一类新的周期为$2p^m$的q阶二元广义分圆序列的线性复杂度

王 艳 薛改娜* 李顺波 惠飞飞
(西安建筑科技大学理学院 西安 710055)

摘 要：该文基于Ding-广义分圆理论，将周期为$2p^m$ (p为奇素数，m为正整数)广义分圆序列的研究推广到任意素数阶情形，构造了一类新序列。通过数论方法分析多项式广义分圆类，确定并计算线性复杂度与序列的2次剩余类和2次非剩余类的划分紧密相关。结果表明该类序列的线性复杂度远远大于周期的一半，能抗击应用Berlekamp-Massey(B-M)算法的安全攻击，是密码学意义上性质良好的伪随机序列。

关键词：广义分圆序列；线性复杂度；2次剩余类；Berlekamp-Massey算法
中图分类号：TN918.4 **文献标识码**：A **文章编号**：1009-5896(2019)09-2151-05
DOI: 10.11999/JEIT180884

The Linear Complexity of a New Class of Generalized Cyclotomic Sequence of Order q with Period $2p^m$

WANG Yan XUE Gaina LI Shunbo HUI Feifei
(*School of Science, Xi'an University of Architecture and Technology, Xi'an* 710055, *China*)

Abstract: Based on the theory of Ding - generalized circle, a new class of generalized cyclotomic sequences of $2p^m$ (p odd prime and m>1) with arbitrary prime order is constructed in this paper. The polynomial cyclotomic classes are analysed by algebra number theory method. Moreover, the linear complexity of the new sequences are determined, which losely related to the division of quadratic residual classes and quadratic non-residual classes. Results show that the linear complexity of this kind of sequence is much larger than half of the period, hence, can fight Berlekamp-Massey's security application attack that is a pseudo-random sequence with good properties in the sense of cryptography.

Key words: Generalized cyclotomic sequence; Linear complexity; Secondary residual class; Berlekamp-Massey (B-M) algorithm

1 引言

伪随机序列具有不可预测性和随机性，可预先确定和重复，因此被广泛应用于扩频通信、测量距离、雷达导航、CDMA通信、全球定位、软件测试和流密码系统等领域[1]。在应用中，一般要求序列具有长的周期性、低的相关性及高的线性复杂度。为了抵抗已知明文攻击，根据B-M(Berlekamp-Massey)算法，好的伪随机序列的线性复杂度必须大于其半个周期。

Ding[2]基于Whiteman广义分圆类构造了一类周期为pq的2阶广义分圆序列，并证明了该类序列具有好的线性复杂度和自相关性质；随后Ding和Helleseth等人[3]共同提出了新的广义分圆类，实现了对剩余类环最大子群的分割，并定义了新的二元序列(简称Ding-广义分圆序列)；Bai等人[4]确定了基于Ding-Helleseth 2阶广义分圆方法构造了周期为pq二元序列的线性复杂度.文献[5]和文献[6]针对周期为p^m的广义分圆序列提出了迹函数的方法并计算出该序列的线性复杂度；文献[7]给出了F_4上周期为$2pq$的一类新的平衡四元广义分圆序列，研究其线性复杂度；文献[8]给出了一类周期为$2p^2$的二元广义分圆序列，分析了该序列的线性复杂度和自相关性质；文献[9]构造了周期为$p^{m+1}q^{n+1}$的二元广义分圆序列，计算了该序列的线性复杂度；周期为$2p^m$的研究集中采用有限域多项式分解理论并计算了该序列的线性复杂度[10–13]；文献[14]研究了周期为p^{n+1}的二元广义分圆序列，采用分圆类的方法得

收稿日期：2018-09-18；改回日期：2019-06-06；网络出版：2019-06-28
*通信作者： 薛改娜 392455200@qq.com
基金项目：国家自然科学基金(11471255)，西安建筑科技大学自然科学专项(1609718034)，西安建筑科技大学人才基金(RC1338)
Foundation Items: The National Natural Science Foundation of China (11471255), The Natural Science Project of Xi'an University of Architecture and Technology (1609718034), The Talent Fund of Xi'an University of Architecture and Technology (RC1338)

