**文章编号:** 0583-1431(2019)02-0233-14 **文献标识码: A**

# 一类新的广义割圆序列的线性复杂度及其自相关值

刘华宁 陈晓林

西北大学数学学院 西安 710127
E-mail: hnliu@nwu.edu.cn; xlchen@stumail.nwu.edu.cn

**摘 要** 最近, 丁存生基于新的割圆类 $(V_0, V_1)$ 构造了循环码并研究了其性质. 本文利用割圆类 $(V_0, V_1)$ 构造了周期为 $pq$ 的 2 阶二元序列, 并计算了其自相关值、线性复杂度和极小多项式.

**关键词** 流密码; 广义割圆类; 广义割圆序列; 自相关值; 线性复杂度
**MR(2010) 主题分类** 94A55, 94A60, 11K45
**中图分类** O156.4

## Autocorrelation Values and Linear Complexity of New Generalized Cyclotomic Squences

Hua Ning LIU Xiao Lin CHEN

*School of Mathematics, Northwest University, Xi'an* 710127*, P. R. China*
*E-mail*: *hnliu@nwu.edu.cn*; *xlchen@stumail.nwu.edu.cn*

**Abstract** Recently Ding has constructed certain cyclic codes by using new cyclotomy $(V_0, V_1)$ and studied the properties. In this paper we construct new binary sequences of order two and length $pq$ by using the cyclotomy $(V_0, V_1)$, and calculate the autocorrelation values, linear complexity and minimal polynomials.

**Keywords** stream cipher; generalized cyclotomy; generalized cyclotomic sequence; autocorrelation value; linear complexity
**MR(2010) Subject Classification** 94A55, 94A60, 11K45
**Chinese Library Classification** O156.4

## 1 引言

伪随机序列在数字模拟、软件测试、雷达系统、扩频通信系统、测距系统、CDMA、全球定位系统、信道编码、码分多址系统、流密码等领域中有着重要的应用, 因此得到了广泛深入的研

收稿日期: 2018-04-15; 接受日期: 2018-06-26
基金项目: 国家自然科学基金资助项目 (11571277); 陕西省工业科技攻关项目 (2016GY-077, 2016GY-080)

究. 设 $\mathbb{F}_l$ 是一个 $l$ 元有限域, $\mathbb{F}_l$ 上的序列 $s^\infty=(s_0,s_1,\ldots)$ 的周期为 $N$. 序列 $s^\infty$ 的周期自相关值 $C_s(w)$ 定义为

$$C_s(w)=\sum_{i=0}^{N-1}(-1)^{s_{i+w}+s_i},$$

其中 $1\le w\le N-1$. 序列 $s^\infty$ 的线性复杂度 $L(s^\infty)$ 是生成 $s^\infty$ 的最短线性反馈移位寄存器的级数, 即满足

$$s_g=c_1s_{g-1}+c_2s_{g-2}+\cdots+c_Ls_{g-L},\quad g\ge L$$

的最小非负整数 $L$, 其中常数 $c_1,\ldots,c_L\in\mathbb{F}_2$. 根据 Berlekamp–Massey 算法, 如果 $L(s^\infty)>\frac{N}{2}$, 则认为序列 $s^\infty$ 具有 "好" 的线性复杂度.

定义

$$s(x)=s_0+s_1x+\cdots+s_{N-1}x^{N-1}.$$

序列 $s^\infty$ 的极小多项式定义为

$$m(x)=\frac{x^N-1}{\gcd(x^N-1,s(x))},$$

此时序列 $s^\infty$ 的线性复杂度满足

$$L(s^\infty)=N-\deg(\gcd(x^N-1,s(x))).$$

设 $m=\mathrm{ord}_N(2)$, $\alpha$ 是有限域 $\mathbb{F}_{2^m}$ 的一个 $N$ 次本原单位根. 根据 Blahut 定理可得

$$L(s^\infty)=N-\left|\left\{t:s(\alpha^t)=0,\ 0\le t<N\right\}\right|.$$

伪随机序列的构造和随机性分析是密码学领域的核心问题. 有限域 $\mathbb{F}_2$ 上的伪随机序列的随机性研究在加密应用中占有十分重要的地位, 自相关值和线性复杂度是测量伪随机序列的性质的两个重要指标. 构造伪随机序列的一个重要方法, 是基于对模 $N$ 剩余类环分割得到的割圆类. 当 $N$ 为素数时, 其割圆类称为经典割圆类; 当 $N$ 为合数时, 其割圆类称为广义割圆类. 相应地, 基于经典割圆类构造的序列称为经典割圆序列; 基于广义割圆类构造的序列称为广义割圆序列. Whiteman [11] 为了寻找剩余差集, 构造了一类关于模 $pq$ 的广义割圆类. 丁存生和 Helleseth [6] 研究了一类新的关于 $p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$ 的广义割圆类. 学者们基于上述两种广义割圆类构造了一些广义割圆序列.

本文假设 $N=pq$, 其中 $p$, $q$ 是两个不同的素数. 根据中国剩余定理, 存在模 $p$ 和 $q$ 公共原根. 设 $g$ 是模 $p$ 和 $q$ 的一个公共原根, 整数 $x$ 满足

$$x\equiv g\ (\mathrm{mod}\ p),\quad x\equiv 1\ (\mathrm{mod}\ q).$$

设 $d=\gcd(p-1,q-1)$, $e=(p-1)(q-1)/d$. 根据文 [11], $d$ 阶 Whiteman 广义割圆类的定义为

$$D_i=\left\{g^sx^i:s=0,1,\ldots,e-1\right\},\quad i=0,1,\ldots,d-1.$$

易证 $\mathbb{Z}_{pq}^*=\bigcup_{i=0}^{d-1}D_i$, 且当 $i\ne j$ 时, 有 $D_i\cap D_j=\emptyset$. 定义

$$P=\{p,2p,\ldots,(q-1)p\},\quad Q=\{q,2q,\ldots,(p-1)q\},\quad Q_0=Q\cup\{0\},$$

可得

$$\mathbb{Z}_{pq} = P \cup Q_0 \bigcup_{i=0}^{d-1} D_i.$$

**命题 1.1** [3] 设 $d = \gcd(p-1, q-1) = 2$, $D_0$ 和 $D_1$ 为 2 阶割圆类. 定义

$$C_0 = \{0\} \cup Q \cup D_0, \quad C_1 = P \cup D_1.$$

关于模 $pq$ 的 2 阶二元广义割圆序列 $s^\infty$ 定义如下

$$s_i = \begin{cases} 0, & \text{如果 } (i \bmod pq) \in C_0, \\ 1, & \text{如果 } (i \bmod pq) \in C_1. \end{cases}$$

设 $m = \mathrm{ord}_{pq}(2)$, $\alpha$ 是有限域 $\mathbb{F}_{2^m}$ 的一个 $pq$ 次本原单位根. 定义 $d_i(x) = \prod_{j \in D_i} \left(x - \alpha^j\right)$, $i = 0, 1$.

