

一类具有优自相关性质的二元序列的 2-adic 复杂度研究

卢栎羽, 柯品惠

(福建省网络安全与密码技术重点实验室; 福建师范大学数学与信息学院, 福建 福州 350117)

摘要: 本文研究了一类具有优自相关性质的二元序列的 2-adic 复杂度. 证明了该类序列的 2-adic 复杂度不小于其周期的一半, 并由此证明了这类序列可抵抗有理逼近算法的攻击.

关键词: 交织结构; 勒让德序列; 2-adic 复杂度

MR(2010) 主题分类号: 94C10; 06E30

中图分类号: TN918.1

文献标识码: A

文章编号: 0255-7797(2020)01-0110-09

1 引言

线性反馈移位寄存器 (LFSRs) 和带进位的反馈移位寄存器 (FCSRs) 是两种伪随机序列发生器. 它们所产生的序列具有良好的伪随机性质, 如低相关性、长周期等. 这些伪随机序列在密码学和通信系统中有着广泛的应用. 理论上, 任何二元周期序列都可以由 LFSR 或 FCSR 生成. 人们通常把能产生序列 s 的最短 LFSRs (或 FCSRs) 的长度称为序列 s 的线性复杂度 (或 2-adic 复杂度), 用符号 $LC(s)$ (或 $\phi_2(s)$) 表示. 而 Berlekamp-Massey 算法 (BMA)^[1] 和 FCSRs 的有理逼近算法 (RAA)^[2] 分别是针对序列的 LFSRs 和 FCSRs 的有效算法. 如果序列的线性复杂度或 2-adic 复杂度偏低, 则该序列在密码学意义下就是不安全的. 因此, 线性复杂度和 2-adic 复杂度被认为是序列的两个重要的安全准则. 而对于流密码中的密钥流生成器产生的周期序列, 为了抵抗 RAA 其 2-adic 复杂度应不小于其周期的一半.

交织技术是分析和设计序列的重要技术之一. 许多最优自相关序列^[3, 4]、低相关序列集^[5, 7]、或低相关区序列集^[8] 都是采用交织技术设计的或者被证明具有特殊的交织结构. 例如, 利用交织结构, Tang 和 Gong 在文献 [3] 中构造了三类具有优自相关性质的序列, 进一步地, Li 和 Tang 在文献 [9] 证明了这些序列具有大的线性复杂度. Arasu 等在文献 [10] 中构造了一类具有最优自相关性质的序列, 进一步地, Wang 和 Du 等在文献 [11] 中证明其具有大的线性复杂度. 后来, Tang 和 Ding 在文献 [4] 中给出了比文献 [3] 和 [10] 更一般的构造. 上述所提到的交织序列基本都由两类不同的序列构成, 且它们的形式为 $s = I(s_0, s_1, s'_0, s'_1)$ 或 $s = I(s_0, s'_0, s_1, s'_1)$. 但是这类序列的 2-adic 复杂度一直没人计算, 直到 Xiong 等在文献 [12] 中提出一种利用循环矩阵去计算二元序列的 2-adic 复杂度的方法, 以及 Hu 在文献 [13] 中提出运用自相关值的精确分布去计算二元序列的 2-adic 复杂度的方法. 此外, 利用循环矩阵, Xiong 等在文献 [12] 中证明了所有具有理想自相关值的序列的 2-adic 复杂度可达到其最大值. Xiong 等在文献 [14] 中证明了两类基于交织结构构造的序列也具有最大 2-adic 复杂

*收稿日期: 2019-03-27 接收日期: 2019-09-10

基金项目: 国家自然科学基金 (61772292; 61772476); 福建省自然科学基金 (2019J01273) 及福建师范大学“网络与信息安全关键理论和技术”校创新团队 (IRTL1207).

作者简介: 卢栎羽 (1995-), 女, 广东韶关, 硕士, 主要研究方向序列设计.

通讯作者: 柯品惠

度. 这两类序列中的一类是由 Tang 和 Ding 构造的^[4], 该序列具有最佳自相关性质; 另一类由 Zhou 等构造^[15], 该序列的相关值可达到最优的 Tang-Fan-Matsufuji 界. 此外, 利用文献 [13] 提出的方法和精确自相关值分布, Sun 等在文献 [16] 和文献 [17] 中分别给出了两类序列的 2-adic 复杂度的下界.

