# $F_q$上一类周期为$2p^2$的四元广义分圆序列的线性复杂度

王 艳 相乃姣* 韩西林 闫联陶
(西安建筑科技大学理学院 西安 710055)

**摘 要**：该文基于广义分圆理论，通过计算$F_q(q=r^m)$上的序列生成多项式的零点个数，确定了一类周期为$2p^2$的四元广义分圆序列的极小多项式和线性复杂度。结果表明，该序列的线性复杂度大于其周期的1/2，能够有效地抵抗Berlekamp-Massey (B-M)算法的攻击，是密码学意义上一类良好的周期伪随机序列。

**关键词**：广义分圆序列；4元序列；线性复杂度；生成多项式；极小多项式
**中图分类号**：TN918.4 **文献标识码**：A **文章编号**：1009-5896(2021)10-2936-08
**DOI**: 10.11999/JEIT210095

# Linear Complexity over $F_q$ of a Class of Generalized Cyclotomic Quaternary Sequences with Period $2p^2$

WANG Yan XIANG Naijiao HAN Xilin YAN Liantao
(*School of Science, Xi' an University of Architecture and Technology, Xi'an* 710055, *China*)

**Abstract**: Based on the theory of generalized cyclotomy, the minimal polynomial and linear complexity of a class of generalized cyclotomic quaternary sequences with period $2p^2$ are determined by explicitly computing the number of zeros of the generating polynomial over $F_q(q=r^m)$. The results show that the linear complexity is more than $p^2$, the half of the period $2p^2$. According to Berlekamp-Massey algorithm, these sequences can be viewed as enough good for the utilizing in cryptography.

**Key words**: Generalized cyclotomic sequences; Quaternary sequences; Linear complexity; Generating polynomial; Minimal polynomial

## 1 引言

伪随机序列在流密码、扩频通信、雷达导航、全球定位等领域中都有着极为重要的应用[1]。伪随机序列的密码学性质，如周期性、相关性、线性复杂度、2-adic复杂度等直接影响着一个流密码算法的安全强度。其中线性复杂度是衡量伪随机序列性质的一个重要指标，根据Berlekamp-Massey(B-M)算法，若一个伪随机序列的线性复杂度大于其周期长度的1/2，则可称其为一个好的伪随机序列。

目前，已有大量的文献研究了广义分圆序列的线性复杂度。Ding[2]基于Whiteman广义分圆理论构造了一类周期为$pq$的2元广义分圆序列，并证明了这类序列具有高的线性复杂度和低的自相关性；Bai等人[3]基于Ding–Helleseth广义分圆理论构造了一类新的周期为$pq$的2元广义分圆序列，并确定了该类序列具有高的线性复杂度；李胜强等人[4]基于Whiteman广义分圆理论，通过选取不同的特征集，构造了一类新的周期为$pq$的2元广义分圆序列，得出该类序列的线性复杂度的下界为$pq-p-q+1$，并指出该类序列为平衡序列。Xiao等人[5]构造了一类新的周期为$p^2$的2元广义分圆序列，计算出了该类序列具有高的线性复杂度，最后提出了一类新的周期为$p^m$的2元广义分圆序列，并给出了一个关于其线性复杂度的猜想；随后Edemskiy等人[6]证明了这个猜想，并将其结果推广到了更一般的情形；Ouyang等人[7]基于Edemskiy等人的工作构造了两类周期为$2p^m$的2元广义分圆序列，并给出了其线性复杂度的取值范围，结果表明这两类序列都具有好的线性复杂度性质。王艳等人[8]研究了一类新的周期为$2p^m$的$q$阶2元广义分圆序列，并证明了该类序列具有高的线性复杂度；Wang等人[9]构造了$F_4$上的一类周期为$2p^mq^n$的4元广义分圆序列，证明了该类序列的线性复杂度可以达到最大；Ke等人[10]构

收稿日期：2021-01-26；改回日期：2021-07-16；网络出版：2021-07-29
*通信作者： 相乃姣 xiangnaijiao@xauat.edu.cn
基金项目：国家自然科学基金(61902304)，陕西省自然科学基础研究计划资助项目(2021JQ-495)
Foundation Items: The National Natural Science Foundation of China (61902304), and The Project Supported by Natural Science Basic Research Plan in Shaanxi Province of China (2021JQ-495)

造了两类新的周期为$2p^m$的4元广义分圆序列，分别确定了这两类序列在$F_4$和$Z_4$上都具有高的线性复杂度。Du等人[11]研究了$F_4$上的周期为$2p$的4元广义分圆序列的线性复杂度，结果表明其最小值为$p+1$；Chen等人[12]确定了$Z_4$上的周期为$2p$的4元广义分圆序列的线性复杂度，结果表明其最小值为$p$；杜小妮等人[13]在Chen的基础上进行了推广，给出了$Z_4$上周期为$2p^2$的4元广义分圆序列的线性复杂度，结果表明该类序列具有好的线性复杂度性质。本文基于文献[13]构造的序列，构造了一类$F_q$上的周期为$2p^2$的4元广义分圆序列，并计算了该类序列在$F_q$上的极小多项式和线性复杂度。本文结构安排如下：第2节给出了$F_q$上一类周期为$2p^2$的4元广义分圆序列；第3节确定了该类序列在$F_q$上的极小多项式和线性复杂度；第4节对文章的工作做了小结和展望。

## 2　基础知识

设$p$是奇素数，$g$是奇数，且$g$是模$p$,$2p$,$p^2$和$2p^2$的公共本原元。记模$2p^2$的剩余类环为$Z_{2p^2}=\{0,1,\cdots,2p^2-1\}$。

对$i=0,1$, 令

$$\begin{aligned}
D_i^{(2p^2)}&=\left\{g^{2k+i}(\mathrm{mod}\ 2p^2):k=0,1,\cdots,\frac{p(p-1)}{2}-1\right\},\\
D_i^{(p^2)}&=\left\{g^{2k+i}(\mathrm{mod}\ p^2):k=0,1,\cdots,\frac{p(p-1)}{2}-1\right\},\\
D_i^{(2p)}&=\left\{g^{2k+i}(\mathrm{mod}\ 2p):k=0,1,\cdots,\frac{p-1}{2}-1\right\},\\
D_i^{(p)}&=\left\{g^{2k+i}(\mathrm{mod}\ p):k=0,1,\cdots,\frac{p-1}{2}-1\right\}
\end{aligned}\tag{1}$$

