arXiv:2305.02921v1 [cs.IT] 4 May 2023

极化码重量枚举的闭式表达：1.5d 重量码字

Mohammad Rowshan*†、Vlad-Florin Drˇagoi*‡ 和 Jinhong Yuan†，IEEE 会士
†新南威尔士大学（UNSW）电气工程与电信学院，澳大利亚悉尼
‡阿拉德奥雷尔·弗拉伊库大学理学院，罗马尼亚阿拉德
m.rowshan@unsw.edu.au，vlad.dragoi@uav.ro，j.yuan@unsw.edu.au

摘要——纠错码的重量分布是决定其纠错性能的关键因素，因此枚举工作至关重要。对于极化码，目前仅能针对最小重量 w_{min}（等于最小距离d）给出显式枚举公式。对于重量大于最小重量的极化码字，若能得到其重量枚举的闭式表达，不仅可以简化枚举过程，还能为构造更优的类极化码提供宝贵见解。本文通过分析轨道的闵可夫斯基和，探究更高重量背后的代数结构。我们的方法以递减单项式码的下三角仿射（LTA）群为基础。具体而言，我们提出了一个重量为 $1.5w_{min}$ 的码字枚举闭式表达。仿真结果表明，该方法有望推广到更高重量。

索引词——极化码、Reed-Muller码、单项式码、下三角仿射群、代数性质、最小汉明距离、最小重量码字、重量分布、枚举、错误系数。

I. 引言

极化码 [1] 是第一类具有显式构造、能够达到二进制输入离散无记忆信道（BI-DMC）对称（香农）容量的信道码。由于短码长和中等码长的极化码展现出卓越的纠错性能，因此它们已被选作第5代移动宽带标准中逻辑控制信道的编码方案 [2]。在过去十年中，极化码一直是编码理论领域关注的焦点。相关研究工作主要集中于低复杂度的码构造方法，以及通过码级联和译码方案提升性能。极化码更为基础的问题，例如其代数特征，则较少受到研究。其中一个主要问题是对重量分布进行代数研究，并寻找具有特定重量的码字枚举的闭式表达式。

码的重量分布决定了码的纠错性能。利用并集界，可以得到线性码在最大似然（ML）译码下的误块率（BLER）上界，其中小重量码字的数量（例如最小重量、第二小重量及更大重量码字的数量，在最大项中起到系数的作用 [3, 第10节1]。文献 [4] 指出，极化码与 Reed-Muller 码同属一个更大的码族，称为递减单项式码。除了 Reed-Muller 码和极化码都具有的多项式结构外，递减性质还带来了新的代数性质。文献 [4], [5] 首次利用这些性质，发现了新的结构性质，例如递减单项式码的对偶仍是递减单项式码，递减单项式码的置换群包含下三角仿射群（LTA(m,2)）作为子群。对极化码代数结构的理解略有加深，使学界得以提出实际应用。文献 [5] 揭示了递减单项式码（因而也包括极化码）中最小重量码字的完整结构。文献 [6] 提出了一种亚线性码构造。置换群对极化码的并行译码有重要贡献 [7]–[13]。此外，Yao、Fazeli 和 Vardy 还将置换群用作其重量枚举算法中的优化工具 [14]。

在取得重大进展、朝着这一目标迈进五十多年后，寻找里德–穆勒码重量分布的闭式表达式仍然是一个未解决的问题。Kasami 和 Tokura [15] 刻画了重量不超过该码最小重量两倍的里德–穆勒码码字。在 [16] 中，研究结果扩展到了对重量小于最小重量 2.5 倍的码字进行枚举。对于极化码，首次进展是在 [5] 中对最小重量码字进行闭式枚举，但研究也就此止步。

由于极化码的重量分布十分重要，后续的研究尝试都集中于采用算法来精确或近似枚举具有不同重量的极化码字。在 [17], 中，作者提出在低噪声信道中发送全零码字，或在极高信噪比下接收，并统计列表规模极大的连续消除列表译码器输出中具有特定重量的重新编码消息。 [18] 中介绍的方法旨在高效计算概率重量分布表达式。 [19] 中的作者提出了一种获取极化码近似距离谱的方法。

*这些作者贡献相同（通讯作者：Vlad-Florin Drˇagoi）。

利用短码的谱以及关于码字中 1 出现情况的概率假设，可以构造长度较大的码。基于 [20]，中构造的 $|u|u+v|$ 码的重量分布， [21] 中递归地求得了由极化变换生成的码字的重量分布。这项工作以及 [5] 中的工作启发了 [14] 的作者提出一种确定性的递归算法，用于统计具有任意重量的极化码的所有码字。然而，由于该算法的复杂度较高，因此无法用于中长码长的情况。

