

一类长度为 $2p^2$ 的二元序列的 2-Adic 复杂度研究*

柯品惠^{1,2}, 卢栎羽¹, 陈智雄³

1. 福建师范大学 数学与统计学院, 福州 350117
2. 福建省应用数学中心 (福建师范大学), 福州 350117
3. 莆田学院 应用数学福建省高校重点实验室, 莆田 351100

通信作者: 陈智雄, E-mail: ptczx@126.com

摘要: 伪随机序列的 2-adic 复杂度表示带进位反馈移位寄存器生成该序列的最短级数, 它表明了该序列抵抗有理逼近攻击的能力. 基于 Xiong 等人给出的研究方法, 分析了一类长度为 $2p^2$ 的广义割圆序列的 2-adic 复杂度. 利用中国剩余定理和 \mathbb{Z}_p 上的“高斯周期”得到了 \mathbb{Z}_{2p^2} 上的“高斯周期”. 证明了上述序列的 2-adic 复杂度在许多情况下可以达到最大值.

关键词: 伪随机序列; 2-adic 复杂度; 高斯周期

中图分类号: TP309.7 文献标识码: A DOI: 10.13868/j.cnki.jcr.000458

中文引用格式: 柯品惠, 卢栎羽, 陈智雄. 一类长度为 $2p^2$ 的二元序列的 2-Adic 复杂度研究[J]. 密码学报, 2021, 8(4): 560–571. [DOI: 10.13868/j.cnki.jcr.000458]

英文引用格式: KE P H, LU L Y, CHEN Z X. 2-adic complexity of a class of binary sequences of length $2p^2$ [J]. Journal of Cryptologic Research, 2021, 8(4): 560–571. [DOI: 10.13868/j.cnki.jcr.000458]

2-Adic Complexity of a Class of Binary Sequences of Length $2p^2$

KE Pin-Hui^{1,2}, LU Li-Yu¹, CHEN Zhi-Xiong³

1. School of Mathematics and Statistics, Fujian Normal University, Fuzhou 350117, China
2. Center for Applied Mathematics of Fujian Province (FJNU), Fuzhou 350117, China
3. Provincial Key Laboratory of Applied Mathematics, Putian University, Putian 351100, China

Corresponding author: CHEN Zhi-Xiong, E-mail: ptczx@126.com

Abstract: The 2-adic complexity of a sequence, which indicates the ability of the sequence to resist the rational approximation attack, is defined to be the shortest length of feedback-with-carry shift registers that can generate the sequence. By using a method introduced by Xiong et al., the 2-adic complexity of a class of generalized cyclotomic sequences of length $2p^2$ is analyzed. Based on that, the “Gauss periods” over \mathbb{Z}_{2p^2} can be computed by using the Chinese Remainder Theorem and the well known “Gauss periods” over \mathbb{Z}_p . It is proved that in many cases, the 2-adic complexity of the aforementioned sequences reaches the maximum value.

Key words: pseudo-random sequences; 2-adic complexity; Gauss periods

* 基金项目: 国家自然科学基金 (61772292, 61772476); 福建省自然科学基金 (2019J01273, 2020J01905)

Foundation: National Natural Science Foundation of China (61772292, 61772476); Natural Science Foundation of Fujian Province (2019J01273, 2020J01905)

收稿日期: 2020-09-08 定稿日期: 2021-03-18

1 引言

伪随机序列在通信和密码学等领域具有广泛的应用^[1]. 理论上, 每个二元序列都可以由线性反馈移位寄存器 (LFSR) 或带进位反馈移位寄存器 (FSCR) 产生. Berlekamp-Massey 算法 (BMA)^[2] 和有理逼近算法 (RAA)^[3] 是目前较为有效的两种攻击算法, 如果已知一定长度的二元序列, 那么可利用上述两种算法来恢复完整的二元序列. 线性复杂度和 2-adic 复杂度是抵御 BMA 和 RAA 攻击的两个重要安全准则. 由 BMA 和 RAA 攻击方式可知, 序列的线性复杂度和 2-adic 复杂度都不应小于该序列周期的一半. 目前, 许多分圆序列和广义分圆序列已被证明具有较高的线性复杂度^[4-7]. 然而, 对于序列的 2-adic 复杂度, 仅有少数几类序列的 2-adic 复杂度是已知的. 因此, 分析已有序列的 2-adic 复杂度以及设计具有高 2-adic 复杂度的伪随机序列成为近年研究的热点.

迄今为止, 计算二元序列的 2-adic 复杂度主要有三种方法. 第一种方法是 Xiong 等^[8] 提出的计算序列的循环矩阵的行列式和两个整数的最大公约数. 在文献 [8] 中, Xiong 等证明了所有具有理想自相关值的序列都具有最大的 2-adic 复杂度. 之后, Xiao 等^[9] 利用相同的方法证明了两类广义分圆二元序列的 2-adic 复杂度可达到最大值. 第二种方法是 Hu^[10] 提出的利用序列的自相关分布来分析二元序列的 2-adic 复杂度. 基于文献 [10] 的研究方法, Sun 等分别给出了文献 [11] 和文献 [12] 中两类二元序列的 2-adic 复杂度的下界, 并且得到了文献 [13] 中 Ding-Helleseth-Lam 序列的 2-adic 复杂度的上下界. 最近, Hofer 和 Winterhof^[14] 用文献 [10] 的方法证明了二素数生成器 (two-prime generator) 的 2-adic 复杂度接近于它的周期. 最后一种方法是直接计算序列的 2-adic 复杂度. 例如, Zhang 等^[15] 利用有限域 \mathbb{F}_q 和 \mathbb{Z}_{2^N-1} 上的“高斯周期”和“二次高斯和”确定了 Ding-Helleseth-Martinsen 序列的 2-adic 复杂度. Yang 等^[16] 推广了文献 [13] 中给出的结果, 并确定了一类二元序列的 2-adic 复杂度的精确值.

最近, Zhang 等^[17] 构造了一类长度为 $2p^2$ 的二元广义分圆序列, 证明了此类二元序列具有较大的线性复杂度. 基于文献 [8] 给出的方法, 本文研究了此类二元广义分圆序列的 2-adic 复杂度. 我们证明了此类序列的 2-adic 复杂度不小于其周期的一半, 并且该序列的 2-adic 复杂度在一些情形下也可以达到最大值.

本文其余部分组织如下. 第 2 节, 给出本文所需的相关概念与知识, 以及一些必要的结果. 第 3 节, 首先, 利用中国剩余定理和 \mathbb{Z}_p 上的“高斯周期”得到了 \mathbb{Z}_{2p^2} 上的“高斯周期”; 然后, 证明了一类长度为 $2p^2$ 的二元序列的 2-adic 复杂度在一些情形下可以达到最大值. 第 4 节对本文工作进行总结.

