环 $\mathbb{Z}/(p^e)$ 上本原序列压缩映射的新结果

熊海, 屈龙江, 李超*

国防科技大学理学院, 长沙 410073

E-mail: xiong.hai@163.com, ljqu_happy@hotmail.com, lichao_nudt@sina.com

收稿日期: 2013-03-25; 接受日期: 2013-08-20; * 通信作者

国家自然科学基金 (批准号: 61272484)、信息保障技术重点实验室开放基金 (批准号: KJ-12-02)、湖南省研究生科研创新 (批准号: CX2013B007) 和国防科大研究生创新 (批准号: B130201) 资助项目

摘要 令 $\mathbb{Z}/(p^e)$ 表示整数剩余类环, 其中 p 为素数且 $e \geq 2$ 为正整数. 令 $f(x)$ 表示 $\mathbb{Z}/(p^e)$ 上的 n 次本原多项式, $G'(f(x), p^e)$ 表示 $\mathbb{Z}/(p^e)$ 上所有由 $f(x)$ 生成的本原序列构成的集合. 设序列 $\mathbf{a} \in G'(f(x), p^e)$, 它有唯一的 p 进制展开 $\mathbf{a} = \mathbf{a}_0 + \mathbf{a}_1 p + \cdots + \mathbf{a}_{e-1} p^{e-1}$. 令 $\varphi(x_0, x_1, \dots, x_{e-1}) = g(x_{e-1}) + \mu(x_0, x_1, \dots, x_{e-2})$ 表示由 $\mathbb{F}_p^e$ 到 $\mathbb{F}_p$ 的一个 e 变元多项式. 那么, φ 可以诱导出一个从 $G'(f(x), p^e)$ 到 $\mathbb{F}_p^\infty$ 的压缩映射. 在 p 为奇素数且 $f(x)$ 为强本原多项式的条件下, 人们已经证明该压缩映射是保熵的. 而本文证明该压缩映射在 $f(x)$ 为本原多项式的条件下仍然是保熵的. 当 $\deg(g(x)) \geq 2$ 时, 我们还要求 $\deg(g(x))$ 为奇数, 或者 $g(x) = x^k + \sum_{i=0}^{k-2} c_i x^i$.

关键词 压缩映射 整数剩余类环 线性递归序列 本原序列

MSC (2010) 主题分类 11B50, 94A55, 94A60

1 引言

线性反馈移位寄存器是用来产生伪随机序列的重要工具. 例如, 有限域上线性反馈移位寄存器所产生的极大长度序列被证明具有许多优良性质, 且广泛应用于密码和通信系统中. 同样地, 整数剩余类环上的极大长度序列也得到了广泛的研究. 例如, 文献 [1–4] 研究了环上极大长度序列的权位序列的基本性质和一些简单形式的压缩映射的保熵性, 文献 [5] 主要研究了具有复杂形式的压缩映射的保熵性. 这些研究表明, 环上极大长度序列和它们的权位序列也拥有许多良好的伪随机性质, 这意味着它们在密码学中具有广泛的应用前景.

1.1 本原多项式

令 p 为素数, e 为正整数, $\mathbb{Z}/(p^e) = \{0, 1, \dots, p^e - 1\}$ 为整数剩余类环. 特别地, 考虑到 $\mathbb{Z}/(p)$ 实际上是 p 元有限域, 我们将其记为 $\mathbb{F}_p$.

令 $f(x)$ 表示 $\mathbb{Z}/(p^e)$ 上的一个 n 次首一多项式, 即 $f(x) \in \mathbb{Z}/(p^e)[x]$. 如果 $f(0) \not\equiv 0 \pmod{p}$, 那么, 存在一个正整数 P 使得 $f(x)$ 在 $\mathbb{Z}/(p^e)[x]$ 中满足 $f(x) \mid x^P - 1$. 满足此条件的最小的正整数 P 称为 $f(x)$ 的周期, 记为 $\text{per}(f(x), p^e)$. 可证明 $\text{per}(f(x), p^e) \leq p^{e-1}(p^n - 1)$. 如果 $f(x)$ 的周期达到了该上界, 那么称 $f(x)$ 是 $\mathbb{Z}/(p^e)$ 上的一个本原多项式. 显然, 如果 $f(x)$ 是 $\mathbb{Z}/(p^e)$ 上的一个本原多项式, 那么它也是 $\mathbb{Z}/(p^k)$ 上的本原多项式, 其中 $1 \leq k \leq e$.

英文引用格式: Xiong H, Qu L J, Li C. Further results on the compression maps of primitive sequences over $\mathbb{Z}/(p^e)$ (in Chinese). *Sci Sin Math*, 2014, 44: 369–379, doi: 10.1360/012014-19

关于 $\mathbb{Z}/(p^e)$ 上的本原多项式, Huang 和 Dai^[6] 有如下结果.

性质 1^[6] 令 $f(x)$ 是 $\mathbb{Z}/(p^e)$ 上的一个 n 次本原多项式, $T = p^n - 1$. 则对任意 $1 \leq i \leq e-1$, 存在 $\mathbb{Z}/(p^e)$ 上的一个次数小于 n 的多项式 $h_i(x)$, 使得

$$x^{p^{i-1}T} \equiv 1 + p^i h_i(x) \pmod{f(x)}.$$

此外, 如果 p 是一个奇素数, 那么, $h_1(x) \equiv h_2(x) \equiv \cdots \equiv h_{e-1}(x) \pmod{p}$. 否则,

$$h_2(x) \equiv \cdots \equiv h_{e-1}(x) \equiv h_1(x) + h_1^2(x) \pmod{(f(x), 2)}.$$

给定 $\mathbb{Z}/(p^e)$ 上的一个本原多项式 $f(x)$, 定义 $h_f(x)$ 如下:

$$h_f(x) = \begin{cases} h_1(x) \pmod{p}, & \text{如果 } p > 2 \text{ 或 } p = e = 2, \\ h_1(x) + h_1^2(x) \pmod{(f(x), 2)}, & \text{其他情形.} \end{cases} \quad (1.1)$$

若 $\deg(h_f(x)) \geq 1$, 则称 $f(x)$ 是 $\mathbb{Z}/(p^e)$ 上的强本原多项式.

1.2 本原序列

本文用 $\mathbf{a}$ (或 a) 来表示 $\mathbb{Z}/(p^e)$ 上的一个序列 (或一个元素), 用 $\mathbf{0}$ 来表示全零序列 $(0, 0, \dots)$.

