂度

令 s^∞ 是一周期为 N 的二元序列.若首一多项式 $f(x)=x^L+a_{L-1}x^{L-1}+\cdots+a_1x+a_0\in Z_2[x]$,使得 $s_{L+t}+a_{L-1}s_{L-1+t}+\cdots+a_1s_{t+1}+a_0s_t=0$,对于所有 $t\geqslant 0$ 均成立,则称 $f(x)$ 是 s^∞ 的特征多项式.易知 s^∞ 的特征多项式不唯一.

称 s^∞ 的特征多项式中次数最小的首一多项式 $m(x)\in Z_2[x]$ 为 s^∞ 的极小多项式.序列的极小多项式存在且唯一.序列 s^∞ 的极小多项式 $m(x)$ 的次数 $\deg(m(x))$ 称为序列 s^∞ 的线性复杂度,记为 $LC(s)$.

定义　$s^N(x)=s_0+s_1x+\cdots+s_{N-1}x^{N-1}\in Z_2[x]$ 为序列 s^∞ 的生成函数,或简记为 $s(x)$.

由文献[14]可知, s^∞ 的极小多项式为

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

显然, s^∞ 的线性复杂度为

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

本文主要利用式(1)(2)求得序列 s^∞ 的极小多项式和线性复杂度.

首先令 θ 是扩域 $\mathrm{GF}(2^m)$ 上的 N 次本原单位根,其中 $\mathrm{GF}(2^m)$ 是 x^N-1 在 Z_2 上的分裂域,由式(2)可得

$$LC(s)=N-|\{t: s(\theta^t)=0, 0\leqslant t\leqslant N-1\}|$$

其中

$$s(x)=\sum_{i\in D_0^{(N)}}x^i+\sum_{i\in P}x^i \tag{3}$$

其次若求序列 s^∞ 的线性复杂度,只需求满足 $s(\theta^i)=0, 0\leqslant i\leqslant N-1$ 的个数,可分情况讨论.

若 $x=\theta^0=1$,则

$$\begin{aligned} s(1) &= \sum_{i\in D_0^{(N)}}1+\sum_{i\in P}1 \\ &= (p-1)(q-1)(r-1)/2+qr-1 \\ &\equiv 0 \bmod 2 \end{aligned}$$

下面讨论 $x=\theta^t, 0<t\leqslant N-1$ 时 $s(x)$ 的值.为了计算方便和引理的提出,进一步分解 P,Q 和 R 并计算其求和的值,本文分别计算 $\sum_{i\in D_0^{(N)}}x^i$, $\sum_{i\in P}x^i$ 的值,从而确定 $s(x)$ 的值.

定义　$P_1=\{pq,2pq,\cdots,(r-1)pq\}$;

$P_2=\{pr,2pr,\cdots,(q-1)pr\}$;

$P_3=P-(P_1\cup P_2)$;

$Q_1=\{rq,2rq,\cdots,(p-1)rq\}$;

$Q_2=Q-Q_1$.

则有 $P=P_1\cup P_2\cup P_3$; $Q=Q_1\cup Q_2$

且 $P_1\cap P_2=P_1\cap P_3=P_2\cap P_3=\varnothing$; $Q_1\cap Q_2=\varnothing$.

因为

$$\begin{aligned}\theta^N-1&=(\theta^p)^{qr}-1\\&=(\theta^p-1)(1+\theta^p+\cdots+\theta^{(qr-1)p})\\&=0\end{aligned}$$

所以 $1+\theta^p+\cdots+\theta^{(qr-1)p}=0$.

换而言之, $\sum_{i\in P}\theta^i=1$.

同理可得

$$0=1+\theta^q+\cdots+\theta^{(pr-1)q}=1+\sum_{i\in P_1}\theta^i+\sum_{i\in Q}\theta^i;$$

$$0=1+\theta^r+\cdots+\theta^{(pq-1)r}=1+\sum_{i\in P_1}\theta^i+\sum_{i\in Q_1}\theta^i+\sum_{i\in R}\theta^i,$$

由
$$\begin{aligned}\theta^N-1&=(\theta^{pq})^r-1\\&=(\theta^{pq}-1)(1+\theta^{pq}+\cdots+\theta^{(r-1)pq})\\&=0\end{aligned}$$

易证 $\sum_{i\in P_1}\theta^i=1$.