(I) 如果 $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 8$ 或者 $p \equiv -3 \pmod 8$, $q \equiv -1 \pmod 8$, 则有

$$L(s^\infty) = pq - 1, \quad m(x) = \frac{x^{pq} - 1}{x - 1}.$$

(II) 如果 $p \equiv -1 \pmod 8$, $q \equiv 3 \pmod 8$ 或者 $p \equiv 3 \pmod 8$, $q \equiv -1 \pmod 8$, 则有

$$L(s^\infty) = (p-1)q, \quad m(x) = \frac{x^{pq} - 1}{x^q - 1}.$$

(III) 如果 $p \equiv -1 \pmod 8$, $q \equiv -3 \pmod 8$ 或者 $p \equiv 3 \pmod 8$, $q \equiv 1 \pmod 8$, 则有

$$L(s^\infty) = pq - p - q + 1, \quad m(x) = \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}.$$

(IV) 如果 $p \equiv 1 \pmod 8$, $q \equiv -1 \pmod 8$ 或者 $p \equiv -3 \pmod 8$, $q \equiv 3 \pmod 8$, 则有

$$L(s^\infty) = \frac{pq + p + q - 3}{2}, \quad m(x) = \frac{x^{pq} - 1}{(x - 1)d_0(x)}.$$

(V) 如果 $p \equiv -1 \pmod 8$, $q \equiv 1 \pmod 8$ 或者 $p \equiv 3 \pmod 8$, $q \equiv -3 \pmod 8$, 则有

$$L(s^\infty) = \frac{(p-1)(q-1)}{2}, \quad m(x) = d_1(x).$$

(VI) 如果 $p \equiv -1 \pmod 8$, $q \equiv 1 \pmod 8$ 或者 $p \equiv 3 \pmod 8$, $q \equiv 3 \pmod 8$, 则有

$$L(s^\infty) = \frac{(p-1)(q+1)}{2}, \quad m(x) = \frac{(x^p - 1)d_1(x)}{x - 1}.$$

**命题 1.2** [4] 设 $d = \gcd(p-1, q-1) = 2$. 定义

$$C_0 = \{0\} \cup Q \cup D_0, \quad C_1 = P \cup D_1.$$

关于模 $pq$ 的二元广义割圆序列 $s^\infty$ 定义为

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

(I) 设 $\frac{(p-1)(q-1)}{4}$ 是偶数, 则有

$$C_s(w) = \begin{cases} q - p - 3, & \text{如果 } w \in P, \\ p + 1 - q, & \text{如果 } w \in Q, \\ -1, & \text{如果 } w \in \mathbb{Z}_N^*. \end{cases}$$

(II) 设 $\frac{(p-1)(q-1)}{4}$ 是奇数, 则有

$$C_s(w)=\begin{cases} q-p-3, & \text{如果 } w\in P,\\ p+1-q, & \text{如果 } w\in Q,\\ -3, & \text{如果 } w\in D_0,\\ 1, & \text{如果 } w\in D_1. \end{cases}$$

**命题 1.3** [12] 设 $d=\gcd(p-1,q-1)=2^k$. 定义

$$C_0=\{0\}\cup Q\cup\Big(\bigcup_{i=0}^{2^{k-1}-1}D_i\Big),\quad C_1=P\cup\Big(\bigcup_{i=2^{k-1}}^{2^k-1}D_i\Big).$$

关于模 $pq$ 的 $2^k$ 阶二元广义割圆序列 $s^\infty$ 定义如下

$$s_i=\begin{cases} 0, & \text{如果 } (i \bmod pq)\in C_1,\\ 1, & \text{如果 } (i \bmod pq)\in C_0. \end{cases}$$

设 $m=\mathrm{ord}_{pq}(2)$, $\alpha$ 是有限域 $\mathbb{F}_{2^m}$ 的一个 $pq$ 次本原单位根. 定义

$$S_i(x)=\sum_{j\in P\cup\left(\bigcup_{t=2^{k-1}+i}^{2^k-1+i}D_t\right)}x^j,\quad i=0,1,\ldots,2^k-1,$$

以及

$$\wedge=\left\{i_j: S_{ij}(\alpha)=0,\ j=0,1,\ldots,2^{k-1}-1\right\}.$$

(I) 设 $g^s\not\equiv 2 \pmod{pq}$ 对所有 $s$ 均成立, 则有

$$L(s^\infty)=(p-1)q,\quad m(x)=\frac{x^{pq}-1}{x^q-1}.$$

(II) 如果存在 $s$ 满足 $g^s\equiv 2 \pmod{pq}$, 则有

$$L(s^\infty)=\frac{(q-1)(p+1)}{2},\quad m(x)=\frac{x^{pq}-1}{(x^p-1)\prod_{i\in\wedge}d_i(x)},$$

其中 $d_i(x)=\prod_{j\in D_i}(x-\alpha^j)$.

**命题 1.4** [8] 设 $d=\gcd(p-1,q-1)=4$. 定义

$$C_0=\{0\}\cup Q\cup D_0,\quad C_1=P\cup D_1\cup D_2\cup D_3.$$

关于模 $pq$ 的二元广义割圆序列 $s^\infty$ 定义如下

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

(I) 设 $\frac{(p-1)(q-1)}{16}$ 是偶数, 则有

$$C_s(w)=\begin{cases} pq, & \text{如果 } w=0,\\ \dfrac{pq-9p+3q-7}{4}, & \text{如果 } w\in P,\\ \dfrac{pq+3p-q+1}{4}, & \text{如果 } w\in Q,\\ \dfrac{2a+pq-6p+2q-7}{4}, & \text{如果 } w\in D_1\cup D_3,\\ \dfrac{-2a+pq-6p+2q-3}{4}, & \text{如果 } w\in D_0\cup D_2, \end{cases}$$

其中整数 $a$ 满足 $a\equiv 1 \pmod 4$, $pq=a^2+4b^2$, $b\in\mathbb{Z}$.