2 基础知识

令 p 为奇素数. 设 2 为模 p^2 的本原根, 当 $k \geq 1$ 时, 则 2 也是模 p^k 的本原根^[18]. 由于 $2 + p^k$ 为奇数, 则 $2 + p^k$ 为模 $2p^k$ 的本原根^[19]. 设 $g = 2 + p^2$, 则 g 是模 $p, 2p, p^2$ 和 $2p^2$ 的公共本原根.

定义

$$\begin{aligned} D_0^{(p^j)} &= \langle g^2 \rangle \bmod p^j, \\ D_0^{(2p^j)} &= \langle g^2 \rangle \bmod 2p^j, \\ D_1^{(p^j)} &= gD_0^{(p^j)} \bmod p^j, \\ D_1^{(2p^j)} &= gD_0^{(2p^j)} \bmod 2p^j. \end{aligned}$$

这里 $j = 1, 2$, $D_0^{(n)}$ 和 $D_1^{(n)}$ 分别定义为与 n 相关的二阶广义分圆类. \mathbb{Z}_n^* 表示与 n 互素的剩余类集, 则有

$$\mathbb{Z}_{2p^j}^* = D_0^{(2p^j)} \cup D_1^{(2p^j)}, \quad Z_{p^j}^* = D_0^{(p^j)} \cup D_1^{(p^j)},$$

和

$$\mathbb{Z}_{2p^2} = \bigcup_{k=0}^1 \bigcup_{j=1}^2 (p^{2-j} D_k^{(2p^j)} \cup 2p^{2-j} D_k^{(p^j)}) \cup \{0, p^2\}.$$

定义

$$C_0 = D_0^{(2p^2)} \cup 2D_0^{(p^2)} \cup pD_0^{(2p)} \cup 2pD_0^{(p)} \cup \{p^2\},$$

和

$$C_1 = D_1^{(2p^2)} \cup 2D_1^{(p^2)} \cup pD_1^{(2p)} \cup 2pD_1^{(p)} \cup \{0\},$$

则 $C_0 \cup C_1 = \mathbb{Z}_{2p^2}$, $C_0 \cap C_1 = \emptyset$, 这里 \emptyset 表示空集. Zhang^[17] 等研究了一类长度为 $2p^2$ 的二阶广义分圆序列 $\{s_i\}$:

$$s_i = \begin{cases} 1, & \text{若 } i \bmod 2p^2 \in C_1; \\ 0, & \text{若 } i \bmod 2p^2 \in C_0. \end{cases} \quad (1)$$

下面介绍一些重要的引理, 本文主要结果的证明将会多次用到它们.

引理 1 设 $t \in D_k^{(n)}$, 则对于任意的 $k, i \in \mathbb{Z}_2$, 有 $tD_i^{(n)} = D_{i+k}^{(n)}$.

引理 2 $2 \in D_i^{(p^2)}$ 当且仅当 $2 \in D_i^{(p)}$, 这里 $i = 0, 1$. 此外, $2 \in D_0^{(p)}$ 当且仅当 $p \equiv \pm 1 \pmod{8}$, $2 \in D_1^{(p)}$ 当且仅当 $p \equiv \pm 3 \pmod{8}$.

引理 3 设 $D_0^{(n)}$ 为 \mathbb{Z}_n^* 上的子群, 且 $|D_0^{(n)}| = \frac{\phi(n)}{2}$, 这里 $\phi(\cdot)$ 为欧拉函数. 此外, $D_0^{(n)}$ 和 $D_1^{(n)}$ 形成 \mathbb{Z}_n^* 的一个划分.

引理 4 设 $d > 1$ 为正整数, 且 $d|n$, 则 $g \in D_1^{(n)}$ 且 $g \bmod d \in D_1^{(d)}$.

上述引理 1–4 的证明, 请参见文献 [20].

引理 5 令 p 为奇素数, 则有 $\gcd(p, 2^{p^2} - 1) = 1$.

证明: 由费马小定理, 可得 $2^p \equiv 2 \pmod{p}$. 于是, 有 $2^{p^2} \equiv (2^p)^p \equiv 2^p \equiv 2 \pmod{p}$, 即 $2^{p^2} - 1 \equiv 1 \pmod{p}$. 所以 $\gcd(p, 2^{p^2} - 1) = 1$. \square

引理 6 (i) 令 p 为奇素数, 则有 $\gcd(p - 1, 2^{p^2} - 1) = 1$; (ii) 令 p 为奇素数且 $p \not\equiv 1 \pmod{3}$, 则有 $\gcd(p - 1, 2^{p^2} + 1) = 1$.

证明: (i) 设 r 为 $2^{p^2} - 1$ 的素因子, $\text{ord}_r 2$ 为 2 模 r 的乘法阶, 则有 $2^{p^2} \equiv 1 \pmod{r}$ 和 $\text{ord}_r 2 | p^2$. 又 p 为奇素数且 $\text{ord}_r 2 \neq 1$. 因此, $\text{ord}_r 2 = p$ 或 $\text{ord}_r 2 = p^2$. 此外, 因为 r 为素数, 故 $\text{ord}_r 2 | (r - 1)$. 于是, $r - 1$ 是 p 的偶数倍, $2^{p^2} - 1$ 的每个因子必须具有 $2kp + 1$ 的形式. 因此, $\gcd(p - 1, 2^{p^2} - 1) = 1$.

(ii) 设 r 为 $2^{p^2} + 1$ 的素因子, 有 $2^{p^2} \equiv -1 \pmod{r}$, 则 $2^{2p^2} \equiv 1 \pmod{r}$. 令 $\text{ord}_r 2$ 为 2 模 r 的乘法阶, 由于 $2^{p^2} \equiv -1 \pmod{r}$, 则 $\text{ord}_r 2 = 2, 2p$ 或 $\text{ord}_r 2 = 2p^2$. 若 $\text{ord}_r 2 = 2$, 则 $r = 3$. 由假设可知, $r = 3$ 不可能为 $p - 1$ 的一个因子. 对于剩余的 $\text{ord}_r 2 = 2p$ 或 $2p^2$ 的情形, 正如我们在 (i) 中所述, 可以类似证明 r 不可能是 $p - 1$ 的因子. \square

引理 7 设 $p > 3$ 为奇素数,

(i) 若 $p \equiv -3 \pmod{8}$ 且 $p \not\equiv 5 \pmod{24}$, 或者 $p \equiv 3 \pmod{8}$, 则 $\gcd(p^2 + p + 1, 2^{p^2} - 1) = 1$;

(ii) 若 $p \equiv \pm 3 \pmod{8}$, 则 $\gcd(p^2 + p + 1, 2^{p^2} + 1) = 1$ or 3.