令

$$f(x) = x^n + \sum_{i=0}^{n-1} c_i x^i \in \mathbb{Z}/(p^e)[x].$$

对任意序列 $\mathbf{a} = (a(0), a(1), \dots)$, $f(x)$ 对序列 $\mathbf{a}$ 的作用定义为 $\mathbf{b} = f(x)\mathbf{a}$, 其中

$$b(t) = f(x)a(t) = a(t+n) + \sum_{i=0}^{n-1} c_i a(t+i) \pmod{p^e}, \quad t \geq 0.$$

如果 $f(x)\mathbf{a} = \mathbf{0}$, 则称 $\mathbf{a}$ 是由 $f(x)$ 生成的序列, $f(x)$ 是 $\mathbf{a}$ 的一个特征多项式或生成多项式.

令 $G(f(x), p^e) = \{\mathbf{a} \mid f(x)\mathbf{a} = \mathbf{0}\}$, $G'(f(x), p^e) = \{\mathbf{a} \mid \mathbf{a} \neq \mathbf{0} \pmod{p}, f(x)\mathbf{a} = \mathbf{0}\}$ 为 $\mathbb{Z}/(p^e)$ 上的两个序列集. 如果 $f(x)$ 是本原多项式, 且 $\mathbf{a} \in G'(f(x), p^e)$, 那么称 $\mathbf{a}$ 为本原序列. 特别地, 当 $e = 1$ 时, 本原序列就是著名的 m 序列.

给定 $\mathbb{Z}/(p^e)$ 上的一条序列 $\mathbf{a}$, 它的每个元素 $a(t)$ 都可以 p 进制展开为

$$a(t) = a_0(t) + a_1(t)p + \cdots + a_{e-1}(t)p^{e-1}.$$

我们称 $\mathbf{a}_i = (a_i(0), a_i(1), \dots)$ 是 $\mathbf{a}$ 的第 i 位权位序列. 特别地, $\mathbf{a}_{e-1}$ 称为最高位权位序列. 显然, 所有权位序列都是 $\mathbb{F}_p$ 上的序列.

1.3 压缩映射

令 $\varphi(x_0, x_1, \dots, x_{e-1})$ 表示一个从 $\mathbb{F}_p^e$ 到 $\mathbb{F}_p$ 的 e 变元多项式函数. 该多项式可以诱导出一个从 $G'(f(x), p^e)$ 到 $\mathbb{F}_p^\infty$ 的压缩映射, 其定义如下:

$$\varphi: \begin{cases} G'(f(x), p^e) \rightarrow \mathbb{F}_p^\infty, \\ \mathbf{a} \rightarrow \mathbf{b} = \varphi(\mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_{e-1}), \end{cases}$$

其中 $\varphi(\mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_{e-1}) = (\varphi(a_0(t), a_1(t), \dots, a_{e-1}(t)))_{t \geq 0}$.

当 $f(x)$ 为本原或强本原多项式时, 人们已得到了许多关于 $G'(f(x), p^e)$ 上的压缩映射的性质. 文献 [6, 7] 独立得到了如下结果.

性质 2 [6, 7] 令 p 为一个素数, $f(x)$ 为 $\mathbb{Z}/(p^e)$ 上的本原多项式, $\varphi(x_0, x_1, \dots, x_{e-1}) = x_{e-1}$, 那么, 由 φ 诱导的从 $G'(f(x), p^e)$ 到 $\mathbb{F}_p^\infty$ 的压缩映射是保熵的. 也就是说, 对任意两条序列 $\mathbf{a}, \mathbf{b} \in G'(f(x), p^e)$, $\mathbf{a} = \mathbf{b}$ 当且仅当 $\mathbf{a}_{e-1} = \mathbf{b}_{e-1}$.

在 $\mathbb{Z}/(2^e)$ 上, 当 $f(x)$ 为强本原多项式时, 黄民强 [8] 得到了一个更一般的结果.

性质 3 [8] 令 $e \geq 2$, $f(x)$ 为 $\mathbb{Z}/(2^e)$ 上的强本原多项式,

$$\varphi(x_0, x_1, \dots, x_{e-1}) = x_{e-1} + cx_{e-2} + \eta(x_0, x_1, \dots, x_{e-3}),$$

那么, 由 φ 诱导的压缩映射是保熵的.

后来, Qi 和 Zhu [9] 改进了黄民强的结果, 得到了如下结论.

性质 4 [9] 令 $e \geq 2$, $f(x)$ 为 $\mathbb{Z}/(2^e)$ 上的强本原多项式,

$$\varphi(x_0, x_1, \dots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \dots, x_{e-2}),$$

那么, 压缩映射 φ 是保熵的.

文献 [10–12] 做了一系列工作, 将性质 4 的结果推广到环 $\mathbb{Z}/(p^e)$ 上, 其中 p 为奇素数.

性质 5 [10] 令 $e \geq 2$, $2 \leq k \leq p-1$, $f(x)$ 为 $\mathbb{Z}/(p^e)$ 上的本原多项式,

$$\varphi(x_0, x_1, \dots, x_{e-1}) = x_{e-1}^k + \eta(x_0, x_1, \dots, x_{e-2}),$$

那么, 压缩映射 φ 是保熵的.

性质 6 [11] 令 $e \geq 2$, $f(x)$ 为 $\mathbb{Z}/(p^e)$ 上的强本原多项式,

$$\varphi(x_0, x_1, \dots, x_{e-1}) = g(x_{e-1}) + \eta(x_0, x_1, \dots, x_{e-2}),$$

其中 $2 \leq \deg g(x) \leq p-1$, 那么, 该压缩映射 φ 是保熵的.

性质 7 [12] 令 $e \geq 2$, $f(x)$ 为 $\mathbb{Z}/(p^e)$ 上的强本原多项式,

$$\varphi(x_0, x_1, \dots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \dots, x_{e-2}),$$

那么, 压缩映射 φ 是保熵的.

在性质 3, 4, 6 和 7 中, 生成多项式 $f(x)$ 总是要求为强本原多项式. 本文将证明在 $f(x)$ 只是本原多项式的条件下, 性质 6 和 7 仍然是正确的. 准确地说, 我们证明了当 $f(x)$ 为本原多项式时, 性质 7 是正确的. 如果

$$g(x) = x^k + \sum_{i=0}^{k-2} c_i x^i,$$

或者 $\deg(g)$ 为奇数, 那么性质 6 在 $f(x)$ 为本原多项式的条件下也是正确的.

1.4 符号说明

在下文中, p 为奇素数, $f(x)$ 表示 $\mathbb{Z}/(p^e)$ 上的 n 次本原多项式, $T = p^n - 1$. 对给定的 $f(x)$, $h_f(x)$ 和 $h_i(x)$ ($1 \leq i \leq n$) 表示 (1.1) 中定义的多项式.