(II) 设 $\frac{(p-1)(q-1)}{16}$ 是奇数, 则有

$$C_s(w)=\begin{cases} pq, & \text{如果 } w=0,\\ \dfrac{pq-9p+3q-7}{4}, & \text{如果 } w\in P,\\ \dfrac{pq+3p-q+1}{4}, & \text{如果 } w\in Q,\\ \dfrac{6a+pq-6p+2q+1}{4}, & \text{如果 } w\in D_0,\\ \dfrac{-2(a-4b)+pq-6p+2q-7}{4}, & \text{如果 } w\in D_1,\\ \dfrac{-2a+pq-6p+2q-7}{4}, & \text{如果 } w\in D_2,\\ \dfrac{-2(a+4b)+pq-6p+2q-7}{4}, & \text{如果 } w\in D_3, \end{cases}$$

其中整数 $a$, $b$ 满足 $pq=a^2+4b^2$ 且 $a\equiv 1 \pmod 4$.

对于 $d=\gcd(p-1,q-1)=2$, 定义

$$V_0=\{g^s x^l : 0\le s\le e-1, 0\le l\le d-1, 2\mid s+l\},$$
$$V_1=\{g^s x^l : 0\le s\le e-1, 0\le l\le d-1, 2\nmid s+l\}.$$

显然, $V_0$ 和 $V_1$ 构成了 $\mathbb{Z}_N^*$ 的一个分割, 且 $V_1=gV_0$. 丁存生 [5] 基于新的割圆类 $(V_0,V_1)$ 构造了循环码并研究了其性质.

本文基于割圆类 $(V_0,V_1)$ 构造了新的二元序列, 并计算了其自相关值和线性复杂度.

**定理 1.5** 设 $d=\gcd(p-1,q-1)=2$. 定义

$$C_0=\{0\}\cup Q\cup V_0,\quad C_1=P\cup V_1.$$

关于模 $pq$ 的 2 阶二元广义割圆序列 $s^\infty$ 定义为

$$s_i=\begin{cases} 0, & \text{如果 } (i \bmod pq)\in C_0,\\ 1, & \text{如果 } (i \bmod pq)\in C_1, \end{cases} \tag{1.1}$$

则有

$$C_s(w)=\begin{cases} pq-2p-2, & \text{如果 } w\in P,\\ 1+p-q-(q-1)\left(\dfrac{w}{p}\right)\left((-1)^{\frac{p-1}{2}}+1\right), & \text{如果 } w\in Q,\\ -q-(q-2)\left(\dfrac{w}{p}\right)\left((-1)^{\frac{p-1}{2}}+1\right), & \text{如果 } w\in \mathbb{Z}_N^*, \end{cases} \tag{1.2}$$

其中 $(\frac{\cdot}{p})$ 表示模 $p$ 的 Legendre 符号.

**定理 1.6** 设 $m=\mathrm{ord}_{pq}(2)$ 且 $\alpha$ 是有限域 $\mathbb{F}_{2^m}$ 的一个 $pq$ 次本原单位根. 定义 $d_0(x)=\prod_{j\in V_0}(x-\alpha^j)$.

(I) 如果 $p\equiv 1 \pmod 8$, 则有

$$L(s^\infty)=\frac{pq+q-p-1}{2},\quad m(x)=\frac{x^{pq}-1}{(x^p-1)d_0(x)}.$$

(II) 如果 $p\equiv -1 \pmod 8$, 则有

$$L(s^\infty)=\frac{pq-p-q+1}{2},\quad m(x)=\frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)d_0(x)}.$$

(III) 如果 $p \equiv 3 \pmod 8$, 则有

$$L(s^\infty) = pq - p - q + 1, \quad m(x) = \frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)}.$$

(IV) 如果 $p \equiv -3 \pmod 8$, 则有

$$L(s^\infty) = pq - p, \quad m(x) = \frac{x^{pq}-1}{x^p-1}.$$

## 2 $V_0$ 和 $V_1$ 的性质

由 $V_0$ 和 $V_1$ 的定义可知, $V_0$ 和 $V_1$ 构成了 $\mathbb{Z}_N^*$ 的一个分割, 且 $V_1 = gV_0$. 为了进一步研究 $V_0$ 和 $V_1$ 的性质, 我们需要下面的引理.

**引理 2.1** 设 $m_1 > 0$, $m_2 > 0$, $a_1, a_2$ 是整数. 同余方程组

$$y \equiv a_1 \pmod{m_1}, \quad y \equiv a_2 \pmod{m_2}$$

有解当且仅当

$$\gcd(m_1, m_2) \mid a_1 - a_2.$$

而且当上述条件成立时, 同余方程组在模 $[m_1, m_2]$ 下只有一个解.

**证明** 参阅文献 [7]. 证毕.

**引理 2.2** 对于 $t \in \mathbb{Z}_N^*$, 有

$$tV_0 = V_0, \quad tV_1 = V_1, \quad t \in V_0,$$
$$tV_0 = V_1, \quad tV_1 = V_0, \quad t \in V_1.$$

**证明** 对于 $t \in V_0$, 记 $t = g^{s_t}x^{l_t}$, 其中 $0 \le s_t \le e-1$, $0 \le l_t \le 1$ 且 $2 \mid s_t + l_t$, 则有

$$\begin{aligned} tV_0 &= g^{s_t}x^{l_t}\left\{g^{s_1}x^{l_1} : 0 \le s_1 \le e-1, 0 \le l_1 \le 1, 2 \mid s_1 + l_1\right\} \\ &= \left\{g^{s_1+s_t}x^{l_1+l_t} : 0 \le s_1 \le e-1, 0 \le l_1 \le 1, 2 \mid s_1 + l_1\right\} \\ &= \left\{g^s x^l : 0 \le s \le e-1, 0 \le l \le 1, 2 \mid s + l\right\} = V_0. \end{aligned}$$

注意到 $V_1 = gV_0$, 可得

$$tV_1 = tgV_0 = gtV_0 = gV_0 = V_1.$$

对于 $t \in V_1$, 运用类似的方法可得 $tV_0 = V_1$ 和 $tV_1 = V_0$. 证毕.