证明: (i) 证明的前半部分类似于文献 [9] 中的引理 9, 这里讨论了 $p \equiv \pm 1 \pmod{4}$ 的情形. 但是, 这两个证明的后半部分是有区别的, 为此我们提供了较为完整的证明. 由引理 4 的证明可知, 对于一些正整数 k , $2p^2 - 1$ 的每个素因子必须具有 $2kp + 1$ 的形式. 如果 $2kp + 1$ 也是 $p^2 + p + 1$ 的素因子, 那么存在一个正整数 s 使得 $p^2 + p + 1 = s(2kp + 1)$. 记 $p^2 + p + 1 \equiv 1 \pmod{p}$ 和 $2kp + 1 \equiv 1 \pmod{p}$. 所以, 可得 $s \equiv 1 \pmod{p}$ 和 $s = \frac{p^2 + p + 1}{2kp + 1} < p + 1$. 因此, $s = 1$ 和 $\gcd(p^2 + p + 1, 2^{p^2} - 1) = 1$ 或 $p^2 + p + 1$.

假设 $r = p^2 + p + 1$ 是 $2^{p^2} - 1$ 的一个素因子. 那么, $2^{p^2} \equiv 1 \pmod{r}$. 若 $p \equiv 3 \pmod{8}$, 则 $r = p^2 + p + 1 \equiv 5 \pmod{8}$, 进而 2 是模 r 的非二次剩余, 即勒让德符号 (二次特征) 为 $(\frac{2}{r}) = -1$. 因此, $(\frac{2^{p^2}}{r}) = -1$, 这与假设 $2^{p^2} \equiv 1 \pmod{r}$ 相矛盾. 于是, 有 $\gcd(p^2 + p + 1, 2^{p^2} - 1) = 1$. 若 $p \equiv -3 \pmod{8}$, 则 p 为大于 3 的素数, 这表明 $p \not\equiv 0 \pmod{3}$. 若 $p \equiv 1 \pmod{3}$, 则素数 $r = p^2 + p + 1 \equiv 0 \pmod{3}$, 这显然

是不成立的. 上述分析表明了 $p \equiv 2 \pmod{3}$. 因此, 由中国剩余定理 $p \equiv 5 \pmod{24}$, 这与 $p \not\equiv 5 \pmod{24}$ 相矛盾. 于是, 假设 $r = p^2 + p + 1$ 是 $2^{p^2} - 1$ 的一个素因子是不成立的. 所以, $\gcd(p^2 + p + 1, 2^{p^2} - 1) = 1$.

(ii) 令 r 为 $2^{p^2} + 1$ 的一个素因子, 由引理 6 的证明, 有 $\text{ord}_r 2 = 2, 2p$ 或 $2p^2$. 如果 $\text{ord}_r 2 = 2$, 那么 $r = 3$. 对其余两种情形, 由于 $r - 1$ 是 p 的偶数倍, 意味着 $2^{p^2} + 1$ 的每个因子必须具有 $2kp + 1$ 的形式. 类似 (i) 的证明, 可得 $\gcd(p^2 + p + 1, 2^{p^2} - 1) = 1, 3$ 或 $p^2 + p + 1$.

假设 $r = p^2 + p + 1$ 是 $2^{p^2} + 1$ 的一个素因子, 那么 $2^{p^2} \equiv -1 \pmod{r}$. 若 $p \equiv 3 \pmod{8}$, 则 $r = p^2 + p + 1 \equiv 5 \pmod{8}$, 那么 2 是模 r 的非二次剩余, 即勒让德符号 (二次特征) 为 $(\frac{2}{r}) = -1$. 因此, $(\frac{2^{p^2}}{r}) = -1$. 然而, 由 $r = p^2 + p + 1 \equiv 1 \pmod{4}$, -1 是模 r 的二次剩余, 这表明 $(\frac{-1}{r}) = 1$. 这与 $2^{p^2} \equiv -1 \pmod{r}$ 矛盾. 如果 $p \equiv -3 \pmod{8}$, 那么 $r = p^2 + p + 1 \equiv 7 \pmod{8}$, 进而 2 是模 r 的非二次剩余, 即勒让德符号 (二次特征) 为 $(\frac{2}{r}) = 1$. 因此, $(\frac{2^{p^2}}{r}) = 1$. 然而, $r = p^2 + p + 1 \equiv 3 \pmod{4}$, -1 是模 r 的二次剩余, 因此 $(\frac{-1}{r}) = 1$. 这与 $2^{p^2} \equiv -1 \pmod{r}$ 矛盾. \square

注 1 借助计算机, 可以验证对不超过 10^5 的所有素数 p , 引理 7 都是成立的. 具体地, 对于所有素数 p , $1 < p \leq 10^5$, 除 $p = 5$ 和 $p = 7253$ 外, 都有 $\gcd(p^2 + p + 1, 2^{p^2} - 1) = 1$. 在这两种情形下, 当 $p \equiv 5 \pmod{24}$ 时, $\gcd(p^2 + p + 1, 2^{p^2} - 1) = 31$ 和 52 613 263, 以及当 $p \equiv \pm 3 \pmod{8}$ 时, $\gcd(p^2 + p + 1, 2^{p^2} + 1) = 1$ 或 3 总是成立的.

3 主要结果

本节我们将首先回顾二元序列的 2-adic 复杂度的有关概念. 然后, 利用中国剩余定理 (Chinese Remainder Theorem, CRT) 和 \mathbb{Z}_p 上的“高斯周期”得到了 \mathbb{Z}_{2p^2} 上的“高斯周期”. 作为本文的主要结果, 我们将基于文献 [8] 提出的计算方法分析式(1)中定义的序列的 2-adic 复杂度.

令 N 为正整数, \mathbb{Z}_N 为模 N 的剩余类环. 设 $s = (s_0, s_1, \dots, s_{N-1})$ 是周期为 N 的二元序列. 定义 $S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x]$, 设

$$\frac{S(2)}{2^N - 1} = \frac{\sum_{i=0}^{N-1} s_i 2^i}{2^N - 1} = \frac{e}{f},$$

这里 $0 \leq e \leq f$, $\gcd(e, f) = 1$. 于是, 整数 $\lfloor \log_2 f \rfloor$ 称为序列 s 的 2-adic 复杂度, 记作 $\phi_2(s)$, 即

$$\phi_2(s) = \left\lfloor \log_2 \frac{2^N - 1}{\gcd(2^N - 1, S(2))} \right\rfloor,$$

这里 $\lfloor z \rfloor$ 表示大于或等于 z 的最小正整数. 在流密码中, 二元序列可以用作密钥流生成器, 而为了抵抗 RAA 攻击, 该序列的 2-adic 复杂度应不小于其周期的一半^[3].

由 2-adic 复杂度的定义可知, 确定 $\gcd(2^N - 1, S(2))$ 是得到序列 2-adic 复杂度的关键步骤. 在给定的条件下, Xiong 等^[8] 证明了该问题可以转化为计算给定序列相关的循环矩阵 A 的行列式, 并确定 $\gcd(\det(A), 2^N - 1)$.