2 主要结果

2.1 已有结论介绍

为了证明本文的主要结论, 我们先介绍一些关于本原序列及其权位序列的已有结果.

Dai^[13] 得到了有关本原序列及其权位序列的周期.

引理 1^[13] 令 $\mathbf{a} \in G'(f(x), p^e)$, 那么, 对任意的 $0 \leq i \leq e-1$, 有 $\text{per}(\mathbf{a}_i) = p^i T$, 其中 $\mathbf{a}_i$ 是 $\mathbf{a}$ 的第 i 位权位序列. 特别地, $\text{per}(\mathbf{a}_{e-1}) = \text{per}(\mathbf{a}) = p^{e-1} T$.

如果 $\mathbf{a} \neq \mathbf{0}$ 是由本原多项式生成的非本原序列, 那么, 它的权位序列的周期性质仍然可以从这个引理得到. 这是因为, 当 k 是满足 $\mathbf{a} \equiv \mathbf{0} \pmod{p^k}$ 的最大正整数时, $\frac{\mathbf{a}}{p^k} = (a(t)/p^k)_{t \geq 0} \in G'(f(x), p^{e-k})$. 在下文中, 我们用到该结论时将不再做解释.

Kuranki 等人^[14] 给出了本原序列不同权位序列之间的一个联系.

引理 2^[14] 令 $e \geq 2$, $\mathbf{a} \in G'(f(x), p^e)$, $\alpha = h_f(x)\mathbf{a}_0 \pmod{p}$, 那么, 对任意的 $j \in \mathbb{Z}/(p)$ 有

$$(x^{jp^{e-2}T} - 1)\mathbf{a}_{e-1} \equiv j\alpha \pmod{p}.$$

也就是说,

$$a_{e-1}(t + jp^{e-2}T) = a_{e-1}(t) + j\alpha(t) \pmod{p},$$

其中 $t \geq 0$.

给定 $a \in \mathbb{F}_p$, 令 $C(x, a)$ 为从 $\mathbb{F}_p$ 到 $\mathbb{F}_p$ 的一个多项式函数, 其定义如下:

$$C(x, a) = \begin{cases} 0, & \text{如果在整数环中 } x + a < p, \\ 1, & \text{其他情形.} \end{cases}$$

多项式 $C(x, a)$ 称为进位函数, 因为它实际上表示的是 $x + a$ 在 p 进制加法中的进位. Tian 和 Qi^[12] 给出了这个函数的多项式表示, 并利用这个多项式得到了权位序列的一个结果.

引理 3^[12] 令 $C(x, a)$ 表示进位函数, $e \geq 3$, $\mathbf{a} \in G'(f(x), p^e)$, $\gamma = h_{e-2}(x)\mathbf{a}_0 \pmod{p^2} = \alpha_0 + \alpha_1 p$, 其中 $h_{e-2}(x)$ 是定义在性质 1 中的多项式, 那么,

$$C(x, a) = \sum_{u=p-a}^{p-1} (1 - (x-u)^{p-1}),$$

而且, $(x^{p^{e-3}T} - 1)a_{e-1}(t) \equiv C(a_{e-2}(t), \alpha_0(t)) + \alpha_1(t) + h_f(x)a_1(t) \pmod{p}$, 其中 $t \geq 0$.

下面的引理与文献 [12, 引理 3] 相比, 所需条件更弱, 但它们的证明是类似的.

引理 4^[12, 引理 3] 令 $e \geq 2$, $\varphi_e(x_0, x_1, \dots, x_{e-1}) = x_{e-1} + \mu_{e-1}(x_0, x_1, \dots, x_{e-2})$, $\mathbf{a}, \mathbf{b} \in G'(f(x), p^e)$, $\alpha = h_f(x)\mathbf{a}_0 \pmod{p}$, $\beta = h_f(x)\mathbf{b}_0 \pmod{p}$. 如果对任意满足 $\alpha(t) \neq 0$ 的 t ,

$$\varphi_e(a_0(t), a_1(t), \dots, a_{e-1}(t)) = \varphi_e(b_0(t), b_1(t), \dots, b_{e-1}(t)), \quad (2.1)$$

那么 $\mathbf{a}_0 = \mathbf{b}_0$.

证明 将多项式 $x^{p^{e-2}T} - 1$ 作用在 (2.1) 两边. 注意到 $\mathbf{a}_i$ 和 $\mathbf{b}_i$ ($0 \leq i \leq e-2$) 的周期都整除 $p^{e-2}T$, 我们可得到

$$(x^{p^{e-2}T} - 1)a_{e-1}(t) \equiv (x^{p^{e-2}T} - 1)b_{e-1}(t) \pmod{p}.$$

根据引理 2 可知, 对任意满足 $\alpha(t) \neq 0$ 的 t , $\alpha(t) = \beta(t)$. 又因为 $\alpha, \beta \in G'(f(x), p)$, 可得 $\alpha = \beta$. 这意味着 $h_f(x)(\mathbf{a}_0 - \mathbf{b}_0) = 0$. 再根据 $\mathbf{a}_0 - \mathbf{b}_0 \in G(f(x), p)$ 且 $\deg h_f(x) < \deg f(x)$, $\mathbf{a}_0 = \mathbf{b}_0$. $\square$

朱宣勇^[15]研究了最高位权位序列中 0 的分布规律, 得到了一个非常有意义的结果.

引理 5 ^[15] 令 $e \geq 2$, $\mathbf{a}, \mathbf{b} \in G'(f(x), p^e)$, $\alpha = h_f(x)\mathbf{a}_0 \bmod p$. 假设对任意满足 $\alpha(t) \neq 0$ 的 t , $a_{e-1}(t) = 0$ 当且仅当 $b_{e-1}(t) = 0$, 那么 $\mathbf{a} = \mathbf{b}$.

2.2 新的引理

下面两个引理的证明都是由我们自己给出的. 引理 6 的证明方法是从 Tian 和 Qi^[12]的方法发展而来, 但我们的方法并不与他们完全一致. 如果 $f(x)$ 不是一个强本原多项式, 那么他们的方法在 $e = 3$ 时将会失效. 然而我们的方法能够克服这一困难, 这也是我们能够推进他们结果的原因.

