

两类周期为 pq 的四元序列在 \mathbb{F}_4 上的线性复杂度

颜霏霏¹, 柯品惠²

(1. 福建师范大学数学与统计学院, 福建 福州 350117)

(2. 分析数学及应用教育部重点实验室(福建师范大学), 福建 福州 350117)

摘要: 本文研究了两类周期为 pq 的四元序列在 \mathbb{F}_4 上的线性复杂度和极小多项式. 利用 [10, 12] 中的方法, 证明了这两类序列在 \mathbb{F}_4 上具有高的线性复杂度, 从而可以抵抗 Berlekamp-Massey 算法的攻击.

关键词: 逆 Gray 映射; 广义分圆; 四元序列; 线性复杂度

MR(2010) 主题分类号: 94A55

中图分类号: O236.2

文献标识码: A

文章编号: 0255-7797(2025)02-0151-10

1 引言

伪随机序列在码分多址、流密码等领域有广泛应用^[1-3]. 二元序列和四元序列是实际应用中的首选序列. 相关性和复杂度是伪随机序列的两个重要指标. 在密码学的相关应用中, 要求使用的序列具有较高的线性复杂度. 通过符号替换, 可建立 \mathbb{Z}_4 上的四元序列和 \mathbb{F}_4 上的四元序列的一一对应关系. 因此, 考察四元序列在 \mathbb{Z}_4 和 \mathbb{F}_4 上的线性复杂度是探究四元序列优劣的必要步骤. 根据 Berlekamp-Massey 算法^[4-5] 以及 Reeds-Sloane 算法^[6] 可知, 使用的四元序列在 \mathbb{F}_4 和 \mathbb{Z}_4 上的线性复杂度至少要达到其周期的一半.

基于经典分圆类和广义分圆类构造的伪随机序列具有较高的复杂度, 近年来受到学者们的关注^[7-12]. 逆 Gray 映射是构造四元序列的一种常用方法^[13]. 文 [9] 利用广义分圆二元序列和逆 Gray 映射构造了一类具有良好自相关性质的四元序列. 文 [10] 确定了文 [9] 中构造的四元序列在 \mathbb{F}_4 和 \mathbb{Z}_4 上的线性复杂度, 并对已有构造进行了改进. 文 [12] 由逆 Gray 映射构造了一类新的周期为 pq 的四元序列, 使用与文 [10] 中相似的方法确定了新序列在 \mathbb{F}_4 上的线性复杂度, 并确定了该序列的 4-adic 复杂度. 文 [11] 分别基于 Whiteman 广义分圆序列和 Ding-Helleseth 广义分圆序列给出了两类周期为 pq 的四元序列, 并计算了序列在 \mathbb{Z}_4 上的线性复杂度.

较之模 4 剩余类环 \mathbb{Z}_4 , 四阶有限域 \mathbb{F}_4 有更好的代数结构, 注意到 \mathbb{Z}_4 和 \mathbb{F}_4 上序列的性质定义和分析方法是不相同的. 关于四元序列在 \mathbb{F}_4 上的复杂度, 文 [14] 考虑了具有优自相关性质的偶数周期四元序列在 \mathbb{F}_4 上的线性复杂度. 文 [15] 考虑了一类基于交织方法构造的四元序列在 \mathbb{F}_4 上的线性复杂度, 该序列的周期也是 pq , 其中 p 和 q 是不同的奇素数. 本文将分析文 [11] 中两类序列在 \mathbb{F}_4 上的线性复杂度和极小多项式. 本文的其余部分组织如下. 第 2 节介绍相关的基本概念以及一些必要的记号. 第 3 节确定文 [11] 中第一类四元序列在 \mathbb{F}_4 上

*收稿日期: 2023-11-18

接收日期: 2024-12-09

基金项目: 国家自然科学基金资助项目 (62272420); 福建省自然科学基金资助项目 (2023J01535).

作者简介: 颜霏霏 (2000-), 女, 福建莆田, 研究生, 主要研究方向: 序列设计, E-mail:ffyfnu@139.com

通讯作者: 柯品惠 (1978-), 男, 教授, 主要研究方向: 编码密码学, E-mail:keph@fjnu.edu.cn

的线性复杂度和极小多项式. 第 4 节确定文 [11] 中第二类四元序列在 \mathbb{F}_4 上的线性复杂度和极小多项式. 第 5 节对文章进行总结.

2 预备知识

设 p 和 q 是两个不同的奇素数, 且 $N = pq$. 定义 $P = \{p, 2p, \dots, (q-1)p\}$, $Q = \{q, 2q, \dots, (p-1)q\}$, Z_N^* 表示剩余类环 Z_N 中所有可逆元素组成的集合. 易知 $Z_N = \{0\} \cup P \cup Q \cup Z_N^*$. 由中国剩余定理, 有 $Z_N \cong Z_p \times Z_q$, 对应的同构映射为 $f(t) = (t_1, t_2)$, 其中 $t \equiv t_1 \pmod{p}$, $t \equiv t_2 \pmod{q}$. 文中 (\cdot) 表示勒让德符号.