到该序列具有高的线性复杂度。文献[15]构造了一类新的周期为p^m的分圆序列，结果发现该序列具有高的线性复杂度，之后文献[16]具体分析了周期为p^2的序列，表明该序列的线性复杂度接近整个周期，是一类好的序列。

本文在文献[14]的基础上，将构造出具有高线性复杂度的序列。具体安排如下：第2节首次构造了一类新的周期为$2p^m$的q阶二元广义分圆序列，该构造是文献[14]给出的构造的推广；第3节利用分圆类的方法对序列进行细划分，保证该序列具有高的线性复杂度。根据B-M算法，获取该序列的任一段子序列均无法用该算法恢复出整个周期序列；第4节，对本文的工作做了小结。

2 新的广义分圆序列的构造

设p为奇素数且$p\equiv 1(\bmod 4)$, $N=2p^m$，整数$m\geq 1$。模$2p^m$的剩余类环为$Z_{2p^m}=\{0,1,\cdots,2p^m-1\}$，模$2p^m$的乘法群$Z_{2p^m}^*=\{a|\gcd(a,p)=1, a=0,1,\cdots,2p^m-1\}$。由于$Z_{2p^m}^*$是循环群，称它的生成元为模$p^m$的本原根。特别地，若$g$是一个模$p^2$的本原根，则$g$也是模$p^m$的本原根。若$g$为偶数时，则取$g+p^m$为模$p^m$的本原根，从而$g$是$Z_{2p^m}^*$的本原根。因此，$g$是$Z_{p^j}^*$和$Z_{2p^j}^*(1\leq j\leq m)$的公共本原根，且有

$$\mathrm{ord}_{2p^m}(g)=\varphi(2p^m)=\varphi(p^m)=p^{m-1}(p-1) \tag{1}$$

记$(i,j)^{(2p^m)}=|(D_i^{(m)}+1)\cap D_j^{(m)}|$为环$Z_{2p^m}$上的广义分圆数。

定义1 任意正整数$n\geq 1$，$0\leq l\leq q-1$，其中奇素数$p=qf+1$，定义$Z_{2p^m}^*$的广义分圆类为

$$D_0^{(p^j)}=\langle g^q\rangle=\left\{g^{qk}(\bmod p^j): k=1,2,\cdots,\frac{\varphi(p^m)}{q}, 1\leq j\leq m\right\} \tag{2}$$

$$D_0^{(2p^j)}=\langle g^q\rangle=\left\{g^{qk}(\bmod 2p^j): k=1,2,\cdots,\frac{\varphi(p^m)}{q} 1\leq j\leq m\right\} \tag{3}$$

$$D_l^{(p^j)}=g^lD_0^{(p^j)}=\{g^{qk+l}(\bmod p^j): l=0,1,\cdots,q-1 \quad 1\leq j\leq m\} \tag{4}$$

$$D_l^{(2p^j)}=g^lD_0^{(2p^j)}=\{g^{qk+l}(\bmod 2p^j): l=0,1,\cdots, q-1,\ 1\leq j\leq m\} \tag{5}$$

其中，$tD^{(n)}=\{tc(\bmod n): c\in D^{(n)}, t\in Z\}$, $|D_l^{(P^m)}|=|D_l^{(2P^m)}|=\dfrac{p^{m-1}(p-1)}{q}$。