Tang 等^[4] 给出了一类具有优相关性质的二元序列的构造. 最近, Yan 等^[18] 推广了文献 [4] 的构造, 并给出了该序列的自相关值的具体分布. 本文将研究该序列的 2-adic 复杂度. 具体地, 本文将在 Tang 和 Yan 等构造的二元序列的基础上, 利用 Hu 的方法, 给出这些序列的 2-adic 复杂度的一个下界. 全文安排如下: 第 2 节给出了交织结构和勒让德序列的定义, 并回顾了 Tang 和 Yan 等给出的一类具有优相关性质的二元序列的构造及其性质; 第 3 节, 给出了该二元序列的 2-adic 复杂度的一个下界; 第 4 节对本文工作做了小结.

2 预备知识

2.1 交织结构

设 v 是一个正整数, $s_i = (s_i(0), s_i(1), \dots, s_i(v-1)), 0 \leq i \leq u-1$ 为 u 个周期为 v 的二元序列. 构造一个 $v \times u$ 矩阵 $I = (I_{i,j})$ 如下

$$I = \begin{bmatrix} s_0(0) & s_1(0) & \cdots & s_{u-1}(0) \\ s_0(1) & s_1(1) & \cdots & s_{u-1}(1) \\ \vdots & \vdots & \ddots & \vdots \\ s_0(v-1) & s_1(v-1) & \cdots & s_{u-1}(v-1) \end{bmatrix}.$$

按行连接上述矩阵可得到一条长为 uv 的周期序列 s , 称序列 s 为 $s_i, 0 \leq i \leq u-1$ 的交织序列, 记为 $s = I(s_0, s_1, \dots, s_{u-1})$, 其中 I 表示交织算子.

2.2 勒让德序列

设 p 是一个奇素数, 勒让德符号定义如下

$$\left(\frac{t}{p}\right) = \begin{cases} 1, & \text{若 } t \in \text{QR}_p, \\ -1, & \text{若 } t \in \text{NQR}_p. \end{cases}$$

其中 QR_p 和 NQR_p 分别为模 p 的二次剩余和非二次剩余.

勒让德序列定义如下

$$l(t) = \begin{cases} 0 \text{ 或 } 1, & \text{若 } t = 0, \\ \frac{1}{2}(1 - (\frac{t}{p})), & \text{其他.} \end{cases}$$

当 $l(0) = 1$ 时, 称 $l(t)$ 为第一类勒让德序列, 记作 $l(t)$; 当 $l(0) = 0$ 时, 称 $l(t)$ 为第二类勒让德序列, 记作 $l_0(t)$.

设 p 是一个奇素数, a 和 b 是周期为 p 的第一类或第二类勒让德序列, 定义二元序列 s 如下

$$s = I(a, L^n(\bar{a}), b, L^n(b)), \quad (2.1)$$

其中 $L^\eta(a)$ 表示序列 a 左循环移 η 位, \bar{a} 表示 a 的补序列.

引理 1 ^[18] 设序列 s 定义如上, 则

(i) 当 $p \equiv 1 \pmod{4}$, 且 $a = l(t), b = l_0(t)$ 时, 序列 s 的自相关值分布如下

$$R_s(\tau) = \begin{cases} -4, & \text{若 } \tau_2 = 0; \\ -4, & \text{若 } \tau_2 = 1 \text{ 且 } \tau_1 + \eta \in \text{QR}_p; \\ 4, & \text{若 } \tau_2 = 1 \text{ 且 } \tau_1 + \eta \in \text{NQR}_p; \\ 0, & \text{若 } \tau_2 = 1 \text{ 且 } \tau_1 - \eta = 0; \\ 0, & \text{若 } \tau_2 = 2; \\ -4, & \text{若 } \tau_2 = 3 \text{ 且 } \tau_1 + 1 - \eta \in \text{QR}_p; \\ 4, & \text{若 } \tau_2 = 3 \text{ 且 } \tau_1 + 1 - \eta \in \text{NQR}_p; \\ 0, & \text{若 } \tau_2 = 3 \text{ 且 } \tau_1 + 1 - \eta = 0. \end{cases}$$