同理可得 $\sum_{i\in P_2}\theta^i=\sum_{i\in Q_1}\theta^i=1$.

因此 $\sum_{i\in P}\theta^i=1$; $\sum_{i\in Q}\theta^i=0$; $\sum_{i\in R}\theta^i=1$.

因为 $\Big(\sum_{i\in D_0^{(N)}}+\sum_{i\in D_1^{(N)}}+\sum_{i\in P}+\sum_{i\in Q}+\sum_{i\in R}\Big)\theta^i=1$,

所以 $\sum_{i\in D_0^{(N)}}\theta^i+\sum_{i\in D_1^{(N)}}\theta^i=1$.

基于以上准备工作,本文下面计算该序列的线性复杂度,首先分情况讨论 $\sum_{i\in D_0^{(N)}}\theta^{it}$, $\sum_{i\in P}\theta^{it}$ 的值,令符号记法如上,分别得到引理 3-5.

引理 3 若 $t\in P_1\cup P_2\cup Q_1$,则 $\sum_{i\in D_0^{(N)}}\theta^{it}=0$.

证明 不失一般性,首先讨论当 $t\in P_1$ 时,由定义知 g 是模 r 的本原元且 $y_1\equiv1(\bmod r)$.则

$$\begin{aligned}D_0^{(N)}\bmod r&=\{g^s\bmod r:s=0,1,\cdots,e-1\}\\&\quad\cup\{g^sy_1\bmod r:s=0,1,\cdots,e-1\}\\&=\{g^s\bmod r:s=0,1,\cdots,r-2\}\\&=\{1,2,\cdots,r-1\}.\end{aligned}$$

且当 s 取遍集合 $\{0,1,\cdots,e-1\}$ 时, $D_0^{(N)}\bmod r$ 将集合 $\{1,2,\cdots,r-1\}$ 中每一元素取 $(p-1)(q-1)/2$ 遍.得

$$\sum_{i\in D_0^{(N)}}\theta^{it}=((p-1)(q-1)/2\bmod2)\sum_{i\in P_1}\theta^i=0$$

当 $t\in P_2\cup Q_1$ 时,同理可证.

引理 4 $\sum_{i\in D_0^{(N)}}\theta^{it}=\begin{cases}(q-1)/2\bmod2,\text{if } t\in Q_2\\(r-1)/2\bmod2,\text{if } t\in R\end{cases}$

证明 首先,若 $t\in Q_2$,

$$\begin{aligned}D_0^{(N)}\bmod pr&=\{g^s\bmod pr:s=0,1,\cdots,e-1\}\\&\quad\cup\{g^sy_1\bmod pr:s=0,1,\cdots,e-1\}\\&=\{g^s\bmod pr:s=0,1,\cdots,\varphi(pr)/2-1\}\\&\quad\cup\{g^sy_1\bmod pr:s=0,1,\cdots,\varphi(pr)/2-1\}\end{aligned}$$

根据环 Z_{pr} 的分圆类[3]可知

$Z_{pr}^*=\{g^sx^i\bmod pr:s=0,1,\cdots,\varphi(pr)/2-1;i=0,1\}$

其中 $\varphi(x)$ 是欧拉函数[13]. 则 $D_0^{(N)}\bmod pr=Z_{pr}^*$. 且当 s 取遍集合 $\{0,1,\cdots,e-1\}$ 时, $D_0^{(N)}\bmod pr$ 将集合 Z_{pr}^* 中每一个元素取 $(q-1)/2$ 遍.

$$\sum_{i\in D_0^{(N)}}\theta^{it}=((q-1)/2\bmod2)\sum_{i\in Z_{pr}^*}\theta^{iq}=(q-1)/2\bmod2$$

