

Z_4 上周期为 $2p^2$ 的四元广义分圆序列的线性复杂度

杜小妮 赵丽萍* 王莲花

(西北师范大学数学与统计学院 兰州 730070)

摘要: 该文根据特征为4的Galois环理论, 在 Z_4 上利用广义分圆构造出一类新的周期为 $2p^2$ (p 为奇素数)的四元序列, 并且给出了它的线性复杂度。结果表明, 该序列具有良好的线性复杂度性质, 能够抗击Berlekamp-Massey (B-M)算法的攻击, 是密码学意义上性质良好的伪随机序列。

关键词: 流密码; 四元序列; 线性复杂度; 广义分圆类; Galois 环

中图分类号: TN918.4

文献标识码: A

文章编号: 1009-5896(2018)12-2992-06

DOI: 10.11999/JEIT180189

Linear Complexity of Quaternary Sequences over Z_4 Derived from Generalized Cyclotomic Classes Modulo $2p^2$

DU Xiaoni ZHAO Liping WANG Lianhua

(College of Mathematics and Statistics, Northwest Normal University, Lanzhou 730070, China)

Abstract: Based on the theory of Galois rings of characteristic 4, a new class of quaternary sequences with period $2p^2$ is established over Z_4 using generated cyclotomy, where p is an odd prime. The linear complexity of the new sequences is determined. Results show that the sequences have larger linear complexity and resist the attack by Berlekamp-Massey (B-M) algorithm. It is a good sequence from the viewpoint of cryptography.

Key words: Stream ciphers; Quaternary sequences; Linear complexity; Generalized classes; Galois rings

1 引言

伪随机序列在通信系统、雷达系统及流密码等方面有着极其广泛的应用^[1]。在密码学领域的应用中, 序列的线性复杂度性质是影响序列伪随机性的一个重要指标, 为了能够抵抗B-M(Berlekamp-Massey)算法的攻击, 一般要求序列的线性复杂度不小于其周期长度的一半。

已有大量文献研究了序列的线性复杂度, 其中文献[2-6]研究了二元序列的线性复杂度, 文献[7]确定了有限域 F_4 上一类四元序列的线性复杂度, 文献[8-10]计算了Galois环 $Z_4 = \{0, 1, 2, 3\}$ 上四元序列的线性复杂度, 文献[11]给出了 Z_4 上基于模 $2p$ (p 为奇素数)的广义分圆的一类四元序列的线性复杂度, 而周期为 $2p^2$ 的四元序列尚未研究。因

而, 本文在文献[11]的基础上进行了推广, 基于模 $2p^2$ 的广义分圆定义了一类 Z_4 上的新四元序列, 并求出了该序列的线性复杂度。值得一提的是, 由于 Z_4 上的零因子使得计算变得困难, 所以本文基于特征为4的Galois环理论来进行研究。

设 p 是奇素数, g 是奇数, 且 g 是模 p^2 和模 $2p^2$ 的公共本原元^[4]。设 S 是集合, 定义 $aS \triangleq \{au \pmod{2p^2} : u \in S\}$, $a + S \triangleq \{a + u \pmod{2p^2} : u \in S\}$ 。模 $2p^2$ 的剩余类环为 $Z_{2p^2} = \{0, 1, \dots, 2p^2 - 1\}$ 。对 $i = 0, 1$, 令 $D_i = \left\{ g^{2k+i} \pmod{2p^2}, k = 0, 1, \dots, \frac{p(p-1)}{2} - 1 \right\}$, 且 $E_i = 2D_i$, $P_0 = pZ_{2p}^*$, $P_1 = 2P_0$, 即有 $Z_{2p^2} = \bigcup_{i=1}^1 (D_i \cup E_i \cup P_i) \cup \{0, p^2\}$ 。显然, $D_0 \cup D_1 \cup P_0$ 是 $Z_{2p^2} \setminus \{p^2\}$ 中所有奇数的集合, $E_0 \cup E_1 \cup P_1$ 是 $Z_{2p^2} \setminus \{0\}$ 中所有偶数的集合。定义 Z_4 上的四元序列 (e_u) 为

$$e_u = \begin{cases} 0, & u = 0 \text{ 或 } u \in D_0 \\ 1, & u \in D_1 \cup P_0 \\ 2, & u = p^2 \text{ 或 } u \in E_1 \\ 3, & u \in E_0 \cup P_1 \end{cases}$$

下文将讨论序列 (e_u) 的线性复杂度^[13]。 (e_u) 的线性复杂度定义为满足 $e_{u+L} + c_1 e_{u+L-1} + \dots + c_{L-1} e_{u+1} + c_L e_u = 0, u \geq 0, c_1, c_2, \dots, c_L \in Z_4$ 的最小