逆 Gray 映射 $\phi = [a, b]$ 定义为

$$\phi[0, 0] = 0, \phi[0, 1] = 1, \phi[1, 1] = 2, \phi[1, 0] = 3.$$

定义二元序列 s_i , $i = 1, 2, 3$ 如下:

$$s_1(t) = \begin{cases} 1, & \text{若 } t \in P; \\ 0, & \text{若 } t \in \{0\} \cup Q; \\ \frac{1 - (\frac{t}{p})(\frac{t}{q})}{2}, & \text{若 } t \in Z_N^*. \end{cases} \quad s_2(t) = \begin{cases} 1, & \text{若 } t \in P; \\ 0, & \text{若 } t \in \{0\} \cup Q; \\ \frac{1 - (\frac{t}{q})}{2}, & \text{若 } t \in Z_N^*. \end{cases}$$

$$s_3(t) = \begin{cases} 1, & \text{若 } t \in P; \\ 0, & \text{若 } t \in \{0\} \cup Q; \\ \frac{1 - (\frac{t}{p})}{2}, & \text{若 } t \in Z_N^*. \end{cases}$$

利用逆 Gray 映射, 文 [11] 定义了第一类四元序列 $s'(t)$ 和第二类四元序列 $s''(t)$ 如下:

$$s'(t) = \phi[s_1(t), s_2(t)]. \quad (1)$$

$$s''(t) = \phi[s_2(t), s_3(t)]. \quad (2)$$

设 A_i, B_i , $i = 0, 1$ 分别表示模 p 和模 q 的平方剩余及非平方剩余, $A_2 = B_2 = \{0\}$. 设 $F_{k,l} = f^{-1}(A_k \times B_l)$, $k, l = 0, 1, 2$. 则 $Z_N = \bigcup_{k,l=0}^2 F_{k,l}$. 那么, 序列 $s'(t)$ 和 $s''(t)$ 可以分别地表示为:

$$s'(t) = \begin{cases} 0, & \text{若 } t \pmod{N} \in F_{0,0} \cup F_{0,2} \cup F_{1,2} \cup \{0\}; \\ 1, & \text{若 } t \pmod{N} \in F_{1,1}; \\ 2, & \text{若 } t \pmod{N} \in F_{0,1} \cup F_{2,0} \cup F_{2,1}; \\ 3, & \text{若 } t \pmod{N} \in F_{1,0}. \end{cases} \quad (3)$$

$$s''(t) = \begin{cases} 0, & \text{若 } t \pmod{N} \in F_{0,0} \cup F_{0,2} \cup F_{1,2} \cup \{0\}; \\ 1, & \text{若 } t \pmod{N} \in F_{1,0}; \\ 2, & \text{若 } t \pmod{N} \in F_{1,1} \cup F_{2,0} \cup F_{2,1}; \\ 3, & \text{若 } t \pmod{N} \in F_{0,1}. \end{cases} \quad (4)$$

定义四阶有限域 $\mathbb{F}_4 = \{0, 1, \mu, \mu^2\}$, 其中 μ 满足 $\mu^2 = \mu + 1$, 即 \mathbb{F}_4 是 \mathbb{F}_2 上以 $1, \mu$ 为基的向量空间. 若 $s = (s(0), s(1), \dots, s(N-1))$ 是 \mathbb{F}_4 上的周期为 N 的四元序列, 则序列 s 的生成多项式为 $M_s(x) = \sum_{t=0}^{N-1} s(t)x^t$, 其极小多项式 $m_s(x)$ 的计算公式为

$$m_s(x) = \frac{x^N - 1}{\gcd(x^N - 1, M_s(x))}. \quad (5)$$

序列 s 的线性复杂度 $LC(s)$ 为

$$LC(s) = N - \deg(\gcd(x^N - 1, M_s(x))). \quad (6)$$

设 t 是 4 模 N 的阶, 即 t 是满足 $4^t \equiv 1 \pmod{N}$ 的最小正整数. 假设 ξ 是 \mathbb{F}_{4^t} 的本原元, 则 $\xi^{\frac{4^t-1}{N}}$ 的阶为 N . 记 $\alpha = \xi^{\frac{4^t-1}{N}}$. 因此 \mathbb{F}_{4^t} 是 $x^N - 1$ 的分裂域. 由 (6) 可得

$$\begin{aligned} LC(s) &= N - \deg(\gcd(x^N - 1, M_s(x))) \\ &= N - |\{v | M_s(\alpha^v) = 0, v = 0, 1, \dots, N-1\}|. \end{aligned} \quad (7)$$

设 $\beta = \alpha^{aq}$, $\gamma = \alpha^{bp}$, 其中 a, b 是满足 $aq + bp = 1$ 的整数. 即 β 和 γ 分别为 \mathbb{F}_{4^t} 上的 p 次和 q 次本原单位根. 设 $R_2(x) = \sum_{i \in A_0} x^i$ 且 $T_2(x) = \sum_{i \in B_0} x^i$. 易知 $R_2(1) = (p-1)/2$, $T_2(1) = (q-1)/2$.

引理 1 [16] (1) 若 $p \equiv \pm 1 \pmod{8}$ 或 $q \equiv \pm 1 \pmod{8}$, 则

$$R_2(\beta^v) = \begin{cases} 1, & \text{若 } v \pmod{p} \in A_0, \\ 0, & \text{若 } v \pmod{p} \in A_1. \end{cases} \quad \text{且} \quad T_2(\gamma^v) = \begin{cases} 1, & \text{若 } v \pmod{q} \in B_0, \\ 0, & \text{若 } v \pmod{q} \in B_1. \end{cases}$$

(2) 若 $p \equiv \pm 3 \pmod{8}$ 或 $q \equiv \pm 3 \pmod{8}$, 则

$$R_2(\beta^v) = \begin{cases} \mu, & \text{若 } v \pmod{p} \in A_0, \\ \mu + 1, & \text{若 } v \pmod{p} \in A_1. \end{cases} \quad \text{且} \quad T_2(\gamma^v) = \begin{cases} \mu, & \text{若 } v \pmod{q} \in B_0, \\ \mu + 1, & \text{若 } v \pmod{q} \in B_1. \end{cases}$$

3 第一类四元序列在 \mathbb{F}_4 上的线性复杂度和极小多项式

为计算序列在 \mathbb{F}_4 上的线性复杂度, 分别把 (3), (4) 式定义的 \mathbb{Z}_4 上的序列修改为 \mathbb{F}_4 上的序列, 即令 $0 = 0, 1 = 1, 2 = \mu + 1, 3 = \mu$. 在不引起混淆的情况下, 把修改后的序列记为 U' 和 U'' .