引理 8 ^[8] 设 s 是周期为 N 的二元序列, $A = (a_{k,j})_{N \times N}$ 是 \mathbb{Z} 上的矩阵, 其中 $a_{k,j} = s_{(k-j) \pmod{N}}$. 若 $\det(A) \neq 0$, 则存在 $u(x), v(x) \in \mathbb{Z}[x]$ 使得

$$u(2)S(2) + v(2)(1 - 2^N) = \det(A).$$

由引理 8, $\gcd(S(2), 2^N - 1)$ 是 $\gcd(\det(A), 2^N - 1)$ 的一个因子. 特别地, 若 $\gcd(\det(A), 2^N - 1) = 1$, 则 $\gcd(S(2), 2^N - 1) = 1$. 此时序列 s 的 2-adic 复杂度达到最大值 $\log_2(2^N - 1)$.

引理 9 ^[8] 设 s 是周期为 N 的二元序列, $A = (a_{k,j})_{N \times N}$ 是 \mathbb{Z} 上的矩阵, 其中 $a_{k,j} = s_{(k-j) \pmod{N}}$, 则

$$\det(A) = \prod_{j=0}^{N-1} S(\omega_N^j),$$

这里 $\omega_N = \exp(2\pi i/N)$ 为 N 次本原单位根.

令 $N = 2p^2, \omega_{2p^2} = \exp(2\pi i/N)$ 为 N 次本原单位根. 定义

$$\begin{aligned}\beta_t &= \sum_{i \in D_t^{(2p^2)}} \omega_{2p^2}^i, \quad \gamma_t = \sum_{i \in 2D_t^{(p^2)}} \omega_{2p^2}^i, \\ \eta_t &= \sum_{i \in pD_t^{(2p)}} \omega_{2p^2}^i, \quad \sigma_t = \sum_{i \in 2pD_t^{(p)}} \omega_{2p^2}^i.\end{aligned}$$

这里 $t = 0, 1$. 由于 ω_{2p^2} 为 $2p^2$ 次单位根, 易知 $\omega_{2p^2}^{2p}$ 为 p 次单位根, $\omega_{2p^2}^2$ 为 p^2 次单位根, $\omega_{2p^2}^p$ 为 $2p$ 次单位根, 分别记为 ω_p, ω_{p^2} 和 ω_{2p} . 记 σ_0 和 σ_1 是 \mathbb{Z}_p 上的“高斯周期”, 下面的引理给出了它们的值.

引理 10 [21] 令符号定义如上, 则

$$\sigma_0 = \begin{cases} \frac{-1+\sqrt{p}}{2}, & \text{若 } p \equiv 1 \pmod{4}; \\ \frac{-1-\sqrt{p}}{2}, & \text{若 } p \equiv 3 \pmod{4}, \end{cases}$$

和

$$\sigma_1 = -1 - \sigma_0.$$

引理 11 [9] 令符号定义如上, 则

$$\gamma_0 = \gamma_1 = 0.$$

当 $i = 0, 1$ 时, 我们需要确定 η_i 和 β_i 的值. 由于 p 为奇素数, 由中国剩余定理可知, \mathbb{Z}_{2p} 与 $\mathbb{Z}_2^* \times \mathbb{Z}_p^*$ 是同构的. 于是, 定义同构映射如下

$$\begin{aligned}f : \mathbb{Z}_{2p}^* &\rightarrow \mathbb{Z}_2^* \times \mathbb{Z}_p^* \\ (p+1)b + pa &\mapsto (a, b).\end{aligned}$$

因此,

$$D_0^{(2p)} \leftrightarrow \{1\} \times D_0^{(p)}, D_1^{(2p)} \leftrightarrow \{1\} \times D_1^{(p)}.$$

进而,

$$\eta_0 = \sum_{i \in pD_0^{(2p)}} \omega_{2p^2}^i = \sum_{i \in D_0^{(2p)}} \omega_{2p}^i = \sum_{b \in D_0^{(p)}} \omega_{2p}^{(p+1)b+p} = - \sum_{b \in D_0^{(p)}} \omega_{2p}^{(p+1)b} = - \sum_{b \in D_0^{(p)}} \omega_p^{\frac{(p+1)}{2}b}.$$

由引理 2, 若 $p \equiv \pm 1 \pmod{8}$, 则 $2 \in D_0^{(p)}$. 因此, $\frac{p+1}{2} = 2^{-1} \pmod{p} \in D_0^{(p)}$, 所以 $\eta_0 = - \sum_{b \in D_0^{(p)}} \omega_p^b = -\sigma_0$. 类似地, 若 $p \equiv \pm 1 \pmod{8}$, 则 $\eta_1 = -\sigma_1$.

若 $p \equiv \pm 3 \pmod{8}$, 则 $2 \in D_1^{(p)}$. 因此, $\frac{p+1}{2} = 2^{-1} \pmod{p} \in D_1^{(p)}$, 所以 $\eta_0 = - \sum_{b \in D_1^{(p)}} \omega_p^b = -\sigma_1$. 类似地, 若 $p \equiv \pm 3 \pmod{8}$, 则 $\eta_1 = -\sigma_0$.

可用类似的方法计算 β_0 和 β_1 . 再次利用中国剩余定理, 可知 \mathbb{Z}_{2p^2} 与 $\mathbb{Z}_2 \times \mathbb{Z}_p$ 同构. 定义同构映射如下

$$\begin{aligned}f : \mathbb{Z}_{2p^2}^* &\rightarrow \mathbb{Z}_2^* \times \mathbb{Z}_{p^2}^* \\ (p^2+1)b + p^2a &\mapsto (a, b).\end{aligned}$$

因此,

$$D_0^{(2p^2)} \leftrightarrow \{1\} \times D_0^{(p^2)}, D_1^{(2p^2)} \leftrightarrow \{1\} \times D_1^{(p^2)}.$$

进而,

$$\beta_0 = \sum_{i \in D_0^{(2p^2)}} \omega_{2p^2}^i = \sum_{b \in D_0^{(p^2)}} \omega_{2p^2}^{(p^2+1)b+p^2} = - \sum_{b \in D_0^{(p^2)}} \omega_{2p^2}^{(p^2+1)b} = - \sum_{b \in D_0^{(p^2)}} \omega_{p^2}^{(\frac{p^2+1}{2})b}.$$

由引理 2, 若 $p \equiv \pm 1 \pmod{8}$, 则 $\frac{p^2+1}{2} \in D_0^{(p^2)}$, 且

$$\beta_0 = - \sum_{b \in D_0^{(p^2)}} \omega_{p^2}^b = -\gamma_0.$$

类似地, 若 $p \equiv \pm 1 \pmod{8}$, 则 $\beta_1 = -\gamma_1$.

若 $p \equiv \pm 3 \pmod{8}$, 则 $\frac{p^2+1}{2} \in D_1^{(p^2)}$, 且

$$\beta_0 = - \sum_{b \in D_1^{(p^2)}} \omega_{p^2}^b = -\gamma_1.$$

类似地, 若 $p \equiv \pm 3 \pmod{8}$, 则 $\beta_1 = -\gamma_0$. 综上所述, 我们有以下引理.