首先介绍一个在后面证明中需要经常用到的一个技巧. 令 $\mathbf{a}, \mathbf{b}$ 和 $\mathbf{c}$ 为三条序列. 设 $\mathbf{c}$ 的周期为 T_1 . 假定对任意的满足 $c(t) \neq 0$ 的 t , $a(t) = b(t)$. 令 T_2 为一个正整数且满足 $T_1 \mid T_2$, 那么当 $c(t) \neq 0$ 时, 显然也有 $c(t + T_2) \neq 0$. 因而对任意满足 $c(t) \neq 0$ 的 t , 有 $a(t + T_2) = b(t + T_2)$. 更进一步, 对任意的满足 $c(t) \neq 0$ 的 t , 有 $(x^{T_2} - 1)a(t) = (x^{T_2} - 1)b(t)$.

引理 6 令 $e \geq 3$, $\varphi_e(x_0, x_1, \dots, x_{e-1}) = x_{e-1} + \mu_{e-1}(x_0, x_1, \dots, x_{e-2})$ 表示从 $\mathbb{F}_p^e$ 到 $\mathbb{F}_p$ 的 e 元多项式函数. 假设 $\mu_{e-1}(x_0, x_1, \dots, x_{e-2}) = \mu_{e-2}(x_0, x_1, \dots, x_{e-3})x_{e-2}^{p-1} + \eta_{e-1}(x_0, x_1, \dots, x_{e-2})$, 其中在 η_{e-1} 的表达式里, x_{e-2} 的次数至多为 $p-2$. 令 $\mathbf{a}, \mathbf{b} \in G'(f(x), p^e)$, $\alpha = h_f(x)\mathbf{a}_0 \bmod p$. 如果对任意满足 $\alpha(t) \neq 0$ 的 t ,

$$\varphi_e(a_0(t), a_1(t), \dots, a_{e-1}(t)) = \varphi_e(b_0(t), b_1(t), \dots, b_{e-1}(t)), \quad (2.2)$$

那么, 对任意满足 $\alpha(t) \neq 0$ 的 t , $\varphi_{e-1}(a_0(t), a_1(t), \dots, a_{e-2}(t)) = \varphi_{e-1}(b_0(t), b_1(t), \dots, b_{e-2}(t))$, 其中 $\varphi_{e-1}(x_0, x_1, \dots, x_{e-2}) = x_{e-2} - \mu_{e-2}(x_0, x_1, \dots, x_{e-3})$.

证明 假定 (2.2) 成立. 根据引理 4, 有

$$\mathbf{a}_0 = \mathbf{b}_0. \quad (2.3)$$

令 $\gamma = h_{e-2}(x)\mathbf{a}_0 \bmod p^2 = h_{e-2}(x)\mathbf{b}_0 \bmod p^2 = \alpha_0 + \alpha_1 p$, 那么,

$$\alpha_0 = h_{e-2}(x)\mathbf{a}_0 \bmod p = h_f(x)\mathbf{a}_0 \bmod p = \alpha.$$

由引理 3 可得

$$(x^{p^{e-3}T} - 1)\mathbf{a}_{e-1} \equiv C(\mathbf{a}_{e-2}, \alpha) + \alpha_1 + h_f(x)\mathbf{a}_1 \bmod p, \quad (2.4)$$

$$(x^{p^{e-3}T} - 1)\mathbf{b}_{e-1} \equiv C(\mathbf{b}_{e-2}, \alpha) + \alpha_1 + h_f(x)\mathbf{b}_1 \bmod p. \quad (2.5)$$

注意到 α 的周期为 T , 将多项式 $x^{p^{e-3}T} - 1$ 作用在 (2.2) 两边, 根据引理 1, 对任意满足 $\alpha(t) \neq 0$ 的 t ,

$$\begin{aligned} & (x^{p^{e-3}T} - 1)a_{e-1}(t) + \mu_{e-1}(a_0(t), a_1(t), \dots, a_{e-2}(t + p^{e-3}T)) - \mu_{e-1}(a_0(t), a_1(t), \dots, a_{e-2}(t)) \\ & \equiv (x^{p^{e-3}T} - 1)b_{e-1}(t) + \mu_{e-1}(b_0(t), b_1(t), \dots, b_{e-2}(t + p^{e-3}T)) \\ & \quad - \mu_{e-1}(b_0(t), b_1(t), \dots, b_{e-2}(t)) \bmod p. \end{aligned} \quad (2.6)$$

又根据引理 2 和 (2.3), $a_{e-2}(t+p^{e-3}T) = a_{e-2}(t) + \alpha(t)$ 且 $b_{e-2}(t+p^{e-3}T) = b_{e-2}(t) + \alpha(t)$. 因此, (2.6) 能够被重写为

$$\begin{aligned} & (x^{p^{e-3}T} - 1)a_{e-1}(t) + \mu_{e-1}(a_0(t), a_1(t), \dots, a_{e-2}(t) + \alpha(t)) - \mu_{e-1}(a_0(t), a_1(t), \dots, a_{e-2}(t)) \\ & \equiv (x^{p^{e-3}T} - 1)b_{e-1}(t) + \mu_{e-1}(b_0(t), b_1(t), \dots, b_{e-2}(t) + \alpha(t)) - \mu_{e-1}(b_0(t), b_1(t), \dots, b_{e-2}(t)) \pmod{p}. \end{aligned}$$

将 (2.4) 和 (2.5) 代入上面同余式, 可得

$$\begin{aligned} & \tau(t) + C(a_{e-2}(t), \alpha(t)) + \mu_{e-1}(a_0(t), a_1(t), \dots, a_{e-2}(t) + \alpha(t)) - \mu_{e-1}(a_0(t), a_1(t), \dots, a_{e-2}(t)) \\ & \equiv C(b_{e-2}(t), \alpha(t)) + \mu_{e-1}(b_0(t), b_1(t), \dots, b_{e-2}(t) + \alpha(t)) \\ & \quad - \mu_{e-1}(b_0(t), b_1(t), \dots, b_{e-2}(t)) \pmod{p}, \end{aligned} \quad (2.7)$$

其中 $\tau = h_f(x)\mathbf{a}_1 - h_f(x)\mathbf{b}_1 \pmod{p}$. 注意到 $\mathbf{a}_0 = \mathbf{b}_0$, 可知 $(\mathbf{a} - \mathbf{b}) \equiv \mathbf{0} \pmod{p}$. 因此, $(\mathbf{a}_1 - \mathbf{b}_1) \pmod{p} \in G(f(x), p)$. 所以, $(\mathbf{a}_1 - \mathbf{b}_1) \pmod{p}$ 的周期整除 T , 这意味着 $\text{per}(\tau) \mid T$.