易知, \mathbb{F}_4 上的序列 U' 的生成多项式为

$$M_{U'}(\alpha^v) = \sum_{t \pmod{N} \in F_{1,1}} \alpha^{vt} + (\mu + 1) \sum_{t \pmod{N} \in F_{0,1} \cup F_{2,0} \cup F_{2,1}} \alpha^{vt} + \mu \sum_{t \pmod{N} \in F_{1,0}} \alpha^{vt}.$$

设 θ 和 η 分别表示模 p 和模 q 的本原根. 由 $F_{1,1} = f^{-1}(A_1 \times B_1) = \{aqt_1 + bpt_2 | t_1 \in A_1, t_2 \in B_1\}$, 可得

$$\sum_{t \pmod{N} \in F_{1,1}} \alpha^{vt} = \sum_{t_1 \in A_1} \sum_{t_2 \in B_1} \alpha^{vaqt_1 + vbpt_2} = \sum_{i \in A_0} (\alpha^{aq})^{v\theta i} \sum_{j \in B_0} (\alpha^{bp})^{v\eta j} = R_2(\beta^{v\theta}) T_2(\gamma^{v\eta}).$$

对其余情形 $F_{i,j}, i, j \in \{0, 1, 2\}$ 类似可证. 综上, 有

$$M_{U'}(\alpha^v) = R_2(\beta^{v\theta})T_2(\gamma^{v\eta}) + (\mu + 1)(R_2(\beta^v)T_2(\gamma^{v\eta}) + T_2(\gamma^v) + T_2(\gamma^{v\eta})) + \mu R_2(\beta^{v\theta})T_2(\gamma^v). \quad (8)$$

将 $R_2(1) = (p-1)/2, T_2(1) = (q-1)/2$ 带入 (8) 中有 $M_{U'}(1) = 0$. (9)

引理 2 设 $U'(t)$ 是 (3) 定义的序列在 \mathbb{F}_4 上对应的四元序列, $M_{U'}(x)$ 是其生成多项式. 则

$$(1) M_{U'}(\alpha^v) = \begin{cases} \mu + 1, & \text{若 } v \in P \text{ 且 } p \pmod{4} \equiv 1, \\ 1, & \text{若 } v \in P \text{ 且 } p \pmod{4} \equiv -1. \end{cases}$$

$$(2) M_{U'}(\alpha^v) = \begin{cases} 0, & \text{若 } v \in Q \text{ 且 } q \pmod{4} \equiv 1, \\ \mu + 1, & \text{若 } v \in Q \text{ 且 } q \pmod{4} \equiv -1. \end{cases}$$

证 设 $v \in P$, 则 $R_2(\beta^v) = (p-1)/2, R_2(\beta^{v\theta}) = (p-1)/2$. 若 $p \pmod{4} \equiv 1$, 则 $R_2(\beta^v) = 0$ 且 $R_2(\beta^{v\theta}) = 0$. 由 (8) 可得 $M_{U'}(\alpha^v) = (\mu + 1)(T_2(\gamma^v) + T_2(\gamma^{v\eta}))$. 由引理 1, $T_2(\gamma^{v\eta}) = \sum_{i \in B_0} \gamma^{v\eta i} = \sum_{i \in B_1} \gamma^{vi} = T_2(\gamma^v) + 1$, 则 $M_{U'}(\alpha^v) = \mu + 1$. 若 $p \pmod{4} \equiv -1$, 则 $R_2(\beta^v) = 1$ 且 $R_2(\beta^{v\theta}) = 1$. 由 (8) 可得 $M_{U'}(\alpha^v) = T_2(\gamma^{v\eta}) + (\mu + 1)(T_2(\gamma^{v\eta}) + T_2(\gamma^v) + T_2(\gamma^{v\eta})) + \mu T_2(\gamma^v) = T_2(\gamma^{v\eta}) + T_2(\gamma^v)$. 由 $T_2(\gamma^{v\eta}) = T_2(\gamma^v) + 1$ 可得, $M_{U'}(\alpha^v) = 1$. $v \in Q$ 的情形类似可证.

引理 3 记号同上. 若 $v \in Z_N^*$, 则

$$M_{U'}(\alpha^v) = \begin{cases} R_2(\beta^\theta)T_2(\gamma^\eta) + (\mu + 1)(R_2(\beta)T_2(\gamma^\eta) + T_2(\gamma) + T_2(\gamma^\eta)) + \mu R_2(\beta^\theta)T_2(\gamma), & \text{若 } v \in F_{0,0}; \\ R_2(\beta)T_2(\gamma) + (\mu + 1)(R_2(\beta^\theta)T_2(\gamma) + T_2(\gamma) + T_2(\gamma^\eta)) + \mu R_2(\beta)T_2(\gamma^\eta), & \text{若 } v \in F_{1,1}; \\ R_2(\beta)T_2(\gamma^\eta) + (\mu + 1)(R_2(\beta^\theta)T_2(\gamma^\eta) + T_2(\gamma) + T_2(\gamma^\eta)) + \mu R_2(\beta)T_2(\gamma), & \text{若 } v \in F_{1,0}; \\ R_2(\beta^\theta)T_2(\gamma) + (\mu + 1)(R_2(\beta)T_2(\gamma) + T_2(\gamma) + T_2(\gamma^\eta)) + \mu R_2(\beta^\theta)T_2(\gamma^\eta), & \text{若 } v \in F_{0,1}. \end{cases}$$

