arXiv:2305.00405v1 [cs.SC] 30 Apr 2023

关于 Rueppel 线性复杂度猜想

Graham H. Norton *

谨以此文深切缅怀 Gladys Jackson（1922—2012）

2023年5月2日

摘要

Dai 首次使用欧几里得算法证明了 Rueppel 猜想，该猜想涉及序列 (1, 1, 0, 1, 0_3, 1, 0_7, 1, 0_{15}, . . .) 的前 n 项的线性复杂度。我们此前已证明，可以为有理数域 $\mathbb{F}$ 上序列的前 n 项附加一个齐次（消去子）理想$\mathbb{F}[x, z]$，并为其构造一对生成形式。这种方法为 Rueppel 猜想提供了另一种证明。我们还证明了这些形式的其他性质，并推导出应用于前 n 项的 LFSR 综合算法的输出。此外，对首生成元去齐次化可得到 Dai 的最小多项式。

关键词：消去子、有限序列、形式、齐次理想、Macaulay 逆系统、线性复杂度。

1 引言

1.1 背景

据猜想 [17] （并通过直接计算验证了 $n \leq 128$ ），二进制序列 (1, 1, 0, 1, 0_3, 1, 0_7, 1, 0_{15}, 1, . . .) 具有完美线性复杂度剖面，即对于任意n，前 n 项的线性复杂度为 $\lfloor (n+1)/2 \rfloor$。根据 [4, 第441], 页，Massey 对 $n = 2^k - 1$ 和 $n = 2^k$验证了这一点。该猜想最早由 Dai 于 [4]证明。她的证明使用了欧几里得算法（扩展欧几里得算法）以及二元有限域（x）的二次扩张中的一个元素 ρ，但未说明其动机。 [4] 中的证明还需要欧几里得算法的一项额外性质，即 [4,命题 2], ，该命题在 [5, 引理 5]中得到证明。

关于另一种证明：对序列在二元有限域$[[x^{-1}]]$上的形式（逆）幂级数应用连分数算法，见 [12, 推论 2]。部分商始终为 x。不过，在 [11], [12] 中，还涉及收敛性和无理性方面的考量，分母和分子则通过多项式除法得到。

*昆士兰大学数学与物理学院，澳大利亚昆士兰州布里斯班 4072。（电子邮件: ghn@maths.uq.edu.au）

线性反馈移位寄存器综合算法出自 [10]；另见 [6, 第 9.9] 节。 [18,第 46–47] 页中，通过线性反馈移位寄存器综合算法推导 $n = 2^k$ 的“连接多项式”。不过， [18] 假定了这一关键结果： Δ_k “差异” k 是二元有限域中的剩余类。据我们所知，尚未有人使用线性反馈移位寄存器综合算法完全证明该猜想（但请参见推论 4.12）。

已知序列的 $2t$项以及其线性复杂度的上界 t 时，可以使用 Berlekamp 解码算法 [2, 算法 7.4] 来求出序列的线性复杂度。 [9,第 441–444] 页和 [7] 中的最小多项式算法也同样如此。然而，这些算法都无法从头开始确定序列的线性复杂度；例如参见例 3.7。我们注意到， [14, 算法 4.2] 无需假设线性复杂度的上界 t 以及序列的 $2t$项，即可确定有理逼近序列。

1.2 概述

令 $n \geq 1$ 和 $(r_0, \ldots, r_{n-1})$ 为该序列的前 n 项。我们直接处理 $(r_0, \ldots, r_{n-1})$，并研究其在 [15] 中定义的“湮灭理想” $\mathcal{I}_{n-1}$ ，从而给出该猜想的完整证明。与 [10] 的线性反馈移位寄存器综合算法相比，相应的算法更容易理解和记忆。我们的主要结果是，在这种归纳式、无算法的构造中，$\Delta_k = \overline{k} \in$ 二元有限域，或者等价地说，“中间移位”为 x ，当且仅当 k 为奇数；见定理 4.4。这带来了 $\mathcal{I}_{n-1}$ 的生成元形式、该猜想的证明、这些理想的其他性质，以及 [4], 推论 5.1 中主定理的一个简短证明。我们以 $(r_0, \ldots, r_9)$ 及其逆形式 $R^{(-9)}$ 为贯穿示例，见例 4.3。

我们的方法更简单：（i）它是归纳式的，会随序列的下一项调整，因此无需像 [4] 那样一开始就考虑所有的（$r_0, \ldots, r_{n-1}$）；（ii）我们不假设存在像 [4] 中的 ρ 这样的元素；（iii）我们使用 $\mathbb{F}[x^{-1}, z^{-1}]$ 和 $\mathbb{F}[x, z]$中的形式，因此无需考虑收敛性或无理性；（iv）我们只处理分母；（v）我们不假设序列的线性复杂度有上界 t ，也不对序列的$2t$ 项作此假设。我们的“中间移位”类似于 [11], [12]的部分商。由此得到的针对（$r_0, \ldots, r_{n-1}$）的算法无需除法或乘法，所需操作不过是对 n进行奇偶性检验；见下文部分（a）和算法 4.13。

更具体地说，前置的第2节讨论了双变量中的 Macaulay“逆系统”以及我们如何对其进行改造。设 $\mathbb{F}$ 是任意一个域。变量 x^{-1}、z^{-1} 中的“逆级数” $\mathbb{F}[[x^{-1}, z^{-1}]]$ 组成的 $\mathbb{F}[x, z]$ 模称为 Macaulay 逆系统（双变量情形）。现在， $\mathbb{F}[x^{-1}, z^{-1}]$ 是 $\mathbb{F}[[x^{-1}, z^{-1}]]$ 的一个 $\mathbb{F}[x, z]$ 子模；参见定义 2.1, [13]。因此，一个“逆形式”，即一个形式 $F \in \mathbb{F}[x^{-1}, z^{-1}]^{\times}$ ，具有一个（齐次）湮灭理想[1]$\mathcal{I}_F \subseteq \mathbb{F}[x, z]$。这一基本代数结构构成了我们线性反馈移位寄存器综合算法的基础：用逆形式替代有限序列，用湮灭形式替代特征多项式，见定理 2.4。

[1] （$s_0, \ldots, s_{n-1}$）的逆形式被称为其生成形式，其湮灭理想在 [1]中的定义有所不同；在 [15, 附录] 中，我们证明了这两个理想相同。

第3节回顾了 [16] 的归纳构造：即构造一对形式 (f, g)，称为“可行有序对（VOP）”，它们生成 $\mathcal{I}_F$；其中 z 不整除 f 的分级字典序（grlex）首项（我们称 f 为“首极小形式”）；z 整除 g 和 $|f| + |g| = 2 - |F|$，其中 $|\ |$ 表示总次数。此方法随后在 [16] 中得到了进一步简化和扩展；参见定理 3.3 、相应的 $\mathcal{O}$（$|F|^2$）算法，以及该算法在 $\mathbb{Q}$ 上的应用示例（例 3.7 ）。

我们还介绍了该构造的若干新特性，例如 $\mathcal{I}_F$ 的最低次数首形式集合，以及 f与 g 始终互素这一事实。

第 4 节专门讨论 $\mathbb{F}$ =二元有限域和 Rueppel 猜想。我们应用构造得到一个 $\mathcal{I}_{n-1}$ 的 VOP。我们的归纳基为 $(f^{(0)}, g^{(0)}) = (x + z, z)$，并证明对于 $k \geq 0$

(a) 二元有限域上的关键结果 $\Delta_k = \overline{k} \in$；等价地，我们有以下两种情况之一：(i) $(f^{(k+1)}, g^{(k+1)}) = (xf^{(k)} + g^{(k)}, zf^{(k-1)})$，若 $k+1$为偶数；或 (ii) $(f^{(k+1)}, g^{(k+1)}) = (f^{(k)}\, zg^{(k)})$ (b) $(f^{(k+1)}\ g^{(k+1)})$ 是一个 V OP f或 $\mathcal{I}_{k+1}$

(c) $|f^{(k+1)}| = \lfloor (k+3)/2 \rfloor$ 是（$r_0, \ldots, r_{k+1}$）的线性复杂度

(d) 或者存在唯一的最低次数首项形式，即 $f^{(k+1)}$(若 $k+1$ 为奇数)，或者最低次数的首形式恰为 $f^{(k+1)}$和 $f^{(k+1)} + g^{(k+1)}$

(e) $f^{(k+1)}(0, 1) = g^{(k+1)}(0, 1) = 1$，因此 f 的倒数 $^{(k+1)}(x, 1)$ 的次数为 $|f^{(k+1)}|$.

