

## 一类周期为 $pq$ 阶为 2 的 Whiteman 广义分圆序列研究

李胜强<sup>①</sup> 周亮<sup>①</sup> 肖国镇<sup>②</sup>

<sup>①</sup>(电子科技大学通信抗干扰技术国家级重点实验室 成都 610054)

<sup>②</sup>(西安电子科技大学综合业务网国家重点实验室 西安 710071)

**摘要:** 线性复杂度是度量序列随机性质最重要的指标之一。该文基于 Whiteman-广义分圆, 构造了一类周期为  $pq$  阶为 2 的广义分圆序列。证明了适当的选取参数  $p$  和  $q$ , 该类序列的线性复杂度的下界为  $pq - p - q + 1$ , 且该类序列为平衡序列。最后指出了准确计算该序列的线性复杂度所必须解决的问题。

**关键词:** 伪随机序列; Whiteman-广义分圆; 线性复杂度; 特征集

中图分类号: TN918.1

文献标识码: A

文章编号: 1009-5896(2009)09-2205-04

## Study on a Class of Whiteman-Generalized Cyclotomic Sequence with Length $pq$ and Order Two

Li Sheng-qiang<sup>①</sup> Zhou Liang<sup>①</sup> Xiao Guo-zhen<sup>②</sup>

<sup>①</sup>(National Key Lab of Communication, University of Electronic Science and Technology of China, Chengdu 610054, China)

<sup>②</sup>(National Key Lab of ISN, Xidian University, Xi'an 710071, China)

**Abstract:** Linear complexity is one of the most important indexes for measuring the randomness properties of sequences. Based on Whiteman-generalized cyclotomy, a new class of generalized cyclotomic sequences with length  $pq$  and order 2 is constructed. It is proved that the lower bound of linear complexity of the sequence is  $pq - p - q + 1$  with the proper selection of parameters  $p$  and  $q$ , and the sequence has balance property. Finally, this paper points out the method for determine linear complexity.

**Key words:** Pseudo-random sequence; Whiteman-generalized cyclotomy; Linear complexity; Characteristic set

### 1 引言

伪随机序列在扩频通信、测量距离、雷达导航、流密码系统等领域都有十分广泛的应用。线性复杂度和相关性质是衡量序列的两个最重要的指标。不同的应用领域对序列的伪随机性质的要求是不同的, 在各种通信领域强调序列必须具有良好的相关特性, 而在流密码系统中则强调序列要有大的线性复杂度。分圆序列就是一类具有良好随机性质的序列<sup>[1,2]</sup>。Whiteman<sup>[3]</sup>和 Ding<sup>[4]</sup>分别提出了两类不同的广义分圆序列, 分别称之为 W-广义分圆和 D-广义分圆。目前, 基于这两类广义分圆已经构造出了多种 W-广义分圆序列和 D-广义分圆序列<sup>[5-11]</sup>, 并且其中的大部分序列均具有良好的相关性质或大的线性复杂度。

Ding 基于 W-广义分圆构造了一类周期为  $pq$  阶为 2 的广义分圆序列, 并证明了该类序列具有好的线性复杂度和自相关性<sup>[5,7]</sup>。本文基于 W-广义分圆, 通过选取不同的序列的特征集, 构造了一类新

的周期为  $pq$  阶数为 2 的 W-广义分圆序列。该序列是平衡序列, 而文献[5]的序列是几乎平衡的。然后本文讨论了该类序列的线性复杂度, 给出了线性复杂度的一个下界, 结论表明序列的线性复杂度可接近周期长。从线性复杂度的角度看, 该序列是复杂度性质好的序列。按 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。