为了简便，本文记$P_0=p\left(D_0^{(2p)}\cup D_1^{(2p)}\right)$, $P_1=2p\left(D_0^{(p)}\cup D_1^{(p)}\right)$, $R=\{0\}$。显然，

$$\begin{aligned}
Z_{2p^2}=&D_0^{(2p^2)}\cup D_1^{(2p^2)}\cup 2D_0^{(p^2)}\cup 2D_1^{(p^2)}\cup P_0\\
&\cup P_1\cup R\cup\{p^2\}
\end{aligned}\tag{2}$$

构造$F_{r^m}(r\geq 5)$上的4元广义分圆序列

$$s(t)=\begin{cases}0, & t\in R\cup D_0^{(2p^2)}\\ 1, & t\in D_1^{(2p^2)}\cup P_0\\ 2, & t\in 2D_1^{(p^2)}\cup\{p^2\}\\ 3, & t\in 2D_0^{(p^2)}\cup P_1\end{cases}\tag{3}$$

设$r$是奇素数，$m$是正整数，$F_{r^m}$是一个特征为$r$的扩域。设$\{s(t):t=0,1,\cdots,N-1\}$是$F_{r^m}$上周期为$N$的序列。序列$\{s(t)\}$在$F_{r^m}$上的线性复杂度是生成序列的最短的线性反馈移位寄存器的级数，记为$LC(s)$，$L$是满足$s(t+L)=c_{L-1}s(t+L-1)+\cdots+c_1s(t+1)+c_0s(t)$，其中$t\geq 0,c_0,c_1,\cdots,c_{L-1}\in F_{r^m}$的最小正整数。序列$\{s(t)\}$的极小多项式定义为$m(x)=x^L-\sum_{i=0}^{L-1}c_ix^i$，生成多项式定义为$S(x)=\sum_{i=0}^{N-1}s(t)x^t$，极小多项式和生成多项式的关系为$m(x)=\dfrac{x^N-1}{\gcd(x^N-1,S(x))}$。序列$\{s(t)\}$的线性复杂度表示为

$$LC(s)=N-\deg(\gcd(x^N-1,S(x)))\tag{4}$$

设$m=\mathrm{ord}_{p^2}(r)$，$\beta$是扩域$F_{r^m}$上的$2p^2$次单位根，由式(4)可得

$$LC(s)=N-\left|\left\{k:S(\beta^k)=0,0\leq k<N\right\}\right|\tag{5}$$

记模$N$的$d$阶分圆数为$(i,j)^{(N)}=\left|(D_i^{(N)}+1)\cap D_j^{(N)}\right|$, $i,j=0,1,\cdots,d-1$。

## 3　主要结论及证明

### 3.1　主要定理及辅助引理

**定理1**　设$r$为奇素数，且满足$r\geq 5,r\neq p$, $m=\mathrm{ord}_{p^2}(r)$，并设$\beta$为扩域$F_{r^m}$上的$2p^2$次单位根。由式(3)定义的周期为$2p^2$的4元广义分圆序列$\{s(t)\}$在$F_{r^m}$上的线性复杂度为

$$LC(s)=\begin{cases}
2p^2-1, & r\left|3p^2+p-2\text{或}r\right|p^2-2\\
2p^2-p+1, & r\left|p-4\text{或}r\right|p-2\\
2p^2-2, & r\left|3p^2+p-2\text{且}r\right|p^2-2\\
2p^2-p, & r\left|p^2-2\text{且}r\right|p-4\text{或}r\left|3p^2\right.\\
 & \left.+p-2\text{且}r\right|p-4\text{ 或}\\
 & r\left|p-2\text{且}r\right|p^2-2\text{ 或}\\
 & r\left|3p^2+p-2\text{且}r\right|p-2\\
2p^2-p-1, & r\left|3p^2+p-2\text{且}r\right|p^2-2\\
 & \text{且}r\left|p-4\text{ 或}r\right|3p^2+p-2\\
 & \text{且}r\left|p^2-2\text{ 且}r\right|p-2\\
2p^2, & r\not|3p^2+p-2\text{且}r\not|p^2-2\\
 & \text{且}r\not|p-4\text{且}r\not|p-2
\end{cases}\tag{6}$$

下面给出证明定理1所需的引理。

**引理1**[10,14]　设$p$为奇素数，有

(1) $2\in D_0^{(p^2)}$当且仅当$2\in D_0^{(p)}$，$2\in D_0^{(p)}$当且仅当$p\equiv\pm 1(\mathrm{mod}\ 8)$。

(2) $2\in D_1^{(p^2)}$当且仅当$2\in D_1^{(p)}$，$2\in D_1^{(p)}$当且仅当$p\equiv\pm 3(\mathrm{mod}\ 8)$。

**引理2**[14]　设$p$为奇素数，有

(1)若$t\in Z_{2p^2}^*,i=0,1,j=1,2$，则

$$tD_i^{(p^j)}(\mathrm{mod}p^j)=\begin{cases}D_i^{(p^j)}, & t\in D_0^{(2p^2)}\\ D_{i+1}^{(p^j)}, & t\in D_1^{(2p^2)}\end{cases}\tag{7}$$

(2)若$t\in Z_{p^2}^*, i=0,1, j=1,2$，则

$$tD_i^{(p^j)}(\mathrm{mod}p^j)=\begin{cases}D_i^{(p^j)}, & t\in D_0^{(p^2)}\\ D_{i+1}^{(p^j)}, & t\in D_1^{(p^2)}\end{cases} \tag{8}$$

**引理3** 设$a$为正整数，$p$为奇素数，若$i,j\in\{0,1\}$，则

(1) 若$a\in D_i^{(2p^2)}$, 则$aP_j=P_j$;

(2) 若 $a\in 2D_i^{(p^2)}$, 则$aD_j^{(2p^2)}=2D_{i+j(\bmod 2)}^{(p^2)}$, $aP_j=P_1$ ;

(3) 若 $a\in P_0$, 则$aD_i^{(2p^2)}=P_0, a\cdot 2D_i^{(p^2)}=P_1$, $aP_0=p^2, aP_1=R$ ;

(4) 若 $a\in P_1$, 则$aD_i^{(2p^2)}=a\cdot 2D_i^{(p^2)}=P_1$, $aP_i=R$ ;

(5) $D_i^{(p^2)}(\mathrm{mod}p)=D_i^{(p)}$, $D_i^{(2p^2)}(\mathrm{mod}p^2)=D_i^{(p^2)}$。