(ii) 当 $p \equiv 1 \pmod{4}$, 且 $a = l_0(t), b = l(t)$ 时, 序列 s 的自相关值分布如下

$$R_s(\tau) = \begin{cases} -4, & \text{若 } \tau_2 = 0; \\ 4, & \text{若 } \tau_2 = 1 \text{ 且 } \tau_1 + \eta \in \text{QR}_p; \\ -4, & \text{若 } \tau_2 = 1 \text{ 且 } \tau_1 + \eta \in \text{NQR}_p; \\ 0, & \text{若 } \tau_2 = 1 \text{ 且 } \tau_1 - \eta = 0; \\ 0, & \text{若 } \tau_2 = 2; \\ 4, & \text{若 } \tau_2 = 3 \text{ 且 } \tau_1 + 1 - \eta \in \text{QR}_p; \\ -4, & \text{若 } \tau_2 = 3 \text{ 且 } \tau_1 + 1 - \eta \in \text{NQR}_p; \\ 0, & \text{若 } \tau_2 = 3 \text{ 且 } \tau_1 + 1 - \eta = 0. \end{cases}$$

(iii) 当 $p \equiv 3 \pmod{4}$, 且 $a = l(t), b = l_0(t)$ 时, 序列 s 的自相关值分布如下

$$R_s(\tau) = \begin{cases} -4, & \text{若 } \tau_2 = 0; \\ -4, & \text{若 } \tau_2 = 1 \text{ 且 } \tau_1 - \eta \in \text{QR}_p; \\ 4, & \text{若 } \tau_2 = 1 \text{ 且 } \tau_1 - \eta \in \text{NQR}_p; \\ 0, & \text{若 } \tau_2 = 1 \text{ 且 } \tau_1 - \eta = 0; \\ 0, & \text{若 } \tau_2 = 2; \\ 4, & \text{若 } \tau_2 = 3 \text{ 且 } \tau_1 + \eta \in \text{QR}_p; \\ -4, & \text{若 } \tau_2 = 3 \text{ 且 } \tau_1 + \eta \in \text{NQR}_p. \end{cases}$$

(iv) 当 $p \equiv 3 \pmod{4}$, 且 $a = l_0(t), b = l(t)$ 时, 序列 s 的自相关值分布如下

$$R_s(\tau) = \begin{cases} -4, & \text{若 } \tau_2 = 0; \\ 4, & \text{若 } \tau_2 = 1 \text{ 且 } \tau_1 - \eta \in \text{QR}_p; \\ -4, & \text{若 } \tau_2 = 1 \text{ 且 } \tau_1 - \eta \in \text{NQR}_p; \\ 0, & \text{若 } \tau_2 = 2; \\ -4, & \text{若 } \tau_2 = 3 \text{ 且 } \tau_1 + \eta \in \text{QR}_p; \\ 4, & \text{若 } \tau_2 = 3 \text{ 且 } \tau_1 + \eta \in \text{NQR}_p; \\ 0, & \text{若 } \tau_2 = 3 \text{ 且 } \tau_1 + 1 - \eta = 0. \end{cases}$$

3 主要结论

设 N 是一个正整数, \mathbb{Z}_N 为模 N 的剩余类环. 设 $s = (s(0), s(1), \dots, s(N-1))$ 为周期为 N 的二元序列, 定义其序列多项式为 $S(x) = \sum_{i=0}^{N-1} s(i)x^i \in \mathbb{Z}[x]$. 由文献 [19] 可知, 若

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

其中 $0 \leq e \leq f$, $\gcd(e, f) = 1$. 则序列 s 的 2-adic 复杂度 $\phi_2(s)$ 为 $\phi_2(s) = \lfloor \log_2 \frac{2^N - 1}{\gcd(2^N - 1, S(2))} \rfloor$, 其中 $\lfloor z \rfloor$ 为小于或等于 z 的最大正整数.

引理 2 [13] 设 $s = (s(0), s(1), \dots, s(N-1))$ 是一条周期为 N 的二元序列, $S(x)$ 为 s 的序列多项式, 记 $T(x) = \sum_{i=0}^{N-1} (-1)^{s(i)} x^i$, 则

$$-2S(x)T(x^{-1}) = N + \sum_{i=1}^{N-1} R_s(i)x^i - T(x^{-1}) \sum_{i=0}^{N-1} x^i \pmod{x^N - 1}.$$

引理 3 设 p 为奇素数且 $p \equiv 1 \pmod{4}$, s 为式 (2.1) 定义的二元序列, 其中 $a = l, b = l_0$, 则有 $\gcd(S(2), 5) = 1$.

