周期为 $2p^2$ 的四阶二元广义分圆序列的线性复杂度

杜小妮　　王国辉*　　魏万银
(西北师范大学数学与统计学院　兰州　730070)

摘　要：该文基于分圆理论，构造了一类周期为 $2p^2$ 的四阶二元广义分圆序列。利用有限域上多项式分解理论研究序列的极小多项式和线性复杂度。结果表明，该序列具有良好的线性复杂度性质，能够抗击 B-M 算法的攻击。是密码学意义上性质良好的伪随机序列。

关键词：流密码；广义分圆序列；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**：1009-5896(2015)10-2490-05
DOI: 10.11999/JEIT150180

Linear Complexity of Binary Generalized Cyclotomic Sequences of Order Four with Period $2p^2$

Du Xiao-ni　　Wang Guo-hui　　Wei Wan-yin
(*College of Mathematics and Statistics*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

Abstract: Based on the theory of generalized cyclotomic, a new class of binaey generalized cyclotomic sequences of order four with period $2p^2$ is established. Using the theory of polynomial factor over finite field, the linear complexity and minimal polynomial of the new sequences are researched. Results show that the sequences has larger linear complexity and can resist the attack by B-M algorithm. It is a good sequence from the viewpoint of cryptography.

Key words: Stream ciphers; Generalized cyclotomic sequence; Linear complexity; Minimal polynomial

1　引言

伪随机序列在扩频通信、测量距离、雷达导航、CDMA 通信、流密码系统等领域有着极为广泛的应用。在密码学领域的应用中，伪随机序列必须具有高的线性复杂度[1]。从安全的角度讲，为抵抗已知明文攻击，序列的线性复杂度必须足够大。根据 B-M 算法[2]，一条好的序列往往要求它的线性复杂度必须不小于其周期长度的一半。

近年来，广义分圆序列由于具有良好的线性复杂度而备受关注[3−12]。其中文献[3]和文献[4]研究了周期为 p^m 的广义分圆序列，并分别给出了计算该序列线性复杂度和迹函数的有效方法。文献[5]和文献[6]给出了两类周期为 $2pq$ 广义分圆序列，并分析了该序列的线性复杂度。文献[7-11]分别对周期为 pq 广义分圆序列的线性复杂度、最小多项式和自相关值等性质进行了讨论。文献[12-15]研究了周期为 $2p^m$ 的二阶广义分圆序列的构造及其线性复杂度性质，而周期为 $2p^2$ 的四阶二元序列尚未研究。因而，本文将研究周期为 $2p^2$ 的四阶二元序列的构造及其线性复杂度。

2　广义分圆序列的构造

设 p 是一个奇素数，且 $p\equiv 1 \pmod 4$。假设 g 是一个模 p^2 的本元根，则 g 也是模 p^k 的本元根，$k\ge 1$。下文中总假设 g 为奇数，若 g 为偶数，则取 $g+p^k$ 为模 p^k 的本元根。定义

$$D_0^{(p^j)}=\left\langle g^4\right\rangle \pmod{p^j},\ D_0^{(2p^j)}=\left\langle g^4\right\rangle \pmod{2p^j}$$

$$D_k^{(p^j)}=g^k D_0^{(p^j)},\ D_k^{(2p^j)}=g^k D_0^{(2p^j)},\ 1\le k\le 3,\ j=1,\ 2$$

其中 $aD^{(n)}=\left\{ab \pmod n\text{: } b\in D^{(n)}\right\}$，并且 $\left|D_k^{(p)}\right|=(p-1)/4$，$\left|D_k^{(p^2)}\right|=[p(p-1)]/4$，$0\le k\le 3$。令 Z_n 是模 n 剩余类环，Z_n^* 表示剩余类环 Z_n 的所有可逆元素的集合，显然有

$$Z_{2p^j}^*=\bigcup_{k=0}^{3} D_k^{(2p^j)},\ Z_{p^j}^*=\bigcup_{k=0}^{3} D_k^{(p^j)},\quad j=1,\ 2$$

$$Z_{2p^2}=\bigcup_{k=0}^{3}\left(2pD_k^{(p)}\cup pD_k^{(2p)}\cup 2D_k^{(p^2)}\cup D_k^{(2p^2)}\right)\cup\left\{p^2\right\}\cup\{0\}$$