**证明** (1)—(4)的证明可参考文献[13]。下证(5)：因为$g$是模$p$和$p^2$的公共本原元，所以

$$\begin{aligned}&D_i^{(p^2)}(\mathrm{mod}\ p)\\&=\left\{g^{2k+i}(\mathrm{mod}\ p), k=0,1,\cdots,\frac{p(p-1)}{2}-1\right\}\\&=\left\{g^{2k+i}(\mathrm{mod}\ p), k=0,1,\cdots,\frac{p-1}{2}-1\right\}\\&=D_i^{(p)}\end{aligned} \tag{9}$$

同理可得$D_i^{(2p^2)}(\mathrm{mod}p^2)=D_i^{(p^2)}$。 证毕

**引理4** 设$p$为奇素数，有

$$2^{-1}(\mathrm{mod}p^2)\in\begin{cases}D_0^{(p^2)}, & p\equiv\pm1(\mathrm{mod}8)\\ D_1^{(p^2)}, & p\equiv\pm3(\mathrm{mod}8)\end{cases} \tag{10}$$

**证明** 根据引理1可得。

**引理5** 设$p$为奇素数，$\beta$为扩域$F_{r^m}$上的$2p^2$次单位根，$r$为奇素数，且满足$r\geq5, r\neq p$,有

$$\beta^{p^2k}\equiv\begin{cases}-1(\mathrm{mod}r), & k\in D_0^{(2p^2)}\cup D_1^{(2p^2)}\cup P_0\cup\{p^2\}\\ 1(\mathrm{mod}r), & k\in 2D_0^{(p^2)}\cup 2D_1^{(p^2)}\cup P_1\cup R\end{cases} \tag{11}$$

**证明** 由$\beta$为$F_{r^m}$上的$2p^2$次单位根可得$\beta^{p^2}=-1$, 所以$k$为偶数时，$\beta^{p^2k}=1$, $k$为奇数时，$\beta^{p^2k}=-1$。 证毕

**引理6** 设$p$为奇素数，$\beta$为$F_{r^m}$上的$2p^2$次单位根，有

$$\sum_{t\in 2D_1^{(p^2)}}\beta^{kt}+\sum_{t\in 2D_0^{(p^2)}}\beta^{kt}+\sum_{t\in P_1}\beta^{kt}\equiv-1(\mathrm{mod}\ r) \tag{12}$$

其中$k\in D_0^{(2p^2)}\cup D_1^{(2p^2)}\cup 2D_0^{(p^2)}\cup 2D_1^{(p^2)}$。

**证明** 由$\beta^0+\beta^{p^2}+\sum_{t\in D_0^{(2p^2)}}\beta^t+\sum_{t\in D_1^{(2p^2)}}\beta^t+\sum_{t\in 2D_0^{(p^2)}}\beta^t+\sum_{t\in 2D_1^{(p^2)}}\beta^t+\sum_{t\in P_0}\beta^t+\sum_{t\in P_1}\beta^t=0$可得。

**引理7** 设$p$为奇素数，$\beta$为$F_{r^m}$上的$2p^2$次单位根，有$\sum_{i\in P_1}\beta^i=-1, \sum_{i\in P_0}\beta^i=1$。

**证明** 由$\beta^{2p^2}-1=(\beta^p-1)(1+\beta^p+\beta^{2p}+\cdots+\beta^{(2p-1)p})=(\beta^{2p}-1)(1+\beta^{2p}+\beta^{2\cdot2p}+\cdots+\beta^{(p-1)\cdot2p})=0$，可得

$$1+\beta^p+\beta^{2p}+\cdots+\beta^{(2p-1)p}=0 \tag{13}$$

$$1+\beta^{2p}+\beta^{2\cdot2p}+\cdots+\beta^{(p-1)\cdot2p}=0 \tag{14}$$

即

$$1+\sum_{i\in P_1}\beta^i+\sum_{i\in P_0}\beta^i+\beta^{p^2}=0 \tag{15}$$

$$1+\sum_{i=1}^{p-1}\beta^{2pi}=0 \tag{16}$$

于是$1+\sum_{i\in 2pD_0^{(p)}\cup 2pD_1^{(p)}}\beta^i=0$, 进而$\sum_{i\in P_1}\beta^i=-1, \sum_{i\in P_0}\beta^i=1$。 证毕

**引理8** 设$p$为奇素数，$r$为奇素数，且满足$r\geq5, r\neq p$, $\beta$为$F_{r^m}$上的$2p^2$次单位根，则有

$$\sum_{t\in D_1^{(2p^2)}}\beta^{kt}\equiv\beta^{p^2k}\sum_{j\in D_1^{(p^2)}}\beta^{2\cdot j\cdot k\cdot(2^{-1}\bmod p^2)}(\mathrm{mod}r) \tag{17}$$

其中$k\in D_0^{(2p^2)}\cup D_1^{(2p^2)}\cup 2D_0^{(p^2)}\cup 2D_1^{(p^2)}$。。

**证明** 记 $M_{p^2}=2\cdot(2^{-1}(\bmod p^2))(\mathrm{mod}2p^2)$, $M_2=p^2\cdot(p^{2\bullet(-1)}(\mathrm{mod}\ 2))(\mathrm{mod}\ 2p^2)$, $Z_2^*$表示$Z_2$中所有可逆元素的集合。当$t\in D_1^{(2p^2)}$，且$j\equiv t(\mathrm{mod}\ p^2)$时，构造从$D_1^{(2p^2)}$到$Z_2^*\times D_1^{(p^2)}$的同构

$$\begin{aligned}D_1^{(2p^2)}&\cong Z_2^*\times D_1^{(p^2)}\\ t&\mapsto(1,j)\end{aligned} \tag{18}$$

由中国剩余定理可得$t\equiv1\cdot M_2+j\cdot M_{p^2}(\mathrm{mod}2p^2)\equiv p^2+j\cdot2\cdot(2^{-1}(\mathrm{mod}p^2))(\mathrm{mod}2p^2)$, 所以

$$\begin{aligned}\sum_{t\in D_1^{(2p^2)}}\beta^{kt}&\equiv\sum_{j\in D_1^{(p^2)}}\beta^{k\cdot(p^2+j\cdot2(2^{-1}\bmod p^2))}\\&\equiv\beta^{p^2k}\sum_{j\in D_1^{(p^2)}}\beta^{2\cdot j\cdot k\cdot(2^{-1}\bmod p^2)}(\mathrm{mod}r)\end{aligned} \tag{19}$$

