arXiv:2603.01287v1 [cs.IT] 1 Mar 2026

# 迭代 Ore 多项式求值与斜 Reed–Muller 码

Andr´e Leroy 和 Nabil Bennenni

Abstract. 本文研究迭代 Ore 多项式的两种求值方法。我们给出许多示例并比较这些求值方法。我们利用求值映射构造 Reed-Muller 码，并明确计算与此类码相关的一些数据。

## 引言

多项式求值是数学许多分支中的一项基石。在非交换代数中，最吸引人的多项式概念之一是 Ore 多项式（又称斜多项式）。已有大量研究探讨了在除环或素环上系数为元素的这类多项式的求值（[**7**],[**10**]）。在编码理论中，多项式求值尤其用于构造 Reed-Muller 码（[**11**], [**5**], [**4**]）。

我们回顾斜多项式环的一般定义。设 $K$ 是一个环，$\sigma \in End(K)$，且 $\delta$ 是 $K$ 上的斜 $\sigma$-导子（即，$\delta$ 是一个从 $K$ 到 $K$的加法映射，使得对于任意 $a$、$b \in K$、$\delta(ab)$，$= \sigma(a)\delta(b)+\delta(a)b$）。斜多项式环 $R = K[t;\sigma,\delta]$ 的元素是多项式$\sum_{i=0}^{n} a_i t^i$，其系数 $a_i \in K$ 写在左侧。这些多项式的加法与通常相同，乘法则基于交换关系 $ta = \sigma(a)t + \delta(a)$，其中 $a \in K$任意。通过这两种运算，$R$ 成为一个环。当 $K$ 是除环时，$R$ 是左主理想整环。若 $\sigma$ 是除环 $K$ 的自同构，则 $R$ 也是右主理想整环。这一构造可以迭代：我们考虑一个环 $K$，以及一列斜多项式环 $R_1 = K[t_1;\sigma_1,\delta_1]$，其中 $\sigma_1 \in End(K)$，且 $\delta_1$是 $K$的 $\sigma_1$-导子。然后构造 $R_2 = R_1[t_1;\sigma_2,\delta_2] = K[t_1;\sigma_1, \delta_1][t_2;\sigma_2,\delta_2]$，其中 $\sigma_2 \in End(R_1)$，且 $\delta_2$ 是 $R_1$的 $\sigma_2$-导子。继续这一构造，我们得到以 $n$ 个非交换变量$R = R_n = K[t_1;\ \sigma_1,\delta_1][t_2;\ \sigma_2,\delta_2]\cdots[t_n;\ \sigma_n,\delta_n]$为变量的迭代多项式环。斜多项式的求值与交换变量情形下的通常求值有很大不同。大多数文献讨论的是系数属于除环（例如 [**10**], [**7**]）的单变量（即 $n = 1$）多项式的右求值。对于基环 $K$ 不一定是除环的情况，伪线性变换非常有用（[**7**]）。当 $K$ 是除环时，即使 $\sigma$ 不是映上 [**9**]的，左求值也得到了研究。在考虑.....的求值时

*Key words and phrases.* 迭代 Ore 多项式求值、斜 Reed-Muller 码。1

在点（$a_1$，…，$a_n$）$\in K^n$处对多项式 $f(t_1, \ldots, t_n) \in R = K[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2]\cdots[t_n; \sigma_n, \delta_n]$ 求值时，我们很快就会遇到一种“非交换现象”：理想 $I = R(t_1 - a_1) + \cdots + R(t_2 - a_2)$可能等于 $R$。我们将说明如何避免这个问题。

Reed-Muller 码是在 $\mathbb{F}_2$ 上由 Reed 于 1954 [11]提出的。Kasami、Lin 和 Peterson 于 [6] 将其定义扩展到了任意有限域 $\mathbb{F}_q$。Reed-Muller 码在密码学中非常有用，确实，它们对线性密码分析具有良好的抵抗能力。感兴趣的读者可参阅 [4], 了解更多详情。Reed-Muller 码是几何码中最简单的一类，其中还包括欧几里得几何码和射影几何码。

本文结构如下。第 2 节介绍了在一般背景下对迭代多项式进行求值的两种方法。我们给出了许多示例，并对这些求值方法进行了比较。第 3 节中，我们应用求值映射来构造 Reed-Muller 码，并计算与此类码相关的一些数据。

## 1. $n$ 个变量的多项式映射。

本节中，我们为任意环 $K$（含单位元）上的迭代 Ore 扩张 $R = K[t_1; \sigma_1、\delta_1][t_2; \sigma_2、\delta_2]\cdots[t_n; \sigma_n、\delta_n]$ 中的多项式定义一种求值概念。全文中，我们要求对于任意 $1 \le i \le n$，$\sigma_i(K) \subset K$ 且 $\delta_i(K) \subset K$。我们将用到关于迭代多项式环的一些事实。

REMARK 1.1. (1) 当 $\delta = 0$ 时，我们将 Ore 扩张记为 $R = K[t; \sigma]$。类似地，当 $\sigma = id$时，记为 $R = K[t; \delta]$。(2) 我们指出，若 $u \in K$ 是一个可逆元素，且对任意 $x \in K$，都有 $\sigma(x) = I_u(x) = uxu^{-1}$，则 $K[t; \sigma; \delta] = K[u^{-1}t; u^{-1}\delta]$。注意，若 $\delta = 0$，这就得到通常的多项式环。(3) 若 $\sigma$ 是环 $K$ 的自同态，且 $x$、$a$ 是 $K$中的元素，我们定义 $\delta_a(x) = ax - \sigma(x)a$。这是 $K$ 上的一个 $\sigma$-导子，称为 $K$上的内导子。注意，在这种情况下，对任意 $x \in K$，有 $(t - a)x = \sigma(x)(t - a)$，因此 $R = K[t; \sigma, \delta] = K[t - a; \sigma]$。(4) 结合前两条说明可知，对任意 $u$、$v \in K$，若 $u$ 是一个可逆元素，则 $K[t; I_u, \delta_v] = K[u^{-1}(t - v)]$ 是通常的多项式环。