收稿日期: 2018-02-11; 改回日期: 2018-08-13; 网络出版: 2018-08-27

*通信作者: 赵丽萍 marching666@126.com

基金项目: 国家自然科学基金(61462077, 61772022), 安徽省自然科学基金(1608085MF143), 上海市自然科学基金(16ZR1411200)

Foundation Items: The National Natural Science Foundation of China (61462077, 61772022), Anhui Province Natural Science Foundation (1608085MF143), Shanghai Municipal Natural Science Foundation (16ZR1411200)

正整数 L 。令 $C(x) = 1 + c_1x + \dots + c_Lx^L \in Z_4[x]$, 显然 $C(0) = 1$ 。设 (e_u) 的生成多项式为 $E(x) = e_0 + e_1x + \dots + e_{2p^2-1}x^{2p^2-1} \in Z_4[x]$, 则

$$\begin{aligned} \text{LC}(e_u) &= \min\{\deg(C(x)) : C(x) \in Z_4[x], \\ &C(0) = 1, E(x)C(x) \equiv 0 \pmod{x^{2p^2} - 1}\} \end{aligned} \quad (1)$$

2 主要结论及其证明

2.1 主要结论

定理 1 (e_u) 的线性复杂度满足

$$\text{LC}(e_u) = \begin{cases} 3p(p-1)/2 + 1, & p \equiv 3 \pmod{8} \\ 3p(p-1)/2 + 2, & p \equiv -3 \pmod{8} \\ 2p(p-1) + 1, & p \equiv -1 \pmod{8} \\ p(p-1) + 2, & p \equiv 1 \pmod{8} \end{cases}$$

2.2 辅助引理

本小节给出证明主要结论所需的引理。如无特殊说明, 本文中的多项式均属于 $Z_4[x]$ 。

设 r 为 2 模 p^2 的阶, 记 $\text{GR}(4^r, 4)$ 是阶为 4^r 且特征为 4 的 Galois 环, 同构于剩余类环 $Z_4[x] \setminus f(x)$, 其中 $f(x) \in Z_4[x]$ 是次数为 r 的基本不可约多项式^[14]。记 $\text{GR}(4^r, 4)$ 的单位群为 $\text{GR}^*(4^r, 4)$, 因为 $p^2 | (2^r - 1)$, 所以 $\text{GR}^*(4^r, 4)$ 包含了一个 $2^r - 1$ 阶的循环子群。任取 $\beta \in \text{GR}^*(4^r, 4)$, 且阶为 p^2 。取

$$\gamma = 3\beta \in \text{GR}^*(4^r, 4)$$

则 γ 的阶为 $2p^2$ 。由式 (1), 为确定 (e_u) 的线性复杂度, 需计算 $E(\gamma^v)$, $v = 0, 1, \dots, 2p^2 - 1$ 的值。

引理 1^[14] 设非零次多项式 $F(x) \in Z_4[x]$, 若 $\xi, \eta \in \text{GR}(4^r, 4)$ 满足 $F(\xi) = F(\eta) = 0$, 且 $\eta - \xi \in \text{GR}^*(4^r, 4)$, 则存在 $F_1(x), F_2(x)$ 使得 $F(x) = (x - \xi) \cdot F_1(x) = (x - \xi)(x - \eta)F_2(x)$, 其中 $F_1(x) = (x - \eta) \cdot F_2(x)$ 。

引理 2 (1) 若 $F(\gamma^v) = 0, v \in A$, 则存在 $F_A(x) \in \text{GR}(4^r, 4)[x]$ 使得

$$F(x) = F_A(x) \prod_{v \in A} (x - \gamma^v)$$

其中, A 取为 D_i , 或 E_i , 或 $P_i, i = 0, 1$ 。

(2) 若 $F(\gamma^v) = 0, v \in \{p^2\} \cup D_0 \cup D_1 \cup P_0$, 则存在 $F_3(x) \in \text{GR}(4^r, 4)[x]$ 使得 $F(x) = F_3(x)(x^{p^2} + 1)$ 。

(3) 若 $F(0) = 1, F(\gamma^v) = 0, v \in Z_{2p^2} \setminus \{0, p^2\}$, 且 $F(\pm 1) \in \{0, 2\}$, 则有 $\deg(F(x)) \geq 2p^2 - 1$ 。进一步, 若 $F(\pm 1) = 0$ 或 $F(\pm 1) = 2$, 则 $\deg(F(x)) \geq 2p^2$ 。

证明 (1) 只证 $A = D_i$ 的情形, 其它情形同理可得。由 γ 的选择, 有 $\frac{(x^{p^2} - 1)}{(x - 1)} = \prod_{m=1}^{p^2-1} (x - \gamma^{2m})$,