证毕

**引理9** 若$p\equiv1(\mathrm{mod}\ 4)$，则$-1\in D_0^{(p)}$；若$p\equiv3(\mathrm{mod}\ 4)$，则$-1\in D_1^{(p)}$。

**证明** 当$p\equiv1(\mathrm{mod}4)$时，不妨设$p=4t+1$，$t$为正整数。因为$\mathrm{ord}_p(g)=p-1$，即$g^{p-1}\equiv$

$1(\mathrm{mod}p)$，所以有$g^{4t}-1\equiv 0(\mathrm{mod}p)$。又因为$g^{4t}-1=(g^{2t}+1)(g^{2t}-1)$，且$g$为模$p$的本原根，所以有$g^{2t}-1\equiv /0(\mathrm{mod}p)$, $g^{2t}+1\equiv 0(\mathrm{mod}p)$，故$-1\equiv g^{2t}(\mathrm{mod}p)$，即$-1\in D_0^{(p)}$。

当$p\equiv 3(\mathrm{mod}4)$时，记$p=4t+3$，$t$为正整数，同理可得$-1\in D_1^{(p)}$。　　证毕

**引理10**[15]　设$p$是一个奇素数。若$p\equiv 1\ (\mathrm{mod}\ 4)$，则

$$(0,1)^{(p^2)}=(1,0)^{(p^2)}=(1,1)^{(p^2)}=\frac{p(p-1)}{4},$$
$$(0,0)^{(p^2)}=\frac{p(p-5)}{4} \tag{20}$$

若$p\equiv 3(\mathrm{mod}\ 4)$，则

$$(0,0)^{(p^2)}=(1,0)^{(p^2)}=(1,1)^{(p^2)}=\frac{p(p-3)}{4},$$
$$(0,1)^{(p^2)}=\frac{p(p+1)}{4} \tag{21}$$

**引理11**　设$p$为奇素数，$\beta$为$F_{r^m}$上的$2p^2$次单位根，$\eta_0=\sum_{i\in 2D_0^{(p^2)}}\beta^i,\eta_1=\sum_{i\in 2D_1^{(p^2)}}\beta^i$，则有$\eta_0=\eta_1=0$。

**证明**　设$\gamma=\beta^2$，因为$\beta$是扩域$F_{r^m}$上的$2p^2$次单位根，所以$\gamma$是扩域$F_{r^m}$上的$p^2$次单位根。记$d=\dfrac{p(p-1)}{2}$，可得

$$\begin{aligned}\eta_0\eta_1&=\sum_{i\in 2D_0^{(p^2)}}\beta^i\sum_{j\in 2D_1^{(p^2)}}\beta^j=\sum_{i\in D_0^{(p^2)}}\gamma^i\sum_{i\in D_1^{(p^2)}}\gamma^j\\&=\sum_{k=0}^{d-1}\gamma^{g^{2k}}\sum_{l=0}^{d-1}\gamma^{g^{2l+1}}\\&=\sum_{k=0}^{d-1}\sum_{l=0}^{d-1}\gamma^{g^{2k}+g^{2l+1}}=\sum_{k=0}^{d-1}\sum_{t=0}^{d-1}\gamma^{g^{2k}+g^{2k+2t+1}}\\&=\sum_{k=0}^{d-1}\sum_{t=0}^{d-1}\gamma^{g^{2k}(1+g^{2t+1})}\end{aligned} \tag{22}$$

由引理3可知当$k$跑遍$\{0,1,\cdots,d-1\}$时，$D_1^{(p^2)}(\mathrm{mod}p)$取$D_1^{(p)}$中每个元素$p$次。下面分两种情况计算$\eta_0\eta_1$。

(1) 当$p\equiv 1(\mathrm{mod}\ 4)$时，根据引理9知$-1\in D_0^{(p)}$，即对任意的$t$，有$g^{2t+1}\equiv -1(\mathrm{mod}p)$,其中$0\le t\le d-1$。存在$v_1,v_2$，使得$g^{2v_1+v_2}=1+g^{2t+1}$，其中$0\le v_1\le d-1,0\le v_2\le 1$。当$t$确定时，有

$$\begin{aligned}\sum_{k=0}^{d-1}\gamma^{g^{2k}(1+g^{2t+1})}&=\sum_{k=0}^{d-1}\gamma^{g^{2k}g^{2v_1+v_2}}\\&=\sum_{k=0}^{d-1}\gamma^{g^{2(k+v_1)+v_2}}=\eta_{v_2}\end{aligned} \tag{23}$$

(a)　若$v_2=0$，则$g^{2v_1}=1+g^{2t+1}$。由$1+g^{2t+1}\in 1+D_1^{(p^2)}$, $g^{2v_1}\in D_0^{(p^2)}$，知$g^{2v_1}=1+g^{2t+1}\in\left(\left(D_1^{(p^2)}+1\right)\cap D_0^{(p^2)}\right)$，即$g^{2v_1}=1+g^{2t+1}$有$\left|(D_1^{(p^2)}+1)\cap D_0^{(p^2)}\right|$个解。由分圆数定义，$g^{2v_1}=1+g^{2t+1}$有$(1,0)^{(p^2)}$个解。

(b)　若$v_2=1$，则$g^{2v_1+1}=1+g^{2t+1}$。由$g^{2v_1+1}\in D_1^{(p^2)}$，知$g^{2v_1+1}=1+g^{2t+1}\in\left(\left(D_1^{(p^2)}+1\right)\cap D_1^{(p^2)}\right)$，即$g^{2v_1+1}=1+g^{2t+1}$有$\left|(D_1^{(p^2)}+1)\cap D_1^{(p^2)}\right|$个解。由分圆数定义，$g^{2v_1+1}=1+g^{2t+1}$有$(1,1)^{(p^2)}$个解。

所以当$t$跑遍$\{0,1,\cdots,d-1\}$时，$g^{2v_1+v_2}=1+g^{2t+1}$有$(1,v_2)^{(p^2)}$个解，因而

$$\begin{aligned}\eta_0\eta_1=&\sum_{k=0}^{d-1}\sum_{t=0}^{d-1}\gamma^{g^{2k}(1+g^{2t+1})}=(1,0)^{(p^2)}\sum_{k=0}^{d-1}\gamma^{g^{2k}}\\&+(1,1)^{(p^2)}\sum_{k=0}^{d-1}\gamma^{g^{2k+1}}\\=&(1,0)^{(p^2)}\eta_0+(1,1)^{(p^2)}\eta_1\end{aligned} \tag{24}$$