因为 θ^q 是扩域 GF(2^m)上的一个 pr 次本原元,由文献[4]知 $\sum_{i\in Z_{pr}^*}\theta^{iq}=1$, 则

$$\sum_{i\in D_0^{(N)}}\theta^{it}=((q-1)/2\bmod2)\sum_{i\in Z_{pr}^*}\theta^{iq}=(q-1)/2\bmod2$$

其次,当 $t\in R$ 时,

$$\begin{aligned}D_0^{(N)}\bmod pq&=\{g^s\bmod pq:s=0,1,\cdots,e-1\}\\&\quad\cup\{g^sy_1\bmod pq:s=0,1,\cdots,e-1\}\\&=\{g^s\bmod pq:s=0,1,\cdots,\varphi(pq)/2-1.\}\\&\quad\cup\{g^sy_1\bmod pq:s=0,1,\cdots,\varphi(pq)/2-1\}\end{aligned}$$

同时可得

$Z_{pq}^*=\{g^sy_1^i\bmod pq:s=0,1,\cdots,\varphi(pq)/2-1;i=0,1\}$.

同理, $D_0^{(N)}\bmod pq=Z_{pq}^*$.可得

$$\sum_{i\in D_0^{(N)}}\theta^{it}=((r-1)/2\bmod2)\sum_{i\in Z_{pq}^*}\theta^{ir}=(r-1)/2\bmod2.$$

引理 5 若 $t\in P_3$,则 $\sum_{i\in D_0^{(N)}}\theta^{it}=0$

证明 因为 $y_1\equiv1(\bmod qr)$,所以

$$\begin{aligned}&\{g^sy_1\bmod qr:s=0,1,\cdots,e-1\}\\&=\{g^s\bmod qr:s=0,1,\cdots,e-1\}\end{aligned}$$

即 $$\sum_{i\in D_0^{(N)}}\theta^{it}=((p-1)\bmod2)\sum_{i\in Z_{qr}^*}\theta^{ip}=0.$$

至此,本文得到 $\sum_{i\in D_0^{(N)}}\theta^{it}$, $0<t\leqslant N-1$ 的值,在引理 6 中讨论 $\sum_{i\in P}\theta^{it}$, $0\leqslant t\leqslant N-1$ 的值.

引理 6 $\sum_{i\in P}\theta^{it}=\begin{cases}1,t\in P\cup R\cup Q_2\cup Z_N^*;\\0,t\in Q_1\cup O.\end{cases}$

证明 分情况讨论.

情况 1 当 $t\in P_1$时, $tP=P_1\cup O$ 且有

$$\sum_{i\in P}\theta^{it}=(q\bmod2)\sum_{i\in P_1}\theta^{it}+(q-1)\bmod2=1,$$

当 $t\in P_2\cup R$ 时, $tP=P_2\cup O$ 且有

$$\sum_{i\in P}\theta^{it}=(r\bmod2)\sum_{i\in P_2}\theta^{it}+(r-1)\bmod2=1;$$

当 $t\in P_3$ 时, $tP=P$ 且 $\sum_{i\in P}\theta^{it}=\sum_{i\in P}\theta^i=1$;简言之,当 t

$\in P\cup R$ 时, $\sum_{i\in P}\theta^{it}=1$.

当 $t\in Q_2$ 时, $tP=P_1\cup O$,则

$$\sum_{i\in P}\theta^{it}=(q\bmod 2)\sum_{i\in P_1}\theta^{it}+(q-1)\bmod 2=1$$

当 $t\in Z_N^*$ 时, $tP=P$,则 $\sum_{i\in P}\theta^{it}=\sum_{i\in P}\theta^{i}=1$;.

情况 2　当 $t\in Q_1\cup O$ 时, $tP=O$,则

$$\sum_{i\in P}\theta^{it}=(qr-1)\bmod 2=0.$$

在引理 3-6 中,本文得到 $\sum_{i\in D_0^{(N)}}\theta^{it}$ 和 $\sum_{i\in P}\theta^{it}$ 的取值结果,借此可确定 $s(\theta^t)$ 的值,即定理 1.