部分（C）证明了 Rueppel 猜想。部分（C）和部分（E）意味着，将线性反馈移位寄存器综合算法应用于 $(r_0, \ldots, r_{2k-1})$，将输出 k 和 $f^{(2k-1)}(x, 1)$ 的倒数。部分（A）意味着，对于 $f^{(2k-1)}(x, 1)$，存在一个递推关系，其特征多项式为 $Y^2 + xY + 1 \in \mathbb{F}(x)[Y]$，这促使我们在 $\mathbb{F}(x)$ 的扩域中使用其根 $\rho^{\pm 1}$。求解这一递推关系可得

$$x\, f^{(2k-1)}(x, 1) = (1 + \rho)\rho^k + (1 + \rho^{-1})\rho^{-k}.$$

最后，对于 $k \geq 1$，按照 [4] 中的方法，使用扩展欧几里得算法为 $(r_0, \ldots, r_{2k-1})$ 求得 $c_k \in \mathbb{F}[x]$。同上所引的引理 3 蕴含 c_k 满足同一递推关系，因此 $c_k(x) = f^{(2k-1)}(x, 1)$。这也简化了 [4] 中主定理的证明，并蕴含若 $k \geq 0$ 且 $l = 2^k$，则

$$f^{(2l-1)}(x, z) = x^l + \sum_{j=0}^{\log_2 l} x^{l-2^j} z^{2^j}.$$

2 预备知识

2.1 符号

一般而言，$\mathbb{F}$ 是一个任意域，且 $\mathrm{R} = \mathbb{F}[x, z]$。R 中的乘法用并置表示。对于 $\varphi, \varphi' \in \mathrm{R}$ 和 $k \in \mathbb{N}^{\times}$，$x^k \varphi + \varphi'$，表示 $x^k \varphi(x, z) + \varphi'(x, z)$，$\varphi + \varphi' z^k$ 也类似。$\varphi \in \mathrm{R}^{\times}$ 的总次数为 $|\varphi|$，其中 $|x| = |z| = 1$。由 $\varphi, \psi \in \mathrm{R}$ 生成的理想记作 $\langle \varphi, \psi \rangle$。

对于逻辑陈述 P, Q, A, B，我们通常将“$(P \| Q)$ 当且仅当 $(A \| B)$”简写为“(P 当 A 时)”和“(Q 当 B 时)”。例如，“中间位移为 $(x^d \| 1)$ 当且仅当 k 为（奇数||偶数）”。

We 还包括常用符号的参考表，以帮助读者。

符号	含义
R	$\mathbb{F}[x,z]$
d_k	$\lvert g^{(k)}\rvert - \lvert f^{(k)}\rvert \in \mathbb{Z}$
$\lvert f\rvert$	形式 $f \in$R$^\times$ 的总次数
$(f^{(k)}, g^{(k)})$	$\mathcal{I}_k$的构造的可行有序对（VOP）
F	M$^\times$ 中的一个逆形式
$\mathbb{F}$	域
$\mathcal{I}_F$	逆形式 F 的湮灭理想
k	中间变量
$\mathcal{L}$	首一非零（首项）形式的集合 φ，其中 $z \nmid$LT(φ)。
M	R-模 $\mathbb{F}[x^{-1}, z^{-1}]$
n	$(s_0, \ldots, s_{n-1})$ 的长度
$(r_0, r_1, \ldots)$	无限二进制序列
$R^{(1-n)}$	$r_{n-1}x^{1-n} + r_{n-2}x^{2-n}z + \cdots + r_0 z^{1-n}$
v(F)	$F \in$M$^\times$ 的阶

希腊字母符号	含义
$\Delta_k = \Delta\ (f^{(k)};\ R^{(-1-k)})$	$f^{(k)}$ 和 $R^{(-1-k)}$的差异
λ_n	$\lvert f_{\ (n-1)}\rvert$
φ, ψ	R$^\times$中的形式
$\varphi \circ F$	作用于 F的形式 φ
ρ	$\mathbb{P}$中的 Y 剩余类。

2.2 Rand Grlex

与 [15]，中一样，我们用 $\succ$ 表示 R$^\times$ 的单项式上的分次字典序（grlex），其中 $|x| = |z| = 1$ 和 $x \succ z \succ 1$。形式 $\varphi \in$ R 的首项记作 LT(φ)。我们定义 $\mathcal{L}$ 为“首项形式”集合:

$$\mathcal{L} = \{\varphi \in \mathrm{R}^\times : \varphi \text{ is a form and } z \nmid \mathrm{LT}(\varphi)\}.$$

我们还使用 $|\ |$ 表示 $\mathbb{F}[x]$上的次数函数，其中 $|0| = -\infty$。回顾一下，$c \in \mathbb{F}[x]^\times$ 的齐次化是形式 $c^\wedge \in$ R，定义为 $c(x,z) = z^{|c|}c(x/z)$；而 $f \in$R$[x,z]^\times \cap \mathcal{L}$的去齐次化是 $f^\vee(x) = f(x,1) \in \mathbb{F}[x]$。于是 $|c^\wedge| = |c|$且$|f^\vee| = |f|$。

2.3 逆形式

在全文中，$F \in$M$^\times$ 表示一个总次数为 $m = |F| \le 0$的典型非零逆形式。

我们还使用 grlex 对 M$^\times = \mathbb{F}[x^{-1}, z^{-1}]^\times$ 中的单项式进行排序，现记为 $\prec$，但满足 $|x^{-1}| = |z^{-1}| = -1$ 和 $x^{-1} \prec z^{-1} \prec 1$。

如果 F也是一个形式，即一个逆形式，我们记作 $F = \sum_{j=m}^{0} F_{j,\ m-j}x^j z^{m-j}$；当 m已知时，我们用 F_j 表示 $F_{j,\ m-j}$。我们将使用指数赋值的一个限制

v 来处理逆形式： F的阶为 $\mathrm{v} = \mathrm{v}(F) = \max\{j : |F| \le j \le 0, F_j \neq 0\}$。用 $a \in \mathbb{F}$ 增广 F 得到 $ax^{m-1} + Fz^{-1}$，这是一个总次数为 $m-1$的逆形式。例如，用 a 增广 z^m 得到 $a\,x^{m-1} + z^{m-1}$。形式 F 通过 $\{F^{(j)}$ 定义逆子形式： $m \le j \le \mathrm{v}\}$ by $F_{(\mathrm{v})} = x^{\mathrm{v}}$ 和

$$F^{(j)} = F_j x^j + F^{(j+1)} z^{-1} = F_j x^j + \cdots + x^{\mathrm{v}} z^{j-\mathrm{v}} \text{for } m \le j \le \mathrm{v} - 1.$$

我们注意到，对于任意 $j \le 0$, $z^j(\circ F\, z^{-j}) = F$。

在全文中， $n \ge 1$ 和（$s_0, \ldots, s_{n-1}$）是一个由 $\mathbb{F}$中的元素构成的非零序列。因此，$F = s_{n-1}x^{1-n} + \cdots + s_0 z^{1-n}$是（$s_0, \ldots, s_{n-1}$）的逆形式，$s_{-\mathrm{v}(F)}$ 对应于该序列中的第一个非零项， $a\,x^{m-1} + Fz^{-1}$ 对应于增广序列（$s_0, \ldots, s_{n-1}, a$）， 而 F的逆子形式对应于（$s_{-\mathrm{v}(F)}, \ldots, s_{n-1}$）的初始子序列。

2.4 逆多项式模 M

我们回顾一下文献 [13] 中的逆多项式 R-模 $\mathrm{M} = \mathbb{F}[x^{-1}, z^{-1}]$ 。

定义 2.1 对于非负整数 p, q, u, v

$$x^p z^q \circ x^{-u} z^{-v} = \begin{cases} x^{p-u} z^{q-v} & \textit{if } p-u \le 0, q-v \le 0 \\ 0 & \textit{otherwise.} \end{cases} \tag{1}$$

R 模 M 的模结构可通过将 (1) 线性扩展到整个 R 和 M 而得到 .