(2) 当$p\equiv 3(\mathrm{mod}\ 4)$时，根据引理9知$-1\in D_1^{(p)}$，则存在$t$，使得$g^{2t+1}\equiv -1(\mathrm{mod}p)$，即$g^{2t+1}+1\equiv 0(\mathrm{mod}p)$，其中$0\le t\le d-1$。设$L=\{t:g^{2t+1}\not\equiv -1(\mathrm{mod}p),0\le t\le d-1\}$。注意到$g^{2t+1}+1\equiv 0\ (\mathrm{mod}p)$有$p$个不同的解，当$t$跑遍$\{0,1,\cdots,d-1\}$时，$g^{2t+1}+1$恰好取$pZ_p$中每个元素1次。当$k$跑遍$\{0,1,\cdots,d-1\}$时，$g^{2k}(g^{2t+1}+1)$恰好取$pZ_p$中每个元素$d$次。与(1)类似有$\sum_{k=0}^{d-1}\gamma^{g^{2k}(g^{2t+1}+1)}=\sum_{k=0}^{d-1}\gamma^{g^{2k}(g^{2k+1}+1)}=\eta_{v_2}$，且$g^{2v_1+v_2}=1+g^{2t+1}$有$(1,v_2)^{(p^2)}$个解。

所以可得

$$\begin{aligned}\eta_0\eta_1=&\sum_{k=0}^{d-1}\sum_{t=0}^{d-1}\gamma^{g^{2k}(1+g^{2t+1})}=\sum_{k=0}^{d-1}\sum_{t\in L}\gamma^{g^{2k}(1+g^{2t+1})}\\&+\sum_{k=0}^{d-1}\sum_{t\in Z_d-L}\gamma^{g^{2k}(1+g^{2t+1})}\\=&\sum_{k=0}^{d-1}\sum_{k\in pZ_p}\gamma^{g^{2t}k}+\sum_{k=0}^{d-1}\sum_{t\in L}\gamma^{g^{2k}(1+g^{2t+1})}\\=&d\sum_{k\in pZ_p}\gamma^{g^{2t}k}+\sum_{k=0}^{d-1}\sum_{t\in L}\gamma^{g^{2k}(1+g^{2t+1})}\\=&(1,0)^{(p^2)}\eta_0+(1,1)^{(p^2)}\eta_1\end{aligned} \tag{25}$$

根据引理6、引理7和引理10知$\eta_0+\eta_1=0$，且$\eta_0\eta_1=0$，所以得$\eta_0=\eta_1=0$。　　证毕

序列$\{s(t)\}$的生成多项式为

$$S(x)=2x^{p^2}+\sum_{t\in D_1^{(2p^2)}\cup P_0}x^t+2\sum_{t\in 2D_1^{(p^2)}}x^t+3\sum_{t\in 2D_0^{(p^2)}\cup P_1}x^t \tag{26}$$

**引理12** 设$p$为奇素数，$\beta$为$F_{r^m}$上的$2p^2$次单位根，$r$为奇素数，且满足$r\geq 5, r\neq p$, 则当$k\in Z_{2p^2}$时，$S(\beta^k)$的值可以确定为

$$S(\beta^k)=\begin{cases}3p^2+p-2(\mathrm{mod}r), & k=0\\ 2(p^2-2)(\mathrm{mod}r), & k=p^2\\ 2(p-4)(\mathrm{mod}r), & k\in P_0\\ 4(p-2)(\mathrm{mod}r), & k\in P_1\\ -4(\mathrm{mod}r), & k\in D_0^{(2p^2)}\cup D_1^{(2p^2)}\\ -2(\mathrm{mod}r), & k\in 2D_0^{(p^2)}\cup 2D_1^{(p^2)}\end{cases} \tag{27}$$

**证明** 设$\gamma=\beta^2$，即$\gamma$为$p^2$次单位根。由式(26)，当$k=0$时，有

$$\begin{aligned}S(\beta^0)\equiv&S(1)\\ \equiv&2+\sum_{t\in D_1^{(2p^2)}\cup P_0}1^t+2\sum_{t\in 2D_1^{(p^2)}}1^t\\ &+3\sum_{t\in 2D_0^{(p^2)}\cup P_1}1^t\\ \equiv&2+\frac{p(p-1)}{2}+(p-1)+2\cdot\frac{p(p-1)}{2}\\ &+3\cdot\frac{p(p-1)}{2}+3(p-1)\\ \equiv&3p^2+p-2(\mathrm{mod}r)\end{aligned} \tag{28}$$

当$k=p^2$时，根据引理5，有

$$\begin{aligned}S(\beta^{p^2})\equiv&2(\beta^{p^2})^{p^2}+\sum_{t\in D_1^{(2p^2)}\cup P_0}(\beta^{p^2})^t\\ &+2\sum_{t\in 2D_1^{(p^2)}}(\beta^{p^2})^t+3\sum_{t\in 2D_0^{(p^2)}\cup P_1}(\beta^{p^2})^t\\ \equiv&2\cdot(-1)+\sum_{t\in D_1^{(2p^2)}\cup P_0}(-1)^t+2\sum_{t\in 2D_1^{(p^2)}}(-1)^t\\ &+3\sum_{t\in 2D_0^{(p^2)}\cup P_1}(-1)^t\\ \equiv&-2-\frac{p(p-1)}{2}-(p-1)+2\cdot\frac{p(p-1)}{2}\\ &+3\cdot\frac{p(p-1)}{2}+3(p-1)\\ \equiv&2(p^2-2)(\mathrm{mod}r)\end{aligned} \tag{29}$$

当$k\in P_0$时，根据引理3和引理5，有

$$\begin{aligned}S(\beta^k)\equiv&2(\beta^k)^{p^2}+\sum_{t\in D_1^{(2p^2)}}(\beta^k)^t+2\sum_{t\in 2D_1^{(p^2)}}(\beta^k)^t\\ &+3\sum_{t\in 2D_0^{(p^2)}}(\beta^k)^t+\sum_{t\in P_0}(\beta^k)^t+3\sum_{t\in P_1}(\beta^k)^t\\ \equiv&-2+\sum_{t\in P_0}\beta^t+2\sum_{t\in P_1}\beta^t+3\sum_{t\in P_1}\beta^t\\ &+3(p-1)-(p-1)\\ \equiv&2(p-4)(\mathrm{mod}r)\end{aligned} \tag{30}$$