对任意 $j \in \mathbb{F}_p$, 将多项式 $x^{jp^{e-3}T}$ 作用在 (2.7) 两边, 可得

$$\begin{aligned} & \tau(t) + C(a_{e-2}(t) + j\alpha(t), \alpha(t)) + \mu_{e-1}(a_0(t), a_1(t), \dots, a_{e-2}(t) + \alpha(t) + j\alpha(t)) \\ & \quad - \mu_{e-1}(a_0(t), a_1(t), \dots, a_{e-2}(t) + j\alpha(t)) \\ & \equiv C(b_{e-2}(t) + j\alpha(t), \alpha(t)) + \mu_{e-1}(b_0(t), b_1(t), \dots, b_{e-2}(t) + \alpha(t) + j\alpha(t)) \\ & \quad - \mu_{e-1}(b_0(t), b_1(t), \dots, b_{e-2}(t) + j\alpha(t)) \pmod{p}. \end{aligned} \quad (2.8)$$

注意到 $\alpha(t) \neq 0$, 所以, j 遍历 $\mathbb{F}_p$ 时, $j\alpha(t)$ 也遍历 $\mathbb{F}_p$. 定义 $\mathbb{F}_p$ 上的两个函数如下:

$$\begin{aligned} L(x; t) &= \tau(t) + C(a_{e-2}(t) + x, \alpha(t)) + \mu_{e-1}(a_0(t), a_1(t), \dots, a_{e-2}(t) + \alpha(t) + x) \\ & \quad - \mu_{e-1}(a_0(t), a_1(t), \dots, a_{e-2}(t) + x) \\ R(x; t) &= C(b_{e-2}(t) + x, \alpha(t)) + \mu_{e-1}(b_0(t), b_1(t), \dots, b_{e-2}(t) + \alpha(t) + x) \\ & \quad - \mu_{e-1}(b_0(t), b_1(t), \dots, b_{e-2}(t) + x). \end{aligned}$$

根据 (2.8), 可知对任意满足 $\alpha(t) \neq 0$ 的 t , $L(x; t) = R(x; t)$. 比较上面两个多项式关于 x^{p-2} 的系数, 根据引理 3, 对任意满足 $\alpha(t) \neq 0$ 的 t ,

$$\begin{aligned} & \sum_{u=p-\alpha(t)}^{p-1} (a_{e-2}(t) - u) - \mu_{e-2}(a_0(t), a_1(t), \dots, a_{e-3}(t))\alpha(t) \\ & \equiv \sum_{u=p-\alpha(t)}^{p-1} (b_{e-2}(t) - u) - \mu_{e-2}(b_0(t), b_1(t), \dots, b_{e-3}(t))\alpha(t) \pmod{p}. \end{aligned}$$

上式能够被化简为

$$a_{e-2}(t) - \mu_{e-2}(a_0(t), a_1(t), \dots, a_{e-3}(t)) \equiv b_{e-2}(t) - \mu_{e-2}(b_0(t), b_1(t), \dots, b_{e-3}(t)) \pmod{p}.$$

引理证毕. $\square$

引理 7 令 $e \geq 2$, $\mathbf{a}, \mathbf{b} \in G'(f(x), p^e)$, $\alpha = h_f(x)\mathbf{a}_0 \pmod{p}$, $\beta = h_f(x)\mathbf{b}_0 \pmod{p}$. 假设对任意满足 $\alpha(t) \neq 0$ 的 t , 存在 $\lambda, \delta \in \mathbb{F}_p$ 满足

$$b_{e-1}(t) = \lambda a_{e-1}(t) + \delta \pmod{p}. \quad (2.9)$$

那么 $\lambda = 1$, $\delta = 0$ 或者 $\lambda = \delta = p - 1$.

证明 首先, 我们证明 $\lambda \neq 0$ 且 $b_0 = \lambda a_0 \bmod p$.

如果对任意满足 $\alpha(t) \neq 0$ 的 t , (2.9) 成立, 根据引理 2, 对任意满足 $\alpha(t) \neq 0$ 的 t , $\beta(t) = \lambda \alpha(t) \bmod p$. 又因为 β 和 α 都是由 $f(x)$ 生成的 m 序列, 所以, $\beta = \lambda \alpha \bmod p$. 再由 β 和 α 的定义可知, $b_0 = \lambda a_0 \bmod p$. 注意到 $b_0 \neq 0$, 故而, $\lambda \neq 0$.

下面用归纳法证明本引理.

假定 $e = 2$. 令 $c = b - \lambda a \bmod p^2$, 那么有 $c_0 = 0$. 下面分 $c_1 = 0$ 和 $c_1 \neq 0$ 两种情形来证明引理在 $e = 2$ 时成立.

(1) 若 $c_1 = 0$, 此时, 必有 $c = 0$. 因为 a_0 和 α 都是由 $f(x)$ 生成的 m 序列, 可以找到一个整数 s 满足 $\alpha(s) \neq 0$ 且 $a_0(s) = 1$, 故 $b_0(s) = \lambda$. 此时有

$$0 = c(s) = b(s) - \lambda a(s) \bmod p^2 = (b_1(s) - \lambda a_1(s))p + (b_0(s) - \lambda a_0(s)) \bmod p^2 = \delta p \bmod p^2,$$

这意味着 $\delta = 0$. 因而, 对任意满足 $\alpha(t) \neq 0$ 的 t , $b_1 = \lambda a_1 \bmod p$. 根据引理 5 可知, $a = b$. 此时, 我们有 $\lambda = 1$, $\delta = 0$.

(2) 假定 $c_1 \neq 0$. 那么, c_1 是由 $f(x)$ 生成的 m 序列, 这是因为 $c \in G(f(x), p^2)$ 且 $c_0 = 0$. 对任意满足 $\alpha(t) \neq 0$ 的 t ,

$$c_1(t) = \frac{c(t)}{p} \bmod p = b_1(t) - \lambda a_1(t) - \frac{\lambda a_0(t) - b_0(t)}{p} \bmod p.$$

因此, 对任意满足 $\alpha(t) \neq 0$ 的 t ,

$$c_1(t) = \delta - \frac{\lambda a_0(t) - b_0(t)}{p} \bmod p.$$

因为 α 和 a_0 都是由 $f(x)$ 生成的 m 序列, 可知

$$\{1, 2, \dots, p-1\} \subseteq \{a_0(t) \mid \alpha(t) \neq 0\}.$$

注意到 $b_0(t) = \lambda a_0(t) \bmod p$, 可知

$$\left\{ \frac{\lambda a_0(t) - b_0(t)}{p} \mid \alpha(t) \neq 0 \right\} = \{0, 1, \dots, \lambda - 1\}.$$

因此,

$$|\{c_1(t) \mid \alpha(t) \neq 0\}| = |\{(\delta - i) \bmod p \mid 0 \leq i \leq \lambda - 1\}| = \lambda. \quad (2.10)$$

因为 c_1 也是由 $f(x)$ 生成的 m 序列, 可得 $\lambda = p - 1$. 因此 c_1 和 α 是线性相关的, 这意味着 $0 \notin \{c_1(t) \mid \alpha(t) \neq 0\}$. 再根据 (2.10), 可得 $\delta = p - 1$.