由线性性可知，不失一般性，我们可以假设一个逆形式 F 满足$F_{\mathrm{v}} = 1$，即 $F = F_m x^m + \cdots + F_{\mathrm{v}-1} x^{\mathrm{v}-1} z^{m-\mathrm{v}+1} + x^{\mathrm{v}} z^{m-\mathrm{v}}$。模 M 是 Macaulay 的“逆系统” $\mathbb{F}[[x^{-1}, z^{-1}]]$ 的一个 R 子模，但我们不需要这一事实；详情请见[13]。

逆形式 F 的湮灭理想为

$$\mathcal{I}_F = \{\varphi \in \mathrm{R} : \varphi \circ F = 0\}.$$

命题 2.2（*[15,* 命题 3.*7]*）理想 $\mathcal{I}_F$ 是齐次的。

命题 2.3（*[15,* 引理 3.*1]*）对于形式 $\varphi \in \mathrm{R}$ 和 $F \in \mathrm{M}$，若 $d = |\varphi| + |F|$满足以下条件之一：(i) $d > 0$ 且 $\varphi \circ F = 0$，或 (ii)

$$\varphi \circ F = \sum_{j=d}^{0} [\varphi \cdot F]_j\, x^j z^{d-j}.$$

因此，如果 $n > -|F|$，我们显然有 $x^n \in \mathcal{I}_F$。

2.5 双射

接下来，我们详细说明序列的特征多项式与其逆形式 F（下文称为 [14,）的首项湮灭形式之间的双射。这需要采用 [4] 中定义 2.7], [1] 所述的特征多项式定义（其中序列按负数索引）。我们按照自然顺序使用多项式系数，而不采用顺序相反的“反馈系数”，也不使用工程学文献中的“移位寄存器”。这个定义使我们能够展示序列的特征多项式集合与 R 的齐次理想 $\mathcal{I}_F$ 的首形式之间存在双射。

设 $(s_0, \ldots, s_{n-1})$ 是一个序列。那么，如果 c 是首一的且满足 (i) $l = |c| \geq n$ 或 (ii), 则 $c \in \mathbb{F}[x]^\times$ 是 $(s_0, \ldots, s_{n-1})$ 的特征多项式

$$c_l s_{k+l} + \cdots + c_0 s_k = 0 \text{ for } 0 \leq k \leq n - l - 1. \tag{2}$$

我们定义集合

$$\chi(s_0, \ldots, s_{n-1}) = \{c \in \mathbb{F}[x]^\times : c \textit{ is a characteristic polynomial of } (s_0, \ldots, s_{n-1})\},$$

它不是一个理想。

由于 x^n 是 $(s_0, \ldots, s_{n-1})$ 的一个（平凡地）特征多项式，$\chi(s_0, \ldots, s_{n-1})$ 非空，并且

$$\lambda = \lambda(s_0, \ldots, s_{n-1}) = \min\{|c| : \ c \in \chi(s_0, \ldots, s_{n-1})\}$$

是定义良好的。因此，$(s_0, \ldots, s_{n-1})$ 的最小多项式，即 $\lambda = \lambda(s_0, \ldots, s_{n-1})$ 的最低次数特征多项式，是定义良好的，并称为 $(s_0, \ldots, s_{n-1})$ 的线性复杂度。注意，在 [4], 中，$(s_0, \ldots, s_{n-1})$ 的特征多项式记作 c_n，也就是说，它按序列的长度编号，而不是按序列的最后一项编号。

回忆一下，$\mathcal{L}$ 是 R 中首一首项形式的集合，即满足 $z \nmid \mathrm{LT}(\varphi)$ 的 φ。如果 F 是逆形式，则 $x^{1-|F|} \in \mathcal{I}_F^\times \cap \mathcal{L}$。因此 $\mathcal{I}_F^\times \cap \mathcal{L} \neq \emptyset$，我们可以考虑 $\mathcal{I}_F^\times \cap \mathcal{L}$ 中总次数最小的形式。于是定义

$$\lambda_F = \min\{|f| : \ f \in \mathcal{I}_F^\times \cap \mathcal{L}\}$$

并称 λ_F 为 F 的线性复杂度。

定理 2.4 设 $(s_0, \ldots, s_{n-1})$ 是一个逆形式为 $F \in \mathbf{M}^\times$ 的序列。那么 $\wedge, \vee$ 是互为保次数双射的对象。

$$\wedge : \chi(s_0, \ldots, s_{n-1}) \leftrightarrows \mathcal{I}_F^\times \cap \mathcal{L} : \vee$$

由 $\wedge(c) = c^\wedge$ 和 $\vee(f) = f^\vee$，使得对于 $c \in \chi(s_0, \ldots, s_{n-1})$，$|\wedge(c)| = |c|$，并且对于 $f \in \mathcal{I}_F^\times \cap \mathcal{L}$，$|\vee(f)| = |f|$。因此 $\lambda(s_0, \ldots, s_{n-1}) = \lambda(F)$。

证明。我们有 $|F| = 1 - n$ 和 $|c^\wedge| = |c| = l$。由命题 2.3，$c^\wedge \circ F = 0$ 当且仅当 $[c^\wedge \cdot F]_j = 0$ 对 $l + |F| \leq j \leq 0$成立。现在，$c \in \chi(s_0, \ldots, s_{n-1})$ 当且仅当 c满足 (2)；将 k代入 $-j$，可见方程 (2) 等价于 $[c^\wedge \cdot F]_j = 0$ 对

$l+|F| \le j \le 0$，即等价于 $c^\wedge \in \mathcal{I}_F \cap \mathcal{L}$。这意味着 $c \in \chi(s_0,\dots,s_{n-1})$ 当且仅当 $c^\wedge \in \mathcal{I}_F^\times \cap \mathcal{L}$；我们得到了所需的双射，因此 $\lambda(s_0,\dots,s_{n-1}) = \lambda(F)$。
□

注 2.5 我们不使用方程 (2)，而是采用等价的 l 和“连接”多项式 $\gamma \in \mathbb{F}[x]^\times$，使其满足

$$\gamma_0 s_j + \cdots + \gamma_l s_{j-l} = 0 \text{ for } l \le j \le n-1$$

其中 $\gamma_0 = 1$ 和 γ_l 可以为零（令 $j = k+l$ 和 $\gamma(x) = \tilde{c}(x) = x^l \cdot c(x^{-1})$ 为 c 的倒数，并将其化为首一形式）。然后，线性反馈移位寄存器综合算法返回 l 和 γ。遗憾的是，这种表述方式（使用倒数多项式）削弱了我们的代数方法。

下一节将回顾如何在 $\mathcal{L}$ 中从 $\mathcal{I}_F$ 构造 f 的一个生成元，因此我们自动得到 F 的一个最小湮灭子，进而得到 $(s_0,\dots,s_{n-1})$ 的一个最小多项式 $f^\vee$。负指标序列的最小多项式，以及计算这些多项式及其对应分子的算法，已在 [14] 中研究。

3 可行有序对

3.1 归纳构造与算法

我们回顾如何从 [15] 为 $\mathcal{I}_F$ 构造一对生成形式，并给出一个算法运行的示例。此构造采用迭代方式，具有简单的归纳基（命题 3.1）和不繁琐的归纳步骤（定理 3.3）。

设 F 是一个逆形式。若形式的有序对 $(f,g) \in \mathrm{R}^2$ 满足以下条件，我们称其为 $\mathcal{I}_F$ 的可行有序对（VOP）：
(i) f,g 是非零首一形式，$f \in \mathcal{L}$ 和 $z|g$；(ii) $\mathcal{I}_F = \langle f,g\rangle$（我们称 f 为首生成元，称 g 为 $\mathcal{I}_F$ 的余生成元）；(iii) $|f|+|g| = 2-|F|$。

P命题 3.1（*[15, 命题 3.8]*）若 $F = x^m$，则 $\mathcal{I}_F = \langle x^{1-m}, z\rangle$。

读者可以验证，$(f,g) = (x^{1-m}, z)$ 是 $\mathcal{I}_{x^m}$ 的可行有序对（VOP）。若 $f \in \mathcal{I}_F \cap \mathcal{L}$，我们称 f 为 $\mathcal{I}_F$ 的首项形式。

给定 $\mathcal{I}_F$ 的一个可行有序对（VOP）(f,g)，以及某个 $a \in \mathbb{F}$ 的 $G = ax^{m-1} + Fz^{-1}$，我们需要知道如何构造 $\mathcal{I}_G$ 的一个可行有序对（VOP）(φ,ψ)。这需要引入“差异”的概念，以说明 a 和 $\mathcal{I}_F$ 如何影响 $\mathcal{I}_G$。这是我们对 [10] 中引入的“差异”概念的类比；它是将 f 扩展为 $\mathcal{I}_G$ 的首项形式的障碍。

定义 3.2 如果 $f \in \mathcal{I}_F^\times$ 是一种形式，且 $G = ax^{m-1} + z^{-1}F$，那么 f 与 G 的差异为

$$\Delta(f;G) = [f \cdot G]_{(|f|+|G|,0)} \in \mathbb{F} \quad \text{if } |f|+|G| \le 0$$

以及 $\Delta(f;G) = 0$ 否则。

归纳步骤如下:

定理 3.3（*[15,* 命题 4.6，定理 4.*12]*）设 (f,g) 是 $\mathcal{I}_F$, $a\in\mathbb{F}$和 $G=ax^{|F|-1}+Fz^{-1}$的 VOP。假设 $g\notin\mathcal{I}_G$并令 $\Delta'=\Delta(g;\,G)\in\mathbb{F}^\times$, $d=|g|-|f|$,$\Delta=\Delta(f;\,G)\in\mathbb{F}$。若 $\Delta=0$，令 $(\varphi,\psi)=(f,zg)$ 且 $d=d+1$。

但若 $\Delta\neq 0$，令 $q=\Delta/\Delta'$ 并

$$(\varphi,\psi)=\begin{cases}(f-q\,x^{-d}g,\,z\,g) & if\ d\le 0\\ (x^{+d}f-q\,g,\,zf) & otherwise.\end{cases}$$

则 (φ,ψ) 是 G 的 VOP，并且显然，若 $d\le 0$ 则 $|\varphi|=|f|$，否则 $|\varphi|=|g|$。特别地，$|\varphi|=\max\{|g|,|f|\}$。

对于下一次迭代，(i) $e=|\psi|-|\varphi|=1$ 若 $\Delta=0$ 且 $e=1-|d|$ 若 $\Delta\neq 0$ (ii) 若 $d>0$, $b\in\mathbb{F}$ 且 $\Delta(\varphi;\ b\,x^{|G|-1}+Gz^{-1})\neq 0$，则令 $\Delta'=\Delta$，否则 Δ' 保持不变。

注记 3.4 (i) 标准初始化为 $(f,g)=(1,0)$，从而当 $F_0=0$ 时得到 $\mathcal{I}_{F^{(0)}}=\mathrm{R}$，但在此情况下 $|f|+|g|=2-m$ 会失败。因此，我们先求出 $\mathrm{v}(F)$，并使用 $(f,g)=(x^{1-\mathrm{v}(F)},z)$ 的构造进行初始化。例如，$\mathcal{I}_{F^{(0)}}=\langle x,z\rangle$ 当 $F_0\neq 0$ 时。

(ii) 给定一种形式 F，我们迭代该构造，以确定 $\mathcal{I}_{F^{(j)}}$ where$m\le j\le\mathrm{v}$ 和 $F^{(m)}=F$ 的一个 VOP。

(iii) 迭代应用该构造不需要以某个特定的 VOP 初始化；我们可以用 $F^{(j)}$ 的任意已知 VOP (f,g) 初始化。

(iv) 若 $\mathbb{F}=$ 属于二元有限域，我们可以省去 Δ'。

(v) 读者可以轻易验证，我们可以写成 $(\varphi,\psi)=(f,g)M$，其中 M 是三个可能的矩阵形式之一，其系数属于 $\mathbb{F}[x]$，并且取决于 Δ、q 和 d。

命题 3.5 (*[15,* 命题 3.*5]*) 若 (f,g) 是 F 的一个 VOP，则 $\lambda(F)=|f|$。

我们通常记 $d_k=|g^{(k)}|-|f^{(k)}|$ 和 $\Delta_k=\Delta(f^{(k)};\,F_{(-k-1)})$。当 $\mathbb{F}=$ 属于二元有限域时，我们将 x^{d_k}（若 $\Delta_k\neq 0$ 且 $d_k>0$）和 x^{-d_k}（若 $\Delta_k\neq 0$ 且 $d_k\le 0$）称为该构造中的中间位移。

接下来我们回顾一下 [15, 算法 4.22]。这是一种 $\mathcal{O}(m^2)$ 算法，[15, 命题 4.25], 的证明比 [8]更简短，也更容易理解。

算法 3.6（$\mathbb{F}$ 任意域）

Input: $F\in\mathrm{M}^\times$ 的逆形式。
Output: $\mathcal{I}_F$ 的 VOP (f,g)。

(* 归纳基：找到 $F^{(\mathrm{v})}$ 和 $\mathcal{I}_F$ 的 VOP *)[$j\leftarrow 1$;
repeat $j\leftarrow j-1$ until $(F_j\neq 0)$; $\mathrm{v}\leftarrow j$; $(f,g)\leftarrow($
$x^{1-\mathrm{v}},z)$;

(* 归纳步骤 *)

$\Delta' \leftarrow 1$; $G \leftarrow x^{\mathrm{v}}$; $d \leftarrow \mathrm{v}$;

`for` $j \leftarrow \mathtt{v} - 1$ `downto` $|F|$ `do`

$\lceil\ G \leftarrow F_j x^j + G z^{-1}$; $\Delta \leftarrow \Delta(f; G)$; $q \leftarrow \Delta/\Delta'$;
`if` $(\Delta \neq 0)$ `then if` $(d \leq 0)$ `then` $f \leftarrow f - q\, x^{-d}\, g$;
`else` $\lceil t \leftarrow f$; $f \leftarrow x^{+d} f - q\, g$; $g \leftarrow t$;
$\Delta' \leftarrow \Delta$; $d \leftarrow -d$; $\rfloor$
$g \leftarrow zg$; $d \leftarrow 1 + d$;$\rfloor$

`return` (f, g).$\rfloor$

我们通过重新考察例 4.8], 中的序列 (1, 0, 0, 0, −1, 1, 0, 0, 1, −2, . . .) ∈$\mathbb{Q}^{10}$ 来说明算法 3.6，其中该序列被视为一个线性递归序列的初始项，且其最小多项式的次数至多为 5。我们将在不作这些假设的情况下求出它的（唯一）最小多项式 $x^5 + x - 1$ 。

例 3.7 序列 (1, 0, 0, 0, −1, 1, 0, 0, 1, −2) $\in \mathbb{Q}^{10}$ 定义了逆形式 $F = -2x^{-9} + x^{-8}z^{-1} + x^{-5}z^{-4} - x^{-4}z^{-5} + z^{-9} \in \mathbb{Q}[x^{-1}, z^{-1}]$。 F的子形式如下:

j	$F^{(j)}$
0	1
−1	z^{-1}
−2	z^{-2}
−3	z^{-3}
−4	$-x^{-4} + z^{-4}$
−5	$x^{-5} - x^{-4}z^{-1} + z^{-5}$
−6	$x^{-5}z^{-1} - x^{-4}z^{-2} + z^{-6}$
−7	$x^{-5}z^{-2} - x^{-4}z^{-3} + z^{-7}$
−8	$x^{-8} + x^{-5}z^{-3} - x^{-4}z^{-4} + z^{-8}$
−9	$-2x^{-9} + x^{-8}z^{-1} + x^{-5}z^{-4} - x^{-4}z^{-5} + z^{-9}$

并且我们得到 $\mathcal{I}_F$ 的 VOP ($f^{(9)}, g^{(9)}$)，如以下摘要所示。 :

k	d_{k-1}	Δ'_{k-1}	Δ_{k-1}	q_{k-1}	$(f^{(k)}, g^{(k)})$
0	−	1	−	−	(x, z)
1	0	1	0	0	(x, z^2)
2	1	1	0	0	(x, z^3)
3	2	1	0	0	(x, z^4)
4	3	1	−1	−1	$(x^4 + z^4, xz)$
5	−2	−1	1	−1	$(x^4 + x^3z + z^4, xz^2)$
6	−1	−1	1	−1	$(x^4 + x^3z + x^2z^2 + z^4, xz^3)$
7	0	−1	1	−1	$(x^4 + x^3z + x^2z^2 + xz^3 + z^4, xz^4)$
8	1	1	1	−1	$(x^5 + x^4z + x^3z^2 + x^2z^3 + 2xz^4, f^{(7)}z)$
9	0	1	1	1	$(x^5 + xz^4 - z^5, f^{(7)}z^2)$

使得 $\mathcal{I}_F = \langle x^5 + xz^4 - z^5, x^4z^2 + x^3z^3 + x^2z^4 + xz^5 + z^6 \rangle$。此外，由于 $|g^{(9)}| = 6 > 5 = |f^{(9)}|$, $f^{(9)} = x^5 + xz^4 - z^5 \in \mathbb{Q}[x, z]$ 是F的唯一（首一）最小首项形式，且 $\lambda(s) = |f^{(9)}| = 5$。特别地，给定有限序列的唯一最小多项式为 $x^5 + x - 1 \in \mathbb{Q}[x]$。因此，根据注 2.5，线性反馈移位寄存器综合算法将返回 $f^{(9)\vee}$ 的首一化倒数，即 $x^5 - x^4 - 1$。

