第 36 卷 第 4 期 应 用 数 学 学 报 Vol. 36 No. 4
2013 年 7 月 ACTA MATHEMATICAE APPLICATAE SINICA July, 2013

Galois 环上极大周期序列的平移等价 *

张晓磊

(中国科学院信息工程研究所 信息安全国家重点实验室, 北京 100093)

(广州大学数学与信息科学学院, 广州 510006)

(数学与交叉科学广东普通高校重点实验室 (广州大学), 广州 510006)

(E-mail: zxl@is.ac.cn)

胡 磊

(中国科学院信息工程研究所 信息安全国家重点实验室, 北京 100093)

(E-mail: hu@is.ac.cn)

摘 要 本文给出了 Galois 环上两个具有相同特征多项式的极大周期序列是否平移等价的一个判定方法, 以及在两个序列平移等价的情况下, 利用模 p 方幂提升技术, 给出了一个计算它们的平移距离的方法.

关键词 Galois 环; 极大周期序列; 平移等价

MR(2000) 主题分类 11T71

中图分类 O157.4

1 背景介绍

Galois 环是有限域和整数剩余类环的自然推广. 近年来, 由于整数剩余类环和 Galois 环上序列能用于生成好的二元非线性码、数字信号序列和加密密钥, Galois 环上的序列和编码得到了广泛的研究, 它们在编码理论 [1,2], 通信 [3−5] 以及密码学 [6] 等领域有着广泛的应用.

Galois 环上的极大周期序列是序列研究中的一类重要序列. 利用 Galois 环的扩张的迹映射, Galois 环上极大周期序列在给定特征多项式下的代数表示在 [7−9] 中得到了完全的刻画. 在实际应用中, 平移等价的序列被认为是相同的. 因此, 判断两个极大周

本文 2011 年 8 月 22 日收到. 2012 年 1 月 30 日收到修改稿.

* 国家 973 计划 (2013CB834203) 和国家自然科学基金 (61070172,10990011) 资助项目.

期序列是否平移等价，以及求出平移等价序列间的平移距离是很重要的应用问题. 本文中，我们研究解决了 Galois 环上极大周期序列的相应问题. 我们的方法分成两个步骤，首先通过求解有限域上离散对数的方法求出 Galois 环上两个具有相同特征多项式的极大周期序列模 q^n-1 剩余意义下的平移距离，然后通过迭代求解模 p^i 的线性同余关系判定 Galois 环上两个极大周期序列是否平移等价并求出完整的平移距离.

2　预备知识

设 p 是一个素数，e 是一个正整数. 整数的剩余类环 $\mathbb{Z}_{p^e}$ 是一种特殊的 Galois 环. 本质上，Galois 环是某个 $\mathbb{Z}_{p^e}$ 的一个非分歧扩张，它可以用三个整数 p, e 和 d 来刻画，其中 p^e 是环的特征，d 是扩张次数. 这样的 Galois 在环同构的意义下是唯一的，我们把它记为 $\mathrm{GR}(p^e, d)$.

设 R 是 Galois 环 $\mathrm{GR}(p^e, d)$ 且 $q=p^d$, 则 R 是一个以 pR 为极大理想的局部环，它的剩余类域 R/pR 是有限域 $\mathbb{F}_q$. 记 $\bar{\cdot}$ 为 R 到 $R/pR\cong\mathbb{F}_q$ 的自然同态，它诱导出 $R[x]$ 到 $\mathbb{F}_q[x]$ 的一个同态，同样记为 $\bar{\cdot}$.

若 $f(x)$ 是 $\mathbb{Z}_{p^e}$ 上的首一 d 次多项式，且 $\overline{f}(x)$ 是 $\mathbb{F}_q[x]$ 上的不可约多项式，则 Galois 环 $\mathrm{GR}(p^e, d)$ 可以通过构造商环 $\mathbb{Z}_{p^e}[x]/\big(f(x)\big)$ 得到. 容易看出，$\mathrm{GR}(p^e, d)$ 有 p^{ed} 个元素.