综合情形 (1) 和 (2) 的论述, 可知引理在 $e = 2$ 时成立.

现在假定引理在 $2 \leq e \leq k$ 时成立. 下面证明它在 $e = k + 1$ 时也成立. 令 $c = b - \lambda a \bmod p^{k+1}$. 设 $h_{k-1}(x)a_0 \bmod p^2 = \alpha_0 + \alpha_1 p$ 且 $h_{k-1}(x)b_0 \bmod p^2 = \beta_0 + \beta_1 p$, 那么, $\alpha = \alpha_0$ 且 $\beta = \beta_0$. 将多项式 $x^{p^{k-2}T} - 1$ 作用在 (2.9) 两边, 根据引理 3,

$$C(b_{k-1}(t), \beta(t)) + \beta_1(t) + h_f b_1(t) \equiv \lambda(C(a_{k-1}(t), \alpha(t)) + \alpha_1(t) + h_f a_1(t)) \bmod p.$$

再将多项式 $x^{jp^{k-2}T}$ 作用在上式两边. 当 $k \geq 3$ 时, 因为 β_1 和 α_1 的周期为 T , 且 b_1 和 a_1 的周期为 pT , 我们有

$$C(b_{k-1}(t) + j\beta(t), \beta(t)) + \beta_1(t) + h_f b_1(t) \equiv \lambda(C(a_{k-1}(t) + j\alpha(t), \alpha(t)) + \alpha_1(t) + h_f a_1(t)) \pmod{p}. \quad (2.11)$$

需要指出的是, 当 $k = 2$ 时, 上式仍然成立, 这是因为 $\beta = \lambda\alpha$, $b_1(t + jT) = b_1(t) + j\beta(t)$ 且 $a_1(t + jT) = a_1(t) + j\alpha(t)$.

定义 $\mathbb{F}_p$ 上的两个函数如下:

$$\begin{aligned} L(x; t) &= C(b_{k-1}(t) + \lambda x, \beta(t)) + \beta_1(t) + h_f b_1(t), \\ R(x; t) &= \lambda(C(a_{k-1}(t) + x, \alpha(t)) + \alpha_1(t) + h_f a_1(t)). \end{aligned}$$

那么, 根据 (2.11), 对任意满足 $\alpha(t) \neq 0$ 的 t , $L(x; t) = R(x; t)$. 比较这两个函数关于 x^{p-2} 的系数, 可得

$$\sum_{u=p-\beta(t)}^{p-1} (b_{k-1}(t) - u) \lambda^{p-2} \equiv \lambda \sum_{u=p-\alpha(t)}^{p-1} (a_{k-1}(t) - u) \pmod{p}.$$

上式能够化简为

$$b_{k-1}(t) = \lambda a_{k-1}(t) + \frac{\lambda - 1}{2} \pmod{p}. \quad (2.12)$$

与 (2.12) 的证明类似, 对任意满足 $\alpha(t) \neq 0$ 的 t ,

$$b_j(t) = \lambda a_j(t) + \frac{\lambda - 1}{2} \pmod{p}, \quad (2.13)$$

其中 $1 \leq j \leq k-1$.

根据归纳假设, $\lambda = 1$ 或 $\lambda = p-1$.

如果 $\lambda = 1$, 根据引理 5 和 (2.12), $\mathbf{a} = \mathbf{b} \pmod{p^k}$. 因此, $\mathbf{c}_k \in G(f(x), p)$. 又根据 (2.9), 对任意满足 $\alpha(t) \neq 0$ 的 t , $c_k(t) = b_k(t) - a_k(t) = \delta$. 注意到 α 是由 $f(x)$ 生成的 m 序列, 可得 $\mathbf{c}_k = \mathbf{0}$ 且 $\delta = 0$. 否则, $\mathbf{c}_k$ 也是由 $f(x)$ 生成的 m 序列, 这与 α 是由 $f(x)$ 生成的 m 序列且 $\{c_k(t) \mid \alpha(t) \neq 0\} = \{\delta\}$ 矛盾.

如果 $\lambda = p-1$, 令 $\mathbf{d} = \mathbf{a} + \mathbf{b} \pmod{p^{k+1}}$. 我们可得到如下论断.

论断 1 $\mathbf{d} = \mathbf{0}$.

如果 $\mathbf{d} \neq \mathbf{0}$, 令 i 为满足 $\mathbf{d}_i \neq \mathbf{0}$ 的最小整数 (我们总是有 $i \geq 1$, 这是因为 $\mathbf{b}_0 = \lambda \mathbf{a}_0 \pmod{p}$). 那么, $\mathbf{d}_i$ 必定是由 $f(x)$ 生成的 m 序列. 令 $S = \{0 \leq t \leq T-1 \mid \alpha(t) \neq 0, a_0(t) \neq 0\}$. 因为 α 和 $\mathbf{a}_0$ 都是由 $f(x)$ 生成的 m 序列, 易知 $|S| = p-1$, 如果 $n = 1$; 或者 $|S| \geq p^{n-2}(p-1)^2$, 如果 $n \geq 2$. 对任意 $t \in S$, 注意到 $0 < a(t) \pmod{p^i} + b(t) \pmod{p^i} < 2p^i$ 且 $\mathbf{d} \pmod{p^i} = \mathbf{0}$, 我们有

$$a(t) \pmod{p^i} + b(t) \pmod{p^i} = p^i.$$

因此, 对任意 $t \in S$, $d_i(t) = a_i(t) + b_i(t) + 1 \pmod{p}$. 当 $i = k$ 时, 根据 (2.9), 可知此时 $d_i(t) = \delta + 1$, 若 $i < k$ 时, 根据 (2.13), 可知此时 $d_i(t) = 0$, 这与 $\mathbf{d}_i$ 为 m 序列相矛盾.

该论断成立. 因此, 存在一个整数 s 满足 $\alpha(s) \neq 0, a_0(s) \neq 0$. 此时,

$$a(s) \pmod{p^k} + b(s) \pmod{p^k} = p^k.$$

因此, $d_k(s) = a_k(s) + b_k(s) + 1 \pmod{p} = \delta + 1 \pmod{p} = 0$. 这意味着 $\delta = p-1$.