设C和x分别为环Z_{2p^m}上任意的一个子集和一个元素，定义下列运算：$C+x=\{c+x: c\in C\}$，$xC=\{xc: c\in C\}$，显然有

$$Z_{2p^j}^*=\bigcup_{l=0}^{q-1}D_l^{(2p^j)} \tag{6}$$

$$Z_{p^j}^*=\bigcup_{l=0}^{q-1}D_l^{(p^j)} \tag{7}$$

$$Z_2^*=\{1\} \tag{8}$$

则，

$$\begin{aligned}Z_{2p^m}&=\bigcup_{j=1}^{m}(p^{m-j}Z_{2p^j}^*\cup 2p^{m-j}Z_{p^j}^*))\cup p^mZ_2^*\cup\{0\}\\&=\bigcup_{j=1}^{m}(p^{m-j}D_l^{(2p^j)}\cup 2p^{m-j}D_l^{(p^j)}))\cup\{p^m\}\cup\{0\}\end{aligned} \tag{9}$$

$$Z_{p^m}=\bigcup_{j=1}^{m}(p^{m-j}Z_{p^j}^*))\cup\{0\} \tag{10}$$

为了进一步说明，定义$H_l{}^{(p^j)}=p^{m-j}D_l{}^{(p^j)}: H_l{}^{(2p^j)}=p^{m-j}D_l{}^{(2p^j)}$，记

(1) 当$p\equiv\pm 1(\bmod 8)$时，$I=0,1,\cdots,q/2-1$, $J=q/2,q/2+1,\cdots,q-1$，

$$\left.\begin{aligned}&c_0=\bigcup_{j=1}^{m}(H_I{}^{(2p^j)}\cup 2H_I{}^{(p^j)})\cup\{p^m\}\\&c_1=\bigcup_{j=1}^{m}(H_J{}^{(2p^j)}\cup 2H_J{}^{(p^j)})\cup\{0\}\\&Z_{2p^m}=c_0\cup c_1\\&c_0\cap c_1=\varnothing\end{aligned}\right\} \tag{11}$$

周期为$2p^m$的q阶广义分圆序列s定义为

$$s_i=\begin{cases}1, & i \bmod 2p^m\in c_1\\0, & i \bmod 2p^m\in c_0\end{cases},\ i\geq 0 \tag{12}$$

(2) 当$p\equiv\pm 3(\bmod 8)$时，

$$\left.\begin{aligned}&\tilde{c}_0=\bigcup_{j=1}^{m}(H_J{}^{(2p^j)}\cup 2H_I{}^{(p^j)})\cup\{p^m\}\\&\tilde{c}_1=\bigcup_{j=1}^{m}(H_I{}^{(2p^j)}\cup 2H_J{}^{(p^j)})\cup\{0\}\\&Z_{2p^m}=\tilde{c}_0\cup\tilde{c}_1\\&\tilde{c}_0\cap\tilde{c}_1=\varnothing\end{aligned}\right\} \tag{13}$$

周期为$2p^m$的q阶广义分圆序列$\tilde{s}$定义为

$$\tilde{s}_i=\begin{cases}1, & i \bmod 2p^m\in\tilde{c}_1\\0, & i \bmod 2p^m\in\tilde{c}_0\end{cases},\ i\geq 0 \tag{14}$$

利用$p\equiv\pm 1(\bmod 8)$和$p\equiv\pm 3(\bmod 8)$对周期为$2p^m$的q阶广义分圆序列进行细划分，保证了构造的一类新周期序列具有高的线性复杂度。

3 新的广义分圆序列的线性复杂度

设$s=(s_0,s_1,s_2,\cdots,s_{N-1})$是周期为$2p^m$的$q$阶

二元广义分圆序列，有限序列S的生成多项式为$s(x)=s_0+s_1x+\cdots+s_{N-1}x^{N-1}$，线性复杂度$\mathrm{LC}(S)$定义为满足$c_0s_i+c_1s_{i-1}+\cdots+c_ls_{i-l}=0(l\le i\le n)$的最小正整数$l$，其中$c_0=1$且$c_1,\ c_2,\ \cdots,\ c_l\in \mathrm{GF}(q)$，多项式$c(x)=1+c_1x+\cdots+c_lx^l$称为$S$的极小多项式。$s$序列的线性复杂度可表示为

$$\begin{aligned}\mathrm{LC}(s)&=\deg(m(x))\\&=N-\deg(\gcd(x^N-1,\ s(x))\end{aligned}\tag{15}$$