Galois 环 $R=\mathrm{GR}(p^e, d)$ 的子集 $\Sigma_R=\{a\in R|a^q=a\}$ 称为 R 的 Teichmüller 集. 集合 $\Sigma_R^*=\Sigma_R\backslash\{0\}$ 在 R 的乘法下是一个 $q-1$ 阶循环群. 映射 $\bar{\cdot}$ 限制在 Σ_R^* 上得到 Σ_R^* 到 $\mathbb{F}_q^*$ 的一个群同构. R 中的元素 a 可以唯一表示为

$$a=a_0+pa_1+\cdots+p^{e-1}a_{e-1},\ a_0,\ a_1,\ \cdots,\ a_{e-1}\in\Sigma_R,$$

这个表示称为 p-adic 表示. a 为 R 中可逆元的充分必要条件是 $a_0\neq 0$. 记

$$\Pi_R=\{1+pa_1+\cdots+p^{e-1}a_{e-1}|a_1,\cdots,a_{e-1}\in\Sigma_R\},$$

它是 R 的一个乘法子群，其元素在剩余类域上的约化为 1. R 的可逆元子群 R^* 可以分解为 Σ_R^* 与 Π_R 的直积 $\Sigma_R^*\times\Pi_R$. 容易看出 $|\Sigma_R^*|=q-1$, $|\Pi_R|=q^{e-1}$, 以及 $|R^*|=(q-1)q^{e-1}$. 如果 $d'|d$, 那么 $R'=\mathrm{GR}(p^e, d')$ 是 $R=\mathrm{GR}(p^e, d)$ 的一个子环. 类似有限域的迹映射，我们可以定义 R 到 R' 的相对迹函数为

$$\mathrm{Tr}(a)=\sum_{i=0}^{d/d'-1}(a_0^{p^{d'i}}+pa_1^{p^{d'i}}+\cdots+p^{e-1}a_{e-1}^{p^{d'i}}).$$

Tr 是 R 的一个 $R'-$ 自同构，即它使得 R' 的元素映射成自身. 更多 Galois 环的基本知识可以参考 [10,11].

R 上的序列为 $\underline{s}=(s_k)_{k\in\mathbb{N}}$, 其中 $s_k\in R$. R 上全体序列的集合记为 Ω. 对 Ω 中的序列 $\underline{s}$, 若存在正整数 k 使得对一切 $i\in\mathbb{N}$ 都有 $s_i=s_{i+k}$, 则称 $\underline{s}$ 是周期的，并称满足条件的最小的正整数 k 为 $\underline{s}$ 的周期，记为 $\mathrm{per}(\underline{s})$. 若 $f(x)=c_0+c_1x+\cdots+c_nx^n\in R[x]$, 定义

$f(x)\underline{s} = c_0L^0(\underline{s}) + c_1L^1(\underline{s}) + \cdots + c_nL^n(\underline{s})$, 其中 $L^i(a_0, a_1, a_2, \cdots) = (a_i, a_{i+1}, a_{i+2}, \cdots)$. 因此, Ω 可以自然地看作一个 $R[x]$- 模. 若 $f(x)\underline{s}$ 为全零序列 $\underline{0}$, 则称 $f(x)$ 为 $\underline{s}$ 的零化多项式. Ω 中以 $f(x)$ 为零化多项式的全体序列的集合记为 $\Omega(f)$, 显然它是 Ω 的一个 $R[x]-$ 子模. 若 $\underline{s} \in \Omega(f)$, 容易证明

$$c_0s_i + c_1s_{i+1} + \cdots + c_ns_{i+n} = 0, \qquad i \in \mathbb{N}.$$

对于 n 次首一多项式 $f(x)$, 序列 $\underline{s}$ 的第 j 项 s_j 被其之前的 n 项完全确定. 若 $f(x)$ 的常数项为 R 的可逆元, 则 $\underline{s}$ 的任意一项亦可由其后 n 项完全确定. 我们把序列 $\underline{s}$ 的如下连续 n 项构成的 n 维向量 $(s_i, s_{i+1}, \cdots, s_{i+n-1})$ 称为 $\underline{s}$ 的第 i 个状态, 并把第 0 个状态 $(s_0, s_1, \cdots, s_{n-1})$ 称为 $\underline{s}$ 的初始状态. 由于 R 是有限环, 所以长度为 n 的不同状态是有限的, 因此 $\Omega(f)$ 中的序列都是周期序列.

众所周知, 有限域上序列的周期与有限域上的多项式周期密切相关. 对于 Galois 环上的多项式, 也有相应的多项式周期概念. 设 $f(x)$ 是 Galois 环 R 上一个多项式, 若存在正整数 r 使得 $f(x)|x^r - 1$, 则称 $f(x)$ 是周期的, 并称满足此条件的最小正整数 r 为 $f(x)$ 的周期, 记为 $\mathrm{per}(f)$. 不难证明, $f(x)$ 为周期多项式的充分必要条件为 $f(0) \in R^*$.