在这项工作中，我们向前迈出一步，通过枚举重量为 1.5 $\mathrm{w}_{\min}$. 的码字，部分解决了极化码重量分布这一长期悬而未决的问题。我们的结果适用于任意递减单项式码。要解决这一问题，我们需要认识到，对于极化码而言，推导给定重量码字枚举的闭式公式确实复杂且具有挑战性。研究递减单项式码的一般情形有诸多优势，也有望统一已有结果（Reed-Muller码的情形）与极化码的情形。为实现这一目标，我们的结果建立在两个关键要素之上：置换群（LTA(m, 2)）以及 Kasami 和 Tokura 关于重量小于 2 $\mathrm{w}_{\min}$ [15] 的分类定理。 [15] 中的定理适用于任意多项式码，并给出了重量小于 2 $\mathrm{w}_{\min}$. 的任意码字的多项式形式（在仿射变换下）。此类码字可以定义为最小重量码字之和；最小重量码字则定义为 LTA(m, 2) 的轨道中的多项式的取值向量，该多项式对应于一个最高次数的单项式 f ，设其次数为 $\deg(f) = r$。因此，这类和的重量由两个最小重量码字重叠的位置数决定。这引出了我们研究中的一个关键要素，即理解两个轨道 LTA(m, 2) $\cdot f +$ LTA(m, 2) $\cdot g$ 的闵可夫斯基和，其中 f 、 g 是最高次数的单项式（ f 、 g 定义最小重量码字）。

第一步是将 [15]的研究结果转用于递减单项式码的情形。为此，我们将确立以下内容：

- 找出生成和及和的乘积的完整轨道的子群；
- 给定一个重量为 1.5 $\mathrm{w}_{\min}$的码字 $\boldsymbol{c}$ ，计算最大次数单项式，例如 f 和 g ，使得 $\boldsymbol{c}$ 是属于集合 LTA(m, 2) $\cdot f +$ LTA(m,2) $\cdot g$.中的多项式的取值

下一步是确定轨道的闵可夫斯基和的基数。我们证明，如果变量 f 和 g 满足特定的序关系，那么 LTA(m, 2) $\cdot f +$ LTA(m, 2) $\cdot g$ 的基数等于两个集合 LTA(m, 2) $\cdot f$ 和 LTA(m, 2) $\cdot g$. 的基数之积。为了证明这一结果，我们将引入多项式碰撞的概念。非正式地说，两个不同的多项式对 (P, Q)、$(P^*, Q^*) \in$LTA(m, 2)$\cdot f \times$LTA(m, 2)$\cdot g$ 构成一次碰撞，如果 $P + q = P^* + Q^*$. 。我们证明，通过因式分解过程（这得益于递减的序关系），在单项式层面 (f, g) 发生碰撞，就会导致 $(f/h, g/h)$，其中 $h =$gcd(f, g)。接下来，我们刻画所有可能的碰撞情形，从而找出全部不变量。我们的结果直接推得一个简单公式，可用于计算当 f 和 g 的次数为 2 时，闵可夫斯基和 LTA(m, 2) $\cdot f +$LTA(m, 2) $\cdot g$ 的基数。

虽然上述结果颇具理论性，但我们确实将其应用于一项实际挑战。我们求出了重量为 1.5 $\mathrm{w}_{\min}$. 的码字的闭式公式。首先回顾一下，重量为 1.5 $\mathrm{w}_{\min}$ 的码字属于某些单项式 f 和 g 的轨道之和，其中这两个单项式的最大次数分别为 $\deg(f) = \deg(g) = r$，且满足 $\deg(\gcd(f, g)) = r - 2$. 。我们证明，不同的此类单项式对定义的闵可夫斯基和彼此不相交（这一性质类似于最小重量码字的轨道互不相交）。最后，我们给出这类码字的计数公式，并在不同的极化码上进行测试。我们得到了短码长码的知名结果，以及 Reed-Muller码的公式。我们进一步扩展了仿真，并给出了长极化码的重量计数。

II. 预备知识

A. 编码理论的基本概念与记号

我们用 $\mathbb{F}_2$ 表示含有两个元素的有限域，用 $\oplus$ 表示该域中的加法运算。此外，连续整数的子集记为 $[\ell, u]$、$\{\ell, \ell+1, \ldots, u\}$，以及 $[n]$、$[0, n-1]$。向量 $\boldsymbol{c} = [c_0, \ldots, c_{N-1}] \in \mathbb{F}_2^N$ 的支撑集是 $\boldsymbol{c}$ 的非零坐标所对应的指标集合，即 $\mathrm{supp}(\boldsymbol{c}) \ \{i \in [N] \mid c_i \neq 0\}$。集合的基数记为 $|\cdot|$ ，集合差记为 $\setminus$。向量 $\boldsymbol{c} \in \mathbb{F}_2^N$ 的汉明重量为 $\mathrm{w}(\boldsymbol{c}) \ |\mathrm{supp}(\boldsymbol{c})|$。给定两个向量 $\boldsymbol{c} = [c_0, c_1, \ldots, c_{N-1}]$ 和 $\boldsymbol{c}' = [c_0', c_1', \ldots, c_{N-1}']$， $\boldsymbol{c}$ 与 $\boldsymbol{c}'$ 之间的汉明距离定义为 $\boldsymbol{c}$ 与 $\boldsymbol{c}'$ 不同的坐标数，即 $\mathrm{d}(\boldsymbol{c}, \boldsymbol{c}') = |\{i \in [N] \mid c_i \neq c_i'\}|$。

