d-元广义分圆序列的线性复杂度及自相关函数性质分析

柯品惠* 李瑞芳 张胜元
(福建师范大学网络安全与密码技术重点实验室 福州 350007)

摘 要：该文推广了 Liu Fang 等人(2010)给出的周期为 p^n， p 为奇素数， n 为正整数的广义分圆序列的构造，并确定了新构造序列的线性复杂度和自相关函数值的分布。结果表明，推广的构造保持了原构造的高线性复杂度等伪随机特性。由于取值更灵活，较之原构造新构造序列的数量要大得多。

关键词：网络安全；广义分圆；线性复杂度；自相关
中图分类号：TN918.1 **文献标识码**： A **文章编号**：1009-5896(2012)12-2881-04
DOI: 10.3724/SP.J.1146.2012.00804

Analysis of the Linear Complexity and the Autocorrelation of a Class of d-ary Generalized Cyclotomic Sequence

Ke Pin-hui Li Rui-fang Zhang Sheng-yuan
(*Key Laboratory of Network Security and Cryptology*, *Fujian Normal University*, *Fuzhou* 350007, *China*)

Abstract: The construction of the generalized cyclotomic sequence with length p^n for a prime p and a positive integer n given by Liu Fang *et al.* (2010) is generalized in this paper. The linear complexity and the autocorrelation values of the new defined sequences are also determined. The results show that the new defined sequences keep the pseudo-random properties of the original sequence, that is, the high linear complexity and undesirable autocorrelation properties. Owing to the flexible ways to assign values to different generalized cyclotomic classes, the new construction contains more classes of generalized cyclotomic sequences when it is compared with the original one.

Key words: Network security; Generalized cyclotomy; Linear complexity; Autocorrelation

1 引言

伪随机序列在密码学和通信系统中被广泛地应用。序列的线性复杂度定义为生成该序列的最短的线性移位寄存器的长度。在密码学相关领域的应用中，伪随机序列必须具有高的线性复杂度[1,2]。由 Berlekamp-Massey 算法可知，一条序列的线性复杂度必须不小于其周期长度的一半。同时，在码分多址，扩频通信和雷达等应用中，序列要有好的自相关性质。

由于具有较好的代数结构，人们对分圆序列进行了深入研究。文献[3]给出了 Legendre 序列的线性复杂度。文献[4,5]等分别计算了周期为 p^2 和 p^3 的二元广义分圆序列的线性复杂度和自相关函数，并进一步地，分别研究了周期为 p^m 的二元广义分圆序列的相应的性质。文献[6]研究了周期为 p^m 的 q- 元广义分圆序列的线性复杂度和自相关函数。最近，文献[7,8]构造了具有高线性复杂度的周期为 $2p^m$ 的二元和四元广义分圆序列。

本文将在文献[6]基础上，给出更多的具有高线性复杂度的周期为 p^m 的 d- 元广义分圆序列，同时分析了相应的自相关函数的性质。具体地，本文安排如下：第 2 节给出了周期为 p^m 的 d- 元广义分圆序列的构造，该构造是文献[6]给出的构造的推广；第 3 节利用文献[9]的方法，确定了新构造序列的线性复杂度；第 4 节，分析了新构造序列的自相关函数的性质；在第 5 节，对本文的工作做了小结。

2 d -元广义分圆序列

对正整数 N， Z_N 表示模 N 的剩余类环， Z_N^* 表示 Z_N 中可逆元的集合。设 H 是 Z_N 的子集及 $a \in Z_N$，定义 $a+H=\{a+h(\bmod N)|\ h\in H\}, a\cdot H=\{a\cdot h(\bmod N)|\ h\in H\}$。设 p 是素数， g 是 $Z_{p^2}^*$ 的本原元，则 g 是 $Z_{p^i}^*, i\ge 1$ 的本原元[10]。设 $d\,|\,(p-1)$，定义 $D_0^{(p^i)}=<g^d>=\{g^{dt}(\bmod p^i)|0\le t<\varphi(p^i)/d\}$, $D_l^{(p^i)}=g^l D_0^{(p^i)}$, $1\le l<d$，称 $D_l^{(p^i)}, l=0,\cdots,d-1$ 为