由$N=2p^m$可知，$(x^{P^m}-1)^2\in \mathrm{GF}(2)$。令$\theta$是$\mathrm{GF}(2)$上的$p^m$次本原单位根，其中$\mathrm{GF}(2)$是$x^N-1$在$Z_2$上的分裂域。根据式(15)可得

$$\mathrm{LC}(s)=N-\{a:s(\theta^a)=0,\ 0\le a\le p^m-1\}\tag{16}$$

文献[14]中采用有限域多项式分解理论并计算线性复杂度，但这种计算是复杂的。本节将推广到任意素数阶情形下，采用分圆类的方法得到具有高的线性复杂度序列。

根据定义1，式(12)和式(14)给出序列s和$\tilde{s}$的生成多项式分别为

$$\begin{aligned}s(x)&=\sum_{i\in c_1}x^i\\&=1+\sum_{j=1}^{m}\left(\sum_{i\in H_J^{(2p^j)}}x^i+\sum_{i\in 2H_J^{(p^j)}}x^i\right)\in F_2[x]\end{aligned}\tag{17}$$

$$\begin{aligned}\tilde{s}(x)&=\sum_{i\in c_1}x^i\\&=1+\sum_{j=1}^{m}\left(\sum_{i\in H_1^{(2p^j)}}x^i+\sum_{i\in 2H_J^{(p^j)}}x^i\right)\in F_2[x]\end{aligned}\tag{18}$$

记

$$\left.\begin{aligned}S_l^{(j)}(x)&=\sum_{i\in H_1^{(2p^j)}}x^i\\T_l^{(j)}(x)&=\sum_{i\in 2H_l^{(p^j)}}x^i\\L_l(x)&=\sum_{i\in D_l^{(p)}}x^i\end{aligned}\right\}\tag{19}$$

并记

$$\left.\begin{aligned}&|D_l^{(P^m)}|=|D_l^{(2P^m)}|=\frac{p^{m-1}(p-1)}{q}\\&Z_{2p^j}^*=\bigcup_{l=0}^{q-1}D_l^{(2p^j)}\\&Z_{p^j}^*=\bigcup_{l=0}^{q-1}D_l^{(p^j)}\end{aligned}\right\}\tag{20}$$

其中，p为奇素数且$0\le l\le q-1$。

为求一类新的周期为$2p^m$的q阶广义分圆序列的线性复杂度，给出如下引理：

引理1　$D_l^{(2p^j)}(\bmod p^j)=D_l^{(p^j)}(0\le l\le q-1,\ 1\le j\le m)$。

证明　根据$D_l^{(2p^j)}$的定义可知，当s跑遍$D_l^{(2p^j)}$时，s模p^j跑遍$D_l^{(p^j)}$中每个元素p^j次。因此$D_l^{(2p^j)}(\bmod p^j)=D_l^{(p^j)}$且$|D_l^{(2p^j)}|=|D_l^{(p^j)}|$。　证毕

推论1[4,15]　$2\in D_l^{(p)}$当且仅当$2\in D_l^{(p^j)}0\le l\le q-1,\ 1\le j\le m$。

引理2　若p是奇素数，且2是模p^2的本原根，则$2D_l^{(2p^j)}=2D_l^{(p^j)}(0\le l\le q-1,\ 1\le j\le m)$。

证明　根据2是模p^2的本原根且由推论1得$2\in\bigcap_{j=1}^{m}D_l^{(p^j)}$，

$$\begin{aligned}2D_l^{(2p^j)}&=2\left\{g^{qk+l}(\bmod 2p^j)\ :k=1,\cdots,\ \frac{\varphi(p^m)}{q}\right\}\\&=\left\{2g^{qk+l}(\bmod 2p^j)\ :k=1,\cdots,\ \frac{\varphi(p^m)}{q}\right\}\\&=\left\{2(g^{qk+l}(\bmod p^j))\ :k=1,\cdots,\ \frac{\varphi(p^m)}{q}\right\}\\&=2\left\{(g^{qk+l}(\bmod p^j))\ :k=1,\cdots,\ \frac{\varphi(p^m)}{q}\right\}\\&=2D_l^{(p^j)}\end{aligned}\tag{21}$$