证 若 $v \in F_{0,0}$, 则 $v \pmod{p} \in A_0$ 且 $v \pmod{q} \in B_0$, 则 $R_2(\beta^{v\theta}) = \sum_{i \in A_0} \beta^{v\theta i} = \sum_{i \in A_0} \beta^{\theta i} = R_2(\beta^\theta), T_2(\gamma^{v\eta}) = \sum_{i \in B_0} \gamma^{v\eta i} = \sum_{i \in B_0} \gamma^{\eta i} = T_2(\gamma^\eta), T_2(\gamma^v) = \sum_{i \in B_0} \gamma^{vi} = \sum_{i \in B_0} \gamma^i = T_2(\gamma)$ 且 $R_2(\beta^v) = \sum_{i \in A_0} \beta^{vi} = \sum_{i \in A_0} \beta^i = R_2(\beta)$. 则由 (8), $M_{U'}(\alpha^v) = R_2(\beta^\theta)T_2(\gamma^\eta) + (\mu + 1)(R_2(\beta)T_2(\gamma^\eta) + T_2(\gamma) + T_2(\gamma^\eta)) + \mu R_2(\beta^\theta)T_2(\gamma)$. 其余情形类似可证.

引理 4 记号同上, 则

(1) 若 $p \pmod{8} \equiv \pm 1$, 当 $q \pmod{8} \equiv \pm 1$ 或 $q \pmod{8} \equiv \pm 3$, 则

$$M_{U'}(\alpha^v) = \begin{cases} \mu + 1, & \text{若 } v \in F_{0,0}, \\ \mu, & \text{若 } v \in F_{1,1}, \\ 1, & \text{若 } v \in F_{1,0}, \\ 0, & \text{若 } v \in F_{0,1}. \end{cases} \text{ 或 } M_{U'}(\alpha^v) = \begin{cases} 1, & \text{若 } v \in F_{0,0}, \\ 0, & \text{若 } v \in F_{1,1}, \\ \mu + 1, & \text{若 } v \in F_{1,0}, \\ \mu, & \text{若 } v \in F_{0,1}. \end{cases}$$

(2) 若 $p \pmod{8} \equiv \pm 3$, 当 $q \pmod{8} \equiv \pm 1$ 或 $q \pmod{8} \equiv \pm 3$, 则

$$M_{U'}(\alpha^v) = \begin{cases} \mu, & \text{若 } v \in F_{0,0}, \\ \mu + 1, & \text{若 } v \in F_{1,1}, \\ 0, & \text{若 } v \in F_{1,0}, \\ 1, & \text{若 } v \in F_{0,1}. \end{cases} \text{ 或 } M_{U'}(\alpha^v) = \begin{cases} 0, & \text{若 } v \in F_{0,0}, \\ 1, & \text{若 } v \in F_{1,1}, \\ \mu, & \text{若 } v \in F_{1,0}, \\ \mu + 1, & \text{若 } v \in F_{0,1}. \end{cases}$$

证 对不同的情形, 证明方法是类似的, 因此只证明 $p \pmod{8} \equiv \pm 1$ 且 $q \pmod{8} \equiv \pm 1$ 的情形. 当 $p \pmod{8} \equiv \pm 1$ 且 $q \pmod{8} \equiv \pm 1$ 时, 由引理 1 和引理 3, 若 $v \in F_{0,0}$, 则 $M_{U'}(\alpha^v) = 0 + (\mu + 1)(0 + 1 + 0) + \mu \times 0 = \mu + 1$; 若 $v \in F_{1,1}$, 则 $M_{U'}(\alpha^v) = 1 + (\mu + 1)(0 + 0 + 1) + \mu \times 0 = \mu$; 若 $v \in F_{1,0}$, 则 $M_{U'}(\alpha^v) = 0 + (\mu + 1)(0 + 1 + 0) + \mu \times 1 = 1$; 若 $v \in F_{0,1}$, 则 $M_{U'}(\alpha^v) = 0 + (\mu + 1)(1 + 0 + 1) + \mu \times 0 = 0$.

定理 1 记号同上. 记 $H_1(x) = \prod_{t \in F_{0,0}} (x - \alpha^t)$, $H_2(x) = \prod_{t \in F_{1,1}} (x - \alpha^t)$, $H_3(x) = \prod_{t \in F_{1,0}} (x - \alpha^t)$, $H_4(x) = \prod_{t \in F_{0,1}} (x - \alpha^t)$ 且 $Q(x) = \prod_{t \in Q} (x - \alpha^t)$. 则 $U'(t)$ 的线性复杂度 $LC(U'(t))$ 和极小多项式 $m_{U'}(x)$ 如下:

(1) 若 $p \pmod{8} \equiv \pm 1$ 且 $q \pmod{8} \equiv 1$, 则

$$LC(U'(t)) = \frac{3pq - 3p + q - 1}{4}, m_{U'}(x) = \frac{x^{pq} - 1}{(x - 1)H_4(x)Q(x)};$$