综上所述, 引理成立. $\square$

事实上, 在 $f(x)$ 为强本原多项式的条件下, Zhu 和 Qi^[11] 得到了一个更强的结论.

引理 8^[11] 令 $f(x)$ 为强本原多项式, 其他符号与引理 7 一致. 那么, $\lambda = 1, \delta = 0$.

我们的结论要弱, 然而我们要求的条件也更弱. 但这足以用来证明我们的主要结论, 而且我们的方法与他们不相同.

2.3 保熵映射的新结论

本小节将给出本文的主要结论. 第一个结果是性质 7 的推广.

定理 1 令 $e \geq 2$, $f(x)$ 是 $\mathbb{Z}/(p^e)$ 上的一个 n 次本原多项式,

$$\varphi_e(x_0, x_1, \dots, x_{e-1}) = x_{e-1} + \mu_{e-1}(x_0, x_1, \dots, x_{e-2})$$

且 $\mathbf{a}, \mathbf{b} \in G'(f(x), p^e)$, $\alpha = h_f(x)\mathbf{a}_0 \bmod p$. 那么,

$$\varphi_e(a_0(t), a_1(t), \dots, a_{e-1}(t)) = \varphi_e(b_0(t), b_1(t), \dots, b_{e-1}(t)) \quad (2.14)$$

对任意满足 $\alpha(t) \neq 0$ 的 t 成立当且仅当 $\mathbf{a} = \mathbf{b}$.

证明 充分性的证明是平凡的, 仅给出必要性的证明. 如果 (2.14) 成立, 那么, 根据引理 4 可知, $\mathbf{a}_0 = \mathbf{b}_0$.

当 $e = 2$ 时, 将 $\mathbf{a}_0 = \mathbf{b}_0$ 代入 (2.14) 可得, 对任意满足 $\alpha(t) \neq 0$ 的 t , $a_1(t) = b_1(t)$. 根据引理 5, 可知此时定理成立.

假设当 $2 \leq e \leq k$ 时, 定理都成立. 当 $e = k + 1$ 时, 设

$$\mu_k(x_0, x_1, \dots, x_{k-1}) = \mu_{k-1}(x_0, x_1, \dots, x_{k-2})x_{k-1}^{p-1} + \eta_k(x_0, x_1, \dots, x_{k-1}),$$

其中 $\eta_k(x_0, x_1, \dots, x_{k-1})$ 关于 x_{k-1} 的次数至多为 $p - 2$. 根据引理 6, 对任意满足 $\alpha(t) \neq 0$ 的 t ,

$$a_{k-1}(t) - \mu_{k-1}(a_0(t), a_1(t), \dots, a_{k-2}(t)) = b_{k-1}(t) - \mu_{k-1}(b_0(t), b_1(t), \dots, b_{k-2}(t)).$$

根据归纳假设, $\mathbf{a} = \mathbf{b} \bmod p^k$. 将此关系代入 (2.14), 对任意满足 $\alpha(t) \neq 0$ 的 t , $a_k(t) = b_k(t)$. 再根据引理 5, 定理在 $e = k + 1$ 时也成立. $\square$

定理 2 令 $p > k > 1$ 为正整数,

$$g(x) = x^k + \sum_{i=0}^{k-1} c_i x^i$$

为 $\mathbb{F}_p$ 上的一个多项式函数, 其中 k 为奇数或者 $c_{k-1} = 0$. 令 $e \geq 2$ 为正整数, $f(x)$ 是 $\mathbb{Z}/(p^e)$ 上的一个 n 次本原多项式,

$$\varphi_e(x_0, x_1, \dots, x_{e-1}) = g(x_{e-1}) + \mu_{e-1}(x_0, x_1, \dots, x_{e-2}),$$

$\mathbf{a}, \mathbf{b} \in G'(f(x), p^e)$, $\alpha = h_f(x)\mathbf{a}_0$ 且 $\beta = h_f(x)\mathbf{b}_0$. 那么,

$$\varphi_e(a_0(t), a_1(t), \dots, a_{e-1}(t)) = \varphi_e(b_0(t), b_1(t), \dots, b_{e-1}(t)) \quad (2.15)$$

对任意满足 $\alpha(t) \neq 0$ 的 t 成立当且仅当 $\alpha = \beta$.

证明 我们略去关于充分性的证明, 而仅给出必要性的证明.

(1) 假设 k 为奇数. 将多项式 $x^{jp^{e-2}T} - 1$ 作用在 (2.15) 两边,

$$g(a_{e-1}(t) + j\alpha(t)) - g(a_{e-1}(t)) = g(b_{e-1}(t) + j\beta(t)) - g(b_{e-1}(t)).$$

根据上式可知, 当 $\alpha(t) \neq 0$ 时, $\beta(t) \neq 0$. 否则, 可找到一个整数 s 满足 $\alpha(s) \neq 0$ 且 $\beta(s) = 0$. 此时, 对任意 $j \in \mathbb{F}_p$, $g(a_{e-1}(s) + j\alpha(s)) - g(a_{e-1}(s)) = 0$, 这与 $p > \deg(g) > 1$ 矛盾. 又因为 α 和 β 都是由 $f(x)$ 产生的 m 序列, 所以有 $\beta = \lambda\alpha$ 且 $\lambda \neq 0$.

令 $L(x; t) = g(a_{e-1}(t) + x) - g(a_{e-1}(t))$, $R(x; t) = g(b_{e-1}(t) + \lambda x) - g(b_{e-1}(t))$. 那么, 对任意满足 $\alpha(t) \neq 0$ 的 t , $L(x; t) = R(x; t)$. 比较这两个多项式关于 x^k 和 x^{k-1} 的系数可得 $\lambda^k = 1$ 和 $ka_{e-1}(t) + c_{k-1} = kb_{e-1}(t)\lambda^{k-1} + c_{k-1}\lambda^{k-1}$. 因此, 对任意满足 $\alpha(t) \neq 0$ 的 t ,

$$b_{e-1}(t) = \lambda a_{e-1}(t) + \frac{c_{k-1}(\lambda - 1)}{k} \pmod{p}.$$

注意到 k 是奇数, 所以, $\lambda \neq p - 1$. 根据引理 5 和 7, 此时定理成立.

(2) $c_{k-1} = 0$ 时, 与第 (1) 部分的证明类似, 可得

$$b_{e-1}(t) = \lambda a_{e-1}(t) + \frac{c_{k-1}(\lambda - 1)}{k} \pmod{p}.$$

因为 $c_{k-1} = 0$, 根据引理 5 和 7, 定理此时也成立. □

需要注意的是, 定理 2 的条件不能再弱化. 下面是一个反例.