2012-06-25 收到，2012-08-22 改回
国家自然科学基金(61102093)，福建省高校服务海西建设重点项目(基于数学的信息化技术研究)和福建省自然科学基金(2010J01319)资助课题
*通信作者：柯品惠 keph@fjnu.edu.cn

Z_{p^i} 的 d 阶广义分圆类。易验证，$Z_{p^i}^* = \bigcup_{l=0}^{d-1} D_l^{(p^i)}$。进一步地，对正整数 $n \ge 1$，$Z_{p^n} \setminus \{0\} = \bigcup_{i=1}^{n} p^{n-i} Z_{p^i}^* = \bigcup_{i=1}^{n}\bigcup_{l=0}^{d-1} p^{n-i} D_l^{(p^i)}$。对 $t \in Z_d$，令 $\pi_i(t) = a^{(i)}t + b^{(i)}$，$i = 0,1,\cdots,n-1$，其中 $a^{(i)}, b^{(i)} \in Z_d$ 且 $(a^{(i)}, d) = 1$。易见，π_i，$i = 0,1,\cdots,n-1$ 是 Z_d 上的双射，且有 $\varphi(d)\cdot d$ 种不同的选取。

对给定的一组 π_i，$i = 0,1,\cdots,n-1$（允许 π_i 相同），按如下方法定义周期为 p^n 的 d-元广义分圆序列 $S = \{s_t\}_{t=0}^{p^n-1}$，其中

$$s_t = \begin{cases} \pi_i(l), & t(\mathrm{mod}\, p^n) \in p^i D_l^{(p^{n-i})}, \\ & 0 \le i < n,\ 0 \le l < d \\ d-1, & t \equiv 0(\mathrm{mod}\, p^n) \end{cases} \tag{1}$$

注：文献[6]给出的序列是上述构造的一个特例，此时，只需取所有的 π_i 均为恒等置换。

3 线性复杂度

本节将给出上节构造的 d-元广义分圆序列 S 在 d 为奇素数情形的线性复杂度。设 d 为奇素数，F_d 表示 d 阶有限域。设 $S = \{s_i\}_{i=0}^{N-1}$ 是 F_d 上周期为 N 的序列，称使得如下递推关系 $s_t = c_1 s_{t-1} + c_2 s_{t-2} + \cdots + c_L s_{t-L}$，$t \ge L$，其中，$c_i \in F_d$，$i = 1,2,\cdots,L$ 成立的最小正整数 L 为序列 S 的线性复杂度，简记为 L_S。并称 $m(x) = x^L - c_1 x^{L-1} - \cdots - c_L$ 为序列 S 的极小多项式。对序列 $S = \{s_i\}_{i=0}^{N-1}$，定义 $S(x) = s_0 + s_1 x + \cdots + s_{N-1}x^{N-1}$ 为序列 S 的生成多项式。进一步地，由文献[1,2]可知 $m(x) = \dfrac{x^N - 1}{\gcd(x^N - 1, S(x))}$ 及

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

引理 1[1] 设 $d|(p-1)$，$D_l^{(p)}$，l=0,1,$\cdots$,$d-1$ 是 Z_p^* 上 d 阶广义分圆类，$a \in D_k^{(p)}$，则 $aD_h^{(p)} = D_{h+k}^{(p)}$，$0 \le h < d$，其中下标模 d 运算。

引理 2[1] 设 $D_l^{(p^i)}$ 是 $Z_{p^i}^*$，$i \ge 1$ 上的 d 阶广义分圆类，则 $D_l^{(p^i)} = D_l^{(p)} + pZ_{p^{i-1}}$。