我们简要回顾多项式 $f(t) \in R = K[t$ 的求值定义：$\sigma, \delta]$ 在元素 $a \in K$ 处的求值。我们将 $f(a) \in K$ 定义为 $K$ 中满足 $f(t) - f(a) \in R(t - a)$ 的唯一元素。特别地，这意味着当 $t - a$ 是多项式 $f(t)$ 的右因子时，$a \in K$ 是多项式 $f(t)$ 的右根。接着，对于任意 $i \ge 0$，我们通过归纳定义映射 $N_i$，如下所示：

$$N_0(a) = 1, \quad N_{i+1}(a) = \sigma(N_i(a))a + \delta(N_i(a)).$$

这就得到了任意多项式 $f(t) = \sum_{i=0}^{n} b_i t^i \in R = K[t$ 在元素 $a \in K$ 处求值的具体公式：$\sigma, \delta]$

$$f(a) = \sum_{i=0}^{n} b_i N_i(a).$$

在定义迭代多项式的求值之前，我们先给出几个经典例子。

EXAMPLE 1.2. (1) 考虑复数 $\mathbb{C}$ 以及记作"–"的共轭。由此构造 Ore 扩张：$R = \mathbb{C}[t; -]$; 此处的交换关系为 $t(a+ib) = (a-ib)t$，其中 $a$，$b \in \mathbb{R}$。元素 $a \in \mathbb{C}$ 是 $t^2+1$ 的一个（右）根，当且仅当 $N_2(a) + 1 = 0$，即 $aa+1 = 0$。由此可知，$t^2+1$ 是 $R$中的不可约多项式。另一方面，容易验证 $t^2+1$ 是中心多项式，因此商 $R/(t^2+1)$ 与四元数代数 $\mathbb{H}$同构。另一方面，多项式 $t^2-1$ 的根恰好是范数为 1 的复数。

(2) 另一类重要的 Ore 扩张可通过如下方式给出：Weyl代数 $A_1 = k[X][Y; id., \frac{d}{dx}]$，其中 $k$ 是一个域。因此，出现的交换关系为 $YX = XY + 1$。在特征零下，这个代数是单代数（除了 0 和 $A_1$之外，它没有任何双边理想）。如果$char(k) = p > 0$，那么 $A_1$ 是其中心 $k[X^p, Y^p]$ 上的一个 $p^2$ 维代数。对 $Y$ 的幂在 $X$ 处求值，例如可得 $Y^2(X) = X^2+1$、$Y^3(X) = X^3+3X$，以及 $Y^4(X) = X^4+6X^2+3$。W

可以 iterate th确保 dure an d get the Weyl algebra $A_n(k)$.

(3) 在编码理论中，形如 $\mathbb{F}_q[t;\theta]$ 的 Ore 扩张已被广泛应用，其中 $q = p^n$，且$\theta$ 是 Frobenius 自同构，其定义为 $\theta(a) = a^p$，其中 $a \in \mathbb{F}_q$（参见 [**2**]）。在 [**7**]，中，这些扩张的求值和因式分解都通过经典的（未扭曲）多项式求值来描述。一般的 Ore 扩张也被用于构造码（[**3**]）。

设定 $f(t_1, t_2, \ldots, t_n) \in R = K[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \cdots [t_n; \sigma_n, \delta_n]$ 以及一个 $n$-元组 $(a_1, a_2, \ldots, a_n) \in K^n$（$K$是一个环，假设在映射 $\sigma_i$和 $\delta_i$作用下保持稳定，且$1 \le i \le n$）。我们希望定义 $f(a_1, a_2, \cdots, a_n)$ 的值。为中间的 Ore 扩张引入记号会比较方便。因此我们令 $R_0 = K$，并且对于 $i \in \{1, \ldots, n-1\}$, $R_i = R_{i-1}[t_i; \sigma_i, \delta_i]$。注意，$R_n = R$。

设 $(a_1, a_2, \cdots, a_n) \in K^n$ 并考虑 $f_0 = f(t_1, \ldots, t_n) \in R = R_{n-1}[t_n; \sigma_n, \delta_n]$。我们可以将 $f_1 = f(t_1, \ldots, t_{n-1}, a_n) \in R_{n-1}$ 定义为$f_0$ 在右侧被 $t_n - a_n$除法所得的余数。这是

$$f_0 = q(t_1, \ldots, t_{n-1})(t_n - a_n) + f_1.$$

按照相同的步骤，我们将 $f_1 = f(t_1, \ldots, t_{n-1}, a_n)$ 除以 $t_{n-1} - a_{n-1}$，得到余数 $f_2 = f(t_1, \ldots, t_{n-2}, a_{n-1}, a_n) \in R_{n-2}$。这就是

$$f_1 = f(t_1, \ldots, t_{n-1}, a_n) = q_2(t_1, t_2, \ldots, t_{n-1})(t_{n-1} - a_{n-1}) + f_2.$$

继续这一过程，我们定义 $f_3 \in R_{n-3}, \ldots f_{n-1} \in R_1, f_n \in R_0 = K$。$f(t)$ 在 $(a_1, \ldots, a_n)$ 处的求值为 $f_n \in K$。

由此得到以下定义。

DEFINITION 1.3. 对于 $f(t_1, \ldots, t_n) \in R = K[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \cdots [t_n; \sigma_n, \delta_n]$和 $(a_1, \ldots, a_n) \in K^n$，我们将 $f(a_1, \ldots, a_n)$ 定义为 $f(t_1, t_2, \ldots, t_n)$ 在 $(a_1, \ldots, a_n)$ 处求值所得的结果，即 $f(t_1, t_2, \ldots, t_n)$ 模 $I_n(a_1, \ldots, a_n) = R_1(t_1 - a_1) + \cdots + R_{n-1}(t_{n-1} - a_{n-1}) + R(t_n - a_n)$ 的代表元，其中，对于 $1 \le i \le n$，$R_i$ 表示 $R_i = K[t_1; \sigma_1, \delta_1] \cdots [t_i; \sigma_i, \delta_i]$。

请注意，$I_n = I_n(a_1、\ldots\ldots、a_n)$ 是 $R$、$+$ 的一个加法子群，通常不是 $R = R_n$ 中的理想。

计算求值的另一种方法是注意到，$R = K[t_1; \sigma_1、 \delta_1][t_2; \sigma_2、 \delta_2]\cdots[t_n; \sigma_n、 \delta_n]$ 中的多项式都能唯一地写成如下形式的单项式之和：$\alpha_{l_1、\ldots\ldots、l_n} t_1^{l_1} t_2^{l_2} \cdots t_n^{l_n}$，其中 $0 \leq l_1、 l_2、\ldots\ldots、 l_n \leq n$ 且 $\alpha_{l_1、\ldots\ldots、l_n} \in K$。和 $\sum_{i=1}^{n} l_i$ 称为单项式的次数，而多项式的次数由次数最高的单项式的次数决定。首先注意，若单项式 $m = m(t_1、\ldots\ldots、 t_n)$ 的次数为 $l$，那么对于任意的 $a \in K^*$，$ma$ 也是次数为 $l$ 的多项式。我们通过归纳定义求值。实际应用中，只需定义单项式的求值。

对于 $(a_1, a_2, \ldots, a_n) \in K^n$ 以及 $m = m(t_1, \ldots, t_n)$，我们定义 $m(a_1, \ldots, a_n)$ 如下：