同样， [2], [7] 和 [9] 的方法不适用于二进制序列，因为我们事先并不知道该序列前 $2t$ 项的线性复杂度上界 t 。

3.2 一些其他性质

若 $m \leq 0$ 和 $F = x^m$ ，则由命题 3.1 可得 $\mathcal{I}_F = \langle x^{1-m}, z \rangle$ ，且 $\gcd(x^{1-m}, z) = 1$。下一个结果表明，所构造的可行 (f, g) 满足 $\gcd(f, g) = 1$。

命题 3.8 如果（f， g）是关于 $\mathcal{I}_F$ 的 VOP，$\gcd(f, g) = 1$ 且 φ、ψ 如所构造，则 $\gcd(\varphi, \psi) = 1$。

证明。若 $\Delta = 0$ and $h | \gcd(f, zg)$成立，则 $h = z$ 或 $h|g$。但若 $z|f$，则 $z|\mathrm{LT}(f)$，这是不可能的，所以 $h | \gcd(f, g)$。假设 $\Delta \neq 0$ and $d \leq 0$。则 $\gcd(\varphi, \psi) = \gcd(f, zg) = \gcd(f, g) = 1$ ，如前所述。另一方面，假设 $d > 0$。若 $h|zf$ and $h|g$，则或者 (i) $h = z$ and $h|\varphi$ ，或者 (ii) $h|f$ and $h|(x^d f - q\, g)$。但 (i) 不可能，因为 $z \nmid \mathrm{LT}(\varphi)$，所以 (ii) 成立，且 $h | \gcd(f, g) = 1$。□

如果 $m \leq 0$ 且 $F = x^m$，那么 (x^{1-m}, z) 是 $\mathcal{I}_F$ 的 VOP，而 x^{1-m} 是最小次数的首项形式。但对于任何满足 $|\varphi| = -m$ 的形式， $x^{1-m} + \varphi\, z$ 也同样如此。更一般地，

推论 3.9（参见 *[12, 定理 1]*）设 (f, g) 是 $\mathcal{I}_F$ 的 VOP，且

$$\Theta = \{\theta \in \mathcal{I}_G \cap \mathcal{L} : \ |\theta| \ is \ minimal\}.$$

Then

$$\Theta = \begin{cases} \{f\} & if\ |g| > |f| \\ \{f\} \cup \{f + \psi \cdot g, \psi \ is\ a\ form\ and\ |\psi| = |f| - |g|\} & otherwise. \end{cases}$$

证明。由于 f 和 g 生成 $\mathcal{I}_F$，当 $|g| > |f|$ 时， f 是唯一的最小次数首项消去形式 $|f|$；但如果 $|g| \leq |f|$ 且 $\psi \in \mathbf{R}^\times$ 是满足 $|\psi| = |f| - |g|$ 的形式，那么 $h = f + \psi \cdot g \in \mathcal{I}_F$ 是首项形式，因为 $\mathrm{LT}(h) = \mathrm{LT}(f)$，且 $|h| = |f|$ 是最小的。□

在 [15, 例 4.24], 中，我们得到 $(f, g) = (x^4 + x^3z + x^2z^2, x^3z + x^2z^2 + xz^3 + z^4)$，这是逆形式 $F = x^{-6} + x^{-4}z^{-2} + x^{-3}z^{-3} + z^{-6}$。此处 $f(0, 1) = 0$。然而，$h = f + g \in \mathcal{I}_F$ 满足 $h(0, 1) = 1$。（事实上， $h \in \mathcal{I}_{z^{-1}F}$。）

更一般地，如果我们有一个逆形式 F，并从 $(x^{1-|F|}, z)$ 开始迭代，那么该构造会给出一个 VOP (f, g)，使得 $\gcd(f, g) = 1$。因此，如果 $f(a, b) = 0$，则对于某个

$a, b \in \mathbb{F}$ 则 $g(a,b) \neq 0$，且若 $|g| \leq |f|$，则 $h = f + x^{|f|-|g|}g$ 是 $\mathcal{I}_F$ 中的首项形式，使得 $h(a,b) \neq 0$。另一方面，若 $|g| > |f|$，则 $h = x^{|g|-|f|}f + g \in \mathcal{I}_F$ 是首项形式，使得 $h(a,b) \neq 0$，但次数增加了 $|g|$。

我们回顾 [15] 中的以下结果，以供后续参考：

定理 3.10 设 F 是 $(s_0, \ldots, s_{n-1})$ 的逆形式，(f, g) 是如上构造的 $\mathcal{I}_F$ 的 VOP，且 (μ, ν) 是在 *[15,* 算法 6.*14]* 中构造的 $(s_0, \ldots, s_{n-1})$ 的最小多项式对。存在一一对应关系 $(f, g) \mapsto (f^\vee, g^\vee)$，满足 $(\mu, \nu) \mapsto (\mu^\wedge, \nu^\wedge z^{n+1-|\mu|-|\nu|})$，其中 $\nu \neq 0$。

备注 3.11 (i) 我们显然有 $|\mu^\wedge| + |\nu^\wedge z^{n+1-|\mu|-|\nu|}| = n+1$，这与 VOP 性质 (iii) 一致，因为 $m = 1 - n$。

（ii）$|g| > |f| \Leftrightarrow n + 1 - |\mu| > |\mu|$ 以及 $\max\{|g|, |f|\} = \max\{n + 1 - |\mu|, |\mu|\}$，参见 *[10]*。

（iii）定理 3.10 意味着我们还可以为 $\mathcal{I}_{(s_0,\ldots,s_{n-1})}$ 计算一对生成元 u 使用 *[14,* 算法 3.*14]*。

3.3 线性复杂度剖面

一个逆形式 F 具有子形式 $F^{(j)}$，其对应于 $m = |F| \leq j \leq \mathrm{v} = \mathrm{v}(F)$，其中 $F_{(\mathrm{v})} = x^{\mathrm{v}}$ 和 $F^{(m)} = F$。我们将 $\lambda(F_{(j)})$ 记作子形式 $F_{(j)}$ 的线性复杂度。

我们将整数序列（$\lambda(F_{(\mathrm{v})}) \ldots, \lambda(F^{(m)})$）称为 F 的线性复杂度剖面。若 $\mathrm{v} = 0$ 且 $\lambda(F^{(-k)}) = \lfloor (k+2)/2 \rfloor$ 对于 $0 \leq k \leq -m$ 成立，则称 F 具有完美线性复杂度剖面（PLCP）。根据定理 2.3，这与序列线性复杂度剖面的通常定义一致。接下来，我们将 PLCP 的概念与定理 3.3 中出现的中间位移联系起来。这是 [12, 定理2] 的一个类似结果；不过，我们不要求无理性假设。

命题 3.12 设 F 是一个具有 $F_0 = 1$ 的逆形式。对于 $1 \leq k < -m$，令 $(f_{(k)}\, g^{(k)})$ 为 $\mathcal{I}_{F^{(-k)}}$ 的 VOP，且 $F_{(-1-k)}$ 为 F 的 $(-1-k)^{th}$ 子形式。令 $\Delta_k = \Delta(f^{(k)}; F_{(-1-k)})$。以下命题等价：

(i) F 具有 PLCP；(ii) 中间移位为 x，当且仅当 k 为奇数。

证明。对于 $k = 1$，$\lfloor (k+1)/2 \rfloor$ 的值为 1，当且仅当 k 为奇数时，该值增加 1。由于 $F_0 = 1$，$(f^{(0)}, g^{(0)}) = (x, z)$，即 $|f(0)| = 1$ 且 $d_0 = 0$。因此，要么 $(f(1)\, g^{(1)}) = (x, z^2)$，要么 $(f^{(1)}, g^{(1)}) = (x + z, z^2)$。接下来，次数 $|f(k)|$ 当且仅当 k 为奇数时增加 1，这等价于：若 k 为奇数，则 $f(k+1) = xf(k) + q_k g^{(k)}$；若 k 为偶数，则 $f(k+1) = f^{(k)} + q_k g^{(k)}$。□

注记 3.13 在命题 3.12 中，当 k 为偶数时，$\Delta_k \in$ 二元有限域是任意的。长度为 n 的随机二进制序列的期望线性复杂度为 $n/2 + c_n$，其中 $0 \leq c_n \leq 5/18$、*[18,*，第 *4]* 章。因此，具有 $s_0 = 1$ 且 s_i 的二进制序列，若在 k 为奇数时选择使得 $\Delta_k = 1$，而在 k 为偶数时随机选择，将具有 PLCP，并且是随机二进制序列的良好近似。

4 Rueppel 猜想

在本文余下部分， $\mathbb{F}$ = 二元有限域。Rueppel 猜想涉及二进制序列 $r = (r_0, r_1, \ldots) = (1, 1, 0, 1, 0_3, 1, 0_7, 1, 0_{15}, 1, \ldots)$，其中 $r_i = 1 \in \mathbb{F}$ 若 $i = 2^k - 1$对于某个 $k \geq 0$ ，否则为 0。