对 $i = 0,1,\cdots,n-1$，定义 $S_i(x) = \sum_{t \in p^i D_0^{(p^{n-i})}} x^t$。从而，对 $l = 0,1,\cdots,d-1$，

$$\sum_{t \in p^i D_l^{(p^{n-i})}} x^t = \sum_{t \in p^i D_0^{(p^{n-i})}} x^{g^l t} = S_i(x^{g^l})$$

进而，式(1)中定义的序列 S 的生成多项式

$$S(x) = d - 1 + \sum_{i=0}^{n-1}\sum_{l=0}^{d-1} \pi_i(l) \cdot \sum_{t \in p^i D_l^{(p^{n-i})}} x^t = d - 1 + \sum_{i=0}^{n-1}\sum_{l=0}^{d-1} \pi_i(l) S_i(x^{g^l})$$

文献[9]给出了下面的引理，进而证明了 Z_{p^n} 上的广义分圆序列的线性复杂度的计算可以转化为 Z_p 上广义分圆序列的计算。

引理 3[9] 设 α 是 p^n 次单位根，m 是满足 $(m, p) = 1$ 的正整数，$i, f \in \{0,1,\cdots,n-1\}$，则

$$S_i(\alpha^{p^f m}) = \begin{cases} 0, & i < n-f-1 \\ S_{n-1}(\alpha^m), & i = n-f-1 \\ R, & i > n-f-1 \end{cases}$$

其中 $R = (p-1)/d$。

定理 1 对式(1)中定义的序列 S，若 $d \in D_0^{(p)}$，则 $L_S = (p^n - 1)/d$。若 $d \notin D_0^{(p)}$，$L_S = p^n$。

证明 设 $R = (p-1)/d$，则对 $i = 0,1,\cdots,n-1$，$l = 0,1,\cdots,d-1$，$|D_l^{(p^i)}| = p^{i-1}R$。从而，

$$\begin{aligned} S(1) &= d - 1 + \sum_{i=0}^{n-1}\sum_{l=0}^{d-1} \pi_i(l) S_i(1) \\ &= d - 1 + \left(\sum_{i=0}^{n-1} p^i R\right)\left(\sum_{l=0}^{d-1} l\right) \\ &= d - 1 + R \cdot \frac{p^n - 1}{p-1} \cdot \frac{d(d-1)}{2} \\ &= \frac{(d-1)(p^n+1)}{2} = d - 1 \end{aligned}$$

设 $m \in p^f D_k^{(p^{n-f})}$，$f \in \{0,1,\cdots,n-1\}$，$k \in \{0,1,\cdots,d-1\}$，$\alpha$ 是 F_d 上的一个扩域上的 p^n 次单位根（由 $(p,d) = 1$ 知，这样的 α 总是存在的）。由引理3，

$$S(\alpha^m) = (d-1) + fR\sum_{t=0}^{d-1} t + \sum_{t=0}^{d-1} \pi_{n-f-1}(t) S_{n-1}(\alpha^{g^{t+k}})$$

由 $p \equiv 1(\mathrm{mod}\, d)$ 及

$$\begin{aligned} &\sum_{t=0}^{d-1} \pi_{n-f-1}(t) S_{n-1}(\alpha^{g^{t+k}}) \\ &= \sum_{t=0}^{d-1} (a^{(n-f-1)}t + b^{(n-f-1)}) S_{n-1}(\alpha^{g^{t+k}}) \\ &= \sum_{t=0}^{d-1} (a^{(n-f-1)}(t+k) + b^{(n-f-1)}) S_{n-1}(\alpha^{g^{t+k}}) \\ &\quad - a^{(n-f-1)}k\sum_{t=0}^{d-1} S_{n-1}(\alpha^{g^{t+k}}) \end{aligned}$$

注意到，$\alpha^{p^{n-1}}$ 是 p 次单位根及

$$\begin{aligned} \sum_{t=0}^{d-1} S_{n-1}(\alpha^{g^{t+k}}) &= \sum_{t=0}^{d-1} \sum_{h \in p^{n-1} D_0^{(p)}} \alpha^{g^{t+k}h} \\ &= \sum_{t=0}^{d-1} \sum_{h \in D_0^{(p)}} (\alpha^{p^{n-1}})^{g^{t+k}h} = -1 \end{aligned}$$