最后, 对于正整数 m, 它的 p-adic 指数是使得 $p^k|m$ 的最大的整数 k, 记作 $v_p(m)$. p-adic 指数可以按如下的方式扩展到 Galois 环上.

定义 1 在 $R = \mathrm{GR}(p^e, d)$ 中, 存在理想升链 $\{0\} = p^eR \subset p^{e-1}R \subset \cdots \subset pR \subset R$. 若 $0 \neq a \in R$, 则存在 $0 \leq i \leq e-1$, 使得 $a \in p^iR$ 但 $a \notin p^{i+1}R$, 定义 $v_p(a) = i$. 定义 $v_p(0) = e$.

3 平移等价问题

设 $\underline{a} = (a_i)_{i\in\mathbb{N}}$, $\underline{b} = (b_i)_{i\in\mathbb{N}}$ 是 $R = \mathrm{GR}(p^e, d)$ 上两个周期序列, 如果对任意 i 有 $b_i = a_{i+k}$, 则称序列 $\underline{a}$ 和 $\underline{b}$ 是平移等价的. 满足这个条件的整数 k 称为序列 $\underline{a}$ 和 $\underline{b}$ 的距离. 容易看出此时有 $\underline{b} = x^k\underline{a}$.

若 f 是 R 上的 n 次周期多项式, 则 $\Omega(f)$ 中的序列都是周期的. 设序列 $\underline{s} \in \Omega(f)$, 根据 [7−9], $\underline{s}$ 的周期满足

$$\mathrm{per}(f) = p^i\mathrm{per}(\overline{f}) \leq p^i(q^n - 1), \qquad 0 \leq i < e.$$

若等号成立, 则称 f 是 R 上的极大周期多项式, $\underline{s}$ 是极大周期序列. [7−9] 对极大周期多项式进行了研究, 并给出了极大周期多项式的刻画, 为构造极大周期多项式提供了便利. 众所周知, 有限域上极大周期多项式所零化的非零序列都是极大周期的, 但对于 R 上的极大周期多项式, 这一结论并不成立. 若 f 为 R 上 n 次极大周期多项式, $\underline{s}$ 是 $\Omega(f)$ 中非零序列, 则有

$$\mathrm{per}(\underline{s}) = p^{e-1-v}(q^n - 1), \qquad v = \min\{v_p(s_{i+j}) \mid i \in \mathbb{N},\ 0 \leq j < n\}.$$

若 $\underline{s}$ 为 R 上极大周期序列，则 $v=0$，即在 $s_i, s_{i+1}, \cdots, s_{i+n-1}$ 中至少有一个是可逆元. 下面的定理给出了 $\Omega(f)$ 中极大周期序列的计数.

定理 1　设 $f(x)\in R[x]$ 为 n 次极大周期多项式，则 $\Omega(f)$ 中共有 $q^{(e-1)n}(q^n-1)$ 个极大周期序列，以平移等价为标准可以分为 $p^{(e-1)(dn-1)}$ 个等价类.

证　设 $\underline{s}$ 为 $\Omega(f)$ 中的一个序列，其初始状态向量为 $(s_0, s_1, \cdots, s_{n-1})$. 若 $\underline{s}$ 是极大周期的，则 $s_0, s_1, \cdots, s_{n-1}$ 中至少有一个可逆元. 根据式 (1)，R 中的可逆元个数为 $(q-1)q^{e-1}$，故满足条件的 $\underline{s}$ 共有 $|R|^n-|R\backslash R^*|^n=q^{(e-1)n}(q^n-1)$ 个. 而极大周期序列的长度为 $p^{e-1}(q^n-1)$，所以每个序列与 $p^{e-1}(q^n-1)$ 个序列等价，等价类的个数为

$$\frac{q^{(e-1)n}(q^n-1)}{p^{e-1}(q^n-1)}=p^{(e-1)(dn-1)}.$$

上述定理表明 $\Omega(f)$ 中本质不同的的极大周期序列个数为 $p^{(e-1)(dn-1)}$. 我们提出如下的平移等价问题：设 $e\geq 2$，$f(x)$ 是 R 上一个 n 次首一极大周期多项式，$\underline{s},\underline{t}$ 是 $\Omega(f)$ 中两个极大周期序列，它们的初始状态分别为 $(s_0,s_1,\cdots,s_{n-1})$ 和 $(t_0,t_1,\cdots,t_{n-1})$. 如何判定 $\underline{s},\underline{t}$ 是否平移等价？若平移等价，如何确定平移等价距离 k，使得 $\underline{t}=x^k\underline{s}$. 这个问题也可以看作一个位置查找问题：确定位置 k，使得 $\underline{t}$ 的初始状态 $(t_0,t_1,\cdots,t_{n-1})$ 是 $\underline{s}$ 的第 k 个状态.