令

收稿日期：2015-02-02；改回日期：2015-07-01；网络出版：2015-07-17
*通信作者：王国辉　wanggh0039@126.com
基金项目：国家自然科学基金(61202395, 61462077, 61262057, 61562077)和教育部“新世纪优秀人才支持计划”基金(NCET-12-0620)
Foundation Items: The National Natural Science Foundation of China (61202395, 61462077, 61262057, 61562077); The Program for New Century Excellent Talents in University (NCET-12-0620)

$$C_0=\bigcup_{i=0}^{1}\left(2pD_i^{(p)}\cup pD_i^{(2p)}\cup 2D_i^{(p^2)}\cup D_i^{(2p^2)}\right)\cup\left\{p^2\right\}$$

$$C_1=\bigcup_{i=2}^{3}\left(2pD_i^{(p)}\cup pD_i^{(2p)}\cup 2D_i^{(p^2)}\cup D_i^{(2p^2)}\right)\cup\{0\}$$

则 $C_0\cup C_1=Z_{2p^2}$，$C_0\cap C_1=\varnothing$。定义周期为 $2p^2$ 的四阶广义分圆序列 s 为

$$s_i=\begin{cases}1, & i\ \left(\mathrm{mod}\ \ 2p^2\right)\in C_1,\\ 0, & i\ \left(\mathrm{mod}\ \ 2p^2\right)\in C_0,\end{cases}\quad i\ge 0 \tag{1}$$

3　广义分圆序列的线性复杂度

有限域 $\mathrm{GF}(q)$ 上周期为 N 的序列 $s=\{s_i\}$ 的线性复杂度 $\mathrm{LC}(s)$ 定义为满足关系式：

$$s_j=c_1s_{j-1}+c_2s_{j-2}+\cdots+c_Ls_{j-L}$$

式中，$j>L,\ c_1,c_2,\cdots,\ c_L\in\mathrm{GF}(q)$ 的最小 L。设 $s(x)=s_0+s_1x^2+\cdots+s_{N-1}x^{N-1}$，则序列 $\{s_i\}$ 的最小多项式 $m(x)$ 和线性复杂度 L 分别由式(2)，式(3)给定：

$$m(x)=\left(x^N-1\right)\Big/\mathrm{gcd}\left(x^N-1,\ s(x)\right)^{[16]} \tag{2}$$

$$L(s)=N-\deg\left(\mathrm{gcd}\left(x^N-1,\ \ s(x)\right)\right)^{[1]} \tag{3}$$

由序列 s 的定义式(1)可知，其生成多项式 $s(x)$ 为

$$s(x)=\sum_{i\in C_1}x^i=1+\sum_{k=2}^{3}\left(\sum_{i\in 2pD_k^{(p)}}x^i+\sum_{i\in pD_k^{(2p)}}x^i+\sum_{i\in 2D_k^{(p^2)}}x^i+\sum_{i\in D_k^{(2p^2)}}x^i\right)\in\mathrm{GF}(2)[x]$$

下文将讨论序列 s 的线性复杂度，首先给出引理 1~引理 9，本文中 $D_i^{(n)}$ 的下标均模 4。

引理 1　设 $t\in D_k^{(p^j)}$，则 $tD_i^{(p^j)}\ (\mathrm{mod}\ \ p^j)=D_{i+k}^{(p^j)}$，$j=1,2$，$0\le k,\ i\le 3$。

证明　若 $t\in D_k^{(p^j)}$，则存在 u 使得

$$t=g^{4u+k}\left(\mathrm{mod}\ \ p^j\right)$$

所以

$$\begin{aligned}&tD_i^{(p^j)}\left(\mathrm{mod}\ \ p^j\right)\\&=\left\{g^{4u+k}g^{4s+i}\left(\mathrm{mod}\ \ p^j\right):\ s=0,\ 1,\cdots,\ \varphi\left(p^j\right)\big/4-1\right\}\\&=\left\{g^{4(u+s)+k+i}\left(\mathrm{mod}\ \ p^j\right):\ s=0,\ 1,\cdots,\ \varphi\left(p^j\right)\big/4-1\right\}\\&=D_{i+k}^{(p^j)}\end{aligned}$$

证毕

引理 2　$D_i^{(p^2)}\ (\mathrm{mod}\ p)=D_i^{(p)}$，$D_i^{(2p^j)}(\mathrm{mod}\ p^j)=D_i^{(p^j)}$，　$j=1,2$，$0\le i\le 3$。