如果对于某些 $1 \leq i \leq n$ 和 $\alpha \in K$，有 $deg(m) = 1$ 且 $m = \alpha t_i$，那么 $m(a_1, \ldots, a_n) = a_i$。因此，假设次数为 $< l$ 的单项式的求值已经定义，并考虑单项式 $m = m(t)$，使得对于某些 $1 \leq j \leq n$，有 $deg(m) = l$ 且 $m = m'(t_1, \ldots, t_j)t_j$，那么 $m(a_1, \ldots, a_n) = m''(a_1, \ldots, a_j)$，其中多项式 $m''(t_1, \ldots, t_j) = m'(t_1, \ldots, t_j)a_j$ 的次数小于 $l$。

关于这一求值，我们来做一些说明。

REMARK 1.4. (1) 首先要指出，在对多项式求值之前，我们必须按照变量的确切顺序$t_1, t_2, \ldots, t_n$（从左到右）书写它。换句话说，在对多项式求值之前，我们必须将它写成形如 $t_1^{l_1} t_2^{l_2} \cdots t_n^{l_n}$ 的单项式之和。

(2) 当然，这并非唯一可能的定义；不过，尽管看起来有些奇怪，如果我们希望零点是右根，这样定义仍然是自然的。让我们更仔细地考察两个变量的情形。换句话说，形如 $g(t_1)(t_2 - a_2)$ 的多项式被 $(a_1, a_2)$ 消去是自然的；但我们不一定会期望 $(a_1, a_2)$ 成为形如 $(t_1 - a_1)h(t_1)$ 的多项式的零点。

（3）由于并未假定基环是交换的，因此即使变量可交换，我们在对多项式求值时也必须非常谨慎。按照这一定义，$t_1 t_2 \in K[t_1, t_2]$ 在（$a$, $b$）处求值得到（$t_1 t_2$）（$a$, $b$）$= ba$。这看起来可能很奇怪，但如果我们借助“算子”来理解求值，即先通过 $b$ 的右乘法，再通过 $a$ 的右乘法，则这一求值就完全合理，表面上的别扭也随之消失。

（4）我们假定不同的自同态 $\sigma_i$满足 $\sigma_i(K) \subseteq K$。换言之，对 $i > 1$而言，$\sigma_i$ 是 $\sigma_i|_K$ 到 $R_{i-1}$的扩张。不同的自同态 $\sigma_i$之间存在某些交换关系。例如，考虑多项式环扩张 $R = K[t_1; \sigma_1][t_2; \sigma_2]$。若令 $\sigma_2(t_1) = \sum_{i=0}^{l} a_i t^i$，计算 $\sigma_2(\sigma_1(a)t_1) = \sigma_2(t_1 a) = \sigma_2(t_1)\sigma_2(a)$，便得到下列方程

$$\forall\ 0 \leq i \leq l, \quad a_i \sigma_1^i(\sigma_2(a)) = \sigma_2(\sigma_1(a))a_i.$$

现在给出一些例子。

EXAMPLE 1.5. (1) 设 $A_1(k) = k[X][Y; id., \frac{d}{dX}]$ 且 $(a, b) \in K^2$，则

- $YX = XY + 1 = X(Y - b) + bX + 1 = X(Y - b) + b(X - a) + ba + 1$ 因此 $(YX)(a, b) = ba + 1$。

- $YX^2 = X^2Y + 2X = X^2(Y-b) + bX^2 + 2X = X^2(Y-b) + bX(X-a) + baX + 2(X-a) + 2a$ 因此 $(YX^2)(a,b) = ba^2 + 2a$。
- $Y^2X = XY^2 + 2Y = XY(Y-b) + bX(Y-b) + bXb + 2(Y-b) + 2b$ 因此 $(Y^2X)(a, b) = b^2a + 2b$。

(2) 考虑双 Ore 扩张 $R = \mathbb{F}_q[t_1; \theta][t_2; \theta]$, 其中 $q = p^n$, $\theta(a) = a^p$, 且 $\theta(t_1) = t_1$。多项式 $p(t_1, t_2) \in R$ 可写为 $p(t_1, t_2) = \sum_{i=0}^{n} p_i(t_1)t_2^i = \sum_{i,j} a_{i,j} t_1^j t_2^i$，并且我们可以轻易验证

$$p(t_1, t_2)(a, b) = \sum_{i,j} \theta^j(N_i(b))N_j(a) = b^{\frac{(p^i-1)p^j}{p-1}} a^{\frac{p^i-1}{p-1}}.$$

现在我们转而讨论另一种可能的多项式求值方式 $f(t_1、\ldots\ldots、t_n) \in R = K[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2]\cdots[t_n; \sigma_n, \delta_n]$ 在 $(a_1, a_2, \ldots\ldots, a_n) \in K^n$。我们考虑 $K$ 中表示 $f$ 的元素，它位于商 $R/I$ 中，其中 $I = R(t-a_1) + R(t-a_2) + \cdots + R(t-a_n)$。集合 $I$ 是 $R$ 的通常左理想，这种求值方式看起来更为经典。现在，我们通过比较 $I_n = R_1(t_1 - a_1) + \cdots + R_{n-1}(t_{n-1} - a_{n-1}) + R(t_n - a_n)$ 和 $I$ 来比较这两种求值方式。

THEOREM 1.6. 设 $K$ 为一个环，且 $R = K[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2]\cdots[t_n; \sigma_n, \delta_n]$。我们考虑 $(a_1, a_2, \ldots, a_n) \in K^n$，并令 $I = R(t-a_1)+R(t-a_2)+\cdots+R(t-a_n)$ 和 $I_n = R_1(t_1-a_1) + \cdots + R_{n-1}(t_{n-1}-a_{n-1}) + R(t_n-a_n)$，其中，对于 $1 \le i \le n$, $R_i R_i = K[t_1; \sigma_1, \delta_1]\cdots[t_i; \sigma_i, \delta_i]$。采用这些记号，以下条件等价：

*(1)* $I_n = I$; *(2)* $R(t_i - a_i) \subseteq I_n$; *(3)* $I \neq R$; *(4)* 对于 $1 \le i < j \le n$，有 $t_j(t_i - a_i) \in I_n$; *(5)* 对于 $1 \le i < j \le n$，有 $\sigma_j(t_i - a_i)a_j + \delta_j(t_i - a_i) \in I_n$; *(6)* 对于 $1 \le i < j \le n$，有 $(t_j t_i)(a_1, \ldots, a_n) = \sigma_j(a_i)a_j + \delta_j(a_i)$。

PROOF. 1) $\Leftrightarrow$ 2) 显然。

2) $\Rightarrow$ 3) 若 $I = R$，则 $I_n = R$ 且对于 $1 \le i \le n$，存在多项式 $g_i(t_1, t_2 \cdots, t_i) \in R_i$ 使得 $1 = \sum_{i=1}^{n} g_i(t_1, \ldots, t_i)(t_i - a_i)$。令 $y_i = t_i - a_i$ 定义变量代换，则对某个 $h_i \in R_i$，有 $1 = \sum_{i=1}^{n} h_i(y_1, \ldots, y_i)y_i$。比较此等式中零次项的系数，便得到矛盾。