4　极大周期序列的平移等价的判定

在本节中，R 表示 Galois 环 $\mathrm{GR}(p^e,d)$. 设 $f(x)=c_0+c_1x+c_2x^2+\cdots+c_nx^n$ 为 $R[x]$ 中的 n 次极大周期多项式，则 $\overline{f}(x)$ 是 $\mathbb{F}_q$ 上的本原多项式. 令 $S=R[x]/\big(f(x)\big)$，S 是 Galois 环 $\mathrm{GR}(p^e,dn)$. 设 θ 为 $f(x)$ 在 S 中一根，则 $S=R[\theta]$. 环 S 中的元素 a 可以表示为 $1, \theta, \cdots, \theta^{n-1}$ 的 R- 线性组合

$$a=a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1}.$$

在本节中，我们将采用上述方式表示 S 中的元素. 下面的引理来自 [12]，给出了 R 上序列的迹表示.

引理 1[12]　设 f 为极大周期多项式，$\underline{s}=(s_0, s_1, \cdots)$ 为 $\Omega(f)$ 中的极大周期序列，则 $\underline{s}$ 具有迹表示 $s_i=\mathrm{Tr}(\xi\theta^i)$，其中 $i\in\mathbb{N}$，ξ 为 S 中一个乘法可逆元.

由上节的讨论可知 $\underline{s}$ 与 $\underline{t}$ 平移等价当且仅当 $\underline{t}$ 的初始状态向量是 $\underline{s}$ 的某个状态向量，不妨设为第 k 个. 根据引理 1，$\underline{s}$ 的第 k 个状态向量可表示为

$$\big(\mathrm{Tr}(\xi\theta^k), \mathrm{Tr}(\xi\theta^{k+1}), \cdots, \mathrm{Tr}(\xi\theta^{k+n-1})\big).$$

这样就把判断两个极大周期序列是否平移等价的问题与某个 θ^k 联系起来了. 如果我们能找到这个 θ^k，并从中求出 k，就能判断两个序列是否平移等价，并能求出平移距离. 对于任意 $k\in\mathbb{N}$，由于 $\theta^k\in R[\theta]$，所以存在 R 中的元素 $x_0, x_1, \cdots, x_{n-1}$，使得

$$\theta^k=x_0+x_1\theta+\cdots+x_{n-1}\theta^{n-1},$$

关于系数 $x_0, \cdots, x_{n-1}$ 我们有如下结论：

定理 2 设 $f(x)$ 是 R 上极大周期多项式， $\Omega(f)$ 中一个极大周期序列 $\underline{s}$ 具有迹表示 $\big(\mathrm{Tr}(\xi\theta^i)\big)_{i\in\mathbb{N}}$. 又设 V_i 是 $\underline{s}$ 的第 i 个状态. 若 $\theta^k = \sum\limits_{i=0}^{n-1} x_i\theta^i$, 其中 $x_0, \cdots, x_{n-1} \in R$, 则 $V_k = \sum\limits_{i=0}^{n-1} x_i V_i$.

证 由于 $\theta^k = \sum\limits_{i=0}^{n-1} x_i\theta^i$, 等式两边乘以 $\xi\theta^j$, $0 \le j \le n-1$; 得到 n 个等式

$$\xi\theta^{k+j} = \sum_{i=0}^{n-1} x_i\xi\theta^{i+j}, \qquad 0 \le j \le n-1. \tag{1}$$

把迹函数 $\mathrm{Tr}(\cdot)$ 作用到这些等式两边，得到

$$s_{k+j} = \sum_{i=0}^{n-1} x_i s_{i+j}, \qquad 0 \le j \le n-1. \tag{2}$$

这组等式可以用 $\underline{s}$ 的状态向量表示为

$$V_k = \sum_{i=0}^{n-1} x_i V_i. \tag{3}$$

定理 2 表明， $\underline{s}$ 的每个状态向量 V_k 都可以用最初的 n 个状态向量 $V_0, V_1, \cdots, V_{n-1}$ 线性表示出来，而且线性表示的系数恰好与用 $1, \theta, \theta^2, \cdots, \theta^{n-1}$ 线性表示 θ^k 的系数保持一致. 如果 $\underline{t}$ 的第 0 个状态是 $\underline{s}$ 的第 k 个状态，我们可以尝试从 (3) 式中解出系数 $x_0, \cdots, x_{n-1}$, 从而得到 θ^k, 然后再确定 k 的大小.