(2) 若 $p \pmod{8} \equiv \pm 1$ 且 $q \pmod{8} \equiv -1$, 则

$$LC(U'(t)) = \frac{3pq + p + q - 5}{4}, m_{U'}(x) = \frac{x^{pq} - 1}{(x - 1)H_4(x)};$$

(3) 若 $p \pmod{8} \equiv \pm 1$ 且 $q \pmod{8} \equiv 3$, 则

$$LC(U'(t)) = \frac{3pq + p + q - 5}{4}, m_{U'}(x) = \frac{x^{pq} - 1}{(x - 1)H_2(x)};$$

(4) 若 $p \pmod{8} \equiv \pm 1$ 且 $q \pmod{8} \equiv -3$, 则

$$LC(U'(t)) = \frac{3pq - 3p + q - 1}{4}, m_{U'}(x) = \frac{x^{pq} - 1}{(x - 1)H_2(x)Q(x)};$$

(5) 若 $p \pmod{8} \equiv \pm 3$ 且 $q \pmod{8} \equiv 1$, 则

$$LC(U'(t)) = \frac{3pq - 3p + q - 1}{4}, m_{U'}(x) = \frac{x^{pq} - 1}{(x - 1)H_3(x)Q(x)};$$

表 1 p 和 q 取不同值时序列 $U'(t)$ 的线性复杂度

p	q	$LC(U'(t))$	$LC(U'(t))$ 满足	pq
17	11	146	$3pq + p + q - 5/4$	187
17	41	520	$3pq - 3p + q - 1/4$	697
31	29	658	$3pq - 3p + q - 1/4$	899
19	17	232	$3pq - 3p + q - 1/4$	323
59	19	859	$3pq + p + q - 5/4$	1121

(6) 若 $p \pmod{8} \equiv \pm 3$ 且 $q \pmod{8} \equiv -1$, 则

$$LC(U'(t)) = \frac{3pq + p + q - 5}{4}, m_{U'}(x) = \frac{x^{pq} - 1}{(x-1)H_3(x)};$$

(7) 若 $p \pmod{8} \equiv \pm 3$ 且 $q \pmod{8} \equiv 3$, 则

$$LC(U'(t)) = \frac{3pq + p + q - 5}{4}, m_{U'}(x) = \frac{x^{pq} - 1}{(x-1)H_1(x)};$$

(8) 若 $p \pmod{8} \equiv \pm 3$ 且 $q \pmod{8} \equiv -3$, 则

$$LC(U'(t)) = \frac{3pq - 3p + q - 1}{4}, m_{U'}(x) = \frac{x^{pq} - 1}{(x-1)H_1(x)Q(x)}.$$

证 当 $p \pmod{8} \equiv \pm 1$ 且 $q \pmod{8} \equiv 1$ 时, 由引理 4, 有 $|\{v|v \in Z_N^*, M_{U'}(\alpha^v) = 0\}| = \frac{(p-1)(q-1)}{4}$, 又由引理 2, 有 $|\{v|v \in P, M_{U'}(\alpha^v) = 0\}| = 0$, $|\{v|v \in Q, M_{U'}(\alpha^v) = 0\}| = p-1$. 结合式 (9), 可得线性复杂度为 $LC(U'(t)) = pq - \frac{(p-1)(q-1)}{4} - (p-1) - 1 = \frac{3pq - 3p + q - 1}{4}$, 且极小多项式为 $m_{U'}(x) = \frac{x^{pq} - 1}{(x-1)H_4(x)Q(x)}$. 其余情形类似可证.

利用 Magma 程序, 验证了取不同参数时 $U'(t)$ 的线性复杂度, 见表 1. 结果与定理 1 结论一致.

4 第二类四元序列在 \mathbb{F}_4 上的线性复杂度和极小多项式

本节计算序列 U'' 在 \mathbb{F}_4 上的线性复杂度. 与第 2 节类似, 同样用 U'' 表示该序列在 \mathbb{F}_4 上的对应. 记号同上. 此时 U'' 的生成多项式为

$$M_{U''}(\alpha^v) = \sum_{t \pmod{N} \in F_{1,0}} \alpha^{vt} + (\mu + 1) \sum_{t \pmod{N} \in F_{1,1} \cup F_{2,0} \cup F_{2,1}} \alpha^{vt} + \mu \sum_{t \pmod{N} \in F_{0,1}} \alpha^{vt}.$$

由 $F_{1,0} = f^{-1}(A_1 \times B_0) = \{aqt_1 + bpt_2 | t_1 \in A_1, t_2 \in B_0\}$, 可得

$$\sum_{t \pmod{N} \in F_{1,0}} \alpha^{vt} = \sum_{t_1 \in A_1} \sum_{t_2 \in B_0} \alpha^{vaqt_1 + vbpt_2} = \sum_{i \in A_0} (\alpha^{aq})^{v\theta i} \sum_{j \in B_0} (\alpha^{bp})^{vj} = R_2(\beta^{v\theta}) T_2(\gamma^v).$$

对其余情形 $F_{i,j}, i, j \in \{0, 1, 2\}$ 类似可证. 综上, 有

$$M_{U''}(\alpha^v) = R_2(\beta^{v\theta})T_2(\gamma^v) + (\mu + 1)(R_2(\beta^{v\theta})T_2(\gamma^{v\eta}) + T_2(\gamma^v) + T_2(\gamma^{v\eta})) + \mu R_2(\beta^v)T_2(\gamma^{v\eta}). \quad (10)$$

$$\text{将 } R_2(1) = (p-1)/2, T_2(1) = (q-1)/2 \text{ 代入 (10) 中有 } M_{U''}(1) = 0. \quad (11)$$