定理 1

$$s(\theta^t)=\begin{cases}1, & t\in P\cup R\\ s(\theta), & t\in D_0^{(N)}\\ 1+s(\theta), & t\in D_1^{(N)}\\ 0, & t\in O\cup Q\end{cases}\tag{4}$$

证明　分情况讨论式(3)的值.

情况 1　当 $t\in P\cup R$ 时, $\sum_{i\in P}\theta^{it}=1$. 且由引理 3~引理 5 可得当 $t\in P$ 时有 $\sum_{i\in D_0^{(N)}}\theta^{it}=0$, 即当 $t\in P$ 时, $s(\theta^t)=1$;

当 $t\in R$ 时

$$s(\theta^t)=(r-1)/2+1=((r+1)/2)\bmod 2.$$

因 $r\equiv 1\bmod 4$,所以当 $t\in R$ 时, $s(\theta^t)=1$.

综上所述,当 $t\in P\cup R$ 时, $s(\theta^t)=1$.

情况 2　当 $t\in D_0^{(N)}$ 时, $tD_0^{(N)}=D_0^{(N)}$,因此

$$s(\theta^t)=\sum_{i\in D_0^{(N)}}\theta^{it}+1=\sum_{i\in D_0^{(N)}}\theta^{i}+1=s(\theta).$$

情况 3　当 $t\in D_1^{(N)}$ 时, $tD_0^{(N)}=D_1^{(N)}$,因此

$$s(\theta^t)=\sum_{i\in D_0^{(N)}}\theta^{it}+1=\sum_{i\in D_1^{(N)}}\theta^{i}+1.$$

因为 $\sum_{i\in D_0^{(N)}}\theta^{i}+\sum_{i\in D_1^{(N)}}\theta^{i}=1$,

所以,当 $t\in D_1^{(N)}$ 时, $s(\theta^t)=1+s(\theta)$;

情况 4　当 $t\in Q_1$ 时,由引理 3 可得 $\sum_{i\in D_0^{(N)}}\theta^{it}=0$,即 $s(\theta^t)=0+0=0$,

当 $t\in Q_2$ 时,由引理 4 可得

$$s(\theta^t)=(q-1)/2+1=((q+1)/2)\bmod 2.$$

因为 $r\equiv 1\bmod 4$, $\gcd(q-1,r-1)=2$,所以 $q\equiv 3\bmod 4$,换言之,当 $t\in Q_2$. 时, $s(\theta^t)=0$.

综上,当 $t\in Q\cup O$ 时, $s(\theta^t)=0$.

定理 2

$$LC(s^\infty)=\begin{cases}pqr-[(p-1)(q+1)(r-1)/2]-p, & 2\in D_0^{(N)}\\ pqr-pr+r-1, & 2\in D_1^{(N)}\end{cases}$$

证明　若 $2\in D_0^{(N)}$,则 $s^2(\theta)=s(\theta^2)=s(\theta)$,所以 $s(\theta)\in\{0,1\}$. 即 $s(\theta)$ 和 $1+s(\theta)$ 有且只有一个为 0. 由定理 1 和式(2)可知

$$LC(s^\infty)=pqr-[(p-1)(q+1)(r-1)/2]-p;$$

若 $2\in D_1^{(N)}$,则 $s^2(\theta)=s(\theta^2)=s(\theta)+1$,即 $s(\theta)$ 和 $1+s(\theta)$ 均不为 0,同理, $LC(s^\infty)=pqr-pr+r-1$.

下面我们来判断 $2\in D_1^{(N)}$ 在什么条件下成立,进而序列 s^∞ 可以达到最大线性复杂度. 文献[15]中给出如何判断一个数是模 N 的平方剩余的定理,即若 $n>1$ 是一奇数,且有如下分解

$$n=\prod_{i=1}^{l}p_i^{e_i}$$

其中 p_i 为不同的素数,且 e_i 为正整数. 另设 $\gcd(a,n)=1$. 那么同余方程 $y^2\equiv a(\bmod n)$ 当 $\left(\frac{a}{p_i}\right)=1$ 对于所有 $i\in\{1,2,\cdots,l\}$ 成立时有 2^l 个模 n 的解,在其他情形下无解.