因此 $p^2 = \prod_{m=1}^{p^2-1} (1 - \gamma^m)(1 + \gamma^m)$, 所以当 $0 \leq m, n < 2p^2$ 且 $m \not\equiv n \pmod{p^2}$ 时, $\gamma^m - \gamma^n \in \text{GR}^*(4^r, 4)$, 从而, 当 $F(\gamma) = 0, m \in D_i$ 时, 由引理 1 得,

$$\prod_{m \in D_i} (x - \gamma^m) | F(x),$$

即该引理得证。

(2) 由 (1) 可得。

(3) 不妨设 $F(-1) = 0$ 。因为 $F(0) = 1$, 则由 (2) 得 $F(x) = (x^{p^2} + 1)F_3(x)$, 且 $2F_3(x) \neq 0$, 显然 $(x^{p^2} - 1) / (x - 1) | 2F_3(x)$, 从而 $\deg(F(x)) \geq 2p^2 - 1$ 。进一步, 若 $F(1) = 0$, 则 $\deg(F(x)) \geq 2p^2$ 。令 $F(\pm 1) \neq 0$, 则 $F(\pm 1) = 2$ 且 $F(\gamma^m) = 0, m \in D_0 \cup D_1 \cup P_0$ 。由 (1) 存在 $Q(x) \in Z_4[x]$, 使得 $F(x) = Q(x)(x^{p^2} + 1) / (x + 1)$, 且 $2Q(x) \neq 0$, 不难得到 $Q(-1) = 2$, 则存在 $G(x) \in Z_4[x]$ 使得 $Q(x) = (x + 1) \cdot G(x) + 2$, 即有, $F(x) = (x^{p^2} + 1) \cdot G(x) + 2(x^{p^2} + 1) / (x + 1)$ 。所以 $(x^{p^2} - 1) | 2F(x)$, 即有 $\deg(F(x)) \geq 2p^2$ 。 证毕

除特殊说明外, 本文中集合的下标均模 2, 且 $i, j \in \{0, 1\}$ 。

引理 3 (1) $v \in D_i$, 则 $vD_j = D_{i+j}, vE_j = E_{i+j}, vP_j = P_j$ 。

(2) 若 $v \in E_i$, 则 $vD_j = E_{i+j}, vP_j = P_1$, 且

$$vE_j = \begin{cases} E_{i+j}, & p \equiv \pm 1 \pmod{8} \\ E_{i+j+1}, & p \equiv \pm 3 \pmod{8} \end{cases}$$

(3) 若 $v \in P_0$, 则 $vD_j = P_0, vE_j = P_1, vP_j = P_j$ 。

(4) 若 $v \in P_1$, 则 $vD_j = vE_j = vP_j = P_1$ 。

(5) $P_0 = p^2 + P_1, P_1 = p^2 + P_0$ 。

(6) 若 $p \equiv \pm 1 \pmod{8}$, 则 $D_i = p^2 + E_i, E_i = p^2 + D_i$; 若 $p \equiv \pm 3 \pmod{8}$, 则 $D_{i+1} = p^2 + E_i, E_{i+1} = p^2 + D_i$ 。

证明 (1) 只证 $vD_j = D_{i+j}$, 其余同理可证。对任意给定的 $v \in D_i$, 若 $u \in D_j$, 则有 $v = g^{i+2k} \pmod{2p^2}, u = g^{j+2l} \pmod{2p^2}, 0 \leq k, l < \frac{p(p-1)}{2}$, 所以 $vu = g^{i+j+2(k+l)} \pmod{2p^2}$, 因此 $vu \in D_{i+j}$ 。又因为 $|vD_j| = |D_{i+j}|$, 所以 $vD_j = D_{i+j}$ 。

(2) 仅考虑 vE_j , 其余证明同 (1)。首先, 从 (1) 得 $vE_j = 2uE_j = 2E_{i+j}$ 。显然, 对任意的 $\omega \in 2E_{i+j}$, 有 $\omega \equiv 4a \pmod{2p^2}, a \in D_{i+j}$, 即 $\omega \in E_0 \cup E_1$, 则存在 $b \in D_0 \cup D_1$ 使得 $\omega = 2b \pmod{2p^2}$, 从而 $b \equiv 2a \pmod{p^2}$ 。当 $p \equiv \pm 1 \pmod{8}$, 即 2 是模 p 的平方剩余^[2], 则 $b \in D_{i+j}$, 从而 $\omega = 2b \in E_{i+j}$, 所以 $vE_j = 2E_{i+j} = E_{i+j}$; 当 $p \equiv \pm 3 \pmod{8}$ 时, 同理可证。