引理 2 R 上极大周期序列 $\underline{s} \in \Omega(f)$, $V_0, V_1, \cdots, V_{n-1}$ 为 $\underline{s}$ 的前 n 个为状态向量，则以它们为行向量的矩阵

$$M = \begin{pmatrix} V_0 \\ V_1 \\ \vdots \\ V_{n-1} \end{pmatrix}$$

是一个可逆矩阵.

证 $\underline{s}$ 是 $\Omega(f)$ 中的极大周期序列，所以它的模的序列 $\overline{\underline{s}}$ 为 $\mathbb{F}_q$ 上的 n 级极大周期序列. $\overline{\underline{s}}$ 的前 n 个周期可以线性表示出 $\overline{\underline{s}}$ 的每一个状态，即可以线性表示出 $\mathbb{F}_q^n$. 可见 $\overline{V_0}, \overline{V_1}, \cdots, \overline{V_{n-1}}$ 是向量空间 $\mathbb{F}_q^n$ 的一组基，因而线性无关. 以 $\overline{V_0}, \overline{V_1}, \cdots, \overline{V_{n-1}}$ 为行向量的矩阵行列式 $\det(\overline{M}) = \overline{\det(M)} \ne 0$, M 为 R 上的可逆矩阵.

上述定理表明， $\underline{s}$ 的前 n 个状态向量是 R- 模 R^n 的一组线性无关生成元. 若 V 是 $\underline{t}$ 的第 0 个状态向量，令

$$(x_0, \cdots, x_{n-1}) = VM^{-1},$$

则有 $V = x_0V_0 + x_1V_1 + \cdots + x_{n-1}V_{n-1}$. 若存在 $k \in \mathbb{N}$ 使得 $\theta^k = x_0 + x_1\theta + \cdots + x_{n-1}\theta^{n-1}$, 则 V 是 $\underline{s}$ 的第 k 个状态向量， $\underline{s}$ 和 $\underline{t}$ 平移等价. 于是我们有如下定理：

定理 3 设 $f(x)$ 为 R 上 n 次极大周期多项式，θ 是 $f(x)$ 在 $S=R[x]/\big(f(x)\big)$ 中一根．$\underline{s},\underline{t}$ 是 $\Omega(f)$ 中两个极大周期序列．设 V 为 $\underline{t}$ 的第 0 个状态向量，$V_0,V_1,\cdots,V_{n-1}$ 是 $\underline{s}$ 的前 n 个状态向量．那么存在 $x_0,x_1,\cdots,x_{n-1}\in R$ 使得

$$V=x_0V_0+x_1V_1+\cdots+x_{n-1}V_{n-1}.$$

进一步，序列 $\underline{s}$ 与 $\underline{t}$ 平移等价的充分必要条件为存在 $k\in\mathbb{N}$, 使得 $\theta^k=\sum\limits_{i=0}^{n-1}x_i\theta^i$.

设 $\tau=\sum\limits_{i=0}^{n-1}x_i\theta^i$, 下面我们考虑 $\theta^k=\tau$ 在什么情况下有解以及如何求解. 这相当于在 Galois 环上求解离散对数. 由于 $f(x)$ 是 n 次极大周期多项式, 所以 θ 的阶为 $p^{e-1}(q^n-1)$, 可设 $0\le k<p^{e-1}(q^n-1)$.

将 $\tau=\theta^k$ 两边模 p 有 $\overline{\tau}=\overline{\theta}^k$. 由于 $\overline{\theta}$ 为 $\mathbb{F}_{q^n}$ 上的本原元，利用有限域上求解离散对数的方法可以求得一个整数

$$k_{e-1}=\log_{\overline{\theta}}\overline{\tau},\qquad 0\le k_{e-1}<q^n-1. \tag{4}$$

显然 $k=k_{e-1}\pmod{q^n-1}$. 令

$$k=k_{e-1}+k'(q^n-1), \tag{5}$$

容易验证 $k'<p^{e-1}$, 设其 p 进制展开为

$$k'=k_0+k_1p+\cdots+k_{e-2}p^{e-2}, \tag{6}$$

下面给出求解 $k_0,k_1,\cdots,k_{e-2}$ 的方法.