本文已设 $r\equiv 1\bmod 4$, $\gcd(p-1,q-1)=2$, $\gcd(p-1,r-1)=2$ 和 $\gcd(q-1,r-1)=2$. 由此可得引理 7.

引理 7　2 是模 $N=pqr$ 的平方剩余当且仅当 $p\equiv -1(\bmod 8)$, $q\equiv -1(\bmod 8)$, $r\equiv 1(\bmod 8)$.

注 1　由引理 1 可知,若 2 是模 N 的平方剩余,则必有 $2\in G$;则当 $p\equiv -1(\bmod 8)$, $q\equiv -1(\bmod 8)$, $r\equiv 1(\bmod 8)$时, $2\in D_0^{(N)}$,换言之,若 $2\in D_1^{(N)}$,则 2 是模 N 平方非剩余. 因此 $LC(s^\infty)=pqr-[(p-1)(q+1)(r-1)/2]-p$;若使 $LC(s^\infty)=pqr-pr+r-1$,则需满足 $2\in D_1^{(N)}$,即 p,q,r 满足下列条件:

(1) $p\equiv 3(\bmod 8)$, $q\equiv -1(\bmod 8)$, $r\equiv 1(\bmod 8)$;

(2) $p\equiv 3(\bmod 4)$, $q\equiv 3(\bmod 8)$, $r\equiv 1(\bmod 8)$;

(3) $p\equiv 3(\bmod 4)$, $q\equiv 3(\bmod 4)$, $r\equiv -3(\bmod 8)$.

4　极小多项式

令 θ 是扩域 $GF(2^m)$ 上的 N 次本原元,定义

$$c(x)=\prod_{i\in P\cup R}(x-\theta^i),$$

$$q(x)=\prod_{i\in Q}(x-\theta^i),$$

$$d_0(x)=\prod_{i\in D_0^{(N)}}(x-\theta^i),$$

$$d_1(x)=\prod_{i\in D_1^{(N)}}(x-\theta^i).$$

利用多项式根的分解定理可得

$$x^N-1=\prod_{i=0}^{N-1}(x-\theta^i)=(x-1)d_0(x)d_1(x)c(x)q(x).$$

若 $2\in D_0^{(N)}$,则有 $2D_j^{(N)}=D_j^{(N)}$, $j=0,1$. 且

$$d_j(x)^2=\prod_{i\in D_j^{(N)}}(x^2-\theta^{2i})=\prod_{i\in D_j^{(N)}}(x^2-\theta^{i})$$

$$= d_j(x^2).$$

因此，$d_j(x) \in \mathrm{GF}(2)[x]$.

因为 $\gcd(p,2) = \gcd(q,2) = \gcd(r,2) = 1$，所以 $2Q = Q$，$2(P \cup R) = P \cup R$，同理可得 $q(x)$，$c(x) \in \mathrm{GF}(2)[x]$. 综上，若 $2 \in D_0^{(N)}$，

$$x^N - 1 = (x-1)c(x)q(x)d_0(x)d_2(x).$$

注 2[4] 由定理 2 可知，若 $2 \in D_0^{(N)}$，即得 $s(\theta) \in \{0,1\}$. 因此为了叙述方便，取 θ 满足 $s(\theta) = 0$. θ 值取定后可立刻得到 $d_j(x)$，$j = 0,1$ 的表达式.

定理 3 设 θ 定义如上，则序列 s^∞ 的极小多项式为：

$$m(x) = \begin{cases} (x^N-1)/[(x-1)d_0(x)q(x)], & 2 \in D_0^{(N)} \\ (x^N-1)/[(x-1)q(x)], & 2 \in D_1^{(N)} \end{cases} \tag{5}$$

证明[4] 由注 2 可知，若 $2 \in D_0^{(N)}$ 时，$s(\theta) = 0$，由式(4)即得式(5).