定义 4.1 对于 $n \geq 1$， $(r_0, \ldots, r_{n-1})$ 的逆形式为

$$R^{(1-n)} = R^{(1-n)}(x^{-1}, z^{-1}) = \sum_{j=1-n}^{0} r_{-j} x^j z^{1-n-j} \in \mathbb{F}[x^{-1}, z^{-1}]$$

并将 $\mathcal{I}_{n-1}$ 记作 $\mathcal{I}_{R^{(1-n)}}$。

注意， $R^{(1-n)}$和 $\mathcal{I}_{n-1}$的索引采用 $(r_0, \ldots, r_{n-1})$ 的最后一个索引，而非序列的长度。对于 $k \geq 0$，有 $|R^{(1-n)}| = 1 - n$, $R^{(1-2^k)} = \sum_{j=k}^{0} x^{1-2^j} z^{2^j-2^k}$；若 $k \geq 1$，则 $R^{(1-2^k)} = x^{1-2^k} + R^{(1-2^{k-1})} z^{-2^{k-1}}$。此外，若 $2^k - 1 < n < 2^{k+1} - 1$，则 $R^{(-n)} = R^{(1-2^k)} z^{2^k-1-n} \in z^{-1}\mathbf{M}$。

例 4.2 $-9 \leq j \leq 0$ 的逆形式 $R^{(j)}$ 如下：

j	$R^{(j)}$
0	$1 = R^{(0)}$
-1	$x^{-1} + z^{-1} = R^{(-1)}$
-2	$x^{-1}z^{-1} + z^{-2} = R^{(-1)}z^{-1}$
-3	$x^{-3} + x^{-1}z^{-2} + z^{-3} = R^{(-3)}$
-4	$x^{-3}z^{-1} + x^{-1}z^{-3} + z^{-4} = R^{(-3)}z^{-1}$
-5	$x^{-3}z^{-2} + x^{-1}z^{-4} + z^{-5} = R^{(-3)}z^{-2}$
-6	$x^{-3}z^{-3} + x^{-1}z^{-5} + z^{-6} = R^{(-3)}z^{-3}$
-7	$x^{-7} + x^{-3}z^{-4} + x^{-1}z^{-6} + z^{-7} = R^{(-7)}$
-8	$x^{-7}z^{-1} + x^{-3}z^{-5} + x^{-1}z^{-7} + z^{-8} = R^{(-7)}z^{(-1)}$
-9	$x^{-7}z^{-2} + x^{-3}z^{-6} + x^{-1}z^{-8} + z^{-9} = R^{(-7)}z^{(-2)}$】【。

回想一下， $\Delta_{k-1} = \Delta(f^{(k-1)}; R^{(-k)}) = [f_{(k-1)} \cdot R^{(-k)}]_{(|f^{(k-1)}|-k,0)}$ 以及 $q_{k-1} = \Delta_{k-1}$ 当 $0 \leq k - 1 \leq n - 1$时。

例4.3（例4.2续）。首先，由于命题 3.1 中的 $R^{(0)} = 1$、 $\mathcal{I}_0 = \langle f^{(0)}$、 $g^{(0)} \rangle = \langle x$、 $z \rangle$。不过，我们可以并且将取 $(f^{(0)}, g^{(0)}) = (x + z, z)$，使得 $f^{(0)}(0, 1) = 1$。构造的关键要素是次数增量 $d_k = |g^{(k)}| - |f^{(k)}|$ 和差异 Δ_k——这样我们就知道如何更新 $(f^{(k)}, g^{(k)})$。我们得到下表：

k	d_{k-1}	Δ_{k-1}	$f_{(k)}$	$g^{(k)}$
0	–	–	$f^{(0)} = x + \underline{z}$	z
1	0	0	$f_{(0)}$	z^2
2	1	1	$xf^{(1)} + g^{(1)} = x^2 + \underline{xz} + z^2$	$f_{(0)}z$
3	0	0	$f_{(2)}$	$f_{(0)}z^2$
4	1	1	$xf^{(3)} + g^{(3)} = x^3 + x^2z + \underline{z^3}$	$f_{(2)}z$
5	0	0	$f_{(4)}$	$f_{(2)}z^2$
6	1	1	$xf^{(5)} + g^{(5)} = x^4 + \underline{x^3z} + x^2z^2 + z^4$	$f_{(4)}z$
7	0	0	$f_{(6)}$	$f_{(4)}z^2$
8	1	1	$xf^{(7)} + g^{(7)} = x^5 + x^4z + \underline{x^2z^3} + xz^4 + z^5$	$f_{(6)}z$
9	0	0	$f_{(8)}$	$f_{(6)}z^2$。

然后，对于 $0 \le k \le 9$, $f^{(k)} = \lfloor (k+2)/2 \rfloor = \lambda_{k+1}$（回忆一下，$f_{(k)} \circ (r_0, \ldots, r_k) = 0$，其中有 $k+1$ 项）。根据推论 3.9，$f^{(k)}$ 是最小总次数的唯一首项消去形式（当 k 为奇数时）；当 k 为偶数时，$f^{(k)} + g^{(k)}$ 是最小总次数下唯一的另一个首项消去形式。下划线标出的项将在定理 4.4 的证明中显示其意义。

现在我们来介绍主要结果。

定理 4.4 设 $(f_{(0)}\, g^{(0)}) = (x + z, z)$，并且对于 $k \ge 0$，令 $(f^{(k+1)}, g^{(k+1)})$ 如定理 3.3 中所构造。则

(A) 若 k 为偶数，则 $\Delta_k = 0$；否则 $\Delta_k = 1$ 和 $d_k = 1$

(B)

$$(f^{(k+1)}, g^{(k+1)}) = \begin{cases} (f^{(k)}, zg^{(k)}) & \textit{if } k \textit{ is even} \\ (xf^{(k)} + g^{(k)}, zf^{(k)}) & \textit{otherwise} \end{cases}$$

(C) $|f^{(k+1)}| = \lfloor (k+3)/2 \rfloor$ (D) $f^{(k+1)}(0, 1) = g^{(k+1)}(0, 1) = 1$。

证明。我们从 $(f^{(0)}, g^{(0)}) = (x + z, z)$ 开始，归纳应用定理 3.3 和命题 3.12，其中 $\Delta_0 = 0$, $|f^{(0)}| = 1 = \lfloor 2/2 \rfloor$ 和 $f_{(0)}(0, 1) = 1 = g^{(0)}(0, 1)$。

归纳假设该结果对 k 成立。

(A) 对于 $f_{(k+1)}$，我们需要确定 $\Delta_k = [f_{(k)} \cdot R^{(-1-k)}]_{(|f^{(k)}|-1-k,0)}$。令 $P = 2^p - 1 \le k + 1 < 2^{p+1} - 1$，其中 $p \ge 1$，置 $e = |f^{(k)}|$ 和 $l = e - 1 - k$。那么

$$S = R^{(-1-k)} = \left(\sum_{j=p}^{0} x^{1-2^j} z^{2^j - 2^p} \right) z^{P-1-k} \text{ and } \Delta_k = [f^{(k)} \cdot S]_{(l,0)}.$$

我们考虑三种情况：(i) k 为偶数，$P = k + 1$；(ii) k 为偶数，$P < k + 1 < 2^{p+1} - 1$；(iii) k 为奇数且 $P \le k < 2^{p+1} - 1$。

(i) 我们有 $k + 1 = P$，并且必须证明 $\Delta_k = 0$。由于 $k - 1$ 是奇数，归纳假设给出 $\Delta_{k-1} = 1$、$d_{k-1} = 1$ 和 $(f^{(k)}, g^{(k)}) = (xf_{(k-1)} + g^{(k-1)}, zf_{(k-1)})$。此外

$|f_{(k)}| = |f_{(k-1)}| + 1 = k/2 + 1 = 2^{p-1}$，因此 $l = |f^{(k)}| - k - 1 = 2^{p-1} + 1 - 2^p = 1 - 2^{p-1}$。根据部分（A），$f_{(k)}(0,1) = 1$，所以我们可以将 $f^{(k)} \cdot S$ 写成

$$(x^e + \alpha + z^e) \cdot (x^{1-2^p} + x^{1-2^{p-1}} z^{-2^{p-1}} + \beta).$$

于是 $x^e \cdot x^{1-2^p} = x^l$，并且容易验证 $(\alpha + z^e) \cdot (x^{1-2^{p-1}} z^{-2^{p-1}} + \beta) = x^l$ 加上关于$z^{-1}\mathbf{M}$ 的项，因此 $\Delta_k = [f_{(k)} \cdot S]_{(l,0)} = 0$，且 $f_{(k+1)} = f^{(k)}$。