当$k\in P_1$时，根据引理3和引理5，有

$$\begin{aligned}S(\beta^k)\equiv&2(\beta^k)^{p^2}+\sum_{t\in D_1^{(2p^2)}}(\beta^k)^t+2\sum_{t\in 2D_1^{(p^2)}}(\beta^k)^t\\ &+3\sum_{t\in 2D_0^{(p^2)}}(\beta^k)^t+\sum_{t\in P_0}(\beta^k)^t+3\sum_{t\in P_1}(\beta^k)^t\\ \equiv&2+\sum_{t\in P_1}\beta^t+2\sum_{t\in P_1}\beta^t\\ &+3\sum_{t\in P_1}\beta^t+3(p-1)+(p-1)\\ \equiv&4(p-2)(\mathrm{mod}r)\end{aligned} \tag{31}$$

下面讨论当$k\in D_0^{(2p^2)}\cup D_1^{(2p^2)}\cup 2D_0^{(p^2)}\cup 2D_1^{(p^2)}$时$S(\beta^k)$的值，为了简便，记$2_{p^2}^{-1}=2^{-1}(\mathrm{mod}p^2)$,根据引理8可得

$$\begin{aligned}S(\beta^k)\equiv&2(\beta^k)^{p^2}+\sum_{t\in D_1^{(2p^2)}}(\beta^k)^t+2\sum_{t\in 2D_1^{(p^2)}}(\beta^k)^t\\ &+3\sum_{t\in 2D_0^{(p^2)}}(\beta^k)^t+3\sum_{t\in P_1}(\beta^k)^t+\sum_{t\in P_0}(\beta^k)^t\\ \equiv&2(\beta^k)^{p^2}+\beta^{p^2k}\sum_{j\in D_1^{(p^2)}}(\beta^k)^{2\cdot j\cdot 2_{p^2}^{-1}}\\ &+\sum_{t\in 2D_0^{(p^2)}}(\beta^k)^t+\sum_{t\in P_0}(\beta^k)^t+\sum_{t\in P_1}(\beta^k)^t\\ &+2\left(\sum_{t\in 2D_1^{(p^2)}}(\beta^k)^t+\sum_{t\in 2D_0^{(p^2)}}(\beta^k)^t+\sum_{t\in P_1}(\beta^k)^t\right)\\ \equiv&2(\beta^{kp^2}-1)+\beta^{p^2k}\sum_{t\in 2_{p^2}^{-1}D_1^{(p^2)}}(\beta^k)^{2t}\\ &+\sum_{t\in D_0^{(p^2)}}(\beta^k)^{2t}+\sum_{t\in P_0}(\beta^k)^t\\ &+\sum_{t\in P_1}(\beta^k)^t(\mathrm{mod}r)\end{aligned} \tag{32}$$

接下来分两种情况讨论：

(1) 当$p\equiv\pm1(\mathrm{mod}8)$时，根据引理4知$2_{p^2}^{-1}\in D_0^{(p^2)}$，所以

$$S(\beta^k)\equiv 2(\beta^{k^{p^2}}-1)+\beta^{p^2k}\sum_{t\in D_1^{(p^2)}}(\beta^k)^{2t}+\sum_{t\in D_0^{(p^2)}}(\beta^k)^{2t}+\sum_{t\in P_0}(\beta^k)^t+\sum_{t\in P_1}(\beta^k)^t(\mathrm{mod}r) \tag{33}$$

(a) $k\in D_0^{(2p^2)}\cup D_1^{(2p^2)}$时，根据引理2，引理5和引理7可得

$$\begin{aligned}S(\beta^k)\equiv&\,2(-1-1)-\sum_{t\in D_1^{(p^2)}}(\beta^k)^{2t}+\sum_{t\in D_0^{(p^2)}}(\beta^k)^{2t}+\sum_{t\in P_0}(\beta^k)^t+\sum_{t\in P_1}(\beta^k)^t\\ \equiv&-4+\sum_{t\in D_1^{(p^2)}}(\beta^k)^{2t}+\sum_{t\in D_0^{(p^2)}}(\beta^k)^{2t}-2\sum_{t\in D_1^{(p^2)}}(\beta^k)^{2t}+\sum_{t\in P_0}(\beta^k)^t+\sum_{t\in P_1}(\beta^k)^t\\ \equiv&-5-2\sum_{t\in D_1^{(p^2)}}\beta^{2kt}+1\\ \equiv&-4(\mathrm{mod}r)\end{aligned} \tag{34}$$

(b) $k\in 2D_0^{(p^2)}\cup 2D_1^{(p^2)}$时，根据引理5，引理6和引理7可得

$$\begin{aligned}S(\beta^k)\equiv&\,2(1-1)+\sum_{t\in D_1^{(p^2)}}(\beta^k)^{2t}+\sum_{t\in D_0^{(p^2)}}(\beta^k)^{2t}+\sum_{t\in P_1}(\beta^k)^t+\sum_{t\in P_1}\beta^t\\ \equiv&-2(\mathrm{mod}r)\end{aligned} \tag{35}$$

(2) 当$p\equiv\pm3(\mathrm{mod}8)$时，根据引理4知$2_{p^2}^{-1}\in D_1^{(p^2)}$，所以

$$S(\beta^k)\equiv 2(\beta^{k^{p^2}}-1)+\beta^{p^2k}\sum_{t\in D_0^{(p^2)}}(\beta^k)^{2t}+\sum_{t\in D_0^{(p^2)}}(\beta^k)^{2t}+\sum_{t\in P_0}(\beta^k)^t+\sum_{t\in P_1}(\beta^k)^t(\mathrm{mod}r) \tag{36}$$

(a)$k\in D_0^{(2p^2)}\cup D_1^{(2p^2)}$时，根据引理5和引理7可得

$$\begin{aligned}S(\beta^k)\equiv&\,2(-1-1)-\sum_{t\in D_0^{(p^2)}}(\beta^k)^{2t}+\sum_{t\in D_0^{(p^2)}}(\beta^k)^{2t}+\sum_{t\in P_0}\beta^t+\sum_{t\in P_1}\beta^t\\ \equiv&-4(\mathrm{mod}r)\end{aligned} \tag{37}$$

(b)$k\in 2D_0^{(p^2)}$时，存在$k,k=2n,n\in D_0^{(p^2)}$，根据引理2可得

$$2D_0^{(p^2)}(\mathrm{mod}\,p^2)=D_1^{(p^2)},2D_1^{(p^2)}(\mathrm{mod}\,p^2)=D_0^{(p^2)},\ nD_0^{(p^2)}(\mathrm{mod}\,p^2)=D_0^{(p^2)},nD_1^{(p^2)}(\mathrm{mod}\,p^2)=D_1^{(p^2)} \tag{38}$$