引理 12 令符号定义如上, 则有

$$\eta_0 = \begin{cases} -\sigma_0, & \text{若 } p \equiv \pm 1 \pmod{8}; \\ -\sigma_1, & \text{若 } p \equiv \pm 3 \pmod{8}, \end{cases}$$

$$\eta_1 = \begin{cases} -\sigma_1, & \text{若 } p \equiv \pm 1 \pmod{8}; \\ -\sigma_0, & \text{若 } p \equiv \pm 3 \pmod{8}, \end{cases}$$

和

$$\beta_0 = \beta_1 = 0.$$

引理 13 沿用与前面相同的符号, 若 $p \equiv \pm 1 \pmod{8}$, 则有

$$S(\omega_{2p^2}^t) = \begin{cases} p^2, & \text{若 } t \in \{0\}; \\ 1, & \text{若 } t \in \{p^2\} \cup \mathbb{Z}_{2p^2}^*; \\ 1 + 2\sigma_1, & \text{若 } t \in 2D_0^{(p^2)}; \\ 1 + 2\sigma_0, & \text{若 } t \in 2D_1^{(p^2)}; \\ 1, & \text{若 } t \in p\mathbb{Z}_{2p}^*; \\ p + 2p\sigma_1, & \text{若 } t \in 2pD_0^{(p)}; \\ p + 2p\sigma_0, & \text{若 } t \in 2pD_1^{(p)}, \end{cases}$$

这里 $S(\cdot)$ 为式(1)定义的序列所对应的序列多项式.

证明: 我们将引理 13 的证明分为以下几种情形.

(i) 若 $t = 0$, 则

$$S(\omega_{2p^2}^t) = S(1) = \sum_{i \in C_1} 1 = p^2.$$

(ii) 若 $t = p^2$, 则

$$S(\omega_{2p^2}^t) = S(1) + \sum_{i \in D_1^{(2p^2)}} \omega_{2p^2}^{ip^2} + \sum_{i \in 2D_1^{(p^2)}} \omega_{2p^2}^{ip^2} + \sum_{i \in pD_1^{(2p)}} \omega_{2p^2}^{ip^2} + \sum_{i \in 2pD_1^{(p)}} \omega_{2p^2}^{ip^2}$$

$$\begin{aligned}
&= 1 - \frac{p(p-1)}{2} + \frac{p(p-1)}{2} - \frac{(p-1)}{2} + \frac{(p-1)}{2} \\
&= 1.
\end{aligned}$$

(iii) 若 $t \in D_0^{(2p^2)}$, 由引理 1 容易验证 $tD_1^{(2p^2)} \bmod 2p^2 = D_1^{(2p^2)}$, $tD_1^{(p^2)} \bmod p^2 = D_1^{(p^2)}$, $tD_1^{(2p)} \bmod 2p = D_1^{(2p)}$, $tD_1^{(p)} \bmod p = D_1^{(p)}$. 于是

$$\begin{aligned}
S(\omega_{2p^2}^t) &= 1 + \left(\sum_{i \in D_1^{(2p^2)}} + \sum_{i \in 2D_1^{(p^2)}} + \sum_{i \in pD_1^{(2p)}} + \sum_{i \in 2pD_1^{(p)}} \right) \omega_{2p^2}^{ti} \\
&= 1 + \left(\sum_{i \in D_1^{(2p^2)}} + \sum_{i \in 2D_1^{(p^2)}} + \sum_{i \in pD_1^{(2p)}} + \sum_{i \in 2pD_1^{(p)}} \right) \omega_{2p^2}^i \\
&= 1 + \beta_1 + \gamma_1 + \eta_1 + \sigma_1.
\end{aligned}$$

由引理 11 和引理 12, 有 $S(\omega_{2p^2}^t) = 1 + 0 + 0 - \sigma_1 + \sigma_1 = 1$.

(iv) 若 $t \in D_1^{(2p^2)}$, 由引理 1 有 $tD_1^{(2p^2)} \bmod 2p^2 = D_0^{(2p^2)}$, $tD_1^{(p^2)} \bmod p^2 = D_0^{(p^2)}$, $tD_1^{(2p)} \bmod 2p = D_0^{(2p)}$, $tD_1^{(p)} \bmod p = D_0^{(p)}$. 于是

$$\begin{aligned}
S(\omega_{2p^2}^t) &= 1 + \left(\sum_{i \in D_1^{(2p^2)}} + \sum_{i \in 2D_1^{(p^2)}} + \sum_{i \in pD_1^{(2p)}} + \sum_{i \in 2pD_1^{(p)}} \right) \omega_{2p^2}^{ti} \\
&= 1 + \left(\sum_{i \in D_0^{(2p^2)}} + \sum_{i \in 2D_0^{(p^2)}} + \sum_{i \in pD_0^{(2p)}} + \sum_{i \in 2pD_0^{(p)}} \right) \omega_{2p^2}^i \\
&= 1 + \beta_0 + \gamma_0 + \eta_0 + \sigma_0.
\end{aligned}$$

由引理 11 和引理 12, 有 $S(\omega_{2p^2}^t) = 1 + 0 + 0 - \sigma_0 + \sigma_0 = 1$.

(v) 若 $t \in 2D_0^{(p^2)}$, 由引理 1 和引理 2 有 $tD_1^{(2p^2)} \bmod p^2 = 2D_1^{(p^2)}$, $t2D_1^{(p^2)} \bmod p^2 = 2D_1^{(p^2)}$, $tpD_1^{(2p)} \bmod p = 2pD_1^{(p)}$, $t2pD_1^{(p)} \bmod p = 2pD_1^{(p)}$. 于是

$$\begin{aligned}
S(\omega_{2p^2}^t) &= 1 + \left(\sum_{i \in D_1^{(2p^2)}} + \sum_{i \in 2D_1^{(p^2)}} + \sum_{i \in pD_1^{(2p)}} + \sum_{i \in 2pD_1^{(p)}} \right) \omega_{2p^2}^{ti} \\
&= 1 + (2 \sum_{i \in 2D_1^{(p^2)}} + 2 \sum_{i \in 2pD_1^{(p)}}) \omega_{2p^2}^i \\
&= 1 + 2\gamma_1 + 2\sigma_1.
\end{aligned}$$