考虑 $\tau\theta^{-k_{e-1}}$, 一方面，由 (4) 式知 $\tau\theta^{-k_{e-1}}=1\pmod p$, 所以存在 $h_1\in S$, 使得

$$\tau\theta^{-k_{e-1}}=1+ph_1. \tag{7}$$

显然 h_1 可以通过计算 $\tau\theta^{-k_{e-1}}-1$ 并提取 p 得到．另一方面，

$$\tau\theta^{-k_{e-1}}=\theta^k\theta^{-k_{e-1}}=(\theta^{q^n-1})^{k'}. \tag{8}$$

由于 $S^*=\Sigma_S^*\times\Pi_S$, 所以 θ 可以表示为

$$\theta=\theta_0(1+p\theta_1+\cdots+p^{e-1}\theta_{e-1}),$$

其中 $\theta_i\in\Sigma_S$. 特别地，$\theta_0\in\Sigma_S^*$, 其阶为 q^n-1 的一个因子．故

$$\theta^{q^n-1}=(1+p\theta_1+\cdots+p^{e-1}\theta_{e-1})^{q^n-1}.$$

显然 $\theta^{q^n-1}=1\pmod p$, 存在 $g_1\in S$ 使得

$$(1+p\theta_1+\cdots+p^{e-1}\theta_{e-1})^{q^n-1}=1+pg_1, \tag{9}$$

上式模 p^2 有 $(1+p\theta_1)^{q^n-1}=1+pg_1 \pmod{p^2}$, 从而有 $g_1=-\theta_1 \pmod{p}$. 显然 g_1 可以通过计算 $\theta^{q^n-1}-1$, 然后提取 p 得到. 从 (7) 式, (8) 式及 (9) 式有

$$\tau\theta^{-k_{e-1}}=(1+pg_1)^{k'}=1+ph_1, \tag{10}$$

其中 g_1 和 h_1 都是已知的, 而 k' 具有形式 $k_0+pk_1+\cdots+p^{e-2}k_{e-2}$. 引入新符号 k'_i 使得

$$k'_i=k_i+pk_{i+1}+\cdots+p^{e-2-i}k_{e-2}, \qquad 0\le i\le e-2,$$

k'_i 满足 $k'_i=k_i+pk'_{i+1}$, 且 k'_0 就是原来的 k'.

下面我们以 (10) 式为起点, 依次求出 $k_0,\cdots,k_{e-2}$. 根据 [9] 知当 $p>2$ 或 $p=e=2$ 时 $\theta_1\neq 0$; 当 $p=2<e$ 时 $\theta_1\neq 0,1 \pmod{p}$. 所以

$$g_1\neq\begin{cases}0, & (\mathrm{mod}\ p)\ p>2\ \ \text{or}\ \ p=e=2,\\ 0,1, & (\mathrm{mod}\ p)\ p=2<e.\end{cases} \tag{11}$$

把 (10) 式两边模 p^2, 有

$$(1+pg_1)^{k'_0}=1+ph_1 \pmod{p^2}, \tag{12}$$

展开并化简有 $k'_0g_1=h_1 \pmod{p}$, 即 $k_0g_1=h_1 \pmod{p}$. 若在模 p 意义下, h_1 与 g_1 只相差一个 $\mathbb{F}_q$ 的非零常数倍, 即常数属于 $\mathbb{F}_q$, h_1 与 g_1 看成 $\mathbb{F}_q$ 上 $\underline{\theta}$ 的次数 $\le n-1$ 的多项式相差一个 $\mathbb{F}_q$ 的非零常数倍, 则可求得 k_0. 如果不是非零常数倍, 则表明 $\underline{s}$ 与 $\underline{t}$ 并非平移等价.

设 $e>2$. 将 (10) 式两边同时乘以 $(1+pg_1)^{-k_0}$ 有

$$(1+pg_1)^{pk'_1}=(1+ph_1)(1+pg_1)^{-k_0}. \tag{13}$$

由于 $(1+pg_1)^p=1 \pmod{p^2}$, 所以存在 g_2 使得 $(1+pg_1)^p=1+p^2g_2$. 若 $p>2$, 则 $g_2=g_1 \pmod{p}$, 若 $p=2<e$, 则 $g_2=g_1^2+g_1 \pmod{p}$. 由于方程 $x^2+x=1$ 在 $\mathbb{F}_2$ 上无解以及式 (11), 我们有

$$g_2\neq\begin{cases}0, & (\mathrm{mod}\ p),\ p>2,\\ 0,1 & (\mathrm{mod}\ p)\ p=2.\end{cases} \tag{14}$$