根据引理5和引理7可得

$$\begin{aligned}S(\beta^k)\equiv&\,2(1-1)+\sum_{t\in D_0^{(p^2)}}(\beta^k)^{2t}+\sum_{t\in D_0^{(p^2)}}(\beta^k)^{2t}+\sum_{t\in P_1}\beta^t+\sum_{t\in P_1}\beta^t\\ \equiv&\sum_{t\in D_0^{(p^2)}}\gamma^{kt}+\sum_{t\in D_0^{(p^2)}}\gamma^{kt}-2\\ \equiv&\sum_{t\in D_0^{(p^2)}}\gamma^{2nt}+\sum_{t\in D_0^{(p^2)}}\gamma^{2nt}-2\\ \equiv&\sum_{t\in 2D_0^{(p^2)}}\gamma^{nt}+\sum_{t\in 2D_0^{(p^2)}}\gamma^{nt}-2\\ \equiv&\sum_{t\in D_1^{(p^2)}}\gamma^{nt}+\sum_{t\in D_1^{(p^2)}}\gamma^{nt}-2\\ \equiv&\sum_{t\in nD_1^{(p^2)}}\gamma^{t}+\sum_{t\in nD_1^{(p^2)}}\gamma^{t}-2\\ \equiv&\sum_{t\in D_1^{(p^2)}}\gamma^{t}+\sum_{t\in D_1^{(p^2)}}\gamma^{t}-2\\ \equiv&-2(\mathrm{mod}r)\end{aligned} \tag{39}$$

(c)$k\in 2D_1^{(p^2)}$时，同理存在$k,k=2n,n\in D_1^{(p^2)}$，根据引理2、引理5和引理7可得

$$2D_0^{(p^2)}(\mathrm{mod}\,p^2)=D_1^{(p^2)},2D_1^{(p^2)}(\mathrm{mod}\,p^2)=D_0^{(p^2)},\ nD_0^{(p^2)}(\mathrm{mod}\,p^2)=D_1^{(p^2)},\ nD_1^{(p^2)}(\mathrm{mod}\,p^2)=D_0^{(p^2)} \tag{40}$$

$$S(\beta^k)\equiv-2(\mathrm{mod}\,r) \tag{41}$$

证毕

### 3.2 定理1的证明

**证明**　由引理12知$S(\beta^k)$取值有$3p^2+p-2$, $p^2-2,p-4,p-2$，要确定序列$s(t)$的线性复杂度，则需考虑这4种情况的不同组合，分别讨论如下：

(1)若$r\,|3p^2+p-2$，则极小多项式为$m(x)=\dfrac{x^{2p^2}-1}{x-1}$，线性复杂度为$LC(s)=2p^2-1$。

(2)若$r\,|p^2-2$，则极小多项式为$m(x)=\dfrac{x^{2p^2}-1}{x-\beta^{p^2}}$，线性复杂度为$LC(s)=2p^2-1$。

(3)若$r\,|p-4$，则极小多项式为$m(x)=\dfrac{x^{2p^2}-1}{\prod\limits_{k\in P_0}(x-\beta^k)}$，线性复杂度为$LC(s)=2p^2-p+1$。

(4)若$r\,|p-2$，则极小多项式为$m(x)=\dfrac{x^{2p^2}-1}{\prod\limits_{k\in P_1}(x-\beta^k)}$，线性复杂度为$LC(s)=2p^2-p+1$。

(5)若$r|3p^2+p-2$且$r|p^2-2$，则极小多项式为

$m(x)=\dfrac{x^{2p^2}-1}{(x-1)(x-\beta^{p^2})}$，线性复杂度为$LC(s)=2p^2-2$。

(6)若$r|p^2-2$且$r|p-4$，则极小多项式为$m(x)=\dfrac{x^{2p^2}-1}{(x-\beta^{p^2})\prod\limits_{k\in P_0}(x-\beta^k)}$，线性复杂度为$LC(s)=2p^2-p$。

(7)若$r|3p^2+p-2$且$r|p-4$，则极小多项式为$m(x)=\dfrac{x^{2p^2}-1}{(x-1)\prod\limits_{k\in P_0}(x-\beta^k)}$，线性复杂度为$LC(s)=2p^2-p$。

(8)若$r|p-2$且$r|p^2-2$，则极小多项式为$m(x)=\dfrac{x^{2p^2}-1}{(x-\beta^{p^2})\prod\limits_{k\in P_1}(x-\beta^k)}$，线性复杂度为$LC(s)=2p^2-p$。

(9)若$r|3p^2+p-2$且$r|p-2$，则极小多项式为$m(x)=\dfrac{x^{2p^2}-1}{(x-1)\prod\limits_{k\in P_1}(x-\beta^k)}$，线性复杂度为$LC(s)=2p^2-p$。

(10)若$r|3p^2+p-2$且$r|p^2-2$且$r|p-4$，则极小多项式为$m(x)=\dfrac{x^{2p^2}-1}{(x-1)(x-\beta^{p^2})\prod\limits_{k\in P_0}(x-\beta^k)}$，线性复杂度为$LC(s)=2p^2-p-1$。

(11)若$r|3p^2+p-2$且$r|p^2-2$且$r|p-2$，则极小多项式为$m(x)=\dfrac{x^{2p^2}-1}{(x-1)(x-\beta^{p^2})\prod\limits_{k\in P_1}(x-\beta^k)}$，线性复杂度为$LC(s)=2p^2-p-1$。

(12)若 $r\not|3p^2+p-2$且$r\not|p^2-2$且$r\not|p-4$且$r\not|p-2$，则极小多项式为$m(x)=x^{2p^2}-1$, 线性复杂度为$LC(s)=2p^2$。 证毕

**注** 如果$r|p-4$且$r|p-2$，那么有$p\equiv 4\,(\mathrm{mod}\ r)$, $p\equiv 2\,(\mathrm{mod}\ r)$， 则$4\equiv 2\,(\mathrm{mod} r)$, $2\equiv 0\,(\mathrm{mod} r)$。因为$r$为奇素数，且$r\geq 5$，所以这两种情况不同时发生。