由引理 11, 有

$$S(\omega_{2p^2}^t) = 1 + 2\sigma_1.$$

(vi) 若 $t \in 2D_1^{(p^2)}$, 由引理 1 和引理 2 有 $tD_1^{(2p^2)} \bmod p^2 = 2D_0^{(p^2)}$, $t2D_1^{(p^2)} \bmod p^2 = 2D_0^{(p^2)}$, $tpD_1^{(2p)} \bmod p = 2pD_0^{(p)}$, $t2pD_1^{(p)} \bmod p = 2pD_0^{(p)}$. 于是

$$\begin{aligned}
S(\omega_{2p^2}^t) &= 1 + \left(\sum_{i \in D_1^{(2p^2)}} + \sum_{i \in 2D_1^{(p^2)}} + \sum_{i \in pD_1^{(2p)}} + \sum_{i \in 2pD_1^{(p)}} \right) \omega_{2p^2}^{ti} \\
&= 1 + (2 \sum_{i \in 2D_0^{(p^2)}} + 2 \sum_{i \in 2pD_0^{(p)}}) \omega_{2p^2}^i
\end{aligned}$$

$$= 1 + 2\gamma_0 + 2\sigma_0.$$

由引理 11, 有

$$S(\omega_{2p^2}^t) = 1 + 2\sigma_0.$$

(vii) 若 $t \in pD_0^{(2p)}$, 由引理 1 有 $tD_1^{(2p^2)} \bmod 2p = pD_1^{(2p)}$, $|D_1^{(2p^2)}| = p|D_1^{(2p)}|$, $t2D_1^{(p^2)} \bmod p = 2pD_1^{(p)}$, $|D_1^{(p^2)}| = p|D_1^{(p)}|$. 于是

$$\begin{aligned} S(\omega_{2p^2}^t) &= 1 + \left(\sum_{i \in D_1^{(2p^2)}} + \sum_{i \in 2D_1^{(p^2)}} + \sum_{i \in pD_1^{(2p)}} + \sum_{i \in 2pD_1^{(p)}} \right) \omega_{2p^2}^{ti} \\ &= 1 + p \sum_{i \in D_1^{(2p)}} \omega_{2p}^i + p \sum_{i \in D_1^{(p)}} \omega_p^i \\ &= 1 + p\eta_1 + p\sigma_1. \end{aligned}$$

由引理 12, 有

$$S(\omega_{2p^2}^t) = 1 - p\sigma_1 + p\sigma_1 = 1.$$

(viii) 若 $t \in pD_1^{(2p)}$, 由引理 1 有 $tD_1^{(2p^2)} \bmod 2p = pD_0^{(2p)}$, $|D_0^{(2p^2)}| = p|D_0^{(2p)}|$, $t2D_1^{(p^2)} \bmod p = 2pD_0^{(p)}$, $|D_0^{(p^2)}| = p|D_0^{(p)}|$. 于是

$$\begin{aligned} S(\omega_{2p^2}^t) &= 1 + \left(\sum_{i \in D_1^{(2p^2)}} + \sum_{i \in 2D_1^{(p^2)}} + \sum_{i \in pD_1^{(2p)}} + \sum_{i \in 2pD_1^{(p)}} \right) \omega_{2p^2}^{ti} \\ &= 1 + p \sum_{i \in D_0^{(2p)}} \omega_{2p}^i + p \sum_{i \in D_0^{(p)}} \omega_p^i \\ &= 1 + p\eta_0 + p\sigma_0. \end{aligned}$$

由引理 12, 有

$$S(\omega_{2p^2}^t) = 1 - p\sigma_0 + p\sigma_0 = 1.$$

(ix) 若 $t \in 2pD_0^{(p)}$, 由引理 1 和引理 2 有 $tD_1^{(2p^2)} \bmod p = 2pD_1^{(p)}$, $t2D_1^{(p^2)} \bmod p = 2pD_1^{(p)}$. 记 $|D_1^{(2p^2)}| = p|D_1^{(p)}|$ and $|D_1^{(p^2)}| = p|D_1^{(p)}|$. 于是

$$\begin{aligned} S(\omega_{2p^2}^t) &= 1 + \left(\sum_{i \in D_1^{(2p^2)}} + \sum_{i \in 2D_1^{(p^2)}} + \sum_{i \in pD_1^{(2p)}} + \sum_{i \in 2pD_1^{(p)}} \right) \omega_{2p^2}^{ti} \\ &= 1 + p \sum_{i \in 2pD_1^{(p)}} \omega_{2p}^i + p \sum_{i \in 2pD_1^{(p)}} \omega_{2p^2}^i + \sum_{i \in D_1^{(2p)}} 1 + \sum_{i \in 2D_1^{(p)}} 1 \\ &= p + 2p \sum_{i \in 2pD_1^{(p)}} \omega_{2p}^i \\ &= p + 2p \sum_{i \in D_1^{(p)}} \omega_p^i \\ &= p + 2p\sigma_1. \end{aligned}$$

(x) 若 $t \in 2pD_1^{(p)}$, 由引理 1 和引理 2 有 $tD_1^{(2p^2)} \bmod p = 2pD_0^{(p)}$, $t2D_1^{(p^2)} \bmod p = 2pD_0^{(p)}$. 记

$|D_1^{(2p^2)}| = p|D_0^{(p)}|$ 和 $|D_1^{(p^2)}| = p|D_0^{(p)}|$, 则有

$$\begin{aligned}
 S(\omega_{2p^2}^t) &= 1 + (\sum_{i \in D_1^{(2p^2)}} + \sum_{i \in 2D_1^{(p^2)}} + \sum_{i \in pD_1^{(2p)}} + \sum_{i \in 2pD_1^{(p)}}) \omega_{2p^2}^{ti} \\
 &= 1 + \sum_{i \in 2pD_0^{(p^2)}} \omega_{2p^2}^i + \sum_{i \in 2pD_0^{(p^2)}} \omega_{2p^2}^i + \sum_{i \in D_0^{(2p)}} 1 + \sum_{i \in 2D_0^{(p)}} 1 \\
 &= p + 2p \sum_{i \in 2pD_0^{(p)}} \omega_{2p^2}^i \\
 &= p + 2p \sum_{i \in D_0^{(p)}} \omega_p^i \\
 &= p + 2p\sigma_0.
 \end{aligned}$$

综合上述情形, 得证. \square

引理 14 沿用与前面相同的符号, 若 $p \equiv \pm 3 \pmod{8}$, 则有

$$S(\omega_{2p^2}^t) = \begin{cases} p^2, & \text{若 } t \in \{0\}; \\ 1, & \text{若 } t \in \{p^2\}; \\ -2\sigma_0, & \text{若 } t \in D_0^{(2p^2)}; \\ -2\sigma_1, & \text{若 } t \in D_1^{(2p^2)}; \\ 1 + 2\sigma_0, & \text{若 } t \in 2D_0^{(p^2)}; \\ 1 + 2\sigma_1, & \text{若 } t \in 2D_1^{(p^2)}; \\ -2p\sigma_0 - p + 1, & \text{若 } t \in pD_0^{(2p)}; \\ -2p\sigma_1 - p + 1, & \text{若 } t \in pD_1^{(2p)}; \\ p + 2p\sigma_0, & \text{若 } t \in 2pD_0^{(p)}; \\ p + 2p\sigma_1, & \text{若 } t \in 2pD_1^{(p)}. \end{cases}$$

证明: 由于该证明与引理 13 的证明类似, 故省略. \square

定理 1 设 s 是定义在式(1)中的周期为 $N = 2p^2 (p > 3)$ 的广义分圆二元序列. 若 $p \equiv \pm 1 \pmod{8}$, 则序列 s 的 2-adic 复杂度为

$$\phi_2(s) = 2p^2.$$

若 $p \equiv \pm 3 \pmod{8}$ 以及 $p \not\equiv 5 \pmod{24}$, 则序列 s 的 2-adic 复杂度下界为

$$\phi_2(s) \geq p^2.$$

若 $p \equiv 5 \pmod{24}$, 则序列 s 的 2-adic 复杂度下界为

$$\phi_2(s) \geq p^2 + 1.$$

此外, 若 $p \equiv 11 \pmod{24}$, 则序列 s 的 2-adic 复杂度可以达到最大值.