**引理 2.3** $2 \in V_0$ 当且仅当 $p \equiv \pm 1 \pmod 8$, $2 \in V_1$ 当且仅当 $p \equiv \pm 3 \pmod 8$.

**证明** 以下只证明 $2 \in V_0$ 当且仅当 $p \equiv \pm 1 \pmod 8$.

设

$$2 \in V_0 = \left\{g^{2s} : 0 \le s \le \frac{e}{2} - 1\right\} \cup \left\{g^{2s+1}x : 0 \le s \le \frac{e}{2} - 1\right\}.$$

如果 $2 \in \{g^{2s} : 0 \le s \le \frac{e}{2} - 1\}$, 则有 $s_0$ 使得 $2 \equiv g^{2s_0} (\mathrm{mod} p)$ 且 $2 \equiv g^{2s_0} \pmod q$ 成立. 由此推出 2 是模 $p$ 和模 $q$ 的二次剩余. 因此

$$p \equiv \pm 1 \pmod 8, \quad q \equiv \pm 1 \pmod 8.$$

如果 $2 \in \{g^{2s+1}x : 0 \le s \le \frac{e}{2}-1\}$, 则有 $s_0$ 使得 $2 \equiv g^{2s_0+2} \pmod p$ 且 $2 \equiv g^{2s_0+1} \pmod q$ 成立. 因此 2 是模 $p$ 的二次剩余, 且是模 $q$ 的二次非剩余. 故 $p \equiv \pm 1 \pmod 8$, $q \equiv \pm 3 \pmod 8$. 这就证明了必要性.

另一方面, 注意到 $g$ 是 $p$ 和 $q$ 的一个公共原根, 则有

$$2 \equiv g^{s_1} \pmod p, \quad 2 \equiv g^{s_2} \pmod q, \quad 0 \le s_1 \le p-2, \quad 0 \le s_2 \le q-2.$$

如果 $p \equiv \pm 1 \pmod 8$ 且 $q \equiv \pm 1 \pmod 8$, 则 $2 \mid s_1, 2 \mid s_2$, 且 $2 \mid s_1 - s_2$. 由引理 2.1 存在整数 $0 \le s \le e-1$ 满足

$$s \equiv s_1 \pmod{p-1}, \quad s \equiv s_2 \pmod{q-1}.$$

因此 $2 \equiv g^s \pmod{pq}$ 且 $2 \mid s$. 由此推出 $2 \in V_0$.

如果 $p \equiv \pm 1 \pmod 8$, $q \equiv \pm 3 \pmod 8$, 则 $2 \mid s_1$, $2 \nmid s_2$, 且 $2 \mid s_1 - s_2 - 1$. 由引理 2.1 存在整数 $0 \le s \le e-1$ 满足

$$s \equiv s_1 - 1 \pmod{p-1}, \quad s \equiv s_2 \pmod{q-1}.$$

由此推出 $2 \equiv g^s x \pmod{pq}$ 且 $2 \nmid s$. 因此 $2 \in V_0$. 这就证明了充分性.

## 3 自相关值

为了证明定理 1.5, 需要下述关于特征和的引理.

**引理 3.1** 设 $r$ 是整数, 则有

$$\sum_{j=0}^{p-1} \left(\frac{j(j+r)}{p}\right) = \begin{cases} p-1, & p \mid r, \\ -1, & p \nmid r, \end{cases}$$

其中 $(\frac{\cdot}{p})$ 表示模 $p$ 的 Legendre 符号.

**证明** 设 $p \mid r$. 易证

$$\sum_{j=0}^{p-1} \left(\frac{j(j+r)}{p}\right) = \sum_{j=0}^{p-1} \left(\frac{j^2}{p}\right) = p-1.$$

而对于 $p \nmid r$ 可得

$$\begin{aligned} \sum_{j=0}^{p-1} \left(\frac{j(j+r)}{p}\right) &= \sum_{j=0}^{p-1} \left(\frac{jr(jr+r)}{p}\right) = \sum_{j=0}^{p-1} \left(\frac{j(j+1)}{p}\right) = \sum_{j=1}^{p-2} \left(\frac{j(j+1)}{p}\right) \\ &= \sum_{j=1}^{p-2} \left(\frac{j^{-1}+1}{p}\right) = \sum_{j=1}^{p-1} \left(\frac{j^{-1}+1}{p}\right) = \sum_{j=1}^{p-1} \left(\frac{j+1}{p}\right) = \sum_{j=2}^{p-1} \left(\frac{j}{p}\right) = -1. \end{aligned}$$

证毕.

**引理 3.2** 设 $1 \le w \le N-1$, 则有

$$\sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ \gcd(i+w,pq)=1}}^{N-1} \left(\frac{i(i+w)}{p}\right) = \begin{cases} (q-2)(p-1), & w \in P, \\ 1-q, & w \in Q, \\ 2-q, & w \in \mathbb{Z}_N^*, \end{cases}$$

$$\sum_{\substack{i=0\\ \gcd(i,pq)=1\\ p|i+w\\ pq\nmid i+w}}^{N-1}\left(\frac{i}{p}\right)=\begin{cases}0, & w\in P,\\ (q-1)\left(\frac{-w}{p}\right), & w\in Q,\\ (q-2)\left(\frac{-w}{p}\right), & w\in\mathbb{Z}_N^*,\end{cases}$$

$$\sum_{\substack{i=1\\ p|i\\ \gcd(i+w,pq)=1}}^{N-1}\left(\frac{i+w}{p}\right)=\begin{cases}0, & w\in P,\\ (q-1)\left(\frac{w}{p}\right), & w\in Q,\\ (q-2)\left(\frac{w}{p}\right), & w\in\mathbb{Z}_N^*,\end{cases}$$

$$\sum_{\substack{i=0\\ \gcd(i,pq)=1\\ q|i+w}}^{N-1}\left(\frac{i}{p}\right)=0,\qquad \sum_{\substack{i=0\\ q|i\\ \gcd(i+w,pq)=1}}^{N-1}\left(\frac{i+w}{p}\right)=0.$$