引理 5 设 $U''(t)$ 是 (4) 定义的序列在 \mathbb{F}_4 上对应的四元序列, $M_{U''}(x)$ 是其生成多项式. 则

$$(1) M_{U''}(\alpha^v) = \begin{cases} \mu + 1, & \text{若 } v \in P \text{ 且 } p \pmod{4} \equiv 1, \\ \mu, & \text{若 } v \in P \text{ 且 } p \pmod{4} \equiv -1. \end{cases}$$

$$(2) M_{U''}(\alpha^v) = \begin{cases} 0, & \text{若 } v \in Q \text{ 且 } q \pmod{4} \equiv 1, \\ \mu, & \text{若 } v \in Q \text{ 且 } q \pmod{4} \equiv -1. \end{cases}$$

证 设 $v \in P$, 则 $R_2(\beta^v) = (p-1)/2, R_2(\beta^{v\theta}) = (p-1)/2$. 若 $p \pmod{4} \equiv 1$, 则 $R_2(\beta^v) = 0$ 且 $R_2(\beta^{v\theta}) = 0$. 由 (10) 可得 $M_{U''}(\alpha^v) = (\mu + 1)(T_2(\gamma^v) + T_2(\gamma^{v\eta}))$. 由引理 1, $T_2(\gamma^{v\eta}) = \sum_{i \in B_0} \gamma^{v\eta i} = \sum_{i \in B_1} \gamma^{vi} = T_2(\gamma^v) + 1$, 则 $M_{U''}(\alpha^v) = \mu + 1$. 若 $p \pmod{4} \equiv -1$, 则 $R_2(\beta^v) = 1$ 且 $R_2(\beta^{v\theta}) = 1$. 由 (10) 可得 $M_{U''}(\alpha^v) = T_2(\gamma^v) + (\mu + 1)(T_2(\gamma^{v\eta}) + T_2(\gamma^v) + T_2(\gamma^{v\eta})) + \mu T_2(\gamma^{v\eta}) = \mu(T_2(\gamma^v) + T_2(\gamma^{v\eta}))$. 由 $T_2(\gamma^{v\eta}) = T_2(\gamma^v) + 1$ 可得, $M_{U''}(\alpha^v) = \mu$. $v \in Q$ 的情形类似可证.

引理 6 记号同上. 若 $v \in Z_N^*$, 则

$$M_{U''}(\alpha^v) = \begin{cases} R_2(\beta^\theta)T_2(\gamma) + (\mu + 1)(R_2(\beta^\theta)T_2(\gamma^\eta) + T_2(\gamma) + T_2(\gamma^\eta)) + \mu R_2(\beta)T_2(\gamma^\eta), & \text{若 } v \in F_{0,0}; \\ R_2(\beta)T_2(\gamma^\eta) + (\mu + 1)(R_2(\beta)T_2(\gamma) + T_2(\gamma) + T_2(\gamma^\eta)) + \mu R_2(\beta^\theta)T_2(\gamma), & \text{若 } v \in F_{1,1}; \\ R_2(\beta)T_2(\gamma) + (\mu + 1)(R_2(\beta)T_2(\gamma^\eta) + T_2(\gamma) + T_2(\gamma^\eta)) + \mu R_2(\beta^\theta)T_2(\gamma^\eta), & \text{若 } v \in F_{1,0}; \\ R_2(\beta^\theta)T_2(\gamma^\eta) + (\mu + 1)(R_2(\beta^\theta)T_2(\gamma) + T_2(\gamma) + T_2(\gamma^\eta)) + \mu R_2(\beta)T_2(\gamma), & \text{若 } v \in F_{0,1}. \end{cases}$$

证 若 $v \in F_{0,0}$, 则 $v \pmod{p} \in A_0$ 且 $v \pmod{q} \in B_0$, 则 $R_2(\beta^{v\theta}) = \sum_{i \in A_0} \beta^{v\theta i} = \sum_{i \in A_0} \beta^{\theta i} = R_2(\beta^\theta), T_2(\gamma^{v\eta}) = \sum_{i \in B_0} \gamma^{v\eta i} = \sum_{i \in B_0} \gamma^{\eta i} = T_2(\gamma^\eta), T_2(\gamma^v) = \sum_{i \in B_0} \gamma^{vi} = \sum_{i \in B_0} \gamma^i = T_2(\gamma)$ 且 $R_2(\beta^v) = \sum_{i \in A_0} \beta^{vi} = \sum_{i \in A_0} \beta^i = R_2(\beta)$. 则由 (10), $M_{U''}(\alpha^v) = R_2(\beta^\theta)T_2(\gamma) + (\mu + 1)(R_2(\beta^\theta)T_2(\gamma^\eta) + T_2(\gamma) + T_2(\gamma^\eta)) + \mu R_2(\beta)T_2(\gamma^\eta)$. 其余情形类似可证.