3) $\Rightarrow$ 4) 存在 $c \in K$ 使得 $t_j(t_i - a_i) - c \in I_n \subseteq I$。由于 $t_j(t_i - a_i) \in I$，我们得到 $c \in I$，因此根据 3)，必有 $c = 0$。这表明 $t_j(t_i - a_i) \in I_n$。 4) $\Rightarrow$ 5) 由于 $t_j(t_i - a_i) \in I_n$，可得 $\sigma_j(t_i - a_i)t_j + \delta_j(t_i - a_i) \in I_n$。由于 $(t_j - a_j) \in I_n$，我们得到 $\sigma_j(t_i - a_i)a_j + \delta_j(t_i - a_i) \in I_n$。

5) $\Rightarrow$ 6) 这一点是显然的，因为 5) 蕴含 $t_j t_i - \sigma_j(a_i)a_j - \delta_j(a_i) = \sigma_j(t_i)t_j + \delta_j(t_i) - \sigma_j(a_i)a_j - \delta_j(a_i) \in I_n$。

6) $\Rightarrow$ 1) 6) 中的等式蕴含对 $1 \le i < j \le n$ 有 $t_j t_i - \sigma_j(a_i)a_j - \delta_j(a_i) \in I_n$。由此得到 $t_j(t_i - a_i) \in I_n$。又由于我们有 $R_i(t_i - a_i) \subseteq I_n$，故对任意整数 $1 \le i \le j \le n$ 可得出 $t_j(t_i - a_i) \in I_n$，从而对任意 $1 \le i \le n$ 有 $R(t_i - a_i) \subseteq I_n$。由此即得所需的 $I_n = I$。□

REMARK 1.7. 1) 若 $n = 1$，则我们显然有 $I = I_1$，且所有点都是好的。

2）一般而言，这两个加法子集 $I_n \subset I$ 并不相同。如上所述，我们将使用 $I_n$ 进行求值。原因是，当针对 $I$ 进行求值时，我们经常会遇到以下问题：左 $R$-模 $I$ 可能就是整个

环。因此，任何多项式在 $(a_1, a_2 \ldots, a_n)$ 处相对于 $I$ 的求值都为零。在 Weyl代数 $R = A_1(K) = K[t_1][t_2; id, \frac{d}{dt_1}]$ 中，点 $(0, 0)$ 就是这种情况，因为此时我们有 $t_2t_1 - t_1t_2 = 1$，从而得到 $Rt_1 + Rt_2 = R$。而使用我们的求值方式时则不会出现这种情况；例如，$t_2t_1 = t_1t_2 + 1$，因此 $t_2t_1 + I_2(0, 0) = 1 + I_2(0, 0)$，从而多项式 $t_2t_1$ 在 $(0, 0)$ 处的求值恰为 $1$。

3) 事实上，即使我们使用导子为零的 Ore 多项式，$I = R$ 也经常成立。例如，考虑 Ore 扩张 $R = K[t_1; \sigma_1][t_2; \sigma_2]$，其中 $K$ 是一个域，$\sigma_2$ 是 $K[t_1$ 的一个自同态；$\sigma_1]$ 使得 $\sigma_2(t_1) = t_1$。容易验证，对任意 $(a_1, a_2) \in K^2$，我们有 $(t_2 - \sigma_1(a_2))(t_1 - a_1) + (-t_1 + \sigma_2(a_1))(t_2 - a_2) = \sigma_1(a_2)a_1 - \sigma_2(a_1)a_2$。因此，若 $\sigma_1(a_2)a_1 - \sigma_2(a_1)a_2 \neq 0$，则左理想 $I(a_1, a_2) = R$。这表明，模 $I$ 的求值往往是平凡的。再一次，对我们的求值而言情况并非如此，因为我们有 $t_2(t_1 - a_1)$ 由 $\sigma_1(a_2)a_1 - \sigma_2(a_1)a_2$ 模 $I_2(a_1, a_2)$ 表示。

DEFINITION 1.8. 如果对多项式 $inK[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \cdots [t_n; \sigma_n, \delta_n]$ 在点 $(a_1, \ldots, a_n) \in K^n$ 处进行求值的两种方式结果相同，即 $I_n(a_1, \ldots, a_n) = I$，则称点 $(a_1, \ldots, a_n)$ 为好点。

好点的优点是，在这种情况下，通过左理想 $I$ 和 $I_n$ 进行的求值结果相同。当然，我们仍然可以通过加法子集 $I_n = R_1(t_1 - a_1) + \cdots + R_{n-1}(t_{n-1} - a_{n-1}) + R(t_n - a_n)$ 在任意点处对多项式求值。

EXAMPLE 1.9. (1) 在经典情形下（$\sigma_i = id_K$ 和 $\delta_i = 0$，对每个 $1 \leq i \leq n$），每个点 $(a_1, \ldots, a_n) \in K^n$ 都是好点。(2) 如果 $K$ 是除环 $\sigma_1 = id_K$，$\delta_1 = 0$ 且 $\sigma_2 = id, \delta_2 = d/dt_1$，那么对任意 $a, b \in K$，$(t_2 - b)(t_1 - a) = (t_1 - a)(t_2 - b) + 1$。这表明在这种情况下不存在好点。

使用 $I_n$ 而不是 $I$，我们避免了这样的问题：环 $R = K[t_1$ 中的每个多项式的零点都包含某些点；$\sigma_1$，$\delta_1][t_2$；$\sigma_2$，$\delta_2] \cdots [t_n$；$\sigma_n$，$\delta_n]$。

我们将考虑 Reed-Muller 码，因此需要对多个变量的多项式进行求值。我们考虑定义在有限基环（域）$K$ 上的迭代 Ore 多项式。在经典 Reed-Muller 编码中，用于求值的多项式在每个变量上的次数都被限制为某个有界值。事实上，与 $X^q - X \in \mathbb{F}_q[X]$ 相关联的多项式映射恒等于零。因此，我们的首要任务是考察在 Ore 多项式环中与此多项式对应的类比对象。我们需要先介绍几个定义。

DEFINITION 1.10. 设 $a \in K$ 是除环 $K$ 中的一个元素，$\sigma$ 且 $\delta$ 分别是 $K$ 的自同态和 $K$ 上的 $\sigma$-导子。

*(1)* 对于非零的 $x \in K$，我们记 $a^x = \sigma(x)ax^{-1} + \delta(x)x^{-1}$，并令 $\Delta(a) = \{a^x \mid x \in K^*\}$。该集合称为 $a$ 的 $(\sigma, \delta)$ 共轭类。*(2)* 由 $T_a(x) = \sigma(x)a + \delta(x)$ 定义的映射 $T_a: K \longrightarrow K$ 称为与 $a$ 相关联的 $(\sigma, \delta)$ 伪线性映射。*(3)* $a$ 的 $(\sigma, \delta)$ 中心化子是集合 $C^{\sigma,\delta}(a) = \{x \in K^* \mid a^x = a\} \cup \{0\}$。