### 2 双素数周期阶为 2 的 Whiteman 广义分圆及其序列

令  $p$  和  $q$  是不同的素数, 并且满足  $\gcd(p-1, q-1) = 2, p < q$ 。定义  $N = pq$ ,  $e = (p-1)(q-1)/2$ , 由中国剩余定理, 存在  $\text{GF}(p)$  和  $\text{GF}(q)$  的公共本原元  $g$ , 有  $\text{ord}_N(g) = \text{Lcm}(\text{ord}_p(g), \text{ord}_q(g)) = \text{Lcm}(p-1, q-1) = e$ 。令整数  $h$  满足  $h \equiv g \pmod{p}$ ,  $h \equiv 1 \pmod{q}$ 。则阶为 2 的 Whiteman-广义分圆类  $D_0$  和  $D_1$  定义如下<sup>[3]</sup>:  $D_0 = \{g^t : t = 0, 1, \dots, e-1\}$ ,  $D_1 = \{g^t h : t = 0, 1, \dots, e-1\}$ 。这里, 乘法是在模  $N$  剩余类环  $Z_N$  下运算的。可得到<sup>[3]</sup>:  $Z_N^* = D_0 \cup D_1, D_0 \cap D_1 = \emptyset$ , 其中  $Z_N^*$  表示剩余类环  $Z_N$  的所有可逆元素的集合,  $\emptyset$  表示空集。

对  $Z_N$  中的任何子集  $A$  和任意元素  $b$ , 定义  $A \pm b = \{a \pm b : a \in A\}$ ,  $b \cdot A = \{b \cdot a : a \in A\}$ . 定义  $D_0^{(p)} = \{g^{2t} \bmod p : t = 0, 1, \dots, (p-3)/2\}$ ,  $D_0^{(q)} = \{g^{2t} \bmod q : t = 0, 1, \dots, (q-3)/2\}$ ,  $D_1^{(p)} = gD_0^{(p)}$ ,  $D_1^{(q)} = gD_0^{(q)}$ ,  $R = \{0\}$ ,  $P_0 = pD_0^{(q)}$ ,  $P_1 = pD_1^{(q)}$ ,  $Q_0 = qD_0^{(p)}$ ,  $P = P_0 \cup P_1$ ,  $Q = Q_0 \cup Q_1$ ,  $C_1 = P_1 \cup Q_1 \cup D_1$ ,  $C_0 = P_0 \cup Q_0 \cup D_0 \cup R$ , 则  $C_0 \cup C_1 = Z_{pq}$ ,  $C_0 \cap C_1 = \emptyset$ .

双素数周期阶为 2 的 Whiteman 广义分圆序列  $s^\infty$  定义如下: 对于所有的  $i \geq 0$

$$s_i = \begin{cases} 0, & (i \bmod N) \in C_0 \\ 1, & (i \bmod N) \in C_1 \end{cases} \quad (1)$$

显然序列  $s^\infty$  的周期为  $N$ . 二元序列的不平衡度定义为序列中 1 的个数和 0 的个数差的绝对值. 在该序列的一个周期中, 1 出现的个数是  $(pq-1)/2$ , 0 出现的个数是  $(pq+1)/2$ , 所以该序列是平衡序列.

在文献[5]的构造中,  $C_1' = P \cup D_1$ ,  $C_0' = R \cup Q \cup D_0$ . 显然, 本文构造的序列的特征集  $C_1$  和文献[5]中的序列特征集是不同的, 因此两者是不同的序列.

### 3 序列的线性复杂度

令  $s^\infty$  是式(1)中定义的周期为  $N$  的序列, 且  $s^N(x) = s_0 + s_1x + \dots + s_{N-1}x^{N-1}$ , 显然序列  $s^\infty$  的线性复杂度 ( $LC(s^\infty)$ ) 可由下式确定<sup>[1]</sup>:

$$N - \deg(\gcd(x^N - 1, s^N(x))) \quad (2)$$

令  $m$  是 2 模  $N$  的阶, 则  $\text{GF}(2^m)$  有一个  $N$  次单位原根  $\alpha$ . 定义  $s(x) = \sum_{i \in C_1} x^i = \left( \sum_{i \in Q_0} + \sum_{i \in P_1} + \sum_{i \in D} \right) x^i \in \text{GF}(2)[x]$ , 由式(2)有

$$LC(s^\infty) = N - \left| \{j : s(\alpha^j) = 0, 0 \leq j \leq N-1\} \right| \quad (3)$$

注意到

$$s(1) = \left( \frac{p-1}{2} + \frac{q-1}{2} \right) \pmod{2} \quad (4)$$

由于  $0 = \alpha^N - 1 = (\alpha^p)^q - 1 = (\alpha^p - 1)(1 + \alpha^p + \alpha^{2p} + \dots + \alpha^{(q-1)p})$ , 则

$$\alpha^p + \alpha^{2p} + \dots + \alpha^{(q-1)p} = 1, \left( \sum_{i \in P_0} + \sum_{i \in P_1} \right) \alpha^i = 1 \quad (5)$$