(ii) 此处 k 为偶数，$P - k - 1 < 0$ 且 $S \in z^{-1}\mathbf{M}$。与情形 (i) 相同，$(f^{(k)}, g^{(k)}) = (xf_{(k-1)} + g^{(k-1)}, zf_{(k-1)})$，且 $e = |f^{(k)}| = |f_{(k-1)}| = 2^{p-1}$。于是

$$f^{(k)} \cdot S = (x^e + (f^{(k)} + x^e)) \cdot R^{(-P)} z^{P-k-1}$$

$x^e \cdot R^{(-P)} z^{P-k-1}$，$(f_{(k)} + x^e) \cdot x^{-P}$，$(f_{(k)} + x^e) \cdot (R^{(-P)} + x^{-P}) z^{P-k-1} \in z^{-1}\mathbf{M}$，因此 $\Delta_k = 0$，再次有 $f_{(k+1)} = f^{(k)}$。

(iii) 接下来考虑 k 为奇数的情形。对于 $k = 1$, $\Delta_1 = [(x + \underline{z}) \cdot (x^{-1}z^{-1} + z^{-2})]_{(1-2,0)} = 1$；$f^{(1)}$ 的 $\underline{z}$ 项已触发 $\Delta_1 = 1$。读者很容易验证，$\underline{xz} = \alpha z$会触发 $\Delta_3 = 1$，而 $\underline{z}^3 = \beta z$ 会触发 $\Delta_5 = 1$。现在令 k 为奇数，且 $p \geq 3$,$P = 2^p - 1 \leq k < 2^{p+1} - 1$。定义映射 $\alpha, \beta: \mathbf{R} \to \mathbf{R}$，使得 $(\alpha\ f)(x,z) = x \cdot f(x,z)$，且 $(\beta\ f)(x,z) = z^2 \cdot f(x,z)$。由于 $k-1$ 为偶数，归纳假设给出

$$f^{(k)} = f^{(k-1)} = xf^{(k-2)} + g^{(k-2)} = \alpha\ f^{(k-2)} + \beta\ f^{(k-4)},$$

$e = |f^{(k)}| = |f^{(k-1)}| = (k+1)/2$ 和 $l = e + |S| = (k+1)/2 - 1 - k = -(k+1)/2$.

令 $t_k = x^{u_k} z^{v_k}$，其中 $u_k = P - \frac{k+1}{2}$，$v_k = k + 1 - P$。则 $|t_k| = (k+1)/2 = |f_{(k)}|$ 且 $t_k = \alpha^{u_k} \beta^{(v_k-1)/2} z$。由于 z 是 $f_{(1)}$ 的一项，t_k 是 $f_{(2u_k+2v_k-1)} = f_{(k)}$ 的一项。

设 $L = \mathrm{LT}(S)$，其中 $S = R^{(-P)} z^{P-k-1} \in z^{-1}\mathbf{M}$。于是

$$f^{(k)} \cdot S = f^{(k)} \cdot (L + S) + f^{(k)} \cdot L = f^{(k)} \cdot (L + S) + t_k \cdot L + (f^{(k)} + t_k) \cdot L$$

以及 $t_k \cdot L = x^{(k-1)/2} z \cdot x^{-k} z^{-1} = x^l$。显然，$f^{(k)} \cdot (L + S) \in z^{-1}\mathbf{M}$ 且 $(f^{(k)} + t_k) \cdot L \in z^{-1}\mathbf{M}$。因此，$\Delta_k = [f_{(k)} \cdot S]_{(l,0)} = [t_k \cdot L]_{(l,0)} = 1$，$f_{(k)}$ 中的项 t_k 会触发 $\Delta_k = 1$，并且 $(f_{(k+1)}\ g^{(k+1)}) = (xf_{(k)} + g^{(k)}, zf_{(k)})$。

（B）这是部分（A）的一个简单推论。

（C）设 $|f_{(k)}| = \lfloor (k+2)/2 \rfloor$。根据部分（C），若 k 为偶数，则 $|f^{(k+1)}| = |f_{(k)}| = (k+2)/2 = \lfloor (k+3)/2 \rfloor$；若 k 为奇数，则 $|f_{(k+1)}| = |f_{(k)}| + 1 = \lfloor (k+2)/2 \rfloor + 1 = (k+1)/2 + 1 = (k+3)/2 = \lfloor (k+3)/2 \rfloor$。

（D）我们知道，对于 $k = 0$，$f^{(k)}(0,1) = g^{(k)}(0,1) = 1$，所以假设该结论对 k 成立。若 k 为偶数，则 $f^{(k+1)}(0,1) = f_{(k)}(0,1) = 1$，且 $g^{(k+1)}(0,1) = 1$；而若 k 为奇数，则 $f_{(k+1)}(0,1) = g^{(k)}(0,1) = 1$，且 $g^{(k+1)}(0,1) = f^{(k)}(0,1) = 1$。□

注记 4.5 (i) 对于含有两个以上元素的域，当 k 为偶数时，部分（B）的证明中可能无法进行消去。

(ii) 在例4.3中，下划线标出的项会导致差异为 1：对于奇数 k 以及 $2^p - 1 \leq k < 2^{p+1} - 1$、$u_{k+1} = u_k - 1$、$v_{k+2} = v_k + 2$，使得定理 4.4 的证明中的 t_k 取值为 $x^p z^1$、$x^{p-1} z^3$、$x^{p-2} z^5$、……、$x^0 z^{2^p-1}$。

推论 4.6 定义以 R 中元素为项的 2×2 矩阵如下

$$E = \begin{bmatrix} 1 & 0 \\ 0 & z \end{bmatrix} \text{ and } U = \begin{bmatrix} x & z \\ 1 & 0 \end{bmatrix}.$$

那么 (i) 对于 $n \geq 0$，$(f^{(n+1)}, g^{(n+1)}) = (f_{(n)}\, g^{(n)})M_n$，其中 $M_n = E$若 n 为偶数，且 $M_n = U$ 若 n 为奇数

(ii) 对于 $i \geq 1$ 和 $P = UE$

$$(f^{(2i)}, g^{(2i)}) = (x + z, z^2)P^{i-1}U \text{ and } (f^{(2i+1)}, g^{(2i+1)}) = (x + z, z^2)P^i.$$

(iii) 若 $\phi^{(i)}(x) = f_{(i)}(x, 1)$，则 $\phi^{(2i)} = (x + z, z^2)U^i$ 对于 $i \geq 1$。

证明。 Part (i) 是定理 4.4(B) 的重述。(ii) 部分可通过简单归纳法得到。 □

接下来　该结果是命题 3.12 和定理 4.4 的直接推论。

推论 4.7 序列 $(r_0, r_1, \ldots)$ 具有 PLCP。

证明。对于 $n \geq 1$, $\lambda(r_0, r_1, \ldots, r_{n-1}) = |f^{(n-1)}| = \lfloor (n + 1)/2 \rfloor$。□

推论 4.8 令 $n \geq 0$、$(f^{(n)}, g^{(n)})$ 为针对 $\mathcal{I}_n$ 构造的对象，并令 Θ_n 为集合 $\{\theta \in \mathcal{I} \text{ is a leading form}, |\theta| \text{ is minimal}\}$。那么

$$\Theta_n = \begin{cases} \{f^{(n)}\} & \text{if } n \text{ is odd} \\ \{f^{(n)}, f^{(n)} + g^{(n)}\} & \text{otherwise.} \end{cases}$$

证明。这是将推论 3.9 专门应用于 $R^{(-n)}$ 的结果。□

接下来，我们给出 $f^{(2k-1)}$ 去齐次化后的闭式表达式；这也说明了为何要在 $\mathbb{F}(x)$ 的二次扩张中使用 $Y^2 + xY + 1$ 的根。

引理 4.9 若 $h^{(k)} \in \mathbb{F}[x]$、$h^{(1)} = x + 1$、$h^{(2)} = x^2 + x + 1$ 和 $h^{(k)} + x\, h^{(k-1)} + h^{(k-2)} = 0$对于 $k \geq 3$ 成立，则

$$x\, h^{(k)} = (1 + \rho)\rho^k + (1 + \rho^{-1})\rho^{-k}$$

其中 $\rho = \overline{Y} \in \mathbb{F}(x)/(Y^2 + xY + 1) = \mathbb{K}$。

证明。多项式 $h^{(k)}$ 的特征多项式为 $Y^2 + xY + 1 \in \mathbb{F}(x)[Y]$，它是不可约的——容易证明，若对于某些 u，$Y^2 + xY + 1 = (Y + u)(Y + v)$，且 $v \in \mathbb{F}(x)$，则 $x = 0$。因此，令 $\rho = \overline{Y} \in \mathbb{K}$。对 $h^{(k)} = A\rho^k + B\rho^{-k}$ 关于 A求解，$B \in \mathbb{F}(x)$，并满足$h^{(1)} = x + 1$、$h^{(2)} = x^2 + x + 1$，即可得到所需系数。□