证明　根据 $D_i^{(p^2)}$ 的定义可知，当 t 跑遍 $D_i^{(p^2)}$ 时，t 模 p 跑遍 $D_i^{(p)}$ 中每个元素 p 次。所以，

$$D_i^{(p^2)}\ \ (\mathrm{mod}\ \ p)=D_i^{(p)}\ \text{且}\left|D_i^{(p^2)}\right|=p\left|D_i^{(p)}\right|$$

类似地，$D_i^{(2p^j)}\ \ \left(\mathrm{mod}\ \ p^j\right)=D_i^{(p^j)}$ 且 $\left|D_i^{(2p^j)}\right|=\left|D_i^{(p^j)}\right|$。

证毕

引理 3　序列 s 的生成多项式 $s(x)$ 没有重因子。

证明　只需证明 $\mathrm{gcd}(s(x),\ s'(x))=1$，其中

$$s'(x)=\sum_{i\in D_2^{(2p)}}x^{pi-1}+\sum_{i\in D_2^{(2p^2)}}x^{i-1}+\sum_{i\in D_3^{(2p)}}x^{pi-1}+\sum_{i\in D_3^{(2p^2)}}x^{i-1}$$

是 $s(x)$ 的导数。令 $a(x)=1,\ b(x)=x+x^2s'(x)$，由引理 2 可得

$$\begin{aligned}&a(x)s(x)+b(x)s'(x)\\&=s(x)+xs'(x)+x^2\left(s'(x)\right)^2\\&=\sum_{i\in C_1}x^i+\left[\sum_{i\in D_2^{(2p)}}x^{pi}+\sum_{i\in D_2^{(2p^2)}}x^i+\sum_{i\in D_3^{(2p)}}x^{pi}+\sum_{i\in D_3^{(2p^2)}}x^i\right]\\&\quad+\left[\sum_{i\in D_2^{(p)}}x^{2pi}+\sum_{i\in D_2^{(p^2)}}x^{2i}+\sum_{i\in D_3^{(p)}}x^{2pi}+\sum_{i\in D_3^{(p^2)}}x^{2i}\right]\\&=1\end{aligned}$$

根据引理 3 及式(2)可得

$$\begin{aligned}\mathrm{gcd}\left(x^{2p^2}-1,\ \ s(x)\right)&=\mathrm{gcd}\left(\left(x^{p^2}-1\right)^2,\ \ s(x)\right)\\&=\mathrm{gcd}\left(x^{p^2}-1,\ \ s(x)\right)\end{aligned}$$

则序列 s 的最小多项式为

$$m(x)=\frac{x^{2p^2}-1}{\mathrm{gcd}\left(x^{p^2}-1,\ s(x)\right)} \tag{4}$$

若 m 是 2 模 p^2 的阶，有 $p^2\left|2^m-1\right.$，则 $\mathrm{GF}(2^m)$ 为 $x^{p^2}-1$ 的分裂域。假设 α 为 p^2 次单位根，显然 $\alpha\in\mathrm{GF}(2^m)$，则由式(3)可知

$$\begin{aligned}L(s)&=2p^2-\left|\left\{t:s\left(\alpha^t\right)=0\ ,\ 0\le t\le p^2-1\right\}\right|\\&=\deg(m(x))\end{aligned} \tag{5}$$

令

$$A\left(\alpha^t\right)=\sum_{i\in D_2^{(p)}}\alpha^{pti}+\sum_{i\in D_3^{(p)}}\alpha^{pti}+\sum_{i\in D_2^{(p^2)}}\alpha^{ti}+\sum_{i\in D_3^{(p^2)}}\alpha^{ti}$$

则

$$\begin{aligned}s\left(\alpha^t\right)&=1+\sum_{k=2}^{3}\left(\sum_{i\in D_k^{(p)}}\alpha^{2pti}+\sum_{i\in D_k^{(p)}}\alpha^{pti}+\sum_{i\in D_k^{(p^2)}}\alpha^{2ti}+\sum_{i\in D_k^{(p^2)}}\alpha^{ti}\right)\\&=1+A(\alpha^t)+A^2(\alpha^t)\end{aligned}$$