证明: 根据 p 的取值, 下面分两种情况进行讨论.

情形 1: 若 $p \equiv \pm 1 \pmod{8}$, 由引理 8 和引理 13, 可得

$$\begin{aligned}
\det(A) &= \prod_{t=0}^{n-1} S(\omega_{2p^2}^t) \\
&= \prod_{t \in \{0, p^2\}} S(\omega_{2p^2}^t) \prod_{t \in D_0^{(2p^2)}} S(\omega_{2p^2}^t) \prod_{t \in D_1^{(2p^2)}} S(\omega_{2p^2}^t) \times \prod_{t \in 2D_0^{(p^2)}} S(\omega_{2p^2}^t) \prod_{t \in 2D_1^{(p^2)}} S(\omega_{2p^2}^t) \prod_{t \in pD_0^{(2p)}} S(\omega_{2p^2}^t) \\
&\quad \times \prod_{t \in pD_1^{(2p)}} S(\omega_{2p^2}^t) \prod_{t \in 2pD_0^{(p)}} S(\omega_{2p^2}^t) \prod_{t \in 2pD_1^{(p)}} S(\omega_{2p^2}^t) \\
&= p^2 [(1 + 2\sigma_0)(1 + 2\sigma_1)]^{\frac{p(p-1)}{2}} [(p + 2p\sigma_0)(p + 2p\sigma_1)]^{\frac{p-1}{2}} \\
&= p^2 (-p)^{\frac{p(p-1)}{2}} (p^3)^{\frac{p-1}{2}}.
\end{aligned}$$

又 $2^{2p^2} - 1 = (2^{p^2} - 1)(2^{p^2} + 1)$ 和 $\gcd(2^{p^2} - 1, 2^{p^2} + 1) = 1$, 可知 $\gcd(\det(A), 2^{2p^2} - 1) = \gcd(\det(A), 2^{p^2} - 1) \cdot \gcd(\det(A), 2^{p^2} + 1)$.

由于 p 为素数且 $p > 3$, 可得 $2^{p^2} \equiv 2 \pmod{p}$, 所以 $2^{p^2} + 1 \equiv 3 \pmod{p}$. 于是 $\gcd(p, 2^{p^2} + 1) = 1$.

由引理 5, 可知 $\gcd(\det(A), 2^{p^2} - 1) = 1$. 因此

$$\begin{aligned}
\gcd(2^{2p^2} - 1, S(2)) &\leq \gcd(\det(A), 2^{2p^2} - 1) \\
&= \gcd(\det(A), 2^{p^2} - 1) \cdot \gcd(\det(A), 2^{p^2} + 1) \\
&= 1.
\end{aligned}$$

进而,

$$\phi_2(s) = \left\lfloor \log_2 \frac{2^{2p^2} - 1}{\gcd(2^{2p^2} - 1, S(2))} \right\rfloor = \lfloor \log_2 2^{2p^2} - 1 \rfloor = 2p^2.$$

情形 2: 若 $p \equiv \pm 3 \pmod{8}$, 由引理 8 和引理 14, 可得

$$\begin{aligned}
\det(A) &= \prod_{t=0}^{n-1} S(\omega_{2p^2}^t) \\
&= \prod_{t \in \{0, p^2\}} S(\omega_{2p^2}^t) \prod_{t \in D_0^{(2p^2)}} S(\omega_{2p^2}^t) \prod_{t \in D_1^{(2p^2)}} S(\omega_{2p^2}^t) \times \prod_{t \in 2D_0^{(p^2)}} S(\omega_{2p^2}^t) \prod_{t \in 2D_1^{(p^2)}} S(\omega_{2p^2}^t) \prod_{t \in pD_0^{(2p)}} S(\omega_{2p^2}^t) \\
&\quad \times \prod_{t \in pD_1^{(2p)}} S(\omega_{2p^2}^t) \prod_{t \in 2pD_0^{(p)}} S(\omega_{2p^2}^t) \prod_{t \in 2pD_1^{(p)}} S(\omega_{2p^2}^t) \\
&= p^2 [(-2\sigma_0)(-2\sigma_1)]^{\frac{p(p-1)}{2}} [(1 + 2\sigma_0)(1 + 2\sigma_1)]^{\frac{p(p-1)}{2}} \\
&\quad \times [(-2p\sigma_0 - p + 1)(-2p\sigma_1 - p + 1)]^{\frac{p-1}{2}} \times [(p + 2p\sigma_0)(p + 2p\sigma_1)]^{\frac{p-1}{2}} \\
&= p^2 (1 - p)^{\frac{p(p-1)}{2}} p^{\frac{p(p-1)}{2}} (1 - p^3)^{\frac{p-1}{2}} (p^3)^{\frac{p-1}{2}} \\
&= p^{\frac{(p+1)^2}{2}} (p - 1)^{\frac{p^2-1}{2}} (p^2 + p + 1)^{\frac{p-1}{2}}.
\end{aligned}$$

由于 p 为素数且 $p > 3$, 可得 $2^{p^2} \equiv 2 \pmod{p}$, 所以 $2^{p^2} + 1 \equiv 3 \pmod{p}$. 于是 $\gcd(p, 2^{p^2} + 1) = 1$.

若 $p \equiv \pm 3 \pmod{8}$ 以及 $p \not\equiv 5 \pmod{24}$, 由引理 5, 引理 6 和引理 7, 可知 $\gcd(\det(A), 2^{p^2} - 1) = 1$. 因此,

$$\gcd(2^{2p^2} - 1, S(2)) \leq \gcd(\det(A), 2^{2p^2} - 1)$$

$$\begin{aligned}
&= \gcd(\det(A), 2^{p^2} - 1) \cdot \gcd(\det(A), 2^{p^2} + 1) \\
&\leq \gcd(\det(A), 2^{p^2} + 1).
\end{aligned}$$

进而,

$$\phi_2(s) = \left\lfloor \log_2 \frac{2^{2p^2} - 1}{\gcd(2^{2p^2} - 1, S(2))} \right\rfloor \geq \lfloor \log_2(2^{p^2} - 1) \rfloor = p^2.$$

若 $p \equiv 5 \pmod{24}$, 则 $p \equiv 2 \pmod{3}$. 由引理 5, 引理 6 和引理 7, 可知 $\gcd(\det(A), 2^{p^2} + 1) = 1$. 因此,

$$\begin{aligned}
\gcd(2^{2p^2} - 1, S(2)) &\leq \gcd(\det(A), 2^{2p^2} - 1) \\
&= \gcd(\det(A), 2^{p^2} - 1) \cdot \gcd(\det(A), 2^{p^2} + 1) \\
&\leq \gcd(\det(A), 2^{p^2} - 1).
\end{aligned}$$