定理 4.10 对于 $k \geq 1$，我们有

$$x\, f^{(2k-2)}(x, 1) = x\, f^{(2k-1)}(x, 1) = (1 + \rho)\rho^k + (1 + \rho^{-1})\rho^{-k} = x\mu_{2k-1}(x)$$

其中 μ_{2k-1} 在定理 3.10 中定义。

证明。定理 4.4 表明，在引理 4.9 中我们可以取 $h^{(k)} = f^{(2k-2)}(x, 1)$ $f_{(2k-2)} = f_{(2k-1)}$ 和 $|g^{(2k-1)}| = |f^{(2k-1)}| + 1$，因此 $f_{(2k-1)}$ 是唯一的。最后一个等式由定理 3.10 得出。□

推论 4.11（参见 [4, 引理 5]）令 $\eta = (1+\rho)\rho^k + (1+\rho^{-1})\rho^{-k} \in \mathbb{K}$ 如引理 4.9 中所述。则 $\eta \in \mathbb{F}[x]$、$x|\eta$ 和 $|\eta| = k+1$。

推论 4.12 将线性反馈移位寄存器综合算法应用于 $(r_0, \ldots, r_{2k-1})$，返回 k 和 $f^{(2k-1)}(x, 1)$ 的倒数。

证明。根据定理 4.4，$|f^{(2k-1)}(x, 1)| = k$和 $f_{(2k-1)}(0, 1) = 1$。□

定理 4.4 还表明，将算法 3.6 应用于 $R^{(1-n)}$ 时，过程会大大简化：无需通过乘法求出差异，除了奇偶性检验之外几乎不需要做其他操作。

算法 4.13 针对 $R^{(1-n)}$的简化 VOP 算法

Input: 整数 $n \geq 1$。Output: 对于 $\mathcal{I}_{n-1}$，可行有序对 (f, g)。⌈ $(f, g) \leftarrow (x+z, z)$；

for $j \leftarrow 0$ downto $1-n$ do
⌈ *if* j *is odd* then ⌈ $t \leftarrow f$; $f \leftarrow xf + g$; $g \leftarrow t$; ⌋
$g \leftarrow z\,g$; ⌋;

return (f, g).⌋

关于$\mathcal{I}_{n-1}$的其他性质，例如其余维数以及如何计算其（唯一的）约化字典序格罗布纳基，读者可参阅 [15], [16]。

5 [4]的最小多项式

设 $k \geq 1$，并给定一个序列 $(s_0, \ldots, s_{2k-1})$。在 [4], 中，作者使用扩展欧几里得算法为 $(s_0, \ldots, s_{2k-1})$ 构造$c_k \in \mathbb{F}[x]$：令 $s'_{-1} = x^k$，$s'_0 = s_0 x^{k-1} + \cdots + s_{k-1}$，并令$q_k$，$s'_k$，$c_k \in \mathbb{F}[x]$ 由 $c_{-1} = 0$，$c_0 = 1$定义，

$$s'_k = q_k s'_{k-1} + s'_{k-2} \text{ and } |s'_k| < |s'_{k-1}|,\ c_k = q_k c_{k-1} + c_{k-2}\,,$$

在第一个满足 k 的 $s'_k = 0$ 处终止。将此方法应用于 (1, 1, 0, 1, 0$_3$, . . .) 的前 $2k-1$ 项，余数记作 r'_k。作者采用了不同的方法来求出 c_k，现概述如下。矩阵

$$V = \begin{bmatrix} 1 & 0 \\ 0 & x \end{bmatrix}$$

的特征多项式为 Y^2+xY+1，其根为 $\rho^{\pm 1}$（见引理 4.9），特征向量为 $[1\ \rho^{\pm 1}]^{\mathrm{T}}$；对角化 V^k 可得 $q_1(x) = x+1$ 和 $q_k(x) = x$，其中 $k \geq 2$、[4, 见引理 2、3：3]。这意味着，对于 $k \geq 2$，有 $r'_k = x\, r'_{k-1} + r'_{k-2}$。再结合引理 4] 中的进一步对角化与引理 1]，可得 c_k 的公式。

然而，对于 $k \geq 2$，关键事实是 $q_1(x) = x + 1$ 和 $q_k(x) = x$，这给出 $c_1(x) = x + 1$、$c_2(x) = x^2 + x + 1$ 以及 $k \geq 2$ 的 $c_k = x\, c_{k-1} + c_{k-2}$。因此，我们可以将引理 4.9 应用于 c_k。结合定理 4.4，可得

推论 5.1 对于 $k \geq 1$

(i) $c_k(x) = f^{(2k-1)}$

$(x, 1) = f^{(2k-2)}(x, 1) = x^{-1}((1 + \rho)\rho^k + (1 + \rho^{-1})\rho^{-k})$ (ii)

$|c_k| = |f^{(2k-1)}(x, 1)| = k$(iii) c_k 是 $(r_0, \ldots, r_{2k-1})$ 的唯一最小多项式

(iv) $f^{(2k-1)}(x, z) = z^k c_k$({v19)。

如同 [4], 引理 1，前引文表明，若 $k \geq 0$ 且 $l = 2^k$，则 $c_l\ (x) = x^l + \sum_{j=0}^{\log_2 l} x^{l-2^j}$，并且由于 $c_l\ (x) = f^{(2l-1)}\ (x,\ 1)$，

$$f^{(2l-1)}(x, z) = {c_l}^{\wedge}(x, z) = x^l + \sum_{j=0}^{\log_2 l} x^{l-2^j} z^{2^j}.$$

参考文献

[1] Althaler, J. 和 D¨ur, A.《有限线性递推序列与齐次理想》。《工程、通信与计算中的应用代数》7：377–390（1996）。

[2] Be rlekamp, E. R.《代数编码理论》。麦格劳-希尔，纽约（196 8).

[3] Cox, D.、Little, J. 和 O'Shea, D.《理想、簇与算法》（第 3 版），大学数学教材。施普林格，纽约（2007年）。

[4] Dai, Z.-D.《Rueppel 线性复杂度猜想》的证明。IEEE 信息论汇刊，32：440–443（1986年）。

[5] Dai, Z.-D. 和 Wan, Z. 线性反馈移位寄存器综合中 Berlekamp-Massey 算法与欧几里得算法之间的关系。《数学学报》，新辑，4，55-63（1988年）。

[6] Dornhoff, L.L. 和 Hohn, F.《应用现代代数》。麦克米伦，纽约（1978年）。

[7] Fitzpatrick, P. 关于关键方程。IEEE 信息论汇刊，41：1290–1302（1995年）。

[8] Gustavson, F. Berlekamp-Massey线性反馈移位寄存器综合算法分析。IBM《研究与开发杂志》20，204–212（1976年）。

[9] Lidl, R. 和 Niederreiter, H.《有限域》，《数学及其应用百科全书》第20卷，Addison-Wesley，马萨诸塞州雷丁，1983年。[10] Massey, J. L. 移位寄存器综合与BCH译码。《IEEE 信息论汇刊》15：122–127（1969年）。[11] Niederreiter, H. 形式幂级数的连分数、伪随机数与序列的线性复杂度。《一般代数论丛》第5卷，萨尔茨堡会议论文集，221–233。Teubner出版社，斯图加特（1986年）。[12] Niederreiter, H. 具有近乎完美线性复杂度剖面的序列。《密码学进展》，EUROCRYPT ’87（D. Chaum 和 W. L. Price 编），《计算机科学讲义》第304卷，第37–51页。施普林格出版社，柏林（1988年）。[13] Northcott, D. G. 内射包与逆多项式。《伦敦数学学会杂志》8：290–296（1974年）。[14] Norton, G. H. 有限序列的最小实现。《符号计算杂志》20：93–115（1995年）。[15] Norton, G. H. 逆形式的湮灭理想。《工程、通信与计算中的应用代数》28：31–78（2017年）。[16] Norton, G. H. 逆形式的湮灭理想：补遗。《工程、通信与计算中的应用代数》28：491–507（2019年）。[17] Rueppel, R.A. 流密码的新方法。博士论文，电信研究所，瑞士联邦理工学院，苏黎世（1984年）。[18] Rueppel, R.A.《流密码的分析与设计》，《通信与控制工程丛书》，施普林格出版社（1986年）。