引理 7 记号同上, 则

(1) 若 $p \pmod{8} \equiv \pm 1$, 当 $q \pmod{8} \equiv \pm 1$ 或 $q \pmod{8} \equiv \pm 3$, 则

$$M_{U''}(\alpha^v) = \begin{cases} \mu + 1, & \text{若 } v \in F_{0,0}, \\ 0, & \text{若 } v \in F_{1,1}, \\ \mu, & \text{若 } v \in F_{1,0}, \\ 1, & \text{若 } v \in F_{0,1}. \end{cases} \text{ 或 } M_{U''}(\alpha^v) = \begin{cases} \mu, & \text{若 } v \in F_{0,0}, \\ 1, & \text{若 } v \in F_{1,1}, \\ \mu + 1, & \text{若 } v \in F_{1,0}, \\ 0, & \text{若 } v \in F_{0,1}. \end{cases}$$

(2) 若 $p \pmod{8} \equiv \pm 3$, 当 $q \pmod{8} \equiv \pm 1$ 或 $q \pmod{8} \equiv \pm 3$, 则

$$M_{U''}(\alpha^v) = \begin{cases} 0, & \text{若 } v \in F_{0,0}, \\ \mu + 1, & \text{若 } v \in F_{1,1}, \\ 1, & \text{若 } v \in F_{1,0}, \\ \mu, & \text{若 } v \in F_{0,1}. \end{cases} \text{ 或 } M_{U''}(\alpha^v) = \begin{cases} 1, & \text{若 } v \in F_{0,0}, \\ \mu, & \text{若 } v \in F_{1,1}, \\ 0, & \text{若 } v \in F_{1,0}, \\ \mu + 1, & \text{若 } v \in F_{0,1}. \end{cases}$$

证 对不同的情形, 证明方法是类似的, 因此只证明 $p \pmod{8} \equiv \pm 1$ 且 $q \pmod{8} \equiv \pm 1$ 的情形. 当 $p \pmod{8} \equiv \pm 1$ 且 $q \pmod{8} \equiv \pm 1$ 时, 由引理 1 和引理 6, 若 $v \in F_{0,0}$, 则 $M_{U''}(\alpha^v) = 0 + (\mu + 1)(1 + 0 + 0) + \mu \times 0 = \mu + 1$; 若 $v \in F_{1,1}$, 则 $M_{U''}(\alpha^v) = 0 + (\mu + 1)(0 + 1 + 1) + \mu \times 0 = 0$; 若 $v \in F_{1,0}$, 则 $M_{U''}(\alpha^v) = 1 + (\mu + 1)(1 + 0 + 0) + \mu \times 0 = \mu$; 若 $v \in F_{0,1}$, 则 $M_{U''}(\alpha^v) = 0 + (\mu + 1)(0 + 1 + 0) + \mu \times 1 = 1$.

定理 2 记号同上. 记 $H_1(x) = \prod_{t \in F_{0,0}} (x - \alpha^t)$, $H_2(x) = \prod_{t \in F_{1,1}} (x - \alpha^t)$, $H_3(x) = \prod_{t \in F_{1,0}} (x - \alpha^t)$, $H_4(x) = \prod_{t \in F_{0,1}} (x - \alpha^t)$ 且 $Q(x) = \prod_{t \in Q} (x - \alpha^t)$. 则 $U''(t)$ 的线性复杂度 $LC(U''(t))$ 和极小多项式 $m_{U''}(x)$ 如下:

(1) 若 $p \pmod{8} \equiv \pm 1$ 且 $q \pmod{8} \equiv 1$, 则

$$LC(U''(t)) = \frac{3pq - 3p + q - 1}{4}, m_{U''}(x) = \frac{x^{pq} - 1}{(x - 1)H_2(x)Q(x)};$$

(2) 若 $p \pmod{8} \equiv \pm 1$ 且 $q \pmod{8} \equiv -1$, 则

$$LC(U''(t)) = \frac{3pq + p + q - 5}{4}, m_{U''}(x) = \frac{x^{pq} - 1}{(x - 1)H_2(x)};$$

(3) 若 $p \pmod{8} \equiv \pm 1$ 且 $q \pmod{8} \equiv 3$, 则

$$LC(U''(t)) = \frac{3pq + p + q - 5}{4}, m_{U''}(x) = \frac{x^{pq} - 1}{(x - 1)H_4(x)};$$

(4) 若 $p \pmod{8} \equiv \pm 1$ 且 $q \pmod{8} \equiv -3$, 则

$$LC(U''(t)) = \frac{3pq - 3p + q - 1}{4}, m_{U''}(x) = \frac{x^{pq} - 1}{(x - 1)H_4(x)Q(x)};$$

(5) 若 $p \pmod{8} \equiv \pm 3$ 且 $q \pmod{8} \equiv 1$, 则

$$LC(U''(t)) = \frac{3pq - 3p + q - 1}{4}, m_{U''}(x) = \frac{x^{pq} - 1}{(x - 1)H_1(x)Q(x)};$$

(6) 若 $p \pmod{8} \equiv \pm 3$ 且 $q \pmod{8} \equiv -1$, 则

$$LC(U''(t)) = \frac{3pq + p + q - 5}{4}, m_{U''}(x) = \frac{x^{pq} - 1}{(x - 1)H_1(x)};$$

(7) 若 $p \pmod{8} \equiv \pm 3$ 且 $q \pmod{8} \equiv 3$, 则

$$LC(U''(t)) = \frac{3pq + p + q - 5}{4}, m_{U''}(x) = \frac{x^{pq} - 1}{(x - 1)H_3(x)};$$

表 2 p 和 q 取不同值时序列 $U''(t)$ 的线性复杂度

p	q	$LC(U''(t))$	$LC(U''(t))$ 满足	pq
29	19	424	$3pq + p + q - 5/4$	551
23	31	547	$3pq + p + q - 5/4$	713
19	43	627	$3pq + p + q - 5/4$	817
37	17	448	$3pq - 3p + q - 1/4$	629
7	43	237	$3pq + p + q - 5/4$	301

(8) 若 $p \pmod{8} \equiv \pm 3$ 且 $q \pmod{8} \equiv -3$, 则

$$LC(U''(t)) = \frac{3pq - 3p + q - 1}{4}, m_{U''}(x) = \frac{x^{pq} - 1}{(x-1)H_3(x)Q(x)}.$$