证 由

$$S(x) = 1 + \sum_{i \in \text{NQR}_p} x^{4i} + \sum_{i \in \text{QR}_p} x^{4(i+\eta)+1} + \sum_{i \in \text{NQR}_p} x^{4i+2} + \sum_{i \in \text{NQR}_p} x^{4(i+\eta)+3},$$

有

$$\begin{aligned} S(2) &= 1 + \frac{p-1}{2} + 2 \times \frac{p-1}{2} + 4 \times \frac{p-1}{2} + 8 \times \frac{p-1}{2} \\ &= 1 \pmod{5}. \end{aligned}$$

进而 $\gcd(S(2), 5) = 1$.

引理 4 设 p 为奇素数, 则有 (1) $3 | (2^{2p} - 1), 5 | (2^{2p} + 1)$; (2) $\gcd(2p, \frac{2^{2p}+1}{5}) = 1$, $\gcd(2p, \frac{2^{2p}-1}{3}) = 1$.

证 (1) 由 $2^{2p} \equiv 1 \pmod{3}$ 及 $2^{2p} \equiv -1 \pmod{5}$ 易知.

(2) 显然有 $\gcd(2, \frac{2^{2p}+1}{5}) = \gcd(2, \frac{2^{2p}-1}{3}) = 1$. 又由 $2^{2p} + 1 \equiv 5 \pmod{p}$ 及 $2^{2p} - 1 \equiv 3 \pmod{p}$, 知 $\gcd(p, \frac{2^{2p}+1}{5}) = \gcd(p, \frac{2^{2p}-1}{3}) = 1$. 进而

$$\gcd(2p, \frac{2^{2p}+1}{5}) = 1, \quad \gcd(2p, \frac{2^{2p}-1}{3}) = 1.$$

定理 1 设 p 为奇素数且 $p \equiv 1 \pmod{4}$, s 为式 (2.1) 定义的二元序列, 其中 $a = l, b = l_0$, 且 $\eta = \frac{3p+1}{4}$, 则序列 s 的 2-adic 复杂度 $\phi_2(s)$ 满足 $\phi_2(s) \geq 2p$, 即序列 s 的 2-adic 复杂度大于其周期的一半.

证 设 $\tau = 4\tau_1 + \tau_2$, 其中 $0 \leq \tau_1 < p, 0 \leq \tau_2 < 4$. 由引理 1(i) 有

$$\begin{aligned} \sum_{\tau=0}^{4p-1} R_s(\tau)x^\tau &= (-4) \left(\sum_{\tau_2=0, \tau_1 \in \mathbb{Z}_p} x^\tau + \sum_{\tau_2=1, \tau_1+\eta \in \text{QR}_p} x^\tau + \sum_{\tau_2=3, \tau_1+1-\eta \in \text{QR}_p} x^\tau \right) \\ &\quad + 4 \left(\sum_{\tau_2=1, \tau_1+\eta \in \text{NQR}_p} x^\tau + \sum_{\tau_2=3, \tau_1+1-\eta \in \text{NQR}_p} x^\tau \right) \pmod{x^{4p}-1}. \end{aligned}$$