证毕

引理3[10]　设$l\in\{0,1,\cdots q-1\},1\le j\le m$，则有

(1) $D_l^{(p^j)}=\{x+py:\ x\in D_l^{(p)},y\in Z_{p^{j-1}}\}$；

(2) $D_l^{(2p^j)}=\{x+py+\delta_{x,y}:\ x\in D_l^{(p)},y\in Z_{p^{j-1}}\}$，

其中，$\delta_{x,y}=\begin{cases}0,&\text{若}x+py\text{为奇数}\\p^j,&\text{若}x+py\text{为偶数}\end{cases}$。

证明　根据文献[10]，引理3中的(1)显然成立。下证(2)：

任意$x+py\in D_l^{(p^j)}$，若$x+py$为奇数，则$x+py\in D_l^{(2p^j)}$；若$x+py$为偶数，则$x+py+p^k\in D_l^{(2p^j)}$，进而得到$D_l^{(2p^j)}=D_l^{(p^j)}=D_l^{(p)}(\bmod p)$，且$\left|D_l^{(2p^j)}\right|=\left|D_l^{(p^j)}\right|$。　证毕

引理4[1,3]　若$p\equiv\pm1(\bmod 8)$，则$2(\bmod p)\in D_I^{(p)}$，$I=0,1,\cdots,q/2-1$；若$p\equiv\pm3(\bmod 8)$，则$2(\bmod p)\in D_J^{(p)}$，$J=q/2,q/2+1,\cdots,q-1$。

定理1　设$\alpha=\theta^a$，记$a=p^fi\in p^fZ_{2p^{m-j}}^*$，其中$0\le f\le m-1,\ i\in Z_{2p^{m-j}}^*,\ l\in\{0,1,\cdots q-1\},\ 1\le j\le m,\ \beta=\theta^{P^{m-1}}$可得：

(1) 当$p\equiv\pm1(\bmod 8)$时，

$$S_l^{(j)}(\alpha)=\begin{cases}p-1/q\,,\ j\le f\\ L_l(\beta^i)\quad,\ j=f+1\\ 0\qquad\ ,\ j>f+1\end{cases}\tag{22}$$

$$T_l^{(j)}(\alpha)=\begin{cases}p-1/q\,,\ j\le f\\ L_l(\beta^i)\quad,\ j=f+1\\ 0\qquad\ ,\ j>f+1\end{cases}\tag{23}$$

(2) 当$p\equiv\pm3(\bmod 8)$时，

$$S_l^{(j)}(\alpha)=\begin{cases}p-1/q\,,\ j\le f\\ L_l(\beta^i)\quad,\ j=f+1\\ 0\qquad\ ,\ j>f+1\end{cases}\tag{24}$$

$$T_l^{(j)}(\alpha)=\begin{cases}p-1/q\,,\ j\le f\\ L_{l+1}(\beta^i)\,,\ j=f+1\\ 0\qquad\ ,\ j>f+1\end{cases}\tag{25}$$