证 当 $p \pmod{8} \equiv \pm 1$ 且 $q \pmod{8} \equiv 1$ 时, 由引理 7, 有 $|\{v|v \in Z_N^*, M_{U''}(\alpha^v) = 0\}| = \frac{(p-1)(q-1)}{4}$, 又由引理 5, 有 $|\{v|v \in P, M_{U''}(\alpha^v) = 0\}| = 0$, $|\{v|v \in Q, M_{U''}(\alpha^v) = 0\}| = p-1$. 结合式 (11), 可得线性复杂度为 $LC(U''(t)) = pq - \frac{(p-1)(q-1)}{4} - (p-1) - 1 = \frac{3pq-3p+q-1}{4}$, 且极小多项式为 $m_{U''}(x) = \frac{x^{pq}-1}{(x-1)H_2(x)Q(x)}$. 其余情形类似可证.

利用 Magma 程序, 验证了取不同参数时 $U''(t)$ 的线性复杂度, 见表 2. 结果与定理 2 结论一致.

5 总结

由于代数结构的差异, \mathbb{Z}_4 和 \mathbb{F}_4 上序列的综合算法也略有差异. 本文分析了两类四元序列在 \mathbb{F}_4 上的线性复杂度和极小多项式. 证明了这两类四元序列在 \mathbb{F}_4 上的线性复杂度不小于其周期的一半, 即这两类序列具有高的线性复杂度. 因此这两类序列可以有效地抵抗 Berlekamp-Massey 算法的攻击.

参 考 文 献

- [1] Golomb S W, Gong G. Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar[M]. Cambridge: Cambridge University Press, 2005.
- [2] Helleseth T. Sequences with low correlation[J]. Handbook of Coding Theory, 1998, 2: 1765-1853.
- [3] Adachi F, Garg D, Takaoka S, Takeda K. Broadband CDMA techniques[J]. IEEE Wireless Communications, 2005, 12(2): 8-18.
- [4] Berlekamp E R. Nonbinary BCH decoding[J]. IEEE Transactions on Information Theory, 1968, 14(2): 242-242.
- [5] Massey J. Shift-register synthesis and BCH decoding[J]. IEEE Transactions on Information Theory, 1969, 15(1): 122-127.
- [6] Reeds J A, Sloane N J A. Shift register synthesis (modulo m)[J]. SIAM Journal on Computing, 1985, 14(3): 505-513.

- [7] Jiang Ting, Fu Fangwei. Some new classes of quaternary sequences with low autocorrelation property via two binary cyclotomic sequences[J]. *Journal of Applied Mathematics and Computing*, 2023, 69(1): 689–706.
- [8] Ding Cunsheng. Autocorrelation values of generalized cyclotomic sequences of order two[J]. *IEEE Transactions on Information Theory*, 1998, 44(4): 1699–1702.
- [9] Yang Zheng, Ke Pinhui. Construction of quaternary sequences of length pq with low autocorrelation[J]. *Cryptography and Communications*, 2011, 3(2): 55–64.
- [10] Edemskiy V, Ivanov A. Linear complexity of quaternary sequences of length pq with low autocorrelation[J]. *Journal of Computational and Applied Mathematics*, 2014, 259: 555–560.
- [11] Ma Jiang, Zhao Wei, Jia Yanguo, Jiang Haiyang. New generalized cyclotomic quaternary sequences with large linear complexity and a product of two primes period[J]. *Information*, 2021, 12(5): 1–9.
- [12] Zhang Chaoran, Jing Xiaoyan, Xu Zhefeng. The linear complexity and 4-adic complexity of quaternary sequences with period pq [J]. *Journal of Applied Mathematics and Computing*, 2023, 69(2): 2003–2017.
- [13] Krone S, Sarwate D. Quadriphase sequences for spread-spectrum multiple-access communication[J]. *IEEE Transactions on Information Theory*, 1984, 30(3): 520–529.
- [14] Zhao Lu. About the linear complexity of quaternary sequences with even length[J]. *Cryptography and Communications*, 2020, 12(4): 725–741.
- [15] Edemskiy V, Garbar S. The linear complexity of sequences with low autocorrelation from interleaved technique and period pq [A]. Lin Shu, 2022 IEEE Information Theory Workshop[C]. Piscataway, NJ: Institute of Electrical and Electronics Engineers, 2022: 303–308.
- [16] Ding Cunsheng, Hesseseth T, Shan Weijuan. On the linear complexity of Legendre sequences[J]. *IEEE Transactions on Information Theory*, 1998, 44(3): 1276–1278.

LINEAR COMPLEXITY OF TWO CLASSES OF QUATERNARY SEQUENCES WITH PERIOD pq OVER \mathbb{F}_4

YAN Fei-fei¹, KE Pin-hui²

(1. School of Mathematics and Statistics, Fujian Normal University, Fuzhou 350117, China)

(2. Key Laboratory of Analytical Mathematics and Applications of Ministry of Education (Fujian Normal University), Fuzhou 350117, China)

Abstract: In this paper, the linear complexity and minimal polynomial of two classes of quaternary sequences with period pq over \mathbb{F}_4 are investigated. By using the method of [10, 12], it is proved that these two classes of sequences have high linear complexity over \mathbb{F}_4 and thus can resist Berlekamp-Massey algorithm attack.

Keywords: Inverse Gray mapping; generalized cyclotomy; quaternary sequences; linear complexity

2010 MR Subject Classification: 94A55.