由 $\eta = \frac{3p+1}{4}$, 则

$$\begin{aligned} \sum_{\tau=0}^{4p-1} R_s(\tau)x^\tau &= (-4) \left(\sum_{\tau_1=0}^{p-1} x^{4\tau_1} + x^p \sum_{\tau_1 \in \text{QR}_p} x^{4\tau_1} + x^{3p} \sum_{\tau_1 \in \text{QR}_p} x^{4\tau_1} \right) \\ &\quad + 4 \left(x^p \sum_{\tau_1 \in \text{NQR}_p} x^{4\tau_1} + x^{3p} \sum_{\tau_1 \in \text{NQR}_p} x^{4\tau_1} \right) \pmod{x^{4p}-1} \\ &= (-4) \left[\sum_{\tau_1=0}^{p-1} x^{4\tau_1} + x^p \left(\sum_{\tau_1 \in \text{QR}_p} x^{4\tau_1} - \sum_{\tau_1 \in \text{NQR}_p} x^{4\tau_1} \right) \right. \\ &\quad \left. + x^{3p} \left(\sum_{\tau_1 \in \text{QR}_p} x^{4\tau_1} - \sum_{\tau_1 \in \text{NQR}_p} x^{4\tau_1} \right) \right] \pmod{x^{4p}-1} \\ &= (-4) \left[\sum_{\tau_1=0}^{p-1} x^{4\tau_1} + x^p(1+x^{2p}) \sum_{i \in \mathbb{Z}_p^*} \binom{i}{p} x^{4i} \right] \pmod{x^{4p}-1}. \end{aligned}$$

由引理 2, 有

$$S(2)T(2^{-1}) = -2p + 2 \left[\frac{2^{4p}-1}{15} + 2^p(1+2^{2p}) \sum_{i \in \mathbb{Z}_p^*} \binom{i}{p} 2^{4p} \right] \pmod{2^{4p}-1}.$$

进而 $S(2)T(2^{-1}) = -2p \pmod{\frac{2^{2p}+1}{5}}$.

由引理 3 及引理 4, 有 $\gcd(S(2), 2^{4p}-1) \leq 2^{2p}-1$. 因此有 $\frac{2^{4p}-1}{\gcd(S(2), 2^{4p}-1)} \geq 2^{2p}+1$, 由 $\phi_2(s)$ 的定义知结论成立.

推论 1 设 p 为奇素数且 $p \equiv 1 \pmod{4}$, s 为式 (2.1) 定义的二元序列, 其中 $a = l_0, b = l$, 且 $\eta = \frac{3p+1}{4}$, 则序列 s 的 2-adic 复杂度 $\phi_2(s)$ 满足: $\phi_2(s) \geq 2p$, 即序列 s 的 2-adic 复杂度大于其周期的一半.

证 注意到, 该序列和定理 1 中序列很相似, 差别在于交织构造中的基序列略有差异. 进而它们的 2-adic 复杂度的分析类似, 但是具体的计算细节也略有差异. 设 $\tau = 4\tau_1 + \tau_2$, 其中 $0 \leq \tau_1 < p, 0 \leq \tau_2 < 4$, 则

$$\begin{aligned} \sum_{\tau=0}^{4p-1} R_s(\tau)x^\tau &= (-4) \left(\sum_{\tau_2=0, \tau_1 \in \mathbb{Z}_p} x^\tau + \sum_{\tau_2=1, \tau_1+\eta \in \text{NQR}_p} x^\tau + \sum_{\tau_2=3, \tau_1+1-\eta \in \text{NQR}_p} x^\tau \right) \\ &\quad + 4 \left(\sum_{\tau_2=1, \tau_1+\eta \in \text{QR}_p} x^\tau + \sum_{\tau_2=3, \tau_1+1-\eta \in \text{QR}_p} x^\tau \right) \pmod{x^{4p}-1}. \end{aligned}$$

由 $\eta = \frac{3p+1}{4}$, 则

$$\begin{aligned} \sum_{\tau=0}^{4p-1} R_s(\tau)x^\tau &= (-4) \left(\sum_{\tau_1=0}^{p-1} x^{4\tau_1} + x^p \sum_{\tau_1 \in \text{NQR}_p} x^{4\tau_1} + x^{3p} \sum_{\tau_1 \in \text{NQR}_p} x^{4\tau_1} \right) \\ &\quad + 4 \left(x^p \sum_{\tau_1 \in \text{QR}_p} x^{4\tau_1} + x^{3p} \sum_{\tau_1 \in \text{QR}_p} x^{4\tau_1} \right) \pmod{x^{4p}-1} \\ &= (-4) \sum_{\tau_1=0}^{p-1} x^{4\tau_1} + 4x^p(1+x^{2p}) \sum_{i \in \mathbb{Z}_p^*} \binom{i}{p} x^{4i} \pmod{x^{4p}-1}. \end{aligned}$$

由引理 2, 有

$$\begin{aligned} S(2)T(2^{-1}) &= -2p + 2 \frac{2^{4p}-1}{15} + (-2)2^p(1+2^{2p}) \sum_{i \in \mathbb{Z}_p^*} \binom{i}{p} 2^{4i} \pmod{2^{4p}-1} \\ &= -2p \pmod{\frac{2^{2p}+1}{5}}. \end{aligned}$$

类似定理 1 的证明, 由引理 3 及引理 4, 有 $\gcd(S(2), 2^{4p}-1) \leq 2^{2p}-1$. 再由 $\phi_2(s)$ 的定义知结论成立.