例 令 γ 为 $\mathbb{Z}/(p^e)$ 中的一个本原元. 显然, $f(x) = x - \gamma$ 是一个本原多项式, 但不是强本原多项式. 而且序列 $\alpha = (1, \gamma, \gamma^2, \dots)$ 和

$$\beta = (\gamma^{\frac{p^{e-1}(p-1)}{2}}, \gamma^{\frac{p^{e-1}(p-1)}{2}+1}, \gamma^{\frac{p^{e-1}(p-1)}{2}+2}, \dots)$$

都是由 $f(x)$ 生成的本原序列. 易知 $\alpha_{e-1} = -\beta_{e-1} - 1 \pmod{p}$. 令 $\varphi(x_0, x_1, \dots, x_{e-1}) = x_{e-1}(x_{e-1} + 1)$. 容易验证 $\varphi(\alpha) = \varphi(\beta)$.

3 结论

本文研究了 $G'(f(x), p^e)$ 到 $\mathbb{F}_p^\infty$ 的压缩映射的保熵性. 令

$$\varphi(x_0, x_1, \dots, x_{e-1}) = g(x_{e-1}) + \mu(x_0, x_1, \dots, x_{e-2})$$

表示 $\mathbb{F}_p^e$ 到 $\mathbb{F}_p$ 的一个多变元多项式函数. 那么, φ 可以诱导出一个 $G'(f(x), p^e)$ 到 $\mathbb{F}_p^\infty$ 的压缩映射. 在以前的文献 [10–12] 中, 人们已经证明当 $f(x)$ 是强本原多项式时, 该压缩映射是保熵的. 在本文里我们证明了, 当 $\deg(g)$ 为奇数或者

$$g(x) = x^k + \sum_{i=0}^{k-2} c_i x^i$$

时, 只需要 $f(x)$ 是本原多项式, 就能保证该压缩映射是保熵的. 尽管大部分本原多项式都是强本原多项式, 但仍然有无限多的本原多项式不是强本原多项式. 因而我们的结果是有意义的. 此外本文中使用的办法能够简化文献 [10–12] 中的证明.

致谢 感谢评审者提供的宝贵意见.

参考文献

- 1 Qi W F, Yang J H, Zhou J J. ML-sequences over rings $\mathbb{Z}/(2^e)$. In: Lecture Notes in Computer Science, vol. 1514. Berlin: Springer, 1998, 315–326
- 2 Dai Z D, Huang M Q. A criterion for primitiveness of polynomials over $\mathbb{Z}/(2^d)$. Chin Sci Bull, 1991, 36: 892–895
- 3 戚文峰, 周锦君. 环 $\mathbb{Z}/(2^e)$ 上本原序列最高权位的 0, 1 分布. 中国科学 A 辑, 1997, 27: 311–316
- 4 Qi W F, Zhou J J. Distribution of 0 and 1 in highest level of primitive sequences over $\mathbb{Z}/(2^e)$ (II). Chin Sci Bull, 1998, 43: 633–635
- 5 田甜. 带进位的反馈移位寄存器序列分析. 郑州: 信息工程大学, 2010
- 6 Huang M Q, Dai Z D. Projective maps of linear recurring sequences with maximal p -adic periods. Fibonacci Quart, 1992, 30: 139–143
- 7 Kuzmin A S, Nechaev A A. Linear recurring sequences over Galois ring. Russian Math Surveys, 1993, 48: 171–172
- 8 黄民强. 环上本元序列分析及其密码学评价. 北京: 中国科学技术大学研究生院, 1988
- 9 Qi W F, Zhu X Y. Compressing mappings on primitive sequences over and its Galois extension. Finite Fields Appl, 2002, 8: 570–588
- 10 Zhu X Y, Qi W F. Compression mappings on primitive sequences over $\mathbb{Z}/(p^e)$. IEEE Trans Inform Theory, 2004, 50: 2442–2448
- 11 Zhu X Y, Qi W F. Further result of compressing maps on primitive sequences modulo odd prime powers. IEEE Trans Inform Theory, 2007, 53: 2985–2990
- 12 Tian T, Qi W F. Injectivity of compressing maps on primitive sequences over $\mathbb{Z}/(p^e)$. IEEE Trans Inform Theory, 2007, 53: 2960–2966
- 13 Dai Z D. Binary sequences derived from ML-sequences over rings I: Periods and minimal polynomials. J Cryptology, 1992, 5: 193–207
- 14 Kurankin V L, Kuzmin A S, Mikhalev A V, et al. Linear recurring sequences over rings and modules. J Math Sci, 1995, 76: 2793–2915
- 15 朱宣勇. 环上本原序列保熵压缩映射的研究. 郑州: 信息工程大学, 2004

Further results on the compression maps of primitive sequences over $\mathbb{Z}/(p^e)$

XIONG Hai, QU LongJiang & LI Chao

Abstract Let $\mathbb{Z}/(p^e)$ be the integer residue ring with p prime and $e \geq 2$. Let $f(x)$ be a primitive polynomial over $\mathbb{Z}/(p^e)$ with degree n and $G'(f(x), p^e)$ the set of all primitive sequences over $\mathbb{Z}/(p^e)$ generated by $f(x)$. For any sequence $\mathbf{a} \in G'(f(x), p^e)$, it has a unique p -adic expansion $\mathbf{a} = \mathbf{a}_0 + \mathbf{a}_1 p + \cdots + \mathbf{a}_{e-1} p^{e-1}$. Let $\varphi(x_0, x_1, \dots, x_{e-1}) = g(x_{e-1}) + \mu(x_0, x_1, \dots, x_{e-2})$ be a function from $\mathbb{F}_p^e$ to $\mathbb{F}_p$. Then φ can induce a compression mapping from $G'(f(x), p^e)$ to $\mathbb{F}_p^\infty$. In recent years, Zhu, Tian and Qi have proved that the compression mapping is injective under the condition that p is an odd prime and $f(x)$ is a strongly primitive polynomial. In this paper, we improve their results. More exactly, we prove that the compression mapping is also injective only under the condition that p is an odd prime and $f(x)$ is a primitive polynomial. Of course we should ask that $\deg(g(x))$ is an odd number or $g(x) = x^k + \sum_{i=0}^{k-2} c_i x^i$.

Keywords compression mapping, integer residue ring, linear recurring sequence, primitive sequence

MSC(2010) 11B50, 94A55, 94A60

doi: 10.1360/012014-19