证毕

引理 4[17] 符号含义同上，则

$$\sum_{i\in D_0^{(p^2)}}\alpha^i+\sum_{i\in D_2^{(p^2)}}\alpha^i=0,\ \sum_{i\in D_1^{(p^2)}}\alpha^i+\sum_{i\in D_3^{(p^2)}}\alpha^i=0$$

$$\sum_{i\in pZ_p^*}\alpha^i=1,\quad \sum_{i\in Z_{p^2}^*}\alpha^i=1$$

下文中令

$$\left.\begin{aligned}s_{kl}^{(p)}&=\sum_{i\in D_k^{(p)}}\alpha^{pi}+\sum_{i\in D_l^{(p)}}\alpha^{pi}\\ s_{kl}^{(p^2)}&=\sum_{i\in D_k^{(p^2)}}\alpha^{i}+\sum_{i\in D_l^{(p^2)}}\alpha^{i}\end{aligned}\right\}0\le k,\ l\le 3$$

引理 5 符号含义同上，则

$$s\left(\alpha^t\right)=\begin{cases}1+s_{23}^{(p)}+\left(s_{23}^{(p)}\right)^2, & t\in pD_0^{(p)}\cup pD_2^{(p)}\\ 1+s_{03}^{(p)}+\left(s_{03}^{(p)}\right)^2, & t\in pD_1^{(p)}\cup pD_3^{(p)}\end{cases}$$

证明 当$t\in pD_0^{(p)}$时，由引理 1，引理 2 和$\alpha^{p^2}=1$可得

$$\begin{aligned}A(\alpha^t)&=\sum_{i\in D_2^{(p)}}\alpha^{p^2i}+\sum_{i\in D_3^{(p)}}\alpha^{p^2i}+\sum_{i\in D_2^{(p^2)}}\alpha^{pi}+\sum_{i\in D_3^{(p^2)}}\alpha^{pi}\\&=\frac{p-1}{2}+\sum_{i\in D_2^{(p^2)}}\alpha^{pi}+\sum_{i\in D_3^{(p^2)}}\alpha^{pi}\\&=\sum_{i\in D_2^{(p)}}\alpha^{pi}+\sum_{i\in D_3^{(p)}}\alpha^{pi}\end{aligned}$$

因此，$s(\alpha^t)=1+s_{23}^{(p)}+\left(s_{23}^{(p)}\right)^2$。当$t\in pD_2^{(p)}$时，

$$\begin{aligned}A(\alpha^t)&=\sum_{i\in D_0^{(p)}}\alpha^{p^2i}+\sum_{i\in D_1^{(p)}}\alpha^{p^2i}+\sum_{i\in D_0^{(p^2)}}\alpha^{pi}+\sum_{i\in D_1^{(p^2)}}\alpha^{pi}\\&=\frac{p-1}{2}+\sum_{i\in D_0^{(p^2)}}\alpha^{pi}+\sum_{i\in D_1^{(p^2)}}\alpha^{pi}\\&=1+\sum_{i\in D_2^{(p)}}\alpha^{pi}+\sum_{i\in D_3^{(p)}}\alpha^{pi}\end{aligned}$$

因此，$s(\alpha^t)=1+s_{23}^{(p)}+\left(s_{23}^{(p)}\right)^2$。

类似可证明$t\in pD_1^{(p)}\cup pD_3^{(p)}$情形。 证毕

引理 6 符号含义同上，则

$$s\left(\alpha^t\right)=\begin{cases}1+\left(s_{23}^{(p)}+s_{23}^{(p^2)}\right)+\left(s_{23}^{(p)}+s_{23}^{(p^2)}\right)^2,\\ \qquad t\in D_0^{(p^2)}\cup D_2^{(p^2)}\\ 1+\left(s_{03}^{(p)}+s_{03}^{(p^2)}\right)+\left(s_{03}^{(p)}+s_{03}^{(p^2)}\right)^2,\\ \qquad t\in D_1^{(p^2)}\cup D_3^{(p^2)}\end{cases}$$

证明 当$t\in D_0^{(p^2)}$时，由引理 1 可得

$$\begin{aligned}A(\alpha^t)&=\sum_{i\in D_2^{(p^2)}}\alpha^{pi}+\sum_{i\in D_3^{(p)}}\alpha^{pi}+\sum_{i\in D_2^{(p^2)}}\alpha^{i}+\sum_{i\in D_3^{(p^2)}}\alpha^{i}\\&=s_{23}^{(p)}+s_{23}^{(p^2)}\end{aligned}$$