引理 5 设 p 为奇素数且 $p \equiv 3 \pmod{4}$, s 为式 (2.1) 定义的二元序列, 其中 $a=l, b=l_0$, 其序列多项式为 $S(x)$, 则有 $\gcd(S(2), 3) = 1$.

证 由

$$S(x) = 1 + \sum_{i \in \text{NQR}_p} x^{4i} + \sum_{i \in \text{QR}_p} x^{4(i+\eta)+1} + \sum_{i \in \text{NQR}_p} x^{4i+2} + \sum_{i \in \text{NQR}_p} x^{4(i+\eta)+3},$$

有

$$\begin{aligned} S(2) &= 1 + \frac{p-1}{2} + 2 \times \frac{p-1}{2} + 4 \times \frac{p-1}{2} + 8 \times \frac{p-1}{2} \\ &= 1 \pmod{3}. \end{aligned}$$

进而 $\gcd(S(2), 3) = 1$.

定理 2 设 p 为奇素数且 $p \equiv 3 \pmod{4}$, s 为式 (2.1) 定义的二元序列, 其中 $a=l, b=l_0$, 且 $\eta = \frac{3p-1}{4}$, 则序列 s 的 2-adic 复杂度 $\phi_2(s)$ 满足 $\phi_2(s) \geq 2p$, 即序列 s 的 2-adic 复杂度大于其周期的一半.

证 设 $\tau = 4\tau_1 + \tau_2$, 其中 $0 \leq \tau_1 < p, 0 \leq \tau_2 < 4$ 由引理 1(iii), 有

$$\begin{aligned} \sum_{\tau=0}^{4p-1} R_s(\tau)x^\tau &= (-4) \left(\sum_{\tau_2=0, \tau_1 \in \mathbb{Z}_p} x^\tau + \sum_{\tau_2=1, \tau_1-\eta \in \text{QR}_p} x^\tau + \sum_{\tau_2=3, \tau_1+\eta \in \text{NQR}_p} x^\tau \right) \\ &\quad + 4 \left(\sum_{\tau_2=1, \tau_1-\eta \in \text{NQR}_p} x^\tau + \sum_{\tau_2=3, \tau_1+\eta \in \text{QR}_p} x^\tau \right) \pmod{x^{4p}-1}. \end{aligned}$$

由 $\eta = \frac{3p-1}{4}$, 则

$$\begin{aligned} &= (-4) \left(\sum_{\tau_1=0}^{p-1} x^{4\tau_1} + x^p \sum_{\tau_1 \in \text{QR}_p} x^{4\tau_1} + x^{3p} \sum_{\tau_1 \in \text{NQR}_p} x^{4\tau_1} \right) \\ &\quad + 4 \left(x^p \sum_{\tau_1 \in \text{NQR}_p} x^{4\tau_1} + x^{3p} \sum_{\tau_1 \in \text{QR}_p} x^{4\tau_1} \right) \pmod{x^{4p}-1} \\ &= (-4) \sum_{\tau_1=0}^{p-1} x^{4\tau_1} + (-4) \left[x^p \left(\sum_{\tau_1 \in \text{QR}_p} x^{4\tau_1} - \sum_{\tau_1 \in \text{NQR}_p} x^{4\tau_1} \right) \right. \\ &\quad \left. - x^{3p} \left(\sum_{\tau_1 \in \text{QR}_p} x^{4\tau_1} - \sum_{\tau_1 \in \text{NQR}_p} x^{4\tau_1} \right) \right] \pmod{x^{4p}-1} \\ &= (-4) \left[\sum_{\tau_1=0}^{p-1} x^{4\tau_1} + x^p (1-x^{2p}) \sum_{i \in \mathbb{Z}_p^*} \binom{i}{p} x^{4i} \right] \pmod{x^{4p}-1}. \end{aligned}$$