证明 由式(19)知$S_l^{(j)}(\alpha)=\sum_{t\in H_l^{(2p^j)}}\alpha^t=\sum_{t\in p^{m-j}D_l^{(2p^j)}}\theta^{p^fit}=\sum_{t\in p^{m+f-j}D_l^{(2p^j)}}\theta^{it}\in F_2$，(其中，$\theta$是$F_2$上的$p^m$次本原单位根)和$D_l^{(2p^j)}(\bmod p^j)=D_l^{(p^j)}$，可得：当$j\le f$时，$S_l^{(j)}(\alpha)=|D_l^{(p^j)}|=p^{j-1}$。$(p-1)/q=(p-1)/q$；当$j=f+1$时，$S_l^{(j)}(\alpha)=\sum_{t\in D_l^{(p^j)}}\theta^{ip^{m-1}t}=\sum_{t\in D_l^{(p^j)}}\beta^{it}$。其中$\beta=\theta^{P^{m-1}}$，由引理3可知，$D_l^{(p^j)}=D_l^{(p)}+pZ_{p^{j-1}}$，故$S_l^{(j)}(\alpha)=p^{j-1}\sum_{t\in D_l^{(p)}}\beta^{it}=L_l(\beta^i)$；

当$j>f+1$时，假设

$$\left.\begin{aligned}&D_l^{(p^j)}=\left\{x_h+py:x_h\in D_l^{(p)},y\in Z_{p^{j-1}}\right\}\\&\theta^{ip^{m+f}}-1=(\theta^{ip^{m+f-j+1}}-1)\sum_{h=0}^{\frac{p-1}{2}}\sum_{y=0}^{p^{j-1}-1}\theta^{p^{m+f-j}i(x_h+py)}\\&\qquad=0,\theta^{ip^{m+f-j+1}}-1\ne0\\&S_l^{(j)}(\alpha)=\sum_{t\in D_l^{(2p^j)}}\theta^{p^{m+f-j}it}\\&\qquad=\sum_{h=0}^{\frac{p-1}{2}}\sum_{y=0}^{p^{j-1}-1}\theta^{p^{m+f-j}i(x_h+py)}=0\end{aligned}\right\}\tag{26}$$

同理，$T_l^{(j)}(\alpha)=\sum_{t\in 2H_l^{(p^j)}}\alpha^t=\sum_{t\in 2p^{m-j}D_l^{(2p^j)}}\theta^{p^fit}=\sum_{t\in p^{m+f-j}2D_l^{(p^j)}}\theta^{it}$。

若$p\equiv\pm1(\bmod 8)$，根据引理4可得$2\in D_I^{(p)}$，即$2D_l^{(p^j)}=D_{l+I}^{(p^j)}$；

若$p\equiv\pm3(\bmod 8)$，根据引理4可得$2\in D_J^{(p)}$，即$2D_l^{(p^j)}=D_{l+J}^{(p^j)}$。 证毕

定理2 设$\alpha=\theta^a$，记$a=2p^fi\in 2p^fZ_{p^{m-f}}^*$，其中$0\le f\le m-1 i\in Z_{2p^{m-j}}^* l\in\{0,1,\cdots q-1\}$，$1\le j\le m$,$\beta=\theta^{P^{m-1}}$ 可得

(1) 当$p\equiv\pm1(\bmod 8)$时，

$$S_l^{(j)}(\alpha)=\begin{cases}p-1/q\,,\ j\le f\\ L_l(\beta^i)\quad,\ j=f+1\\ 0\qquad\ ,\ j>f+1\end{cases}\tag{27}$$

$$T_l^{(j)}(\alpha)=\begin{cases}p-1/q\,,\ j\le f\\ L_l(\beta^i)\quad,\ j=f+1\\ 0\qquad\ ,\ j>f+1\end{cases}\tag{28}$$

(2) 当$p\equiv\pm3(\bmod 8)$时

$$S_l^{(j)}(\alpha)=\begin{cases}p-1/q\ ,\ j\le f\\ L_{l+1}(\beta^i)\,,\ j=f+1\\ 0\qquad\ ,\ j>f+1\end{cases}\tag{29}$$

$$T_l^{(j)}(\alpha)=\begin{cases}p-1/q\,,\ j\le f\\ L_l(\beta^i)\quad,\ j=f+1\\ 0\qquad\ ,\ j>f+1\end{cases}\tag{30}$$