式子 (13) 可以改写为

$$(1+p^2g_2)^{k'_1}=(1+ph_1)(1+pg_1)^{-k_0}.$$

上式右边是易于计算的, 其结果应该模 p^2 余 1. 若不然, 则表明 $\underline{s}$ 与 $\underline{t}$ 是不平移等价的. 若模 p^2 余 1, 则存在 h_2 使得 $(1+ph_1)(1+pg_1)^{-k_0}=1+p^2h_2$, 即

$$(1+p^2g_2)^{k'_1}=1+p^2h_2. \tag{15}$$

上式两边模 p^3 有 $1+p^2g_2k'_1=1+p^2h_2 \pmod{p^3}$, 即 $k_1g_2=h_2 \pmod{p}$. 由于 $g_2\neq 0 \pmod{p}$, 若 g_1 和 h_1 在模 p 的意义下只相差一个非零常数倍, 则从中可以计算出 k_1. 若模 p 不是非零常数倍的关系, 则表明序列 $\underline{s}$ 和 $\underline{t}$ 不是平移等价的.

一般地，假设我们有

$$(1+p^{i+1}g_{i+1})^{k_i'} = 1+p^{i+1}h_{i+1}, \tag{16}$$

其中 $k_i g_{i+1} = h_{i+1} \pmod p$, 且

$$g_{i+1} \neq \begin{cases} 0, & (\bmod p)\ \ p>2, \\ 0,1, & (\bmod p)\ \ p=2<e. \end{cases} \tag{17}$$

(10) 式两边乘上 $(1+p^{i+1}g_{i+1})^{-k_i}$ 有

$$(1+p^{i+1}g_{i+1})^{pk_{i+1}'} = (1+p^{i+1}h_{i+1})(1+p^{i+1}g_{i+1})^{-k_i}. \tag{18}$$

由于 $(1+p^{i+1}g_{i+1})^p = 1 \pmod{p^{i+2}}$, 所以存在 $g_{i+2} \in S$, 使得

$$(1+p^{i+1}g_{i+1})^p = 1+p^{i+2}g_{i+2}.$$

若 $p>2$, 则 $g_{i+2} = g_{i+1} \pmod p$, 若 $p=2<e$, 则 $g_{i+2} = g_{i+1}^2 + g_{i+1} \pmod p$. 由于方程 $x^2+x=1$ 在 $\mathbb{F}_2$ 上无解以及 (17) 式，有

$$g_{i+2} \neq \begin{cases} 0, & (\bmod p)\ p>2 \\ 0,\ 1 & (\bmod p)\ p=2<e. \end{cases} \tag{19}$$

(18) 式可以改写为

$$(1+p^{i+2}g_{i+2})^{k_{i+1}'} = (1+p^{i+1}h_{i+1})(1+p^{i+1}g_{i+1})^{-k_i}.$$

上式右边是容易计算的，它应该模 p^{i+2} 余 1, 否则 $\underline{s}$ 与 $\underline{t}$ 不平移等价. 若模 p^{i+1} 余 1, 则存在 h_{i+2} 使得 $(1+p^{i+1}h_{i+1})(1+p^{i+1}g_{i+1})^{-k_i} = 1+p^{i+2}h_{i+2}$, 从而 (18) 式变为

$$(1+p^{i+2}g_{i+2})^{k_{i+1}'} = 1+p^{i+2}h_{i+2}. \tag{20}$$

两边模 p^{i+3} 有 $1+k_{i+1}p^{i+2}g_{i+2} = 1+p^{i+2}h_{i+2} \pmod{p^{i+3}}$, 即 $k_{i+1}g_{i+2} = h_{i+2} \pmod p$, 其中 $g_{i+2} \neq 0 \pmod p$. 若 g_{i+2} 和 h_{i+2} 在模 p 的意义下相差一个非零常数倍，则可以求出 k_{i+1}, 若不是非零常数倍，则表明 $\underline{s}$ 与 $\underline{t}$ 并非平移等价. 于是我们把 i 成立的情形提升到了 $i+1$ 也成立. 根据数学归纳法可以看出，如果序列 $\underline{s}$ 和 $\underline{t}$ 平移等价，则我们可以求解出 $k_0, k_1, \cdots, k_{e-2}$, 从而求出平移距离

$$k = k_{e-1} + (q^n-1)(k_0 + k_1 p + \cdots + k_{e-2}p^{e-2}). \tag{21}$$

若在求解过程中，关于某一 k_i 的线性关系无解，则表明 $\underline{s}$ 和 $\underline{t}$ 不是平移等价的.