(3)~(6)显然。 证毕

在 $Z_4[x]$ 中, 令 $D_i(x) = \sum_{u \in D_i} x^u$, $E_i(x) = \sum_{u \in E_i} x^u$, $P_0(x) = \sum_{u \in P_0} x^u$, $P_1(x) = \sum_{u \in P_1} x^u$. 则

$$E(x) = 2x^{p^2} + D_1(x) + P_0(x) + 3E_0(x) + 2E_1(x) + 3P_1(x) \quad (2)$$

注意到在 $GR(4^r, 4)$ 上有

$$D_0(\gamma) + D_1(\gamma) + P_0(\gamma) = \sum_{u \in D_0 \cup D_1 \cup P_0} \gamma^u = 1$$

为计算 $E(\gamma^v)$, 需要如下几个引理。

引理 4 令 $\gamma \in GR^*(4^r, 4)$ 的阶为 $2p^2$, 则 $P_0(\gamma) = 1$ 。

证明 因为 $0 = \gamma^{2p^2} - 1 = (\gamma^p - 1)(P_0(\gamma) + P_1(\gamma) + 1 + \gamma^{p^2}) = (\gamma^{2p} - 1)(P_1(\gamma) + 1)$, 则由 γ 的定义得 $P_1(\gamma) = -1$, $P_0(\gamma) = 1$ 。 证毕

接下来计算 $D_0(\gamma)$ 。记 $[i, j] = |(1 + D_i) \cap E_j|$, $[i, 2] = |(1 + D_i) \cap P_1|$, $i, j \in \{0, 1\}$ 。

引理 5 符号含义同上, 则

$$[0, 0] = \begin{cases} p(p-5)/4, & p \equiv 1 \pmod{8} \\ p(p-3)/4, & p \equiv -1 \pmod{8} \\ p(p+1)/4, & p \equiv 3 \pmod{8} \\ p(p-1)/4, & p \equiv -3 \pmod{8} \end{cases}$$

$$[0, 1] = \begin{cases} p(p-1)/4, & p \equiv 1 \pmod{8} \\ p(p+1)/4, & p \equiv -1 \pmod{8} \\ p(p-3)/4, & p \equiv 3 \pmod{8} \\ p(p-5)/4, & p \equiv -3 \pmod{8} \end{cases}$$

$$[0, 1] = \begin{cases} p-1, & p \equiv 1 \pmod{4} \\ 0, & p \equiv 3 \pmod{4} \end{cases}$$

证明 记 $H_i = \{g^{2n+i} \pmod{p^2} : 0 \leq n < p \cdot (p-1)/2\}$, 且 $R = \{0, p, \dots, (p-1)p\}$ 。则

$$\begin{aligned} \{u \pmod{p^2} : u \in D_i\} &= H_i \\ \{2u \pmod{p^2} : u \in D_i\} &= H_{i+l} \\ \{u \pmod{p^2} : u \in P_1\} &= R \setminus \{0\} \end{aligned}$$

当 $p \equiv \pm 1 \pmod{8}$ 时, $l = 0$; 否则 $l = 1$ 。因此, $[i, j] = |(1 + H_i) \cap H_{j+l}|$, $[0, 2] = |(1 + H_0) \cap (R \setminus \{0\})|$ 。由 $|(1 + H_i) \cap H_j|$ 的取值^[15]。 证毕

引理 6 若 $p \equiv \pm 1 \pmod{8}$, 则 $p^2 + 2 \in D_0$; 否则 $p^2 + 2 \in D_1$ 。

证明 只证 $p \equiv \pm 1 \pmod{8}$ 时的情形。设 $p^2 + 2 \in D_1$, 则存在整数 q 使得 $p^2 + 2 \equiv g^{2n+1} + 2p^2 q$,

即 2 是模 p 的平方非剩余, 矛盾, 所以 $p^2 + 2 \in D_0$ 。 证毕

引理 7 令 $\omega_p = D_0(\gamma)$, 则

$$\omega_p = \begin{cases} 0 \text{ 或 } 1, & p \equiv 1 \pmod{8} \\ 2 \text{ 或 } 3, & p \equiv -3 \pmod{8} \\ 0 \text{ 或 } 3, & p \equiv 3 \pmod{4} \end{cases}$$

证明 只证 $p \equiv 1 \pmod{8}$ 时的情形, 其余情形同理可证。由于

$$\begin{aligned} (\omega_p)^2 &= \sum_{l,m=0}^{\frac{p(p-1)}{2}-1} \gamma^{g^{2l}+g^{2m}} = \sum_{l,m=0}^{\frac{p(p-1)}{2}-1} \gamma^{g^{2l}(g^{2(l-m)}+1)} \\ &= \sum_{m,n=0}^{\frac{p(p-1)}{2}-1} \gamma^{g^{2m}(g^{2n}+1)} \end{aligned} \quad (3)$$