从而，

$$\begin{aligned} &\sum_{t=0}^{d-1} \pi_{n-f-1}(t) S_{n-1}(\alpha^{g^{t+k}}) \\ &= \sum_{t=0}^{d-1} \pi_{n-f-1}(t) S_{n-1}(\alpha^{g^t}) + a^{(n-f-1)}k \end{aligned}$$

进而，

$$S(\alpha^m)=d-1+\sum_{t=0}^{d-1}\pi_{n-f-1}(t)S_{n-1}(\alpha^{g^t})+a^{(n-f-1)}k$$

设 $d\in D_l^{(p)},0\le l<d-1$，则

$$\left[\sum_{t=0}^{d-1}\pi_{n-f-1}(t)S_{n-1}(\alpha^{g^t})\right]^d$$
$$=\sum_{t=0}^{d-1}\pi_{n-f-1}(t)S_{n-1}(\alpha^{g^{t+k}})$$
$$=\sum_{t=0}^{d-1}\pi_{n-f-1}(t)S_{n-1}(\alpha^{g^t})+a^{(n-f-1)}l$$

从而，$\sum_{t=0}^{d-1}\pi_{n-f-1}(t)S_{n-1}(\alpha^{g^t})\in F_d$ 当且仅当 $d\in D_0^{(p)}$。进一步地，若 $d\in D_0^{(p)}$，对 $m\in Z^*_{p^{n-f}}$，$S(\alpha^m)$ 恰有 p^{n-f-1} 个根。从而，对 $\alpha^i,0\le i\ge p^n-1$，$S(x)$ 恰有 $R(1+p+\cdots+p^{n-1})=(p^n-1)/d$ 个根。见式(2)。

证毕

由定理1知，本文构造的序列与文献[6]中给出的序列有相同的线性复杂度。由于本文的构造 π_i 有 $d\cdot(d-1)$ 种选取方法。因此，本文给出的序列数量要大得多。

4　自相关函数值的分布

本节将给出第 2 节给出的序列在 d 为奇素数情形的自相关函数值的分布。设 $S=\{s_i\}_{i=0}^{N-1}$ 是 F_d 上一条周期为 N 的序列，ξ_d 表示复数域 C 中的一个 d 次单位根，$\tau\in\{0,1,\cdots,N-1\}$，称 $R_S(\tau)=\sum_{i=0}^{N-1}\xi_d^{s_t-s_{t+\tau}}$ 为序列 S 在 τ 的自相关函数。显然地，$R_S(0)=N$。

设 $D_i^{(p)},i=0,1,\cdots,d-1$ 表示 Z_p 上的 d 阶分圆类，称 $(i,j)_p=|(D_i+1)\cap D_j|,0\le i,j<d$ 为 Z_p 上的 d 阶分圆数[1]。

引理 4[1]　设 $D_i^{(p)},i=0,1,\cdots,d-1$ 定义同上，$R=(p-1)/d$，则

$$\sum_{i=0}^{d-1}(i,j)_p=\begin{cases}R-1, & j=0\\ R, & j\ne 0\end{cases}$$

引理 5　$D_i^{(p^i)},i=0,1,\cdots,n,t=0,1,\cdots,d-1$ 定义同上，$\tau=p^kb\in p^kD_l^{(p^{n-k})}$，则

(1) 对 $0\le j<k,\ 0\le t<d,\ p^jD_t^{(p^{n-j})}+\tau=p^j\cdot(D_t^{(p^{n-j})}$。

(2) 对 $k+1\le j<n,\ 0\le t<d$，$p^jD_t^{(p^{n-j})}+\tau\subseteq p^kD_l^{(p^{n-k})}$。

(3) 对 $j=k,\ 0\le u,v<d,\ |(p^kD_u^{(p^{n-k})}+\tau)\cap p^kD_v^{(p^{n-k})}|=p^{n-k-1}(u-l,v-l)_p$。