5 结论

本文给出了一种判断两个极大周期序列是否平移等价的方法. 可以看出, 在整个判定过程中, 计算复杂度最大的一步是在 $\mathbb{F}_{q^n}$ 上求解离散对数, 即确定 k_{e-1} 的步骤. 其它的计算都是容易的, 所以判定 Galois 环上两个序列是否平移等价的计算复杂度与在有限域上求离散对数的复杂度相当. 出于这个原因, 在实际应用中我们可以选择一个合适的 Galois 环 S, 使得在其剩余域 $\mathbb{F}_{q^n}$ 上离散对数的求解是容易的. 比如 q^n 比较小, 或者 q^n 虽然大、但 q^n-1 只有小的素因子 [13].

我们提出的方法不仅可以用于判断极大周期序列的平移等价, 也可以用于判断两个一般的不可约周期序列是否平移等价.

参 考 文 献

[1] Calderbank A R, Sloane J A. Modular and p-adic Cyclic Codes. *Designs, Codes and Cryptography*, 1995, 6: 21–35

[2] Interlando J C, Palazzo R, Elia M. On the Decoding of Reed-Solomon and BCH Codes Over Integer Residues Rings. *IEEE Trans. of Information Theory*, 1997, 43(3): 1013–1021

[3] Boztas S, Hammons R, Kumar P V. 4-phase Sequences with Near Optimal Correlation Properties. *IEEE Trans. of Information Theory*, 1991, 37(3): 1101–1113

[4] Kumar P V, Helleseth T, Calderbank A R, Hammons R. Large Families of Quaternary Sequences with Low Correlation. *IEEE Trans. of Information Theory*, 1996, 42(3): 579–592

[5] Udaya P, Siddiqi M. U, Optimal Biphase Sequences with Large Linear Complexities Derived form ML-Sequences over Z_4. *IEEE Trans. of Information Theory*, 1996, 42(1): 206–216

[6] Dai Z D. Binary Sequences Derived form ML-sequences over Rings I: Periods and Minimal Polynomials. *J. of Cryptology*, 1992, 5: 193–207

[7] Dai Z D, Huang M Q. Criteria of Primitive Integral Polynomials Module 2^e. *Chinese Science Bulletin*, 1990, 35(15): 1128–1130

[8] Huang M Q. Maximal Periodic Polynomials over $\mathbb{Z}/(p^d)$. *Science in China* (Series A), 1992, 35(3): 270–275

[9] 祝跃飞. Galois 环上本原多项式的一个判别准则. 数学学报, 1996, 39(6): 783–788
(Zhu Y F. A Criterion for Primitive Polynomials over Galois Rings. *Acta Mathematica Sinica* (Chinese Series), 1996, 39(6): 783–788)

[10] Wan Z X. Lectures on Finite Fields and Galois Rings. Beijing: World Publishing Corporation, 2006

[11] McDonald B. R. Finite Rings With Identity. New York: Deek, 1974

[12] 戚文峰, 戴宗铎. 环 $\mathbb{Z}/(p^d)$ 上序列的迹表示及前馈序列空间结构分析. 应用数学学报, 1997, 20(1): 128–136

(Qi W F, Dai Z D. The Trace-representation of Sequences and the Space of Nonlinear Filtered Sequences over $Z/(p^d)$. *Acat Mathematicae Applicatae Sinica*, 1997, 20(1): 128–136)

[13] Menezes A J, Orschot P G, Vanstone S A. Handbook of Applied Cryptography. Bota Raton: CRC Press, 1996

The Shift Equivalent of Maximal Period Sequences Over a Galois Ring

ZHANG Xiaolei

(*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

(*College of Mathematical and Information Sciences, Guangzhou University, Guangzhou* 510006)

(*Key Laboratory of Mathematics and Interdisciplinary Sciences of Guangdong Higher Education Institutes, Guangzhou University, GuangZhou* 510006)

(*E-mail: zxl@is.ac.cn*)

Hu Lei

(*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

(*E-mail: hu@is.ac.cn*)

Abstract In this paper, we study the condition of shift equivalence of two maximal periodic sequences which have the same characteristic polynomial over a Galois rings, and give an algorithm to decide the shift distance between these two sequences when they are shift equivalent.

Key words Galois ring; maximal periodic sequence; shift equivalence

MR(2000) Subject Classification 11T71

Chinese Library Classification O157.4