且 $g^{2n} + 1 \pmod{2p^2} \in E_0 \cup E_1 \cup P_1 \cup \{0\}$ 。令

$$\lambda_n = \sum_{m=0}^{\frac{p(p-1)}{2}-1} \gamma^{g^{2m}(g^{2n}+1)}$$

下面分 3 种情况讨论:

(1) 令

$$N_i = \left\{ n, 0 \leq n < \frac{p(p-1)}{2}, g^{2n} + 1 \pmod{2p^2} \in E_i \right\}$$

则 $|N_i| = [0, i]$ 。当 $n \in N_i$, 由引理 3, 引理 6 有

$$\lambda_n = \sum_{v \in D_i} \gamma^{2v} = \begin{cases} (-1)^{i+1} \omega_p, & p \equiv \pm 1 \pmod{8} \\ (-1)^i \omega_p, & p \equiv \pm 3 \pmod{8} \end{cases}$$

(2) 令

$$N_2 = \left\{ n, 0 \leq n < \frac{p(p-1)}{2}, g^{2n} + 1 \pmod{2p^2} \in E_i \right\}$$

则 $|N_i| = [0, i]$ 。当 $n \in N_2$, 有

$$\lambda_n = \sum_{v \in P_0} \gamma^{2v} = P_0(\gamma^2) = P_0(-\gamma^{p^2+2}) = -P_0(\gamma)$$

(3) 若 $g^{2n} + 1 \equiv 0 \pmod{2p^2}$, 则 $p \equiv 1 \pmod{4}$ 且 $n = p(p-1)/4$, 因而 $\lambda_n = p(p-1)/2$ 。即: 由式 (3) 得 $(\omega_p)^2 = |N_0|(-\omega_p) + |N_1|\omega_p - |N_2| + p(p-1)/2$ 。又从引理 5 得 $(\omega_p)^2 = \omega_p$, 即 $\omega_p \in \{0, 1\}$ 。 证毕

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

$$E(\gamma^v) = \begin{cases} 2, & v \in D_0 \cup P_1 \\ 2\omega_p + 2, & v \in E_0 \cup E_1 \\ 0, & v \in D_1 \cup P_0 \end{cases}$$

否则

$$E(\gamma^v) = \begin{cases} 2\omega_p, & v \in D_0 \cup D_1 \\ 0, & v \in P_0 \cup P_1 \\ 2, & v \in E_0 \cup E_1 \end{cases}$$

(2) 当 $v = 0$ 时, $E(\gamma^v) = 3p^2 + p + 2$; 当 $v = p^2$ 时, $E(\gamma^v) = 2p$ 。

证明 仅证 (1) 中 $p \equiv \pm 3 \pmod{8}$ 的情形, 其余证明类似。对任意的 $v \in E_i \cup P_1$, 记 $v = 2\bar{v}$, 其中 $\bar{v} \in D_i \cup P_0$, 由引理 3 (5) 和 (6) 得, $p^2 + 2\bar{v} \in D_{j+1} \cup P_0$ 且有 $\gamma^v = \gamma^{2\bar{v}} = -\gamma^{p^2+2\bar{v}}$, 又由引理 3 (1) 可得

$$D_1(\gamma^v) = - \sum_{u \in D_1} \gamma^{u(p^2+2\bar{v})} = \begin{cases} -D_0(\gamma^\omega), & \bar{v} \in D_0 \\ -D_1(\gamma^\omega), & \bar{v} \in D_1 \\ -P_0(\gamma^\omega), & \bar{v} \in P_0 \end{cases}$$

进一步地, 由引理 3 可得, 当 $v \in Z_{2p^2} \setminus \{0, p^2\}$ 时, $P_0(\gamma^v) = (-1)^{v+1}, P_1(\gamma^v) = -1$; 且有

$$D_1(\gamma^v) = \begin{cases} (-1)^{i+1}\omega_p, & v \in D_i \cup E_i \\ (-1)^i, & v \in P_i \end{cases}$$

$$E_i(\gamma^v) = \begin{cases} (-1)^{i+j}\omega_p, & v \in D_j \cup E_{j+1} \\ -1, & v \in P_i \end{cases}$$