由对称性有

$$\left( \sum_{i \in Q_0} + \sum_{i \in Q_1} \right) \alpha^i = 1 \quad (6)$$

注意到

$$\left( \sum_{i \in P} + \sum_{i \in Q} + \sum_{i \in D_0} + \sum_{i \in D_1} \right) \alpha^i + 1 = \sum_{i=0}^{N-1} \alpha^i = 0 \quad (7)$$

**引理 1** 令下文的符号和上文相同, 则

$$\sum_{i \in D_1} \alpha^{ki} = \begin{cases} \frac{(p-1)}{2} \pmod{2}, & k \in P \\ \frac{(q-1)}{2} \pmod{2}, & k \in Q \end{cases}$$

**证明** 当  $k \in P$  时, 由于  $g$  是  $\text{GF}(p)$  和  $\text{GF}(q)$  的公共本原根, 并且  $g$  模  $N$  的阶为  $e$ , 由  $h$  的定义有  $D_1 \pmod{q} = \{g^t h \pmod{q} : t = 0, 1, \dots, e-1\} = \{g^t : t = 0, 1, \dots, e-1\} \pmod{q} = \{1, 2, \dots, q-1\}$ . 当  $t$  跑遍  $\{0, 1, \dots, e-1\}$  时,  $g^t \pmod{q}$  取  $\{1, 2, \dots, q-1\}$  中的每个值  $(p-1)/2$  次. 由式(5)可得:

$$\sum_{i \in D_1} \alpha^{ki} = \left( \frac{p-1}{2} \pmod{2} \right) \sum_{i \in P} \alpha^i = \frac{p-1}{2} \pmod{2}$$

同理可证引理 1 的第 2 部分. 证毕

**引理 2** (文献[4] 引理 7) 如果  $a \in D_j$ , 那么  $aD_i = D_{(i+j) \pmod{2}}$ , 其中  $i, j = 0, 1$ .

**引理 3** 令下文的符号和上文相同, 则

$$s(\alpha^k) = \begin{cases} s(\alpha), & k \in D_0 \cup D_1 \\ \sum_{P_1} \alpha^{ki}, & k \in P \\ \sum_{Q_1} \alpha^{ki}, & k \in Q \end{cases}$$

**证明** 与引理 1 的证明类似, 可以得到  $D_0 \pmod{p} = D_1 \pmod{p} = D_0^{(p)} \cup D_1^{(p)}$ ,  $D_0 \pmod{q} = D_1 \pmod{q} = D_0^{(q)} \cup D_1^{(q)}$ .

若  $k \in D_0$ , 则存在  $t \in \{0, 1, \dots, e-1\}$ , 使得  $k \equiv g^t \pmod{pq}$ . 则有  $k \equiv g^t \pmod{p}$ , 且  $k \equiv g^t \pmod{q}$ . 显然, 当  $t$  为偶数时,  $k$  同时为模  $p$  和模  $q$  的二次剩余; 当  $t$  为奇数时,  $k$  同时为模  $p$  和模  $q$  的二次非剩余. 若  $k \in D_1$ , 则存在  $t \in \{0, 1, \dots, e-1\}$ , 使  $k \equiv g^t h \pmod{pq}$ . 因为  $h \equiv g \pmod{p}$ ,  $h \equiv 1 \pmod{q}$ , 则有  $k \equiv g^{t+1} \pmod{p}$ , 且  $k \equiv g^t \pmod{q}$ . 显然, 当  $t$  为奇数时,  $k$  为模  $p$  的二次剩余且  $k$  为模  $q$  的二次非剩余; 当  $t$  为偶数时,  $k$  为模  $p$  的二次非剩余且  $k$  为模  $q$  的二次剩余.