则$s\left(\alpha^t\right)=1+\left(s_{23}^{(p)}+s_{23}^{(p^2)}\right)+\left(s_{23}^{(p)}+s_{23}^{(p^2)}\right)^2$。当$t\in D_2^{(p^2)}$时，由引理 4 可知

$$\begin{aligned}A(\alpha^t)&=\sum_{i\in D_0^{(p)}}\alpha^{pi}+\sum_{i\in D_1^{(p)}}\alpha^{pi}+\sum_{i\in D_0^{(p^2)}}\alpha^{i}+\sum_{i\in D_1^{(p^2)}}\alpha^{i}\\&=1+s_{23}^{(p)}+s_{23}^{(p^2)}\end{aligned}$$

则$s\left(\alpha^t\right)=1+\left(s_{23}^{(p)}+s_{23}^{(p^2)}\right)+\left(s_{23}^{(p)}+s_{23}^{(p^2)}\right)^2$。

类似可证明$t\in D_1^{(p^2)}\cup D_3^{(p^2)}$情形。 证毕

引理 7[18] $2\in D_0^{(p)}\cup D_2^{(p)}$当且仅当$p\equiv 1 \pmod 8$，$2\in D_1^{(p)}\cup D_3^{(p)}$当且仅当$p\equiv 5 \pmod 8$。

引理 8 符号含义同上，若$p\equiv 5 \pmod 8$时，

(1) 当$2\in D_1^{(p)}$时，

$$s\left(\alpha^t\right)=\begin{cases}1+s_{02}^{(p)}, & t\in pD_0^{(p)}\cup pD_2^{(p)}\cup D_0^{(p^2)}\cup D_2^{(p^2)}\\ 1+s_{13}^{(p)}, & t\in pD_1^{(p)}\cup pD_3^{(p)}\cup D_1^{(p^2)}\cup D_3^{(p^2)}\end{cases}$$

(2) 当$2\in D_3^{(p)}$时，

$$s\left(\alpha^t\right)=\begin{cases}1+s_{13}^{(p)}, & t\in pD_0^{(p)}\cup pD_2^{(p)}\cup D_0^{(p^2)}\cup D_2^{(p^2)}\\ 1+s_{02}^{(p)}, & t\in pD_1^{(p)}\cup pD_3^{(p)}\cup D_1^{(p^2)}\cup D_3^{(p^2)}\end{cases}$$

证明 (1)由引理 7，当$2\in D_1^{(p)}$时，对于$t\in pD_0^{(p)}\cup pD_2^{(p)}$，根据引理 1 和引理 5 知

$$\begin{aligned}s(\alpha^t)&=1+\left(s_{23}^{(p)}\right)+\left(s_{23}^{(p)}\right)^2\\&=1+\sum_{i\in D_0^{(p)}}\alpha^{pi}+\sum_{i\in D_2^{(p)}}\alpha^{pi}=1+s_{02}^{(p)}\end{aligned}$$

对于$t\in D_0^{(p^2)}\cup D_2^{(p^2)}$，根据引理 4 和引理 6 知

$$\begin{aligned}s(\alpha^t)&=1+\left(s_{23}^{(p)}+s_{23}^{(p^2)}\right)+\left(s_{23}^{(p)}+s_{23}^{(p^2)}\right)^2\\&=1+\sum_{i\in D_0^{(p)}}\alpha^{pi}+\sum_{i\in D_2^{(p)}}\alpha^{pi}=1+s_{02}^{(p)}\end{aligned}$$

同理可以证明$t\in pD_1^{(p)}\cup pD_3^{(p)}\cup D_1^{(p^2)}\cup D_3^{(p^2)}$情形。

(2)的证明与(1)类似，在此省略。 证毕

引理 9 符号含义同上，若$p\equiv 1 \pmod 8$时，

(1) 当$2\in D_0^{(p)}$时，$s(\alpha^t)=1$，$t\in Z_{p^2}\setminus\{0\}$。

(2) 当$2\in D_2^{(p)}$时，$s(\alpha^t)=0$，$t\in Z_{p^2}\setminus\{0\}$。

证明(1) 当$2\in D_0^{(p)}$时，对于$t\in pD_0^{(p)}\cup pD_2^{(p)}$，由引理 1 和引理 5 知

$$\left(s_{23}^{(p)}\right)^2=\left(\sum_{i\in D_2^{(p)}}\alpha^{pi}+\sum_{i\in D_3^{(p)}}\alpha^{pi}\right)^2=s_{23}^{(p)}$$