则根据式(2)结论得证。

定义

$$\Gamma_j(x) = \prod_{v \in D_j} (x - \gamma^v), \quad \Lambda_j(x) = \prod_{v \in E_j} (x - \gamma^v)$$

$$M(x) = \prod_{v \in P_0} (x - \gamma^v), \quad N(x) = \prod_{v \in P_1} (x - \gamma^v)$$

$$D_1(x) + 3E_0(x) = \begin{cases} -(x^{p^2} - 1)(-\omega_p + \Gamma_0(x) V_1(x)), & p \equiv \pm 3 \pmod{8} \\ (x - 1) \Gamma_0(x) \Gamma_1(x) N(x) V_2(x), & p \equiv \pm 1 \pmod{8} \end{cases}$$

$$P_0(x) + 3P_1(x) = \begin{cases} (x^{p^2} - 1)(-1 + \Gamma_1(x) V_3(x)), & p \equiv \pm 3 \pmod{8} \\ (x^{p^2} - 1) P_1(x), & p \equiv \pm 1 \pmod{8} \end{cases}$$

$$2x^{p^2} + 2E_1(x) = \begin{cases} 2(x^{p^2} - 1) + (x - 1)M(x)N(x) V_4(x), & p \equiv 3 \pmod{4} \\ 2(x^{p^2} - 1) + M(x)N(x) V_5(x), & p \equiv 1 \pmod{4} \end{cases}$$

证明 仅对 $p \equiv 3 \pmod{8}$ 的情形进行证明, 其余证明类似。由引理 3 得 $D_1(x) + 3E_0(x) = -(x^{p^2} - 1) D_1(x)$ 。由引理 8 可知, 当 $v \in D_0$ 时, 有 $D_1(\gamma^v) = -\omega_p$, 则存在 $V_1(x)$ 使得 $D_1(x) = -\omega_p + \Gamma_0(x) V_1(x)$ 。

注意到

引理 9 $M(x), N(x), \Gamma_j(x), \Lambda_j(x) \in Z_4[x]$ 。

证明 显然 $M(x), N(x) \in Z_4[x]$ 。仅考虑 $\Gamma_0(x)$, 对 $\Gamma_1(x), \Lambda_j(x)$ 同理可得。不难得到 $\Gamma_0(x)$ 的系数满足

$$a_m = (-1)^m \sum_{d_1 < \dots < d_m, d_1, \dots, d_m \in D_0} \gamma^{d_1 + \dots + d_m},$$

$$1 \leq m \leq p(p-1)/2$$

设 γ^b 为和式中的一项, $b \equiv \sum_{k=1}^m d_k \pmod{2p^2}$, $b \not\equiv 0 \pmod{p^2}$ 。由引理 3 易得

$$x - \gamma^{g^{2n} d_k} \prod_{v \in D_0} (x - \lambda^v)$$

所以 $\gamma^{g^{2n} d_1} \dots \gamma^{g^{2n} d_m} = \gamma^{g^{2n} b}$ 为和式的一项, 即 $\gamma^b + \gamma^{g^2 b} + \dots + \gamma^{g^{p(p-1)-2} b} = D_0(\gamma^b)$, 则存在 b_1, b_2, \dots, b_n 使得 $a_m = (-1)^m \sum_{k=0}^n D_0(\gamma^{b_k}) + l$, 其中 $l = \left\{ \begin{aligned} a \mid a \equiv \sum_{k=1}^m d_k \equiv 0 \pmod{p^2} \text{ 且 } d_1 < \dots < d_m, d_1, \dots, \\ d_m \in D_0 \end{aligned} \right\}$ 。又与引理 8 的证明类似可得 $D_0(\gamma^{b_k}) = \omega_p \in Z_4$ 。证毕

由于 γ^v 为 $x^{p^2} + 1$ 的根, $v \in \{p^2\} \cup D_0 \cup D_1 \cup P_0$, 则

$$x^{p^2} + 1 = (x + 1) \Gamma_0(x) \Gamma_1(x) M(x) \quad (4)$$

同样地, 有

$$x^{p^2} - 1 = (x - 1) \Lambda_0(x) \Lambda_1(x) N(x) \quad (5)$$

引理 10 存在 $V_k(x) \in Z_4[x], k = 1, 2, \dots, 5$, 使得

$$P_0(x) + 3P_1(x) = \sum_{u \in P_1} x^{u+p^2} + 3 \sum_{u \in P_1} x^u$$

$$= (x^{p^2} - 1) P_1(x)$$

且 $P_1(\gamma^v) = P_1(\gamma) = -1, v \in D_1$, 则结论易证。

因为 $2x^{p^2} + 2E_1(x) = 2(x^{p^2} - 1) + 2 + 2D_1(x^2)$ 。由引理 8 (1), 当 $v \in P_i$ 时, $2 + 2D_1(\gamma^v) = 0$, 则由

引理2, $2 + 2D_1(x) = M(x)N(x)G(x)$, 其中 $G(x) \in Z_4[x]$ 。即 $2 + 2D_1(x^2) = M(x^2)N(x^2)G(x^2)$ 。由引理3 (5)得 $N(x) = \prod_{v \in P_0} (x - \gamma^{v+p^2})$, 则 $N(x^2) = \prod_{v \in P_1} (x^2 - \gamma^v) = \prod_{v \in P_0} (x - \gamma^v) (x - \gamma^{p^2+u}) = M(x)N(x)$ 。