证明 根据式(19)知$S_l^{(j)}(\alpha)=\sum_{t\in H_l^{(2p^j)}}\alpha^t=\sum_{t\in p^{m-j}D_l^{(2p^j)}}\theta^{2p^fit}=\sum_{t\in p^{m+f-j}2D_l^{(p^j)}}\theta^{it}$，同样地，$T_l^{(j)}(\alpha)=\sum_{t\in 2H_l^{(p^j)}}\alpha^t=\sum_{t\in 2p^{m-j}D_l^{(2p^j)}}\theta^{2p^fit}=\sum_{t\in p^{m+f-j}D_l^{(p^j)}}\theta^{it}$，证明方法如定理2。 证毕

定理3 周期为$2p^m$的q阶广义分圆序列s和$\tilde{s}$的线性复杂度为$2p^m$。

证明 根据定义中式(12)和式(14)可得s和$\tilde{s}$的生成多项式分别为

$$\left.\begin{aligned}s(x)&=\sum_{i\in c_1}x^i=1+\sum_{j=1}^{m}\left(\sum_{i\in H_J^{(2p^j)}}x^i+\sum_{i\in 2H_J^{(p^j)}}x^i\right)\\&\in F_2[x]\\\tilde{s}(x)&=\sum_{i\in c_1}x^i=1+\sum_{j=1}^{m}\left(\sum_{i\in H_I^{(2p^j)}}x^i+\sum_{i\in 2H_J^{(p^j)}}x^i\right)\\&\in F_2[x]\end{aligned}\right\}\tag{31}$$

当$a=0$或$a=p^m$时，可得$S(\theta^a)=\tilde{S}(\theta^a)=1$；

当$p\equiv\pm1(\bmod 8)$时，任意$a\in Z_{2P^m}\backslash\{0,p^m\}$，根据定理1和定理2得$S(\theta^a)=1+2L_0(\beta)=1$或$S(\theta^a)=1+2L_1(\beta)=1$；

当$p\equiv\pm3(\bmod 8)$时，任意$a\in Z_{2P^m}\backslash\{0,p^m\}$根据定理1和定理2得$\tilde{S}(\theta^a)=1$，由式(16)可得：$\mathrm{LC}(s)2=p^m-\{a:s(\theta^a)=0,\ 0\le a\le p^m-1\}=2p^m,\mathrm{LC}(\tilde{s})=2p^m-\{a:\tilde{s}(\theta^a)=0,\ 0\le a\le p^m-1\}=2p^m$。 证毕

4　结束语

本文研究周期为$2p^m$的q阶二元广义分圆序列的线性复杂度，创新点是对伪随机序列通过$p \equiv 1(\bmod 8)$和$p \equiv 3(\bmod 8)$进行分圆类讨论，并计算线性复杂度. 结果表明新序列具有高的线性复杂度且为整个周期，安全性高，能够抵抗B-M算法的攻击，在保密通讯中有广泛的应用。

参 考 文 献

[1] GOLOMB S W and GONG Guang. Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar[M]. Cambridge: Cambridge University Press, 2005: 174–175.

[2] DING Cunsheng. Linear complexity of generalized cyclotomic binary sequences of order 2[J]. *Finite Fields and Their Applications*, 1997, 3(2): 159–174. doi: 10.1006/ffta.1997.0181.

[3] DING Cunsheng, HESSESETH T, and SHAN Weijuan. On the linear complexity of Legendre sequences[J]. *IEEE Transactions on Information Theory*, 1998, 44(3): 1276–1278. doi: 10.1109/18.669398.

[4] BAI Enjian, LIU Xiaojuan, and XIAO Guozhen. Linear complexity of new generalized cyclotomic sequences of order two of length pq[J]. *IEEE Transactions on Information Theory*, 2005, 51(5): 1849–1853. doi: 10.1109/TIT.2005.846450.

[5] YAN Tongjiang, LI Shengqiang, and XIAO Guozhen. On the linear complexity of generalized cyclotomic sequences with the period p^m[J]. *Applied Mathematics Letters*, 2008, 21(2): 187–193. doi: 10.1016/j.aml.2007.03.011.