由引理 2, 当  $k \in D_0$ ,  $k \pmod{p} \in D_0^{(p)}$ , 且  $k \pmod{q} \in D_0^{(q)}$ ,  $kD_1 = D_1$ ,  $kQ_1 = qkD_1^{(p)} = qD_1^{(p)} = Q_1$ ,  $kP_1 = pkD_1^{(q)} = P_1$ , 则  $s(\alpha^k) = \left( \sum_{i \in P_1} + \sum_{i \in Q_1} + \sum_{i \in D_1} \right) \alpha^{ki} =$

$$\left( \sum_{i \in P_1} + \sum_{i \in Q_1} + \sum_{i \in D_1} \right) \alpha^i = s(\alpha).$$

如果  $k \in D_0$ ,  $k \pmod{p} \in D_1^{(p)}$ , 且  $k \pmod{q} \in D_1^{(q)}$ , 则  $kD_1 = D_1$ ,  $kQ_1 = qkD_1^{(p)} = qD_0^{(p)} = Q_0$ ,  $kP_1 = pkD_1^{(q)} = P_0$ , 又由式(5)和式(6), 那么  $s(\alpha^k) =$

$$\left( \sum_{i \in P_1} + \sum_{i \in Q_1} + \sum_{i \in D_1} \right) \alpha^{ki} = \left( \sum_{i \in P_0} + \sum_{i \in Q_0} + \sum_{i \in D_1} \right) \alpha^i = s(\alpha).$$

如果  $k \in D_1$ ,  $k(\bmod p) \in D_0^{(p)}$ , 且  $k(\bmod q) \in D_1^{(q)}$ , 则  $kD_1 = D_0$ ,  $kQ_1 = qkD_1^{(p)} = qD_1^{(p)} = Q_1$ ,  $kP_1 = pkD_1^{(q)} = P_0$ , 又由式(5)和式(7), 那么  $s(\alpha^k)$

$$= \left( \sum_{i \in P_1} + \sum_{i \in Q_1} + \sum_{i \in D_1} \right) \alpha^{ki} = \left( \sum_{i \in P_0} + \sum_{i \in Q_1} + \sum_{i \in D_0} \right) \alpha^i = s(\alpha).$$

如果  $k \in D_1$ ,  $k(\bmod p) \in D_1^{(p)}$ , 且  $k(\bmod q) \in D_0^{(q)}$ , 则  $kD_1 = D_0$ ,  $kQ_1 = qkD_1^{(p)} = qD_0^{(p)} = Q_0$ ,  $kP_1 = pkD_1^{(q)} = P_1$ , 又由式(6)和式(7), 那么  $s(\alpha^k)$

$$= \left( \sum_{i \in P_1} + \sum_{i \in Q_1} + \sum_{i \in D_1} \right) \alpha^{ki} = \left( \sum_{i \in P_1} + \sum_{i \in Q_0} + \sum_{i \in D_0} \right) \alpha^i = s(\alpha).$$

当  $k \in P$  时,  $kQ_1 = \{0\}$ , 由引理 1 有

$$\begin{aligned} s(\alpha^k) &= \left( \sum_{i \in P_1} + \sum_{i \in Q_1} + \sum_{i \in D_1} \right) \alpha^{ki} \\ &= \sum_{i \in D_1^{(p)}} \alpha^{qki} + \sum_{i \in D_1} \alpha^{ki} + \sum_{i \in P_1} \alpha^{ki} \\ &= \left( \frac{p-1}{2} \bmod 2 \right) + \left( \frac{p-1}{2} \bmod 2 \right) + \sum_{i \in P_1} \alpha^{ki} \\ &= \sum_{i \in P_1} \alpha^{ki} \end{aligned}$$

当  $k \in Q$  时,  $kP_1 = \{0\}$ , 由引理 1 有

$$\begin{aligned} s(\alpha^k) &= \left( \sum_{i \in P_1} + \sum_{i \in Q_1} + \sum_{i \in D_1} \right) \alpha^{ki} \\ &= \left( \frac{q-1}{2} \bmod 2 \right) + \left( \frac{q-1}{2} \bmod 2 \right) + \sum_{i \in Q_1} \alpha^{ki} \\ &= \sum_{i \in Q_1} \alpha^{ki} \end{aligned}$$

综上所述, 引理 3 得证。

**引理 4**  $s(\alpha) \in \{0,1\}$  恒成立。

**证明** 因为 2 是域  $\text{GF}(2^m)$  的特征, 则  $[s(\alpha)]^2 = s(\alpha^2)$ 。由引理 3,  $s(\alpha^2) = s(\alpha)$  当且仅当  $2 \in D_0 \cup D_1$ 。由定义知,  $Z_{pq} = D_0 \cup D_1 \cup P \cup Q \cup R$ , 显然,  $2 \notin P \cup Q \cup R$ , 则  $2 \in D_0 \cup D_1$ 。所以  $s(\alpha) \in \{0,1\}$  恒成立。证毕