另一方面, $2 + 2E_1(1) = 0$, 则存在 $V_4(x)$ 使得 $M(x^2)G(x^2) = (x-1)V_4(x)$, 从而 $2x^{p^2} + 2E_1(x) = 2(x^{p^2} - 1) + (x-1)M(x)N(x)V_4(x)$ 。

综上, 即可得 $p \equiv 3 \pmod{8}$ 时的结论。证毕

引理 11 存在 $W_k(x) \in Z_4[x], k = 1, 2, \dots, 4$, 使得

$$E(x) = \begin{cases} (x-1)M(x)N(x)\Gamma_1(x)W_1(x), & p \equiv 3 \pmod{8} \\ M(x)N(x)\Gamma_1(x)W_2(x), & p \equiv -3 \pmod{8} \\ (x-1)M(x)N(x)W_3(x), & p \equiv -1 \pmod{8} \\ M(x)N(x)\Gamma_0(x)\Gamma_1(x)W_4(x), & p \equiv 1 \pmod{8} \end{cases}$$

证明 仅证明 $p \equiv 3 \pmod{8}$ 的情形, 其余证明同理。由引理10和式(5)可得 $E(x) = (x-1) \cdot N(x)H(x)$, 其中, $H(x) = \Lambda_0(x)\Lambda_1(x)(\omega_p+1-\Gamma_0(x) \cdot V_p(x) + \Gamma_1(x)V_p(x)) + M(x)V_p(x)$ 。

又由引理8易得若 $v \in D_0 \cup E_0 \cup E_1$, 则 $H(\gamma^v) \neq 0$; 若 $v \in D_1 \cup P_0$, 则 $H(\gamma^v) = 0$, 则由引理1可得, 存在 $W_1(x) \in Z_4[x]$ 且 $W_1(\gamma^v) \neq 0, v \in D_0 \cup E_0 \cup E_1$ 使得 $H(x) = M(x)\Gamma_1(x)W_1(x)$ 。证毕

2.3 定理1的证明

证明 若 $p \equiv 3 \pmod{8}$ 。由引理11和引理8 (2) 可得 $W_1(\gamma^v) \neq 0, v \in D_0 \cup E_0 \cup E_1 \cup \{p^2\}$, 从而

$$E(x)(x+1)\Gamma_0(x)\Lambda_0(x)\Lambda_1(x) \equiv 0 \pmod{x^{2p^2}-1}$$

所以 $LC(e_u) \leq 3p(p-1)/2 + 1$ 。又因为 $\gcd((x-1) \cdot M(x)N(x)\Gamma_1(x), (x+1)\Gamma_0(x)\Lambda_0(x)\Lambda_1(x)) = 1$, 所以由式(1), 式(4), 式(5)和引理11得 $W_1(x)C(x) \equiv 0 \pmod{(x+1)\Gamma_0(x)\Lambda_0(x)\Lambda_1(x)}$, 则有 $W_1(\gamma^v)C(\gamma^v) = 0, v \in \{D_0 \cup E_0 \cup E_1 \cup \{p^2\}\}$, 从而, 若 $W_1(\gamma^v) \in \text{GR}^*(4^r, 4)$, 则 $C(\gamma^v) = 0$; 若 $2W_1(\gamma^v) \in \text{GR}(4^r, 4) \setminus \{0\}$, 则 $2C(\gamma^v) = 0$ 。显然有 $(x+1)\Gamma_0(x)\Lambda_0(x) \cdot \Lambda_1(x) | 2C(x)$, 即 $LC(e_u) \geq \frac{3p(p-1)}{2} + 1$ 。因此, $LC(e_u) = \frac{3p(p-1)}{2} + 1$ 。

其它情形同理可证。

证毕

3 结束语

本文在 Z_4 上定义了一类周期为 $2p^2$ 的新四元广义分圆序列 (e_u) , 并研究了该序列的关联多项式和线性复杂度。结果表明, 当 $p \equiv 3 \pmod{4}$ 和 $p \equiv -3 \pmod{8}$ 时, 这类序列拥有好的线性复杂度, 能够抵抗B-M算法的攻击, 在保密通讯中可以有广泛的应用。此外, 若定义序列 (s_u) 为

$$s_u = \begin{cases} 0, & u = 0 \text{ 或 } u \in D_0 \\ 1, & u \in D_1 \cup P_0 \\ 2, & u = p^2 \text{ 或 } u \in E_1 \cup P_1 \\ 3, & u \in E_0 \end{cases}$$

与前面的证明类似可得, 该序列的线性复杂度达到最大值, 即当 $p \equiv 1 \pmod{4}$ 时, $LC(s_u) = 2p^2$; 否则 $LC(s_u) = 2p^2 - 1$ 。

参考文献

[1] GOLOMB S W and GONG Guang. Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar[M]. Cambridge: UK, Cambridge University Press, 2005: 174-175.