**证明** 我们仅证明第一个等式, 因为运用相似的方法可得其它等式.

易证

$$\sum_{\substack{i=0\\ \gcd(i,pq)=1\\ \gcd(i+w,pq)=1}}^{N-1}\left(\frac{i(i+w)}{p}\right)=\sum_{\substack{i=0\\ \gcd(i,q)=1\\ \gcd(i+w,q)=1}}^{N-1}\left(\frac{i(i+w)}{p}\right)$$

$$=\sum_{i=0}^{N-1}\left(\frac{i(i+w)}{p}\right)-\sum_{\substack{i=0\\ q|i+w}}^{N-1}\left(\frac{i(i+w)}{p}\right)-\sum_{\substack{i=0\\ q|i}}^{N-1}\left(\frac{i(i+w)}{p}\right)+\sum_{\substack{i=0\\ q|i\\ q|i+w}}^{N-1}\left(\frac{i(i+w)}{p}\right).$$

由引理 3.1 可得

$$\sum_{i=0}^{N-1}\left(\frac{i(i+w)}{p}\right)=\sum_{n=0}^{q-1}\sum_{j=0}^{p-1}\left(\frac{(j+np)(j+np+w)}{p}\right)=q\sum_{j=0}^{p-1}\left(\frac{j(j+w)}{p}\right)$$

$$=\begin{cases}q(p-1), & w\in P,\\ -q, & w\notin P,\end{cases}$$

$$\sum_{\substack{i=0\\ q|i+w}}^{N-1}\left(\frac{i(i+w)}{p}\right)=\sum_{j=0}^{p-1}\left(\frac{(qj-w)qj}{p}\right)=\sum_{j=0}^{p-1}\left(\frac{j(j-w)}{p}\right)=\begin{cases}p-1, & w\in P,\\ -1, & w\notin P,\end{cases}$$

$$\sum_{i=0\ q|i}^{N-1}\left(\frac{i(i+w)}{p}\right)=\sum_{j=0}^{p-1}\left(\frac{qj(qj+w)}{p}\right)=\sum_{j=0}^{p-1}\left(\frac{j(j+w)}{p}\right)=\begin{cases}p-1, & w\in P,\\ -1, & w\notin P,\end{cases}$$

以及

$$\sum_{\substack{i=0\\ q|i\\ q|i+w}}^{N-1}\left(\frac{i(i+w)}{p}\right)=\begin{cases}\sum_{i=0\ q|i}^{N-1}\left(\frac{i(i+w)}{p}\right), & w\in Q,\\ 0, & w\notin Q,\end{cases}$$

$$=\begin{cases}-1, & w\in Q,\\ 0, & w\notin Q.\end{cases}$$

因此

$$\sum_{\substack{i=0\\ \gcd(i,pq)=1\\ \gcd(i+w,pq)=1}}^{N-1}\left(\frac{i(i+w)}{p}\right)=\begin{cases}(q-2)(p-1), & w\in P,\\ 1-q, & w\in Q,\\ 2-q, & w\in \mathbb{Z}_N^*.\end{cases}$$

证毕.

类似地, 可得如下结果.

**引理 3.3** 设 $1\le w\le N-1$, 则有

$$\sum_{\substack{i=0\\ q\mid i\\ q\mid i+w}}^{N-1}1=\begin{cases}p, & w\in Q,\\ 0, & w\notin Q,\end{cases}\qquad \sum_{\substack{i=1\\ p\mid i\\ q\mid i+w}}^{N-1}1=\begin{cases}0, & w\in Q,\\ 1, & w\notin Q,\end{cases}$$

$$\sum_{\substack{i=0\\ q\mid i\\ p\mid i+w\\ pq\nmid i+w}}^{N-1}1=\begin{cases}0, & w\in Q,\\ 1, & w\notin Q,\end{cases}\qquad \sum_{\substack{i=1\\ p\mid i\\ p\mid i+w\\ pq\nmid i+w}}^{N-1}1=\begin{cases}q-2, & w\in P,\\ 0, & w\notin P.\end{cases}$$

现在证明定理 1.5. 设 $\gcd(n,N)=1$. 由 $V_0$ 的定义可得

$$\begin{aligned}n\in V_0 &\Longleftrightarrow \text{存在 } 0\le s\le e-1,\ 0\le l\le 1,\ 2\mid s+l \text{ 满足 } n\equiv g^sx^l \pmod N\\ &\Longleftrightarrow \frac{1}{\phi(N)}\sum_{\substack{s=0\\ 2\mid s+l}}^{e-1}\sum_{l=0}^{1}\sum_{\chi \bmod N}\chi(n)\overline{\chi}(g^sx^l)=1\\ &\Longleftrightarrow \frac{1}{\phi(N)}\sum_{s=0}^{\frac{e}{2}-1}\sum_{l=0}^{1}\sum_{\chi \bmod N}\chi(n)\overline{\chi}(g^{2s+l}x^l)=1.\end{aligned}$$

不难证明

$$\sum_{s=0}^{\frac{e}{2}-1}\overline{\chi}(g^{2s})=\begin{cases}0, & \text{如果 } \chi(g^2)\ne 1,\\ \dfrac{e}{2}, & \text{如果 } \chi(g^2)=1.\end{cases}$$

因此

$$n\in V_0\Longleftrightarrow \frac{1}{4}\sum_{\substack{\chi \bmod N\\ \chi^2(g)=1}}\sum_{l=0}^{1}\overline{\chi}(g^lx^l)\chi(n)=1. \tag{3.1}$$