5 结束语

本文首次构造得到一类新的长度为 pqr 的二阶分圆序列，并给出了该序列的线性复杂度和极小多项式. 文中定理 1 给出了序列生成函数 $s(x)$ 的取值分布情况. 由定理 2 可知，该序列在特定情况下，其线性复杂度可达到 $pqr-pr+r-1$，即该序列具有高线性复杂度. 另外本文根据多项式根的分解定理给出该序列的极小多项式，可以用于分析类似结构的分圆序列的线性复杂度.

参考文献

[1] J L Massey. Shift register synthesis and BCH decoding [J]. IEEE Trans on Information Theory, 1969, 15(1): 122 – 127.

[2] C Ding. Autocorrelation values of generalized cyclotomic sequences of order two [J]. IEEE Trans on Information Theory, 1998, 44(4): 1698 – 1702.

[3] C Ding. Linear complexity of generalized cyclotomic binary sequences of order 2 [J]. Finite Fields and Their Applications, 1997, 3(2): 159 – 174.

[4] E Bai, X Fu, G Xiao. On the linear complexity of generalized cyclotomic sequences of order four over Z_{pq} [J]. IEICE Trans on Fundamentals, 2005, E88 – A(1): 392 – 395.

[5] E Bai, X Liu. Generalized cyclotomic sequences of order four over Z_{pq} and their autocorrelation values [J]. Chinese Journal of Engineering Mathematics, 2008, 25(5): 894 – 900.

[6] S Li, L Zhou. Linear complexity of a new generalized cyclotomic sequences of order four and length pq [A]. International Conference on Communications, Circuits and Systems (ICCCAS) [C]. USA: IEEE, 2009. 331 – 334.

[7] T Yan, S Li, G Xiao. On the linear complexity of generalized cyclotomic sequences with the period p^m [J]. Applied Mathematics Letters, 2008, 21(2): 187 – 193.

[8] V A Edemskiy. About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1} [J]. Designs, Codes and Cryptography, 2011, 61(3): 251 – 260.

[9] J Zhang, C A Zhao, X Ma. Linear complexity of generalized cyclotomic binary sequences with period $2p^m$ [A]. The 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-17) [C]. Bangalore, India, 2007. 93 – 108.

[10] P Ke, J Zhang, S Zhang. On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences with period $2p^m$ [J]. Designs, Codes and Cryptography, 2012, 67(3): 325 – 339.

[11] L Hu, Q Yue, M Wang. The linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$ [J]. IEEE Trans on Information Theory, 2012, 58(8): 5534 – 5543.

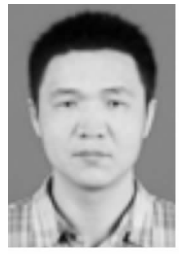
[12] C Ding, T Helleseth. Generalized cyclotomic codes of length $p_1^{e_1} \cdots p_t^{e_t}$ [J]. IEEE Trans on Information Theory, 1999, 45(2): 467 – 474.

[13] 张禾瑞. 近世代数基础(修订版) [M]. 北京：高等教育出版社，2010.

[14] R Lidl, H Neiderreiter. Finite Fields [M]. MA: Addison-Wesley, 1983.

[15] 冯登国，等. 密码学原理与实践(第 3 版) [M]. 北京：电子工业出版社，2009. 147 – 148.

作者简介



常祖领 男，1976 年 12 月出生，河南新乡人. 副教授、硕士生导师，1998 年和 2003 年分别在南开大学获理学学士和理学博士学位，现在郑州大学数学与统计学院工作，主要从事信息论、密码序列设计等方面的研究工作.

E-mail: zuling_chang@zzu.edu.cn

周玉倩 女，1989 年 1 月出生，河南新乡人. 现为北京邮电大学网络与交换技术研究院博士生，主要从事量子密码、密码序列设计等方面的研究工作.

柯品惠 男，1978 年 9 月出生，福建建阳人. 福建师范大学数学与计算机科学学院副教授，主要从事序列设计、编码密码学等方面的研究工作.