[2] 杜小妮, 王国辉, 魏万银. 周期为 $2p^2$ 的四阶二元广义分圆序列的线性复杂度[J]. 电子与信息学报, 2015, 37(10): 2490-2494. doi: 10.11999/JETT150180.

DU Xiaoni, WANG Guohui, and WEI Wanyin. Linear complexity of binary generalized cyclotomic sequences of order four with period $2p^2$ [J]. *Journal of Electronics & Information Technology*, 2015, 37(10): 2490-2494. doi: 10.11999/JETT150180.

[3] 李瑞芳, 柯品惠. 一类新的周期为 $2pq$ 的二元广义分圆序列的线性复杂度[J]. 电子与信息学报, 2014, 36(3): 650-654. doi: 10.3724/SP.J.1146.2013.00751.

LI Ruifang and KE Pinhui. The linear complexity of a new class of generalized cyclotomic sequences with period $2pq$ [J]. *Journal of Electronics & Information Technology*, 2014, 36(3): 650-654. doi: 10.3724/SP.J.1146.2013.00751.

[4] ZHANG Jingwei and ZHAO Changan. The linear complexity of a class of binary sequences with period $2p$ [J]. *Applicable Algebra in Engineering, Communication and Computing*, 2015, 26(5): 475-491. doi: 10.1007/s00200-015-0261-8.

[5] MA Xiao, YAN Tongjiang, ZHANG Daode, et al. Linear complexity of some binary interleaved sequences of period $4N$ [J]. *International Journal of Network Security*, 2016, 18(2): 244-249. doi: 10.6633/IJNS.201603.18(2).06.

[6] EDEMSKIY V and PALVINSKIY A. The linear complexity of binary sequences of length $2p$ with optimal three-level

- autocorrelation[J]. *Information Processing Letters*, 2016, 116(2): 153–156. doi: [10.1016/j.ipl.2015.09.007](https://doi.org/10.1016/j.ipl.2015.09.007).
- [7] DU Xiaoni and CHEN Zhixiong. Linear complexity of quaternary sequences generated using generalized cyclotomic classes modulo $2p$ [J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2011, 94(5): 1214–1217. doi: [10.1587/transfun.E94.A.1214](https://doi.org/10.1587/transfun.E94.A.1214).
- [8] CHEN Zhixiong. Linear complexity and trace representation of quaternary sequences over Z_4 based on generalized cyclotomic classes modulo[J]. *Cryptography and Communications*, 2017, 9(4): 445–458. doi: [10.1007/s12095-016-0185-6](https://doi.org/10.1007/s12095-016-0185-6).
- [9] EDEMSKIY V and IVANOV A. Linear complexity of quaternary sequences of length pq with low autocorrelation[J]. *Journal of Computational and Applied Mathematics*, 2014, 259B: 555–560. doi: [10.1016/j.cam.2013.08.003](https://doi.org/10.1016/j.cam.2013.08.003).
- [10] EDEMSKIY V and IVANOV A. The linear complexity of balanced quaternary sequences with optimal autocorrelation value[J]. *Cryptography and Communications*, 2015, 7(4): 485–496. doi: [10.1007/s12095-015-0130-0](https://doi.org/10.1007/s12095-015-0130-0).
- [11] CHEN Zhixiong and EDEMSKIY V. Linear complexity of quaternary sequences over Z_4 derived from generalized cyclotomic classes modulo[OL]. arXiv preprint arXiv: 1603.05086, 2016.
- [12] IRELAND K and ROSEN M. A Classical Introduction to Modern Number Theory[M]. Germany: Springer Science & Business Media, 2013: 83–120.
- [13] UDAYA P and SIDDIQI M U. Generalized GMW quadriphase sequences satisfying the Welch bound with equality[J]. *Applicable Algebra in Engineering, Communication and Computing*, 2000, 10(3): 203–225. doi: [10.1007/s002000050125](https://doi.org/10.1007/s002000050125).
- [14] WAN Zhexian. Finite Fields and Galois Rings[M]. Singapore, World Scientific Publishing Company, 2011: 23–25.
- [15] CUSICK T W, DING Gunsheng, and RENVALL A R. Stream Ciphers and Number Theory[M]. Dutch, Elsevier, 2004: 112–113.
- 杜小妮: 女, 1972年生, 教授, 博士生导师, 研究方向为密码学与信息安全.
- 赵丽萍: 女, 1993年生, 硕士生, 研究方向为密码学与信息安全.
- 王莲花: 女, 1980年生, 硕士生, 研究方向为密码学与信息安全.