值得一提的是，$\sigma$，$\delta$ 共轭这一概念自然地出现了，因为在计算乘积 $fg$ 时，我们有如下优美公式：$fg(a) = 0$，若 $g(a) = 0$，且 $(fg)(a) = f(a^{g(a)})g(a)$，若 $g(a) \neq 0$。还值得一提的是，在元素 $a \in K$ 处的求值与 $(\sigma$，$\delta)$-伪线性映射 $T_a$ 密切相关

可由等式 $f(a) = f(T_a)(1)$ 得到；更一般地，对于任意 $h \in R = K[t;\ \sigma,\ \delta]$、$a \in K$ 和 $x \in K^*$，$h(T_a)(x) = h(a^x)x$。我们首先需要下面这个广为人知的引理。

THEOREM 1.11. 设 $a$ 是除环 $K$ 的一个元素，且 $f(t) \in R = K[t;\sigma,\delta]$ 是一个次数为 $n$ 的多项式。那么：

*(1)* $C^{\sigma,\delta}(a)$ 是 $K$ 的子除环。*(2)* 映射 $T_a$ 是一个右 $C^{\sigma,\delta}(a)$ 线性映射。*(3)* $f(t)$ 的根至多属于 $n$ 个 $(\sigma,\delta)$-共轭类，记为 $\{\Delta(a_1)\dots,\Delta(a_r)\}, r \le n$；*(4)* $\sum_{i=1}^{r} dim_{C(a_i)} \ker(f(T_{a_i})) \le n$，其中 $C(a_i) := C^{\sigma,\delta}(a_i)$ 对任意 $1 \le i \le r$ 均成立。

PROOF. 读者可参阅 [**10**] 和 [**12**]。 □

注意，上面的第 (4) 点推广了若干经典定理，尤其是 Gordon-Motzkin 定理。该定理指出，系数属于除环 $K$ 的多项式 $f(X) \in K[X]$ 的根至多属于 $n = deg(f)$ 个经典的 $(\sigma = id., \delta = 0)$-共轭类。下面的定理 1.12 可见于 [**7**]。

THEOREM 1.12. 设 $p$ 为素数，$\mathbb{F}_q$ 为含有 $q = p^n$个元素的有限域。记 $\theta$ 为 *Frobenius* 自同构。则：

*a)* 在 $\mathbb{F}_q$中有 $p$ 个不同的 $\theta$-共轭类。 *b)* $C^{\theta}(0) = \mathbb{F}_q$，并且对于 $0 \ne a \in \mathbb{F}_q$，有 $C^{\theta}(a) = \mathbb{F}_p$。 *c)* 在 $\mathbb{F}_q[t;\theta]$中，对于 $a \in \mathbb{F}_q$，所有形如 $t - a$ 的元素的最小左公倍式为多项式 $G(t) := t^{(p-1)n+1} - t$。换言之，$G(t) \in \mathbb{F}_q[t;\theta]$ 的次数最小，且满足对于所有 $a \in \mathbb{F}_q$，$G(a) = 0$。 *d)* 上文 *c)* 中得到的多项式 $G(t)$ 是不变的，即 $RG(t) = G(t)R$。

PROOF. a) 记 $g$ 为循环群 $\mathbb{F}_q^* := \mathbb{F}_q \setminus\{0\}$的一个生成元。由零元素确定的 $\theta$-共轭类缩减为 $\{0\}$，即 $\Delta(0) = \{0\}$。由 1 确定的 $\theta$-共轭类是 $\mathbb{F}_q^*$:$\Delta(1) = \{\theta(x)x^{-1} \mid 0 \ne x \in \mathbb{F}_q\} = \{x^{p-1} \mid 0 \ne x \in \mathbb{F}_q\}$的一个子群。容易验证，$\Delta(1)$ 是由 $g^{p-1}$ 生成的循环群，其阶为 $\frac{p^n-1}{p-1}$。其指数为 $(\mathbb{F}_q^* : \Delta(1)) = p - 1$。由于两个非零元素 $a$，$b$ 共轭当且仅当 $ab^{-1} \in \Delta(1)$，我们确实得到不同的非零 $\theta$-共轭类的数量为 $p - 1$。由此得证。

b) 若 $a \in \mathbb{F}_q$ 非零，则 $C^{\theta}(a) = \{x \in \mathbb{F}_q \mid \theta(x)a = ax\}$，即 $C^{\theta}(a) = \mathbb{F}_p$。c) 对任意 $x \in \mathbb{F}_q$，有 $(t^{(p-1)n+1} - t)(x) = \theta^{(p-1)n}(x) \dots \theta(x)x - x$。由于$\theta^n = id$，且 $N_n(x) := \theta^{n-1}(x) \dots \theta(x)x \in \mathbb{F}_p$，可得 $(t^{(p-1)n+1} - t)(x) = x(\theta^{n-1}(x) \dots \theta(x)x)^{p-1} - x = xN_n(x)^{p-1} - x = 0$。这表明 $G(t)$ 确实消去了 $\mathbb{F}_q$ 的所有元素，因此 $G(t)$ 是线性多项式 $\{(t - a) \mid a \in \mathbb{F}_q\}$ 的一个左公倍式。令 $h(t) := [t - a \mid a \in \mathbb{F}_q]_l$ 表示它们的最小左公倍式。接下来只需证明 $\deg h(t) \ge n(p - 1) + 1$。令$0 = a_0$、$a_1$、.....、$a_{p-1} \in \mathbb{F}_q$为代表 $\theta$-共轭类的元素（参见上文 a)）。用 $C_0$、$C_1$、.....、$C_{p-1}$ 表示它们各自的 $\theta$-中心化子。定理 1.11 前一段中回顾的公式表明，对于任意非零元素 $x \in \mathbb{F}_q$ 和任意元素 $a \in \{a_0, \dots, a_{p-1}\}$，都有 $h(T_a)(x) = h(a^x)x = 0$。因此，对 $0 \le i \le p - 1$，$\ker h(T_{a_i}) = \mathbb{F}_q$。利用定理 1.11 中的不等式 (4) 以及

上文的陈述 $b$)，可得 deg $h(t) \geq \sum_{i=0}^{p-1} dim_{C_i} \ker h(T_{a^i}) = dim_{\mathbb{F}_q}\mathbb{F}_q + \sum_{i=1}^{p-1} dim_{\mathbb{F}_p}\mathbb{F}_q = 1 + (p-1)n$，证毕。d) 由于 $\theta^n = id.$，我们立即得到 $G(t)x = \theta(x)G(t)$，并且显然$G(t)t = tG(t)$。□