由引理 2, 有

$$S(2)T(2^{-1}) = -2p + 2 \left[\frac{2^{4p}-1}{15} + 2^p(1-2^{2p}) \sum_{i \in \mathbb{Z}_p^*} \binom{i}{p} 2^{4p} \right] \pmod{2^{4p}-1}.$$

进而 $S(2)T(2^{-1}) = -2p \pmod{\frac{2^{2p}-1}{3}}$. 由引理 4 及引理 5 可知

$$\gcd(S(2), 2^{4p}-1) \leq \gcd(S(2), \frac{2^{2p}-1}{3}) \cdot \gcd(S(2), 3) \cdot \gcd(S(2), 2^{2p}+1) \leq 2^{2p}+1.$$

再由 $\phi_2(s)$ 的定义, 有

$$\frac{2^{4p}-1}{\gcd(S(2), 2^{4p}-1)} \geq \frac{2^{4p}-1}{2^{2p}+1} = 2^{2p}-1.$$

因此结论成立.

推论 2 设 p 为奇素数且 $p \equiv 3 \pmod{4}$, s 为式 (2.1) 定义的二元序列, 其中 $a = l_0, b = l$, 且 $\eta = \frac{3p-1}{4}$, 则序列 s 的 2-adic 复杂度 $\phi_2(s)$ 满足 $\phi_2(s) \geq 2p$, 即序列 s 的 2-adic 复杂度大于其周期的一半.

证 注意到, 该序列和定理 2 中序列很相似, 差别在于交织构造中的基序列略有差异. 进而它们的 2-adic 复杂度的分析类似, 但是具体的计算细节也略有差异. 设 $\tau = 4\tau_1 + \tau_2$, 其中 $0 \leq \tau_1 < p, 0 \leq \tau_2 < 4$. 由引理 1(iv) 有

$$\begin{aligned} \sum_{\tau=0}^{4p-1} R_s(\tau)x^\tau &= (-4) \left(\sum_{\tau_2=0, \tau_1 \in \mathbb{Z}_p} x^\tau + \sum_{\tau_2=1, \tau_1-\eta \in \text{NQR}_p} x^\tau + \sum_{\tau_2=3, \tau_1+\eta \in \text{QR}_p} x^\tau \right) \\ &\quad + 4 \left(\sum_{\tau_2=1, \tau_1-\eta \in \text{QR}_p} x^\tau + \sum_{\tau_2=3, \tau_1+\eta \in \text{NQR}_p} x^\tau \right) \pmod{x^{4p}-1}. \end{aligned}$$

由 $\eta = \frac{3p-1}{4}$, 则

$$\begin{aligned} \sum_{\tau=0}^{4p-1} R_s(\tau)x^\tau &= (-4) \left(\sum_{\tau_1=0}^{p-1} x^{4\tau_1} + x^p \sum_{\tau_1 \in \text{NQR}_p} x^{4\tau_1} + x^{3p} \sum_{\tau_1 \in \text{QR}_p} x^{4\tau_1} \right) \\ &\quad + 4 \left(x^p \sum_{\tau_1 \in \text{QR}_p} x^{4\tau_1} + x^{3p} \sum_{\tau_1 \in \text{NQR}_p} x^{4\tau_1} \right) \pmod{x^{4p}-1} \\ &= (-4) \sum_{\tau_1=0}^{p-1} x^{4\tau_1} + 4[x^p(1-x^{2p}) \sum_{i \in \mathbb{Z}_p^*} \binom{i}{p} x^{4i}] \pmod{x^{4p}-1}. \end{aligned}$$

由引理 2, 有

$$\begin{aligned} S(2)T(2^{-1}) &= -2p - 2 \frac{2^{4p}-1}{15} + 2[2^p(1-2^{2p}) \sum_{i \in \mathbb{Z}_p^*} \binom{i}{p} 2^{4p}] \pmod{2^{4p}-1} \\ &= -2p \pmod{\frac{2^{2p}-1}{3}}. \end{aligned}$$

由引理 4 及引理 5, $\gcd(S(2), 2^{4p}-1) \leq 2^{2p}+1$. 再由 $\phi_2(s)$ 的定义可知

$$\frac{2^{4p}-1}{\gcd(S(2), 2^{4p}-1)} \geq \frac{2^{4p}-1}{2^{2p}+1} = 2^{2p}-1.$$

4 总结

本文研究了一类具有优自相关性质的二元序列的 2-adic 复杂度, 给出了该类序列的 2-adic 复杂度的一个下界. 本文的结果表明这类序列的 2-adic 复杂度不小于其周期的一半, 这意味着这些序列可以抵抗针对带进位的反馈移位寄存器的有理逼近算法的攻击.