设 $\mathrm{ind}_{g,p}(n)$ 表示以 $g$ 为底的 $n$ 对模 $p$ 的指标, 满足 $n\equiv g^{\mathrm{ind}_{g,p}(n)} \pmod p$, $0\le \mathrm{ind}_{g,p}(n)\le p-2$, 且 $\mathrm{ind}_{g,q}(n)$ 表示以 $g$ 为底的 $n$ 对模 $q$ 的指标, 满足 $n\equiv g^{\mathrm{ind}_{g,q}(n)} \pmod q$, $0\le \mathrm{ind}_{g,q}(n)\le q-2$. 记 $\chi=\chi_1\chi_2$, 其中 $\chi_1$ 是模 $p$ 的一个特征, $\chi_2$ 是模 $q$ 的一个特征. 设

$$\chi_1(n)=\begin{cases}e\left(\dfrac{m_1\mathrm{ind}_{g,p}(n)}{p-1}\right), & \text{如果 } \gcd(n,p)=1,\\ 0, & \text{如果 } \gcd(n,p)>1,\end{cases}$$

$$\chi_2(n)=\begin{cases}e\left(\dfrac{m_2\mathrm{ind}_{g,q}(n)}{q-1}\right), & \text{如果 } \gcd(n,q)=1,\\ 0, & \text{如果 } \gcd(n,q)>1,\end{cases}$$

其中 $1 \le m_1 \le p-1$, $1 \le m_2 \le q-1$, 且 $e(y) = \mathrm{e}^{2\pi \mathrm{i} y}$, 则有

$$\begin{aligned}\chi^2(g) = 1 &\Longleftrightarrow e\left(\frac{2m_1}{p-1}\right) e\left(\frac{2m_2}{q-1}\right) = 1\\ &\Longleftrightarrow e\left(\frac{2m_1(q-1)+2m_2(p-1)}{(p-1)(q-1)}\right) = 1\\ &\Longleftrightarrow (p-1)(q-1) \mid 2m_1(q-1)+2m_2(p-1)\\ &\Longleftrightarrow \frac{(p-1)(q-1)}{4}\Big| m_1\frac{q-1}{2} + m_2\frac{p-1}{2}.\end{aligned}$$

因此

$$\frac{p-1}{2}\Big| m_1, \quad \frac{q-1}{2}\Big| m_2.$$

记

$$m_1 = \frac{p-1}{2}\cdot n_1, \quad m_2 = \frac{q-1}{2}\cdot n_2,$$

则有

$$\chi_1(n) = \begin{cases} e\left(\dfrac{n_1 \mathrm{ind}_{g,p}(n)}{2}\right), & \text{如果 } \gcd(n,p)=1,\\ 0, & \text{如果 } \gcd(n,p)>1,\end{cases}$$

$$\chi_2(n) = \begin{cases} e\left(\dfrac{n_2 \mathrm{ind}_{g,q}(n)}{2}\right), & \text{如果 } \gcd(n,q)=1,\\ 0, & \text{如果 } \gcd(n,q)>1,\end{cases}$$

其中 $1 \le n_1 \le 2$, $1 \le n_2 \le 2$. 因此

$$\begin{aligned}\sum_{l=0}^{1} \overline{\chi}(g^l x^l) &= \sum_{l=0}^{1} \overline{\chi}_1(g^{2l})\overline{\chi}_2(g^l) = \sum_{l=0}^{1} e\left(-\frac{l n_2}{2}\right)\\ &= \begin{cases} 2, & \text{如果 } 2 \mid n_2,\\ 0, & \text{如果 } 2 \nmid n_2.\end{cases}\\ &= \begin{cases} 2, & \text{如果 } \chi_2 = \chi_0,\\ 0, & \text{如果 } \chi_2 \ne \chi_0.\end{cases}\end{aligned} \tag{3.2}$$

结合 (3.1) 和 (3.2) 立即可得

$$n \in V_0 \Longleftrightarrow \frac{1}{2}\sum_{\substack{\chi \bmod p\\ \chi^2=\chi_0}} \chi(n) = 1 \Longleftrightarrow \frac{1}{2}\left(1+\left(\frac{n}{p}\right)\right) = 1, \tag{3.3}$$

其中 $(\frac{\cdot}{p})$ 表示模 $p$ 的 Legendre 符号. 则对于

$$0 \le n \le N-1,$$

由 $s^\infty$ 的定义可得

$$(-1)^{s_n} = \begin{cases} \left(\dfrac{n}{p}\right), & \gcd(n,pq)=1,\\ 1, & q \mid n,\\ -1, & p \mid n, n>0.\end{cases} \tag{3.4}$$

设 $1 \le w \le N-1$, 有

$$\begin{aligned} C_s(w) &= \sum_{i=0}^{N-1} (-1)^{s_{i+w}+s_i} \\ &= \sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ \gcd(i+w,pq)=1}}^{N-1} \left(\frac{i(i+w)}{p}\right) + \sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ q|i+w}}^{N-1} \left(\frac{i}{p}\right) - \sum_{\substack{i=0 \\ \gcd(i,pq)=1 \\ p|i+w \\ pq\nmid i+w}}^{N-1} \left(\frac{i}{p}\right) \\ &\quad + \sum_{\substack{i=0 \\ q|i \\ \gcd(i+w,pq)=1}}^{N-1} \left(\frac{i+w}{p}\right) + \sum_{\substack{i=0 \\ q|i \\ q|i+w}}^{N-1} 1 - \sum_{\substack{i=0 \\ q|i \\ p|i+w \\ pq\nmid i+w}}^{N-1} 1 \\ &\quad - \sum_{\substack{i=1 \\ p|i \\ \gcd(i+w,pq)=1}}^{N-1} \left(\frac{i+w}{p}\right) - \sum_{\substack{i=1 \\ p|i \\ q|i+w}}^{N-1} 1 + \sum_{\substack{i=1 \\ p|i \\ p|i+w \\ pq\nmid i+w}}^{N-1} 1, \end{aligned} \tag{3.5}$$

则由引理 3.2 和 3.3 立即可得

$$C_s(w) = \begin{cases} pq-2p-2, & \text{如果 } w \in P, \\ 1+p-q-(q-1)\left(\dfrac{w}{p}\right)((-1)^{\frac{p-1}{2}}+1), & \text{如果 } w \in Q, \\ -q-(q-2)\left(\dfrac{w}{p}\right)((-1)^{\frac{p-1}{2}}+1), & \text{如果 } w \in \mathbb{Z}_N^*. \end{cases}$$

这就证明了定理 1.5.