即$s(\alpha^t)=1$。对于$t\in D_0^{(p^2)}\cup D_2^{(p^2)}$，由引理 6 知

$$s\left(\alpha^t\right)=1+\left(s_{23}^{(p)}+s_{23}^{(p^2)}\right)+\left(s_{23}^{(p)}+s_{23}^{(p^2)}\right)^2=1$$

同理$t\in pD_1^{(p)}\cup pD_3^{(p)}\cup D_1^{(p^2)}\cup D_3^{(p^2)}$时，$s(\alpha^t)=1$。

因此，当 $t \in Z_{p^2} \setminus \{0\}$ 时，$s(\alpha^t)=1$。

(2)的证明与(1)类似，在此省略。　　证毕

显然，当 $t=0$ 时，

$$A\left(\alpha^0\right)=A(1)=\frac{p-1}{2}+\frac{p(p-1)}{2}=\frac{p^2-1}{2}=0(\bmod\ 2)$$

则

$$s\left(\alpha^t\right)=1 \tag{6}$$

定理 1　当 $p \equiv 5\ (\bmod\ 8)$ 时，序列 s 的最小多项式为 $x^{2p^2}-1$，线性复杂度为 $2p^2$。

证 明　当 $2 \in D_1^{(p)}$ 且 $t \in pD_0^{(p)} \cup pD_2^{(p)} \cup D_0^{(p^2)} \cup D_2^{(p^2)}$ 时，由引理 8 可知

$$\left(s\left(\alpha^t\right)\right)^2=1+\left(s_{02}^{(p)}\right)^2=s_{02}^{(p)} \neq s\left(\alpha^t\right)$$

当 $t \in pD_1^{(p)} \cup pD_3^{(p)} \cup D_1^{(p^2)} \cup D_3^{(p^2)}$ 时，

$$\left(s\left(\alpha^t\right)\right)^2=1+\left(s_{13}^{(p)}\right)^2=s_{13}^{(p)} \neq s\left(\alpha^t\right)$$

因此，当 $t \in Z_{p^2} \setminus \{0\}$ 时，$s(\alpha^t) \neq 0$。对于 $2 \in D_3^{(p)}$ 时，同理有 $s(\alpha^t) \neq 0$。由式(4)，式(5)，式(6)可知 $\gcd(x^{p^2}-1, s(x))=1$，则最小多项式 $m(x)=x^{2p^2}-1$，线性复杂度 $\mathrm{LC}(s)=2p^2$。　　证毕

定理 2　当 $p \equiv 1\ (\bmod\ 8)$ 时，序列 s 的最小多项式为 $x^{2p^2}-1$ 或 $(x^{p^2}-1)(x-1)$，线性复杂度为 $2p^2$ 或 p^2+1。

证明　由引理 9，对于 $t \in Z_{p^2} \setminus \{0\}$ 时，有

$$s\left(\alpha^t\right)=\begin{cases}1, & 2 \in D_0^{(p)} \\ 0, & 2 \in D_2^{(p)}\end{cases}$$

则由式(4)，式(5)和式(6)可知：

$$\gcd\left(x^{p^2}-1,\ s(x)\right)=\begin{cases}1, & 2 \in D_0^{(p)} \\ \dfrac{x^{p^2}-1}{x-1}, & 2 \in D_2^{(p)}\end{cases}$$

因此，

$$m(x)=\begin{cases}x^{2p^2}-1, & 2 \in D_0^{(p)} \\ \left(x^{p^2}-1\right)(x-1), & 2 \in D_2^{(p)}\end{cases}$$

$$\mathrm{LC}(s)=\begin{cases}2p^2, & 2 \in D_0^{(p)} \\ p^2+1, & 2 \in D_2^{(p)}\end{cases}$$

证毕

4　结论

本文研究了周期为 $2p^2$ 的四阶二元广义分圆序列的构造，并分别在 $p \equiv 1\ (\bmod\ 8)$ 和 $p \equiv 5\ (\bmod\ 8)$ 的情形下讨论了序列的线性复杂度和最小多项式。结果表明，线性复杂度是 $2p^2$ 或 p^2+1。因此，这个序列拥有好的线性复杂度，能够抵抗 B-M 算法的攻击，在保密通讯中可以有广泛的应用。

参 考 文 献

[1] Golomb S W and Gong G. Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar Applications[M]. Cambridge: UK, Cambridge University Press, 2005: 174–175.