参考文献

- [1] Massey J L. Shift-register synthesis and BCH decoding[J]. IEEE Transactions on Information Theory, 1969, 15: 122-127.
- [2] Klapper A, Goresky M. Feedback shift registers, 2-adic span, and combiners with memory[J]. Journal of Cryptology, 1997, 10: 111-147.
- [3] Tang X H, Gong G. New constructions of binary sequences with optimal autocorrelation value/magnitude[J]. IEEE Transactions on Information Theory, 2010, 56(3): 1278-1286.
- [4] Tang X H, Ding C S. New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value[J]. IEEE Transactions on Information Theory, 2010, 56(12): 6398-6405.
- [5] Gong G. Theory and applications of q -ary interleaved sequences[J]. IEEE Transactions on Information Theory, 1995, 41(2): 400-411.
- [6] Cai K, Weng G B, Cheng X Q. Binary almost-perfect sequence sets[J]. IEEE Transactions on Information Theory, 2010, 56(7): 3594-3604.

- [7] Gong G. New designs for signal sets with low cross correlation, balance property, and large linear span: $GF(p)$ case[J]. *IEEE Transactions on Information Theory*, 2002, 48(11): 2847–2867.
- [8] Zhou Z C, Tang X H, Gong G. A new class of sequences with zero or low correlation zone based on interleaving technique[J]. *IEEE Transactions on Information Theory*, 2008, 54(9): 4267–4273.
- [9] Li N, Tang X H. On the linear complexity of binary sequences of period $4N$ with optimal autocorrelation/magnitude[J]. *IEEE Transactions on Information Theory*, 2011, 57(11): 7597–7604.
- [10] Arasu K T, Ding C S, Helleseth T, Kumar P V, Martinsen H M. Almost difference sets and their sequences with optimal autocorrelation[J]. *IEEE Transactions on Information Theory*, 2001, 47(7): 2934–2943.
- [11] Wang Q, Du X N. The linear complexity of binary sequences with optimal autocorrelation[J]. *IEEE Transactions on Information Theory*, 2010, 56(12): 6388–6397.
- [12] 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.
- [13] 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(4): 5803–5804.
- [14] Xiong H, Qu L J, Li C. 2-Adic complexity of binary sequences with interleaved structure[J]. *Finite Fields and Their Applications*, 2015, 33(15): 14–28.
- [15] Tang X H, Fan P Z, Matsufuji S. Lower bounds on the maximum correlation of spreading sequences set with low or zero correlation zone[J]. *Electron Letters*, 2000, 36: 551–552.
- [16] 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*, 2018, <https://doi.org/10.1007/s12095-018-0300-y>.
- [17] 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.
- [18] Yan T J, Gong G. Some notes on constructions of binary sequences with optimal autocorrelation[J]. 2014, <https://arxiv.org/abs/1411.4340>.
- [19] Klapper A, Goresky M. Feedback shift registers, 2-adic span, and combiners with memory[J]. *Journal of Cryptology*, 1997, 10(2): 111–147.

STUDY OF 2-ADIC COMPLEXITY OF A CLASS OF BINARY SEQUENCES WITH OPTIMAL AUTOCORRELATION VALUES

LU Li-yu, KE Pin-hui

(*Fujian Provincial Key Laboratory of Network Security and Cryptology; College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, China*)

Abstract: In this paper, we study the 2-adic complexity of a class of binary sequences with optimal autocorrelation values. We prove that the 2-adic complexity of the considering sequences is not less than a half of its period. So this sequences can resist the attack of rational approximate algorithm.

Keywords: interleaved structures; Legendre sequences; 2-adic complexity

2010 MR Subject Classification: 94C10; 06E30