## 4 线性复杂度

设

$$s(x) = s_0 + s_1 x + \cdots + s_{pq-1}x^{pq-1} = \sum_{i \in C_1} x^i, \tag{4.1}$$

且 $\alpha$ 是有限域 $\mathbb{F}_{2^m}$ 的一个 $pq$ 次本原单位根, 其中 $m = \mathrm{ord}_{pq}(2)$. 根据 Blahut 定理, 序列 $s^\infty$ 的线性复杂度为

$$L(s^\infty) = pq - \left|\left\{t : s(\alpha^t) = 0,\ 0 \le t < pq\right\}\right|. \tag{4.2}$$

**引理 4.1** 设 $s(x), \alpha$ 定义如上, 则对于 $0 \le t \le N-1$ 有

$$s(\alpha^t) = \begin{cases} s(\alpha), & \text{如果 } t \in V_0, \\ s(\alpha)+1, & \text{如果 } t \in V_1, \\ 1+\left(\dfrac{p-1}{2} \bmod 2\right), & \text{如果 } t \in P, \\ 0, & \text{如果 } t \in \{0\} \cup Q. \end{cases}$$

**证明** 设 $t\in V_0$, 则由引理 2.2 可得

$$s(\alpha^t)=\sum_{i\in P}\alpha^{ti}+\sum_{i\in V_1}\alpha^{ti}=\sum_{j\in tP}\alpha^{j}+\sum_{j\in tV_1}\alpha^{j}=\sum_{i\in P}\alpha^{i}+\sum_{i\in V_1}\alpha^{i}=s(\alpha).$$

对于 $t\in V_1$, 注意到

$$\begin{aligned}0&=\alpha^{pq}-1=(\alpha-1)(1+\alpha+\cdots+\alpha^{pq-1})\\&=(\alpha-1)\bigg(1+\sum_{i\in V_0}\alpha^{i}+\sum_{i\in V_1}\alpha^{i}+\sum_{i\in P}\alpha^{i}+\sum_{i\in Q}\alpha^{i}\bigg),\end{aligned}$$

则由引理 2.2 可得

$$\begin{aligned}s(\alpha^t)&=\sum_{i\in P}\alpha^{ti}+\sum_{i\in V_1}\alpha^{ti}=\sum_{j\in tP}\alpha^{j}+\sum_{j\in tV_1}\alpha^{j}=\sum_{i\in P}\alpha^{i}+\sum_{i\in V_0}\alpha^{i}\\&=\sum_{i\in P}\alpha^{i}+\sum_{i\in Q}\alpha^{i}+s(\alpha)+1=s(\alpha)+1.\end{aligned}$$

设 $t\in P$. 由 $x$ 和 $V_1$ 的定义可得

$$\begin{aligned}V_1 \bmod q&=\left\{g^sx^l \bmod q:0\le s\le e-1,0\le l\le 1,2\nmid s+l\right\}\\&=\left\{g^{2s}x \bmod q:0\le s\le \frac{e}{2}-1\right\}\cup\left\{g^{2s+1} \bmod q:0\le s\le \frac{e}{2}-1\right\}\\&=\left\{g^{2s} \bmod q:0\le s\le \frac{e}{2}-1\right\}\cup\left\{g^{2s+1} \bmod q:0\le s\le \frac{e}{2}-1\right\}\\&=\left\{g^{s} \bmod q:0\le s\le e-1\right\}=\left\{1,2,\ldots,q-1\right\}.\end{aligned}$$

当 $s$ 取遍 $\{0,1,\ldots,e-1\}$, $l$ 取遍 $\{0,1\}$, 且 $2\nmid s+l$ 时, $V_1 \bmod q$ 取集合 $\{1,2,\ldots,q-1\}$ 中每个元素 $\frac{p-1}{2}$ 次, 则有

$$\begin{aligned}s(\alpha^t)&=\sum_{i\in P}\alpha^{ti}+\sum_{i\in V_1}\alpha^{ti}=\sum_{i\in P}\alpha^{i}+\left(\frac{p-1}{2} \bmod 2\right)\sum_{i\in P}\alpha^{i}\\&=1+\left(\frac{p-1}{2} \bmod 2\right).\end{aligned}$$

设 $t\in Q$. 由 $x$ 和 $V_1$ 的定义可得

$$\begin{aligned}V_1 \bmod p&=\left\{g^sx^l \bmod p:0\le s\le e-1,0\le l\le 1,2\nmid s+l\right\}\\&=\left\{g^{2s}x \bmod p:0\le s\le \frac{e}{2}-1\right\}\cup\left\{g^{2s+1} \bmod p:0\le s\le \frac{e}{2}-1\right\}\\&=\left\{g^{2s+1} \bmod p:0\le s\le \frac{e}{2}-1\right\}\\&=\left\{g,g^3,\ldots,g^{p-2}\right\}.\end{aligned}$$

当 $s$ 取遍 $\{0,1,\ldots,e-1\}$, $l$ 取遍 $\{0,1\}$, 且 $2\nmid s+l$ 时, $V_1 \bmod p$ 取集合 $\left\{g,g^3,\ldots,g^{p-2}\right\}$ 中每个元素 $(q-1)$ 次, 则有

$$\begin{aligned}s(\alpha^t)&=\sum_{i\in P}\alpha^{ti}+\sum_{i\in V_1}\alpha^{ti}\\&=((q-1) \bmod 2)+((q-1) \bmod 2)\times\sum_{i\in\{g,g^3,\ldots,g^{p-2}\}}\alpha^{ti}=0.\end{aligned}$$

此外

$$s(1)=\left(q-1+\frac{(p-1)(q-1)}{2}\right) \bmod 2=0.$$

这就证明了引理 4.1. 证毕.

**引理 4.2** $2\in V_0$ 当且仅当 $s(\alpha)\in\{0,1\}$.

**证明** 注意到有限域 $\mathbb{F}_{2^m}$ 的特征为 2, 因此 $s(\alpha)^2=s(\alpha^2)$. 设 $2\in V_0$, 则由引理 2.2 可得 $2V_i=V_i$, $i=0,1$. 因此

$$s(\alpha)^2=s(\alpha^2)=\sum_{i\in P}\alpha^{2i}+\sum_{i\in V_1}\alpha^{2i}=\sum_{i\in P}\alpha^i+\sum_{i\in V_1}\alpha^i=s(\alpha).$$

由此可得 $s(\alpha)\in\{0,1\}$.