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

[3] 杜小妮, 阎统江, 石永芳. 周期为 p^m 的广义割圆序列的线性复杂度[J]. 电子与信息学报, 2010, 32(4): 821–824.
Du Xiao-ni, Yan Tong-jiang, and Shi Yong-fang. Linear complexity of generalized cyclotomic sequences with period p^m[J]. *Journal of Electronics & Information Technology*, 2010, 32(4): 821–824.

[4] Du Xiao-ni and Chen Zhi-xun. Trace representation of binary generalized cyclotomic squences with length p^m[J]. *IEICE Transactions on Fundamentals of Electronices Communications and Computer Sciences*, 2011, E94-A(2): 761–765.

[5] 李瑞芳, 柯品惠. 一类新的周期为 $2pq$ 的二元广义分圆序列的线性复杂度[J]. 电子与信息学报, 2014, 36(3): 650–654.
Li Rui-fang and Ke Pin-hui. The linear complexity of a new class of generalized cyclotomic sequences with period $2pq$[J]. *Journal of Electronics & Information Technology*, 2014, 36(3): 650–654.

[6] Chang Zu-ling and Li Dan-dan. On the linear complexity of the quaternary cyclotomic sequences with the period $2pq$[J]. *IEICE Transactions on Fundamental of Electronics Communications and Computer Sciences*, 2014, E97-A(2): 679–684.

[7] Li Xiao-ping, Ma Wen-ping, and Yan Tong-jiang. Linear complexity of binary Whiteman generalized cyclotomic sequences of order 4[J]. *IEICE Transactions on Fundamentals of Electronices Communications and Computer Sciences*, 2013, 96A(1): 363–366.

[8] Zhao Chun-e and Ma Wen-ping. Autocorrelation values of generalized cyclotomic sequences of order six[J]. *IEICE Transactions on Fundamentals of Electronices Communications and Computer Sciences*, 2013, E96-A(10): 2045–2048.

[9] Edemskiy V and Lvanov A. Linear complexity of quaternary sciences of length pq with low autocorrelation[J]. *Journal of Computational and Applied Mathematics*, 2014, 259B: 555–560.

[10] Ke Pin-hui, Lin Chang-lu, and Zhang Sheng-yuan. Linear

complexity of quaternary sciences with odd period and low autocorrelation[J]. *The Journal of China Universities of Posts and Telecommunications*, 2014, 21(5): 89–93.

[11] Li Dan-dan and Wen Qiao-yan. Linear complexity of generalized cyclotomic quaternary sequences with period pq[J]. *IEICE Transactions on Fundamentals of Electronices Communications and Computer Sciences*, 2014, E97-A(5): 1153–1158.

[12] Yan Tong-jiang and Li Xiao-ping. Some note on the generalized cyclotomic sequence of length $2p^m$ and p^m[J]. *IEICE Transactions on Fundamentals of Electronices Communications and Computer Sciences*, 2013, E96-A(10): 997–1000.

[13] Zhang Jing-wei, Zhao Chang-an, and Ma Xiao. Linear complexity of generalized cyclotomic binary sequences with the period $2p^m$[J]. *Applicable Algebra in Engineering, Communication and Computing*, 2010, 21(2): 93–108.

[14] Zhang Jing-wei, Zhao Chang-an, and Ma Xiao. On the linear complexity of generalized cyclotomic binary sequences with length $2p^2$[J]. *IEICE Transactions on Fundamentals of Electronices Communications and Computer Sciences*, 2010, E93-A(1): 302–308.

[15] Ke Pin-hui and Zhang J. On the linear complexity and autocorrelation of generalized cyclotomic binary sequences with length $2p^m$[J]. *Designs*, *Codes and Cryptograpy*, 2013, 67(3): 325–339.

[16] Cusick T and Ding Cun-sheng. Stream Ciphers and Number Theory[M]. Elsevier Science, 2004: 198-212.

[17] Yan Tong-jiang, Huang Bing-jia, and Xiao Guo-zhen. Cryptographic properties of some binary generalized cyclotomic sequences with length p^2[J]. *Information Science*, 2008, 178(4): 1078–1086.

[18] Ding Cun-sheng and Hellseth. T. New generalized cyclotomy and its applications[J]. *Finite Field Their Applications,* 1998, 4(2): 140–166.

杜小妮： 女，1972 年生，教授，研究方向为密码学与信息安全.

王国辉： 男，1991 年生，硕士生，研究方向为密码学与信息安全.

魏万银： 女，1989 年生，硕士生，研究方向为密码学与信息安全.