**引理 5**

(1) 如果  $k \in P$ ,  $\sum_{i \in P_1} \alpha^{ki} \in \{0,1\}$  当且仅当  $q \equiv \pm 1(\bmod 8)$ 。

(2) 如果  $k \in Q$ ,  $\sum_{i \in Q_1} \alpha^{ki} \in \{0,1\}$  当且仅当  $p \equiv \pm 1(\bmod 8)$ 。

**证明** 引理 5 的证明可以参看文献[6]的引理 5。

注: 由文献[6]的讨论可知, 对固定的  $\alpha$ , 当  $q \equiv \pm 1(\bmod 8)$  时,  $\sum_{i \in P_1} \alpha^{ki} (k \in P_0)$  和  $\sum_{i \in P_1} \alpha^{ki} (k \in P_1)$  恰好其中一个为 0。不妨固定  $\alpha$ , 使得当  $k \in P_0$  时,  $\sum_{i \in P_1} \alpha^{ki} = 0$ 。类似地, 当  $p \equiv \pm 1(\bmod 8)$  时, 可以选定  $\alpha$ , 使得当  $k \in Q_0$  时,  $\sum_{i \in Q_1} \alpha^{ki} = 0$ 。

下面举一个例子说明, 适当的选择  $p$  和  $q$ , 可以

使得  $s(\alpha) = 1$ 。

**例** 取  $p = 3$ ,  $q = 7$ , 则  $N = 21$ ,  $e = 6$ , 由中国剩余定理求得  $g = 5$ ,  $h = 8$ , 由此可计算出  $D_0 = \{1, 4, 5, 16, 17, 20\}$ ,  $D_1 = \{2, 8, 10, 11, 13, 19\}$ ,  $P_0 = \{3, 6, 12\}$ ,  $P_1 = \{9, 15, 18\}$ ,  $Q_0 = \{7\}$ ,  $Q_1 = \{14\}$ 。设  $\alpha$  是有限域  $\text{GF}(2^m)$  上的 21 次单位原根。求  $s(\alpha) = \left( \sum_{i \in P_1} + \sum_{i \in Q_1} + \sum_{i \in D_1} \right) \alpha^i$  的值。

因为  $\alpha$  是有限域  $\text{GF}(2^m)$  上的 21 次单位原根, 容易求得使  $2^m \equiv 1(\bmod 21)$  成立的最小  $m$  为 6, 所以  $\alpha \in \text{GF}(2^6)$ 。容易找到一个  $\text{GF}(2)$  上的 6 次不可约多项式  $x^6 + x + 1$ , 令  $\beta$  是  $\text{GF}(2^6)$  的一个生成元,  $\beta^6 + \beta + 1 = 0$ , 且有  $\alpha = \beta^3$ 。则  $\text{GF}(2^6)$  上的所有元素都可以用次数不大于 6 的  $\beta$  的多项式表示。因此由  $\beta^6 = \beta + 1$  可计算验证

$$\begin{aligned} s(\alpha) &= \left( \sum_{i \in P_1} + \sum_{i \in Q_1} + \sum_{i \in D_1} \right) \alpha^i = \alpha^9 + \alpha^{15} \\ &\quad + \alpha^{18} + \alpha^{14} + \alpha^2 + \alpha^8 + \alpha^{10} + \alpha^{11} + \alpha^{13} + \alpha^{19} \\ &= \beta^{27} + \beta^{45} + \beta^{54} + \beta^{42} + \beta^6 + \beta^{24} + \beta^{30} \\ &\quad + \beta^{33} + \beta^{39} + \beta^{57} = 1 \end{aligned}$$

下面通过定理 1 给出本文构造的序列的线性复杂度的下界。

**定理 1** 适当的选取  $p, q$ , 使得  $s(\alpha) = 1$ 。可使得序列的线性复杂度满足  $LC(s^\infty) \geq pq - p - q + 1$ 。

**证明** 由引理 4 可知,  $s(\alpha) \in \{0,1\}$ 。选择适当的  $p, q$ , 使  $s(\alpha) = 1$ 。由引理 3 和式(3)得

$$\begin{aligned} LC(s^\infty) &= pq - \left| \left\{ k : s(\alpha^k) = 0, k \in D_0 \cup D_1 \right\} \right| \\ &\quad - \left| \left\{ k : \sum_{i \in P_1} \alpha^{ki} = 0, k \in P \right\} \right| \\ &\quad - \left| \left\{ k : \sum_{i \in Q_1} \alpha^{ki} = 0, k \in Q \right\} \right| \\ &\quad - \left| \left\{ k : s(\alpha^k) = 0 \right\}, k \in R \right| \\ &\geq pq - (q-1) - (p-1) - 1 \\ &= pq - p - q + 1 \end{aligned}$$