设 $2\in V_1$, 则由引理 4.1 可得

$$s(\alpha^2)=s(\alpha)+1.$$

因此 $s(\alpha)^2=s(\alpha)+1$, 且 $s(\alpha)\notin\{0,1\}$. 注意到 $2\in V_0\cup V_1$, 这就证明了引理 4.2. 证毕.

现在证明定理 1.6. 设 $\alpha$ 定义如上, 则 $\alpha^p$ 是 $x^q-1$ 的一个 $q$ 次本原单位根, $\alpha^q$ 是 $x^p-1$ 的一个 $p$ 次本原单位根. 可得

$$x^p-1=\prod_{i\in\{0\}\cup Q}(x-\alpha^i),\quad x^q-1=\prod_{i\in\{0\}\cup P}(x-\alpha^i).$$

设 $d_i(x)=\prod_{j\in V_i}(x-\alpha^j)$, $i=0,1$. 易证

$$x^N-1=(x-1)(x-\alpha)\cdots(x-\alpha^{N-1})=\frac{(x^p-1)(x^q-1)d_0(x)d_1(x)}{(x-1)}.$$

**情形 I** 设 $p\equiv 1 \pmod 8$. 由引理 2.3, 4.1, 4.2 以及选取合适的 $\alpha$, 可得

$$s(\alpha^t)=\begin{cases}1, & \text{如果 } t\in P\cup V_1,\\ 0, & \text{如果 } t\in\{0\}\cup Q\cup V_0.\end{cases}$$

由此可知

$$L(s^\infty)=pq-p-\frac{(p-1)(q-1)}{2}=\frac{pq+q-p-1}{2},\quad m(x)=\frac{x^{pq}-1}{(x^p-1)d_0(x)}.$$

**情形 II** 设 $p\equiv -1 \pmod 8$. 由引理 2.3, 4.1, 4.2 以及选取合适的 $\alpha$, 可得

$$s(\alpha^t)=\begin{cases}1, & \text{如果 } t\in V_1,\\ 0, & \text{如果 } t\notin V_1.\end{cases}$$

由此可得

$$L(s^\infty)=\frac{(p-1)(q-1)}{2},\quad m(x)=\frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)d_0(x)}.$$

**情形 III** 设 $p\equiv 3 \pmod 8$. 由引理 2.3, 4.1, 4.2 可得

$$s(\alpha^t)=\begin{cases}0, & \text{如果 } t\in\{0\}\cup P\cup Q,\\ \neq 0, & \text{如果 } t\in V_0\cup V_1.\end{cases}$$

因此

$$L(s^\infty)=pq-p-q+1,\quad m(x)=\frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)}.$$

**情形 IV** 设 $p \equiv -3 \pmod 8$. 由引理 2.3, 4.1, 4.2 可得

$$s(\alpha^t) = \begin{cases} 0, & \text{如果 } t \in \{0\} \cup Q, \\ \neq 0, & \text{如果 } t \notin \{0\} \cup Q. \end{cases}$$

从而

$$L(s^\infty) = pq - p, \quad m(x) = \frac{x^{pq}-1}{x^p - 1}.$$

这就证明了定理 1.6.

## 5 结论

本文基于丁存生在文 [5] 中提出的割圆类 $(V_0, V_1)$, 构造了新的周期为 $pq$ 的 2 阶二元广义割圆序列 $s^\infty$, 并研究其性质: 自相关值、线性复杂度和极小多项式. 该序列在一个周期内取值为 0 的个数为 $\frac{pq+p-q+1}{2}$, 取值为 1 的个数为 $\frac{pq+q-p-1}{2}$. 定理 1.5 表明新序列 $s^\infty$ 的自相关值是多值的. 定理 1.6 表明 $s^\infty$ 的线性复杂度取值为 $(pq+q-p-1)/2$, $(p-1)(q-1)/2$, $pq-p-q+1$, $pq-p$, 这仅取决于 $p \pmod 8$ 的值. 因此当 $p \equiv 1, \pm 3 \pmod 8$ 且 $p < q$ 时, $L(s^\infty) > \frac{pq}{2}$, 序列 $s^\infty$ 具有 "好" 的线性复杂度. 定理 1.6 也表明新序列 $s^\infty$ 与文献 [3] 中广义割圆序列的线性复杂度在某些方面具有相似性, 但本文的条件更简单.

## 参 考 文 献


[1] Bai E., Fu X., Xiao G., On the linear complexity of generalized cyclotomic sequences of order four over $Z_{pq}$, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2005, **E88-A**(1): 392–395.

[2] Bai E., Liu X., Xiao G., Linear complexity of new generalized cyclotomic sequences of order two of length $pq$, *IEEE Transactions on Information Theory*, 2005, **51**(5): 1849–1853.

[3] Ding C., Linear complexity of generalized cyclotomic binary sequences of order 2, *Finite Fields and Their Applications*, 1997, **3**(2): 159–174.

[4] Ding C., Autocorrelation values of generalized cyclotomic sequences of order two, *IEEE Transactions on Information Theory*, 1998, **44**(4): 1699–1702.

[5] Ding C., Cyclotomic constructions of cyclic codes with length being the product of two primes, *IEEE Transactions on Information Theory*, 2012, **58**(4): 2231–2236.

[6] Ding C., Helleseth T., New generalized cyclotomy and its applications, *Finite Fields and Their Applications*, 1998, **4**(2): 140–166.

[7] Ding C., Pei D., Salomaa A., Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography, World Scientific, Singapore, 1996.

[8] Hu L., Yue Q., Autocorrelation value of Whiteman generalized cyclotomic sequence, *Journal of Mathematical Research with Applications*, 2012, **32**(4): 415–422.

[9] Hu L., Yue Q., Wang M., The linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$, *IEEE Transactions on Information Theory*, 2012, **58**(8): 5534–5543.

[10] Li S., Chen Z., Sun R., et al., On the randomness of generalized cyclotomic sequences of order two and length $pq$, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2007, **E90-A**(9): 2037–2041.

[11] Whiteman A. L., A family of difference sets, *Illinois Journal of Mathematics*, 1962, **6**(2): 107–121.

[12] Yan T., Du X., Xiao G., et al., Linear complexity of binary Whiteman generalized cyclotomic sequences of order $2^k$, *Information Sciences*, 2009, **179**(7): 1019–1023.