通过使用Magma，我们计算下面的例子来验证本文的结果。

**例1** 设$p=5,g=3,r=7$，则周期为50的4元广义分圆序列为00312121303031212130303122213030312121303031212130。

由Magma计算得$LC(s)=2p^2-p+1=92$，且$r,p$符合文中的第(12)种情况$r\not|3p^2+p-2$且$r\not|p^2-2$且$r\not|p-4$且$r\not|p-2$。

**例2** 设$p=7,g=3,r=5$，则周期为98的4元广义分圆序列为00313121302021303131213020213031312130202130313121302021303131223020213031312130202130313121302021303131213020213031312130202130313121302021。

由Magma计算得$LC(s)=2p^2-p+1=92$，且$r,p$符合文中的第(4)种情况$r\,|p-2$。

**例3** 设$p=7,g=3,r=11$，则由Magma计算得$LC(s)=2p^2=98$,且$r,p$ 符合文中的第(12)种情况$r\not|3p^2+p-2$且$r\not|p^2-2$且$r\not|p-4$且$r\not|p-2$。

**例4** 设$p=11,g=7,r=17$，则周期为242的4元广义分圆序列为00302031303121202131213030203130312120213121303020313031212021312130302031303121202131213030203130312120213121303020313031212021312130302031303121202131213030203130312120213121。

由Magma计算得$LC(s)=2p^2-1=241$，且$r,p$符合文中的第(2)种情况$r\,|p^2-2$。

**例5** 设$p=17,g=3,r=7$，则周期为578的4元广义分圆序列为00313121302120203130202120312131303031312130212020313020212031213130303131213021202031302021203121313030313121302120203130202120312131303031312130212020313020212031213130303131213021202031302021203121313030313121302120203130202120312131303031312130212020313020212031213130303131213021202033302021203121313030313121302120203130202120312131303031312130212020313020212031213130303131213021202031302021203121313030313121302120203130202120312131303031312130212020313020212031213130303131213021202031302021203121313030313121302120203130202120312131303031312130212020313020212031213130303131213021202031302021203121313030313121302120203130202120312131303031312130212020313020212031213130。

由Magma计算得$LC(s)=2p^2-2=576$，且$r,p$符合文中的第(5)种情况 $r|3p^2+p-2$且$r|p^2-2$。

## 4 结束语

本文基于杜小妮等人[13]的工作，构造了一类周期为$2p^2$的4元广义分圆序列，研究了这类序列在$F_q$上的极小多项式和线性复杂度。结果表明，这类序列在$F_q$上的线性复杂度的最小值为$2p^2-p-1$，大于其周期的1/2，即这类序列有高的线性复杂度，能够有效地抵抗B-M算法的攻击。后期研究该类序列4-adic复杂度也将是有意义的工作。

## 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] 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.

[4] 李胜强, 周亮, 肖国镇. 一类周期为$pq$阶为2的Whiteman广义分圆序列研究[J]. 电子与信息学报, 2009, 31(9): 2205–2208.
LI Shengqiang, ZHOU Liang, and XIAO Guozhen. Study on a class of Whiteman-Generalized cyclotomic sequence with length $pq$ and order two[J]. *Journal of Electronics & Information Technology*, 2009, 31(9): 2205–2208.

[5] 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.

[6] EDEMSKIY V, LI Chunlei, ZENG Xiangyong, *et al*. The linear complexity of generalized cyclotomic binary sequences of period $p^n$[J]. *Designs, Codes and Cryptography*, 2019, 87(5): 1183–1197. doi: 10.1007/s10623-018-0513-2.

[7] OUYANG Yi and XIE Xianhong. Linear complexity of generalized cyclotomic sequences of period $2p^m$[J]. *Designs, Codes and Cryptography*, 2019, 87(11): 2585–2596. doi: 10.1007/s10623-019-00638-5.

[8] 王艳, 薛改娜, 李顺波, 等. 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[J]. 电子与信息学报, 2019, 41(9): 2151–2155. doi: 10.11999/JEIT180884.
WANG Yan, XUE Gaina, LI Shunbo, *et al*. The linear complexity of a new class of generalized cyclotomic sequence of order $q$ with period $2p^m$[J]. *Journal of Electronics & Information Technology*, 2019, 41(9): 2151–2155. doi: 10.11999/JEIT180884.

[9] WANG Qiuyan, WU Chenhuang, YANG Minghui, *et al*. A kind of quaternary sequences of period $2p^mq^n$ and their linear complexity[J]. arXiv preprint arXiv: 2001.10839, 2020.

[10] KE Pinhui, ZHONG Yan, and ZHANG Shengyuan. Linear complexity of a new class of quaternary generalized cyclotomic sequence with period $2p^m$[J]. *Complexity*, 2020, 2020: 6538970. doi: 10.1155/2020/6538970.

[11] DU Xiaoni and CHEN Zhixiong. Linear complexity of quaternary sequences generated using generalized cyclotomic classes modulo $2p$[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2011, E94-A(5): 1214–1217. doi: 10.1587/transfun.E94.A.1214.

[12] CHEN Zhixiong and EDEMSKIY V. Linear complexity of quaternary sequences over $Z_4$ derived from generalized cyclotomic classes modulo $2p$[J]. arXiv preprint arXiv: 1603.05086, 2016.

[13] 杜小妮, 赵丽萍, 王莲花. $Z_4$上周期为$2p^2$的四元广义分圆序列的线性复杂度[J]. 电子与信息学报, 2018, 40(12): 2992–2997. doi: 10.11999/JEIT180189.
DU Xiaoni, ZHAO Liping, and WANG Lianhua. Linear complexity of quaternary sequences over $Z_4$ derived from generalized cyclotomic classes modulo $2p^2$[J]. *Journal of Electronics & Information Technology*, 2018, 40(12): 2992–2997. doi: 10.11999/JEIT180189.

[14] ZHANG Jingwei, ZHAO Changan, and MA Xiao. On the linear complexity of generalized cyclotomic binary sequences with length $2p^2$[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2010, E93-A(1): 302–308. doi: 10.1587/transfun.E93.A.302.

[15] DING Cunsheng and HELLESETH T. New generalized cyclotomy and its applications[J]. *Finite Fields and Their Applications*, 1998, 4(2): 140–166. doi: 10.1006/ffta.1998.0207.



王　艳：女，1982年生，副教授，研究方向为序列密码.
相乃姣：女，1996年生，硕士生，研究方向为序列密码.
韩西林：女，1996年生，硕士生，研究方向为序列密码.
闫联陶：女，1996年生，硕士生，研究方向为序列密码.


责任编辑：余　蓉