(4) $-\tau\in p^kD_l^{(p^{n-k})}$ 且 $\bigcup_{i=k+1}^{n-1}p^iZ^*_{p^{n-i}}\cup\{0\}\subseteq p^kD_l^{(p^{n-k})}+\tau$。

证明　分情况讨论如下：

(1) 对 $0\le j<k,\ 0\le t<d,\ p^jD_t^{(p^{n-j})}+\tau=p^j\cdot(D_t^{(p^{n-j})}+p^{k-j}b)$。

由引理 2，$D_t^{(p^{n-j})}+p^{k-j}b(\bmod p^{n-j})=D_t^{(p)}+pZ_{p^{n-j-1}}(\bmod p^{n-j})$。

因此，$p^jD_t^{(p^{n-j})}+\tau=p^jD_t^{(p^{n-j})}$。

(2) 对 $k+1\le j<n,0\le t<d$，$p^jD_t^{(p^{n-j})}+\tau=p^j\cdot D_t^{(p^{n-j})}+p^kb=p^k(p^{j-k}D_t^{(p^{n-j})}+b)$。

由 $b\in D_l^{(p^{n-k})}$ 及引理 2，$p^jD_t^{(p^{n-j})}+\tau\subseteq p^kD_l^{(p^{n-k})}$。

(3) 对 $j=k,0\le u,v<d$，由引理 2，

$$|(p^kD_u^{(p^{n-k})}+\tau)\cap p^kD_v^{(p^{n-k})}|$$
$$=|p^k(D_u^{(p)}+b+pZ_{p^{n-k-1}})\cap p^k(D_v^{(p)}+pZ_{p^{n-k-1}})|$$
$$=p^{n-k-1}(u-l,v-l)_p$$

(4) 由 $d\,|\,(p-1)$ 且 d 为奇素数，知 $d\,|\,(p-1)/2$。又由 $g^{(p-1)/2}\equiv-1(\bmod p)$，$-1\in D_0^{(p)}$。不妨设 $b=b_1+pb_2$，其中 $b_1\in D_l^{(p)},b_2\in Z_{p^{n-k+1}}$，则 $-b_1\in D_l^{(p)}$ 且 $p^k(-b_1+pZ_{p^{n-k-1}})\subseteq p^kD_l^{(p^{n-k})}$。另一方面，

$$p^k(-b_1+pZ_{p^{n-k-1}})+\tau=p^{k+1}Z_{p^{n-k-1}}$$
$$=p^{k+1}(Z^*_{p^{n-k-1}}\cup pZ^*_{p^{n-k-2}}\cup\cdots\cup p^{n-k-2}Z^*_p)\cup\{0\}$$
$$=\bigcup_{i=k+1}^{n-1}p^iZ^*_{p^{n-i}}\cup\{0\}$$

因此，$\bigcup_{i=k+1}^{n-1}p^iZ^*_{p^{n-i}}\cup\{0\}\subseteq p^kD_l^{(p^{n-k})}+\tau$。　　证毕

引理 6　设 $(i,j)_d,0\le i,j<d$ 表示 Z_p 上的 d 阶分圆数，ξ_d 表示复数域 C 中的一个 d 次单位根，则

$$\sum_{u=0}^{d-1}\sum_{v=0}^{d-1}(u,v)_d\xi_d^{u-v}=-1$$

证明　设 $-1\in D_{l_0}^{(p)}$，由分圆数的性质知[1]，$(u,v)_d=(l_0-v,u-v)_d$。令 $u-v=w$，则

$$\sum_{u=0}^{d-1}\sum_{v=0}^{d-1}(u,v)_d\xi_d^{u-v}=\sum_{u=0}^{d-1}\sum_{v=0}^{d-1}(l_0-u,u-v)_d\xi_d^{u-v}$$
$$=\sum_{w=0}^{d-1}\sum_{v=0}^{d-1}(l_0-v,w)_d\xi_d^w=\sum_{w=0}^{d-1}\xi_d^w\sum_{v=0}^{d-1}(l_0-v,w)$$