现在我们考虑一个迭代 Ore 扩张 $K[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2]\cdots[t_n; \sigma_n, \delta_n]$，其中 $K$ 是一个有限环。借用代数几何中的经典记号，我们考虑

$$I(K^n) = \{f(t_1, \ldots, t_n) \in R \mid \forall (a_1, \ldots, a_n) \in K^n, f(a_1, \ldots, a_n) = 0\}.$$

换言之： $I(K^n) = \cap_{(a_1,\ldots,a_n)} I_n(a_1, \ldots, a_n)$。对于 Ore 扩张$\mathbb{F}_q[t_1; \theta]\ldots[t_n; \theta]$，其中 $\theta$是 $\mathbb{F}_q = \mathbb{F}_{p^n}$的 Frobenius 自同构，上述定理表明，对于任意 $1 \leq i \leq n$，$t_i^{(n-1)p} - t_i \in I(K^n)$。鉴于此，对于任意 $1 \leq i \leq n$，我们引入 $R_i = K[t_1; \sigma_1, \delta_1]\ldots[t_i; \sigma_i, \delta_i]$ 中满足 $G_i \in I(K^n)$ 的最小次数首一多项式 $G_i = G_i(t_1, \ldots t_i)$。采用这些记号，我们现在可以陈述以下命题。

PROPOSITION 1.13. 设 $K$ 为有限环，并对 $1 \leq i \leq n$，考虑上文定义的多项式 $G_i \in R_i = K[t_1, \sigma_1, \delta_1]\ldots[t_i, \sigma_i, \delta_i]$。那么

$$I(K^n) = R_1G_1(t_1) + R_2G_2(t_1, t_2) + \cdots + R_nG_n(t_1, \ldots, t_n).$$

PROOF. 显然， $R_1G_1(t_1) + R_2G_2(t_1, t_2) + \cdots + R_nG_n(t_n) \subseteq I(K^n)$。现在，若多项式 $f \in K[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2]\cdots[t_n; \sigma_n, \delta_n]$ 属于 $I(K^n)$，那么，对于任意 $(a_1, \ldots, a_n) \in K^n$, $f(a_1, a_2, \ldots, a_n) = 0$。将求值过程中得到的连续余数记如下。对于任意 $(a_1, \ldots, a_n) \in K^n$ ，我们有

$f(t_1, \ldots, t_n) = q_1(t_1, \ldots, t_n)(t_n - a_n) + f_1(t_1, \ldots, t_{n-1}, a_n)$.
$f_1(t_1, \ldots, t_{n-1}, a_n) = q_2(t_1, \ldots, t_{n-1})(t_{n-1} - a_{n-1}) + f_2(t_1, \ldots, t_{n-2}, a_{n-1}, a_n)$.
Continuing this process, we get
$f_{n-2}(t_1, t_2, a_3, \ldots, a_n) = q_{n-1}(t_1, t_2)(t_2 - a_2) + f_{n-1}(t_1, a_2 \ldots, a_n)$ and
$f_{n-1}(t_1, a_2 \ldots, a_n) = q_n(t_1)(t_1 - a_1) + f_n(a_1, \ldots, a_{n-1}, a_n)$.

由于 $f(a_1, a_2, \ldots, a_n) = f_n(a_1, \ldots, a_{n-1}, a_n) = 0$，我们得出，对任意 $(a_1, \ldots, a_n \in K^n$, $f_{n-1}(t_1, a_2 \ldots, a_n) \in R_1(t_1 - a_1)$，即 $f_{n-1}(t_1, a_2 \ldots, a_n) \in R_1G_1(t_1)$。类似地，我们有 $f_{n-2}(t_1, t_2, a_3, \ldots, a_n) - f_{n-1}(t_1, a_2 \ldots, a_n) \in R_2 \cap I(K^n) = R_2G_2(t_1, t_2)$。简单的归纳表明，对任意 $1 \leq i \leq n$，我们有 $f_{n-i}(t_1, \ldots t_i, a_{i+1}, \ldots, a_n) - f_{n-i+1}(t_1, \ldots, t_{i-1}, a_i, \ldots, a_n) \in R_iG_i$。由此我们相继得到 $f \in R_nG_n + f_1 \subseteq R_nG_n + R_{n-1}G_{n-1} + f_2 \subseteq R_nG_n + R_{n-1}G_{n-1} + R_{n-3}G_{n-3} + f_3 \subseteq R_1G_1(t_1) + R_2G_2(t_1, t_2) + \cdots + R_nG_n(t_1, \ldots, t_n)$。这给出了所需的结果。□

## 2. 使用迭代斜多项式环的斜 Reed–Muller 码

本节第一部分将介绍关于交换多项式环上的 Reed-Muller 码的一些预备知识。

令 $m$为正整数，并令 $P_1$, $P_2$, ....., $P_n$为仿射空间 $\mathbb{A}^m(\mathbb{F}_q)$ 中的 $n = q^m$ 个点。对于任意满足 $0 \leq r \leq m(q-1)$ 的整数 $r$，令 $\mathcal{R}_m \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_m]/(x_1^p - x_1, x_2^p - x_2, \cdots, x_m^p - x_m)$ 表示次数小于或等于 $r$ 的多项式集合。

DEFINITION 2.1. 令 $f=\sum_{i=0}^{n} a_I X^I$ 为 $\mathbb{F}_q[x_1,x_2,\ldots,x_m]$ 中的一个多项式，其中对于 $I=(i_1,\ .....,\ i_n)$，我们定义 $X^I$ 为 $x^{i_1}x^{i_2}\cdots x^{i_n}$。在 $b=(b_1,b_2\ldots b_n)\in\mathbb{F}_q^n$ 处的算子求值$\mathrm{ev}(f)$ 定义为

$$\begin{aligned}&\mathcal{R}_m\to\mathbb{F}_q\\ \mathrm{ev}:\quad &f=\sum_{i\in I}a_iX^i\mapsto f(b)=\sum_{i\in I}a_i(b^i).\end{aligned}$$

长度为 $n=q^m$ 的 Reed-Muller 码可以通过对多项式 $f$ 在 $R_m$ 中的所有点 $P_1,\ P_2,\ \cdots,\ P_n$ 求值获得，其中这些点位于仿射空间 $\mathbb{A}^m(\mathbb{F}_q)$。阶为 $r$ 的 Reed-Muller 码定义为

$$\mathcal{R}_q(r,m)=\{(f(P_1),f(P_2),\ldots,f(P_n))\mid f\in R_m\}=\{\mathrm{ev}(f):f\in R_m,\deg f\leqslant r\}.$$