[6] DU Xiaoni, YAN Tongjiang, and XIAO Guozhen. Trace representation of some generalized cyclotomic sequences of length pq[J]. *Information Sciences*, 2008, 178(16): 3307–3316. doi: 10.1016/j.ins.2007.11.023.

[7] 魏万银, 杜小妮, 王国辉. 周期为$2pq$的四元序列线性复杂度研究[J]. 计算机工程, 2016, 42(3): 161–164. doi: 10.3969/j.issn.1000-3428.2016.03.029.

WEI Wanyin, DU Xiaoni, and WANG Guohui. Research on linear complexity of quaternary sequences with period $2pq$[J]. *Computer Engineering*, 2016, 42(3): 161–164. doi: 10.3969/j.issn.1000-3428.2016.03.029.

[8] 杜小妮, 王国辉, 魏万银. 周期为$2p^2$的四阶二元广义分圆序列的线性复杂度[J]. 电子与信息学报, 2015, 37(10): 2490–2494. doi: 10.11999/JEIT150180.

DU Xiaoni, WANG Guohui, and WEI Wanyin. Linear complexity of binary generalized cyclotomic sequences of order four with period $2p^2$[J]. *Journal of Electronics & Information Technology*, 2015, 37(10): 2490–2494. doi: 10.11999/JEIT150180.

[9] HU Liqin, YU Qin, and WANG Minhong. The linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$[J]. *IEEE Transactions on Information Theory*, 2012, 58(8): 5534–5543. doi: 10.1109/TIT.2012.2196254.

[10] ZHANG Jingwei, ZHAO Chang'an, and MA Xiao. Linear complexity of generalized cyclotomic binary sequences of length $2p^m$[J]. *Applicable Algebra in Engineering, Communication and Computing*, 2010, 21(2): 93–108. doi: 10.1007/s00200-009-0116-2.

[11] TAN Lin, XU Hong, and QI Wenfeng. Remarks on the generalized cyclotomic sequences of length $2p^m$[J]. *Applicable Algebra in Engineering, Communication and Computing*, 2012, 23(5/6): 221–232. doi: 10.1007/s00200-012-0177-5.

[12] KE Pinhui, ZHANG Jie, and ZHANG Shengyuan. On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2p^n$[J]. *Designs, Codes and Cryptography*, 2013, 67(3): 325–339. doi: 10.1007/s10623-012-9610-9.

[13] EDEMSKIY V and ANTONOVA O. The linear complexity of generalized cyclotomic sequences with period $2p^n$[J]. *Applicable Algebra in Engineering, Communication and Computing*, 2014, 25(3): 213–223. doi: 10.1007/s00200-014-0223-6.

[14] EDEMSKIY V. 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. doi: 10.1007/s10623-010-9474-9.

[15] 刘龙飞, 杨凯, 杨晓元. 新的周期为p^m的GF(h)上广义割圆序列的线性复杂度[J]. 通信学报, 2017, 38(9): 39–45. doi: 10.11959/j.issn.1000-436x.2017181.

LIU Longfei, YANG Kai, and YANG Xiaoyuan. On the linear complexity of a new generalized cyclotomic sequence with length p^m over GF(h)[J]. *Journal on Communications*, 2017, 38(9): 39–45. doi: 10.11959/j.issn.1000-436x.2017181.

[16] XIAO Zibi, ZENG Xiangyong, LI Chunlei, *et al*. New generalized cyclotomic binary sequences of period p^2[J]. *Designs, Codes and Cryptography*, 2018, 86(7): 1483–1497. doi: 10.1007/s10623-017-0408-7.

王　艳：女，1982年生，副教授，研究方向为序列密码.

薛改娜：女，1992年生，硕士生，研究方向为序列密码.

李顺波：男，1979年生，副教授，研究方向为流密码分析.

惠飞飞：女，1992年生，硕士生，研究方向为流密码分析.