由引理 4，

$$\sum_{w=0}^{d-1}\xi_d^w\sum_{v=0}^{d-1}(l_0-v,w)=(R-1)+R\xi_d+R\xi_d^2+\cdots$$
$$+R\xi_d^{d-1}=-1$$

证毕

定理 2　设序列 S 由式(1)定义，ξ_d 表示复数域 C 中的一个 d 次单位根，则序列 S 的自相关函数值为

$$R_S(\tau)=\begin{cases}p^n, & \tau=0\\ \xi_d^{d-1-\pi_k(l)}+p^n-p^{n-k}-p^{n-k-1}+\xi_d^{\pi_k(l)+1}, & \\ \qquad \tau\in p^kD_l^{(p^{n-k})} & \end{cases}$$

其中 $0 \le k < n, 0 \le l < d$ 。

证明 若 $\tau = 0$，结论显然。若 $\tau \in p^k D_l^{(p^{n-k})}$，则

$$\begin{aligned} R_S(\tau) &= \sum_{i=0}^{p^n-1} \xi_d^{s_t - s_{t+\tau}} = \xi_d^{d-1-\pi_k(l)} \\ &\quad + \sum_{m=0}^{n-1}\sum_{h=0}^{d-1} \sum_{t\in p^m D_h^{(p^{n-m})}} \xi_d^{s_t - s_{t+\tau}} \\ &= \xi_d^{d-1-\pi_k(l)} + \sum_{m=0}^{k-1}\sum_{h=0}^{d-1} \sum_{t\in p^m D_h^{(p^{n-m})}} \xi_d^{s_t - s_{t+\tau}} \\ &\quad + \sum_{h=0}^{d-1} \sum_{t\in p^k D_h^{(p^{n-k})}} \xi_d^{s_t - s_{t+\tau}} \\ &\quad + \sum_{m=k+1}^{n-1}\sum_{h=0}^{d-1} \sum_{t\in p^m D_h^{(p^{n-m})}} \xi_d^{s_t - s_{t+\tau}} \end{aligned}$$

由引理 5，

$$\sum_{m=0}^{k-1}\sum_{h=0}^{d-1} \sum_{t\in p^m D_h^{(p^{n-m})}} \xi_d^{s_t - s_{t+\tau}} = \sum_{m=0}^{k-1} |Z_{p^{n-m}}^*| = p^n - p^{n-k}$$

$$\begin{aligned} &\sum_{h=0}^{d-1} \sum_{t\in p^k D_h^{(p^{n-k})}} \xi_d^{s_t - s_{t+\tau}} \\ &= p^{n-k-1} \sum_{u=0}^{d-1}\sum_{v=0}^{d-1} (u-l, v-l)_d \xi_d^{\pi_k(u)-\pi_k(v)} \\ &\quad + \sum_{h=0}^{d-1} \xi_d^{\pi_k(l)-h} (R + pR + \cdots + p^{n-k-2}R) + \xi_d^{\pi_k(l)-(d-1)} \end{aligned}$$

由于 ξ_d 是 d 次单位根，$\sum_{h=0}^{d-1} \xi_d^h = 0$。从而，

$$\sum_{h=0}^{d-1} \xi_d^{\pi_k(l)-h} (R + pR + \cdots + p^{n-k-2}R) = 0$$

再由 $(a^{(k)}, d) = 1$ 及引理 6，

$$\begin{aligned} &\sum_{u=0}^{d-1}\sum_{v=0}^{d-1} (u-l, v-l)_d \xi_d^{\pi_k(u)-\pi_k(v)} \\ &= \sum_{u=0}^{d-1}\sum_{v=0}^{d-1} (u-l, v-l)_d \xi_d^{a^{(k)}(u-v)} = -1 \end{aligned}$$

因此，

$$\sum_{h=0}^{d-1} \sum_{t\in p^k D_h^{(p^{n-k})}} \xi_d^{s_t - s_{t+\tau}} = -p^{n-k-1} + \xi_d^{\pi_k(l)+1}$$