函数 $\mathrm{ev}:\mathcal{R}_m\to\mathbb{F}_q$ 是代数同态（见 [1]）。因此，Reed-Muller 码由码字 ev(*f*) 生成，其中 $f$ 是 $m$ 个变量的单项式集合中次数小于或等于 $r$ 的单项式。记作

$$\mathcal{M}=\{X_1^{a_1}X_2^{a_2}\ldots X_n^{a_n}\}.$$

**2.1. 迭代斜多项式与 Reed-Muller 码**。在最近的一篇论文中，作者通过在有限域 [5] 上使用含三个变量的迭代 Ore 扩张来定义斜 Reed-Muller 码。作者使用了内导子和内自同构（参见备注 1.1），通过变量替换即可消去这些结构。他们的思路是使用 Gr¨obner 基进行计算，并使用了该领域现有的软件。然而，他们的方法使用了我们记号中的理想 $I$，因此遇到了 $I$ 可能等于整个迭代 Ore 扩张 $R$ 的问题。他们的一些计算有误，为了后续研究，我们将在下文简要予以纠正。下文中的变量 $X_i$ 与他们论文中使用的变量相同。

**1.** 令 $\mathbb{F}_4=\mathbb{F}_2(\alpha)$，其中 $\alpha^2=\alpha+1$。在环 $R_1=\mathbb{F}_4[Y_1;\ \theta]$ 其中 $\theta$ 是 Frobenius 自同构，我们令 $X_1=Y_1+1$，并且有交换关系

$$X_1\alpha=(Y_1+1)\alpha=\theta(\alpha)Y_1+\alpha=\theta(\alpha)X_1+\theta(\alpha)+\alpha=\alpha^2X_1+1.$$

**2.** 在环 $R_2=R_1[Y_2]$ 中，我们令 $X_2=\alpha^2Y_2+Y_1+\alpha^2$，从而有 $R_2=R_1[X_2;\ \theta_\alpha,\ \delta_{X_1+\alpha}]$，其中对于任意 $x\in R_1$，$\theta_\alpha(x)=\alpha^{-1}x\alpha$。在 $R_2$ 中，除上述交换关系 $X_1\alpha=\alpha^2X_1+1$ 外，还有

$$X_2\alpha=\alpha X_2+X_1+1\quad\text{and}\quad X_2X_1=\alpha X_1X_2+\alpha^2X_2+\alpha^2X_1^2+\alpha^2.$$

**3.** 在环 $R_3=R_2[Y_3]$ 中，我们令 $X_3=\alpha^2Y_3+\alpha Y_1+\alpha$。于是有 $R_3=R_2[X_3;\ \theta_\alpha,\ \delta_{\alpha X_1}]$，其中如上所述，对于任意 $x\in\mathbb{F}_4$，$\theta_\alpha(x)=\alpha^{-1}x\alpha$。除上述交换关系外，还有

$$\begin{aligned}&X_3\alpha=\alpha X_3+\alpha X_1+\alpha,\\ &X_3X_1=\alpha X_1X_3+\alpha^2X_3+\alpha^2X_1^2+\alpha^2X_1,\\ &X_3X_2=X_2X_3+\alpha^2X_1X_3+\alpha^2X_3+X_1X_2+\alpha X_1^2+\alpha^2X_1+X_2+1.\end{aligned}$$

当然，$X_1$，$X_2$，$X_3$ 中的单项式并不是 $Y_1$，$Y_2$，$Y_3$ 中的单项式，反之亦然。变量 $Y_1$，$Y_2$，$Y_3$ 的优势显而易见。我们继续使用这些变量，并考虑，

$$R_n = R_{n-1}[Y_n] = R_1[Y_2, Y_3, \ldots, Y_n] = \mathbb{F}_4[Y_1, \theta][Y_2, Y_3, \ldots, Y_n].$$

与交换情形一样，存在能消去$\mathbb{F}_q^n$中任意元素的多项式。根据定理 1.12 和 1.13，在我们的情形下有 $I(K^n) = R_1G_1 + R_2G_2 + \cdots + R_nG_n$，其中 $G_1 = Y_1^3 - Y_1$，且对任意$2 \leq i \leq n$ 都有 $G_i = Y_i^4 - Y_i$（注意， $G_1$ 的形式源自定理 1.12）。这个迭代斜多项式环带来了一类新的斜 Reed–Muller 码，它由 $m$ 个变量中次数小于或等于 $r$ 的单项式基的求值生成，具体如下

$$\mathcal{M} = \left\{ Y_1^{l_1} Y_2^{l_2} \ldots Y_n^{l_n} \right\}.$$

根据上文给出的迭代斜多项式环， $f \in R_m$在 $b = (b_1, b_2 \ldots b_n)$处的求值 $\in \mathbb{F}_q^n$定义为

$$\begin{aligned} & R_m \to \mathbb{F}_q \\ \text{ev}: \quad & f(X_1, X_2, \ldots, X_n) \mapsto f(b_1, \ldots, b_n) = \sum_{i=0}^{n} P(b_2, \ldots, b_n)\theta^{\frac{i(i+1)}{2}}(b_1). \end{aligned}$$

其中 $f(X_1, X_2, \ldots, X_n) = g(Y_1)P(Y_2, \ldots, Y_n) \in R_1G_1 + R_2G_2 + \cdots + R_nG_n$。通过迭代斜多项式环和求值，我们在以下命题中得到斜 Reed–Muller 码的新新族。

PROPOSITION 2.2. 参数为 $r$ 和 $m$ 、定义在 $R_m = \mathbb{F}_q[X_1; \theta_1, \delta_1] \ldots [X_m; \theta_m, \delta_m]$ 上的斜 *Reed–Muller* 码由下式生成。

$$\mathcal{R}(r, m) \stackrel{\text{def}}{=} \left\{ \sum_{i=0}^{n} P(b_2, \ldots, b_n)\theta^{\frac{i(i+1)}{2}}(b_1) : P \in R_m \ such \ that \ \deg P \leqslant \deg G_n \right\}.$$

用于构造 Reed-Muller 码 $\mathcal{R}(r, m)$ 的生成矩阵的行，其选择方式是选取次数小于或等于 $r = (n-1)p+1$ 的单项式 $Y_1^{l_1} Y_2^{l_2} \ldots Y_n^{l_n}$。此选择基于单项式的阶。Reed-Muller 码 $\mathcal{R}(r, m)$ 的置换群是仿射变换 $x \to Ax + b$ 的集合，其中 $A \in \mathbb{F}_q^{m \times m}$ 是一个可逆矩阵，且 $b \in \mathbb{F}_q^m$。