进而,

$$\phi_2(s) = \left\lfloor \log_2 \frac{2^{2p^2} - 1}{\gcd(2^{2p^2} - 1, S(2))} \right\rfloor \geq \lfloor \log_2(2^{p^2} + 1) \rfloor = p^2 + 1.$$

若 $p \equiv 11 \pmod{24}$, 则由中国剩余定理可知, $p \equiv 3 \pmod{8}$ 和 $p \equiv 2 \pmod{3}$. 再由引理 7(ii) 中的证明可知, 3 不可能是 $p^2 + p + 1$ 的因子. 于是, 由引理 6 和引理 7, 可得 $\gcd(\det(A), 2^{p^2} \pm 1) = 1$. 因此,

$$\phi_2(s) = \left\lfloor \log_2 \frac{2^{2p^2} - 1}{\gcd(2^{2p^2} - 1, S(2))} \right\rfloor = \lfloor \log_2(2^{2p^2} - 1) \rfloor = 2p^2.$$

□

4 结论

本文研究了一类具有高线性复杂度的二元广义分圆序列的 2-adic 复杂度. 利用 Xiong 等^[8] 给出的计算方法以及数论相关知识, 证明了在一些条件下, 此类序列的 2-adic 复杂度可以达到最大. 我们的结果表明了此类序列的 2-adic 复杂度不小于其周期的一半, 即此类序列同时具有高的 2-adic 复杂度. 因此, 可以有效抵抗有理逼近算法的攻击.

参考文献

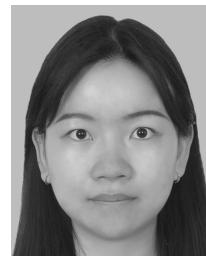
- [1] GOLOMB S W, GONG G. Signal Design for Good Correlation[M]. Cambridge University Press, Cambridge, 2005: Chapters 1–5. [DOI: 10.1017/CBO9780511546907]
- [2] MASSEY J. Shift-register synthesis and BCH decoding[J]. IEEE Transactions on Information Theory, 1969, 15(1): 122–127. [DOI: 10.1109/TIT.1969.1054260]
- [3] KLAPPER A, GORESKY M. Feedback shift registers, 2-adic span, and combiners with memory[J]. Journal of Cryptology, 1997, 10(2): 111–147. [DOI: 10.1007/s001459900024]
- [4] DING C S, HELLESETH T, SHAN W. On the linear complexity of Legendre sequences[J]. IEEE Transactions on Information Theory, 1998, 44(3): 1276–1278. [DOI: 10.1109/18.669398]
- [5] HELLESETH T, MAAS M, MATHIASSEN E, et al. Linear complexity over F_p of Sidelnikov sequences[J]. IEEE Transactions on Information Theory, 2004, 50(10): 2468–2472. [DOI: 10.1109/TIT.2004.834854]
- [6] HU L Q, YUE Q, WANG M H. The linear complexity of Whiteman’s generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$ [J]. IEEE Transactions on Information Theory, 2012, 58(8): 5534–5543. [DOI: 10.1109/TIT.2012.2196254]
- [7] LI N, TANG X H. On the linear complexity of binary sequences of period $4N$ with optimal auto-correlation/magnitude[J]. IEEE Transactions on Information Theory, 2011, 57(11): 7597–7604. [DOI: 10.1109/TIT.2011.2159575]

- [8] XIONG H, QU L J, LI C. A new method to compute the 2-adic complexity of binary sequences[J]. IEEE Transactions on Information Theory, 2014, 60(4): 2399–2406. [DOI: 10.1109/TIT.2014.2304451]
- [9] XIAO Z B, ZENG X Y, SUN Z M. 2-adic complexity of two classes of generalized cyclotomic binary sequences[J]. International Journal of Foundations of Computer Science, 2016, 27(7): 879–893. [DOI: 10.1142/S0129054116500350]
- [10] HU H G. Comments on a new method to compute the 2-adic complexity of binary sequences[J]. IEEE Transactions on Information Theory, 2014, 60(9): 5803–5804. [DOI: 10.1109/TIT.2014.2336843]
- [11] SUN Y H, WANG Q, YAN T J. A lower bound on the 2-adic complexity of the modified Jacobi sequence[J]. Cryptography and Communications, 2019, 11(2): 337–349. [DOI: 10.1007/s12095-018-0300-y]
- [12] SUN Y H, WANG Q, YAN T J. The exact autocorrelation distribution and 2-adic complexity of a class of binary sequences with almost optimal autocorrelation[J]. Cryptography and Communications, 2018, 10(3): 467–477. [DOI: 10.1007/s12095-017-0233-x]
- [13] SUN Y H, YAN T J, CHEN Z X. The 2-adic complexity of a class of binary sequences with optimal autocorrelation magnitude[J]. Cryptography and Communications, 2020, 12(4): 675–683. [DOI: 10.1007/s12095-019-00411-4]
- [14] HOFER R, WINTERHOF A. On the 2-adic complexity of the two-prime generator[J]. IEEE Transactions on Information Theory, 2018, 64(8): 5957–5960. [DOI: 10.1109/TIT.2018.2811507]
- [15] ZHANG L L, ZHANG J, YANG M H, et al. On the 2-adic complexity of the Ding-Helleseth-Martinsen binary sequences[J]. IEEE Transactions on Information Theory, 2020, 66(7): 4613–4620. [DOI: 10.1109/TIT.2020.2964171]
- [16] YANG M H, ZHANG L L, FENG K Q. On the 2-adic complexity of a class of binary sequences of period $4p$ with optimal autocorrelation magnitude[C]. In: Proceedings of 2020 IEEE International Symposium on Information Theory (ISIT). IEEE, 2019, 2915–2920. [DOI: 10.1109/ISIT44484.2020.9174142]
- [17] ZHANG J W, ZHAO C A, MA X. 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, 93(1): 302–308. [DOI: 10.1587/transfun.E93.A.302]
- [18] BURTON D M. Elementary Number Theory[M]. McGraw-Hill, New York, 1998: Chapters 1–2. [DOI: 10.1017/cbo9780511615825.004]
- [19] NATHANSON M B. Elementary Methods in Number Theory[M]. Springer, New York, 2003: 83–120. [DOI: 10.1007/978-0-387-22738-2_3]
- [20] DING C S, 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]
- [21] DING C S. Codes from Different Sets[M]. World Scientific, Singapore, 2015: Chapters 1–2. [DOI: 10.1142/9789814619363-0007]

作者信息



柯品惠 (1978–), 福建建阳人, 博士, 教授。主要研究领域为序列密码。
keph@fjnu.edu.cn



卢栎羽 (1995–), 广东南雄人, 硕士研究生。主要研究领域为序列密码。
962521894@qq.com



陈智雄 (1972–), 福建莆田人, 博士, 教授。主要研究领域为序列密码。
ptczx@126.com