再由引理 5，

$$\begin{aligned} &\sum_{m=k+1}^{n-1}\sum_{h=0}^{d-1} \sum_{t\in p^m D_h^{(p^{n-m})}} \xi_d^{s_t - s_{t+\tau}} \\ &= \sum_{m=k+1}^{n-1}\sum_{h=0}^{d-1} \sum_{t\in p^m D_h^{(p^{n-m})}} \xi_d^{\pi_m(h)-\pi_k(l)} \\ &= \sum_{m=k+1}^{n-1}\sum_{h=0}^{d-1} \xi_d^{\pi_m(h)-\pi_k(l)} (R + pR + \cdots + p^{n-k-2}R) = 0 \end{aligned}$$

综上，对 $\tau \in p^k D_l^{(p^{n-k})}$，

$R_S(\tau) = \xi_d^{d-1-\pi_k(l)} + p^n - p^{n-k} - p^{n-k-1} + \xi_d^{\pi_k(l)+1}$ 证毕

由定理 2，容易得到如下推论：

推论 1[6] 若取 $\pi_i, i = 0,1,\cdots,n-1$ 均为 Z_d 上的恒等置换，则序列 S 的自相关函数值为

$$R_S(\tau) = \begin{cases} p^n, & \tau = 0 \\ \xi_d^{d-1-l} + p^n - p^{n-k} - p^{n-k-1} + \xi_d^{l+1}, \\ \qquad \tau \in p^k D_l^{(p^{n-k})} \end{cases}$$

其中 $0 \le k < n,\ 0 \le l < d$ 。

5 结束语

通过允许在 $Z_{p^i}^*, 1 \le i < n$ 的每个分圆类上可以灵活取值，本文推广了文献[6]在 SETA2010 给出的广义分圆序列的构造。进一步地，利用文献[9]给出的方法，我们计算了新构造的序列的线性复杂度。同时，计算了新构造序列的自相关函数。结果表明，新构造的序列保持了原构造的伪随机特性，即高的线性复杂度，但是不理想的自相关特性。因此，在应用这类序列的时候，应该有针对性的选择使用。

参 考 文 献

[1] Cusick T, Ding C, and Renvall A. Stream Ciphers and Number Theory[M]. North-Holland Mathematical Library 55, 1998: 198–212.

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

[3] Ding C, Hellseth T, and Shan W. On the linear complexity of Legendre sequences[J]. *IEEE Transactions on Information Theory*, 1998, 44(3): 1276–1278.

[4] Kim Y J, Jin S Y, and Song H Y. Linear complexity and Autocorrelation of prime cube sequences[C]. 2007, LNCS 4851: 188–197.

[5] Yan T, Li S, and Xiao G. On the linear complexity of generalized cyclotomic sequences with the period p^m[J]. *Applied Mathematics Letters*, 2008, (21): 87–193.

[6] Liu F, Peng D Y, Tang X H, *et al*.. On the autocorrelation and the linear complexity of q-Ary prime n-square sequence [C]. SETA 2010, LNCS 6338: 139–150.

[7] Ke P H, Zhang J, and Zhang S Y. On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2p^m$ [OL]. Designs Codes and Cryptography, DOI. 10.1007/s10623-012-9610-9, 2012.

[8] Ke P H and Zhang S Y. New classes of quaternary cyclotomic sequence of length $2p^m$ with high linear complexity[J]. *Information Processing Letters*, 2012, 12(16): 646–650.

[9] 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.

[10] Burton D M. Elementary Number Theory [M]. Maidenhead: UK, McGraw-Hill Education Press, 1998: 92-105.

柯品惠： 男，1978 年生，副教授，研究兴趣包括序列设计、现代密码学中的布尔函数.

李瑞芳： 女，1988 年生，硕士生，研究方向为序列设计.

张胜元： 男，1966 年生，教授，研究领域为编码密码学、组合数学及信息安全.