**2.2. 使用多项式映射构造斜 Reed–Muller 码** $n$ **（变量）**。本节介绍如何使用 $n$ 个变量上的多项式映射构造斜 Reed–Muller 码。我们知道，Reed-Muller 码定义为由 $m$ 个变量上次数小于或等于 $r$ 的单项式基的求值所生成的码。在 $m$ 个变量上的单项式集合记作

$$\mathcal{M} = \left\{ t_1^{l_1} t_2^{l_2} \ldots t_n^{l_n} \right\}.$$

请注意，在迭代 Ore 扩张 $K[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \cdots [t_n; \sigma_n, \delta_n]$ 的情况下，总可以对一个词中的不定元排序，使得我们只需考虑形如 $t_1^{l_1} t_2^{l_2} \ldots t_n^{l_n}$ 的词。现在我们给出在 $R = K[t_1, \sigma_1, \delta_1][x_2, \sigma_2, \delta_2], \ \cdots, \ [x_n, \sigma_n, \delta_n]$ 中若干单项式在 $(a_1, \ a_2, \ \cdots, \ a_n) \in K^n$. 处的求值

(1) 考虑多项式环 $R = K[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2]$ ，并计算多项式 $t_1t_2$ 在 $(a_1, a_2) \in K^2$处的值。我们有 $t_1t_2 = t_1(t_2 - a_2) + t_1a_2 = t_1(t_2 - a_2) + \sigma_1(a_2)t_1 + \delta_1(a_2)$。由此得到 $(t_1t_2)(a_1, a_2) = \sigma_1(a_2)a_1 + \delta_1(a_2)$。

(2) 考虑多项式环 $R = K[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2][t_3; \sigma_3, \delta_3]$ ，并计算多项式 $t_1t_2t_3$ 在 $(a_1, a_2, a_3) \in K^3$处的值。我们有 $t_1t_2t_3 = t_1t_2(t_3 - a_3) + t_1t_2a_3 = t_1t_2(t_3 - a_3) + t_1(\sigma_2(a_3)t_2 + \delta_2(a_3)) = t_1t_2(t_3 - a_3) + t_1\sigma_2(a_3)t_2 + t_1\delta_2(a_3) = t_1t_2(t_3 - a_3) + \sigma_1(\sigma_2(a_3))t_1t_2 + \sigma_1(\delta_2(a_3))t_1 + \delta_1(\delta_2(a_3))$。由此得到 $(t_1t_2t_3)(a_1, a_2, a_3) = \sigma_1(\sigma_2(a_3))a_1a_2 + \sigma_1(\delta_2(a_3))a_1 + \delta_1(\delta_2(a_3))$。(3) 考虑多项式环 $R = K[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2][t_3; \sigma_3, \delta_3][t_4; \sigma_4, \delta_4]$。我们有 $(t_1t_2t_3t_4)(a_1, a_2, a_3, a_4) = \sigma_1(\sigma_2(\sigma_3(a_4)a_3)a_2)a_1 + \delta_1(\sigma_2(\sigma_3(a_4)a_2)a_3) + \sigma_1(\delta_2(\sigma_3(a_4)a_3))a_1 + \delta_1(\delta_2(\sigma_3(a_4)a_3)) + \sigma_1(\sigma_2(\delta_3(a_4))a_2)a_1 + \delta_1(\sigma_2(\delta_3(a_4))a_2) + \sigma_1(\delta_2(\delta_3(a_4)))a_1 + \delta_1(\delta_2(\delta_3(a_4)))$。

$n$ 变量上的多项式映射及其求值在以下示例中导出了一族新的斜 Reed–Muller 码。

EXAMPLE 2.3。 在此示例中，我们给出了用2 个或3 个变量上的多项式映射构造 ***Reed-Muller*** 码的方法。在这些示例中，我们对 $\sigma_1$ 使用了 ***Frobenius***自同构，对 $\sigma_2$ 和 $\sigma_3$使用了恒等映射。所有导子均为零。

(1) 在 $R = \mathbb{F}_4[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2]$上对集合单项式 $\{1, t_1, t_2, t_1t_2\}$ 求值，得到参数为 $[16, 4, 8]$. 的 ***Reed-Muller*** 码。(2) 在 $R = \mathbb{F}_4[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2]$上对集合单项式 $\{1, t_1, t_2, t_2t_1\}$ 求值，得到参数为 $[16, 4, 7]$. 的 ***Reed-Muller*** 码。(3) 在$R = \mathbb{F}_4[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2][t_3; \sigma_3, \delta_3]$ 上对集合单项式 $\{1, t_1, t_2, t_1, t_3, t_1t_3, t_2t_3, t_1t_2t_3\}$ 求值，得到参数为 $[64, 8]$. 的 ***Reed-Muller*** 码

## 参考文献


[1]M. Bardet、V. Dragoi、A. Otmani 和 J.P. Tillich, *Algebraic properties of polar codes from a new polynomial formalism*, IEEE信息论国际研讨会（ISIT），230–234，2016年。[2] D. Boucher 和 F. Ulmer, *Coding with skew polynomial rings*, 《符号计算杂志》，第**44**卷，（2009年），1644-1656。[3] M. Boulagouaz、A. Leroy, *$(\sigma, \delta)$-codes*, 《通信数学进展》，第**7** 卷（4）（2013年），463-474。[4] I. Dumer、R. Fourquet 和 C. Tavernier, *Cryptanalysis of Block Ciphers via Decoding of LongReed-Muller Codes*, 《代数与组合编码理论》（ACCT 2010），俄罗斯新西伯利亚，2010年9月。[5] W. Geiselmann、F. Ulmer, *Skew Reed-Muller codes*, 《当代数学》，第727卷，（2019年），107–116。[6] T. Kasami、S. Lin、W. 和 Peterson, *New generalizations of the Reed-Muller codes–I: Prim-* , 《*itive codes* 1968 189 199 IEEE信息论汇刊》，第**14**卷，2（ ），–。[7] A. Leroy, *Noncommutative polynomial maps* , 《代数及其应用杂志》，第**11**卷，（2012年），第04期，。[8] T. Y. Lam、A. Leroy 和 A. Ozturk: *Wedderburn polynomials over division rings,* II，金奈拉马努金研究所（印度）举办的会议论文集，《当代数学》（**456**）（2008年），第73-98页。[9] T.Y. lam 和 A. Leroy, *Principal one-sided ideals in Ore polynomial rings*, 《当代数学》，第**259**卷，普罗维登斯，罗得岛州；美国数学会（2000年），333–352。[10] T.Y.Lam、A. Leroy 和 A. Ozturk, *Wedderburn polynomials over division rings, II*, 《当代数学》，第**456** 卷（2008年），73–98。[11] D.E. Muller, *Application of Boolean algebra to switching circuit design and to error detection*, 《IRE电子计算机专业组汇刊》，第**3** 卷（1954年），6–12。

[12] A. Leroy, A.Ozturk: *Algebraic and F-independent sets in* 2*-firs*, 《代数通讯》, 第**32** 卷（5）（2004）, 1763-1792。
Université Artois, UR 2462,
Laboratoire de Mathématiques de Lens (LML), F-62300Lens, France*Email address*:
andre.leroy@univ-artois.frUSTHB, Faculté de Mathématiques,
BP 32 El Alia Bab Ezzouar Algiers Algeria*Email address*: nabil.bennenni@gmail.com