## 4 结束语

本文构造的广义分圆序列和文献[5]中的广义分圆序列都是基于 Whiteman 广义分圆类构造的。不同之处在于序列的特征集的选取。文献[5]中的构造把集合  $P$  直接划入特征集  $C_1$  中, 而把  $Q$  划入  $C_0$  中, 所构造的序列的不平衡度是  $q - p - 1$ 。本文把集合  $P$  和  $Q$  分别再分成两个元素个数相等的两个子集合, 分别为  $P_0, P_1$  和  $Q_0, Q_1$ 。之后把  $P_1$  和  $Q_1$  一起划入特征集  $C_1$  中, 这样构造出来的序列是平衡序列。要确定该序列的线性复杂度的具体值, 必须找出  $p, q$  的取值和多项式  $s(\alpha)$  的关系。目前这一问题

有待进一步研究。因此不能给出该序列的具体的线性复杂度的大小。但是本文确定了该序列的线性复杂度的一个下界。由定理1的结论,适当地选择 $p$ 和 $q$ ,可以使得序列的线性复杂度 $LC(s^\infty) \geq pq - p - q + 1$ ,即序列的线性复杂度均接近周期长。从线性复杂度的角度看,该序列是复杂度性质好的序列。按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。

最后,我们指出进一步的研究内容:(1)研究该类Whiteman-广义分圆序列的自相关性质。(2)研究 $p$ 和 $q$ 的取值与多项式 $s(\alpha)$ 的取值之间的关系。

### 参 考 文 献

- [1] Cusick T, Ding C, and Renvall A. Stream Ciphers and Number Theory[M]. Elsevier/North-Holland. North-Holland Mathematical Library 55, 1998: 195-226.
- [2] Ding C and Helleseht T. On cyclotomic generator of order  $r$  [J]. *Information Processing Letters*, 1998, 66(1): 21-25.
- [3] Whiteman A L. A family of difference sets [J]. *Illinois Journal of Mathematics*, 1962, 6(2): 107-121.
- [4] Ding C and Helleseht T. New generalized cyclotomy and its applications[J]. *Finite Fields and Their Applications*, 1998, 4(2): 140-166.
- [5] Ding C. Linear complexity of generalized cyclotomic binary sequences of order 2[J]. *Finite Fields and Their Applications*, 1997, 3(2): 159-174.
- [6] Bai E J, Liu X J, and Xiao G Z. Linear complexity of new generalized cyclotomic sequences of order of length  $pq$ [J]. *IEEE Transactions on Information Theory*, 2005, 51(5): 1849-1853.
- [7] Ding C. Autocorrelation values of generalized cyclotomic sequences of order two[J]. *IEEE Transactions on Information Theory*, 1998, 44(4): 1699-1702.
- [8] Li S Q, Chen Z X, and Sun R, et al. On the randomness of generalized cyclotomic sequences of order two and length  $pq$  [J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2007, E90-A(9): 2037-2041.
- [9] Li S Q, Chen Z Q, and Fu X T, et al. Autocorrelation values of new generalized cyclotomic sequences of order two and length  $pq$  [J]. *Journal of Computer Science and Technology*, 2007, 22(6): 830-834.
- [10] Chen Z X and Li S Q. Some notes on generalized cyclotomic sequences of length  $pq$ [J]. *Journal of Computer Science and Technology*, 2008, 23(5): 843-850.
- [11] Yan T J, Li S Q, and Xiao G Z. On the linear complexity of generalized cyclotomic sequences with the period  $p^m$  [J]. *Applied Mathematics Letters*, 2008, 21(2): 187-193.

李胜强: 男, 1980年生, 博士, 讲师, 研究方向为流密码设计与分析和安全保密通信。

周 亮: 男, 1961年生, 教授, 博士生导师, 研究方向为编码理论。

肖国镇: 男, 1934年生, 教授, 博士生导师, 研究方向为代数编码和密码学。