如果 $\mathcal{C}$ 的最小距离为，一个 K 维子空间 $\mathcal{C}$ of $\mathbb{F}_2^N$ 被称为域 $\mathbb{F}_2$ 上的线性（N, K, d）码，

$$d_{min} = \mathrm{d}(\mathcal{C}) \triangleq \min_{\boldsymbol{c}, \boldsymbol{c}' \in \mathcal{C}, \boldsymbol{c} \neq \boldsymbol{c}'} \mathrm{d}(\boldsymbol{c}, \boldsymbol{c}') = d.$$

不难看出，汉明范数诱导出汉明距离，反之亦然。因此，我们有（见 [3, 第 3.3] 节）

$$\mathrm{w}_{\min} \triangleq \min_{\boldsymbol{c} \in \mathcal{C}, \boldsymbol{c} \neq 0} \mathrm{w}(\boldsymbol{c}) = \mathrm{d}(\mathcal{C}).$$

对于码，我们通常使用简写（N, K），其中 N 和 K 分别表示码的码长和维数。 $\mathcal{C}$ 中的向量称为码字。我们还将码 $\mathcal{C}$ 中重量为 w 的所有码字收集到集合 W_{w} 中，记为

$$W_{\mathrm{w}}(\mathcal{C}) = \{\boldsymbol{c} \in \mathcal{C} \mid \mathrm{w}(\boldsymbol{c}) = \mathrm{w}\}.$$

一个（N, K）码 $\mathcal{C}$ 的生成矩阵 $\boldsymbol{G}$ 是 $\mathbb{F}_2^{K \times N}$ 中的一个 $K \times N$ 矩阵，其行是 $\mathcal{C}$ 中 $\mathbb{F}_2$ 线性无关的码字。于是 $\mathcal{C} = \{\boldsymbol{v}\boldsymbol{G}\colon \ \boldsymbol{v} \in \mathbb{F}_2^K\}$。

在每个信息比特的信噪比（SNR）较高的二进制输入加性高斯白噪声（BI-AWGN）信道下，根据 [3, 第 10.1], 节， E_b/N_0 the

采用软判决最大似然（ML）译码的线性码的误块率（BLER）上界为

$$P_e^{ML} \leq \sum_{\mathrm{w}=\mathrm{w}_{\min}}^{N} A_{\mathrm{w}} Q(\sqrt{2\,\mathrm{w}\cdot R\cdot E_b/N_0}), \qquad (1)$$

其中，A_{w} 表示重量为 w 的码字数量（或等价地表示为 $A_{\mathrm{w}} = |W_{\mathrm{w}}(\mathcal{C})|$）；$Q(\cdot)$ 是正态分布 $\mathcal{N}(0,1)$ 的尾概率，用于求取发送序列及其对应失真接收序列的成对错误概率；R、K/N 是码率。在相关文献中，$A_{\mathrm{w}_{\min}}$ 被称为错误系数，因为它是计算 BLER 上界时最大项的系数。可以观察到，在二者具有相同 $\mathrm{w}_{\min}$的情况下，$A_{\mathrm{w}_{\min}}$ 较小的码预计比$A_{\mathrm{w}_{\min}}$较大的码具有更小的 BLER。需要注意的是，本文通过求取所有 $\mathrm{w} < 2\mathrm{w}_{\min}$（特别是 $\mathrm{w} = 1.5\mathrm{w}_{\min}$）对应的 A_{w}，考虑了其他主导项，从而更准确地衡量码的性能。

B. 单项式码

单项式是一个单项代数表达式，表示 $\mathbf{x} \triangleq (x_0, \ldots, x_{m-1})$ 中任意变量子集的乘积。假设 $\mathbf{i} = (i_0, \ldots, i_{m-1})$，其中 $i_j \in \{0,1\}$，则一个 m 元单项式表示为

$$\mathbf{x}^{\mathbf{i}} = \prod_{j=0}^{m-1} x_j^{i_j} = x_0^{i_0} \cdots x_{m-1}^{i_{m-1}}.$$

为简便起见，我们用 $f = \mathbf{x}^{\mathbf{i}}$ 表示一个单项式。此外，用 $\deg(\mathbf{x}^{\mathbf{i}})$ 表示单项式 $\mathbf{x}^{\mathbf{i}}$ 的次数（我们有 $\deg(\mathbf{x}^{\mathbf{i}}) = \mathrm{w}(\mathbf{i})$），并用 表示所有单项式构成的集合。

$$\mathcal{M}_m \triangleq \left\{\mathbf{x}^{\mathbf{i}} \mid \mathbf{i} \in \mathbb{F}_2^m\right\}.$$

对于任意次数为 $1 \leq s \leq m$ 的单项式 $f \in \mathcal{M}_m$，记作 $f = x_{l_1} \ldots x_{l_s}$，其中 $0 \leq l_1 \leq l_2 \cdots \leq l_s \leq m-1$，该单项式的支撑集记为 $\mathrm{ind}(f) = \{l_1, \ldots, l_s\}$。注意，单项式 $f = x_0^{f_0} \ldots x_{m-1}^{f_{m-1}}$ 的支撑集包含所有满足 $f_j = 1$ 的 j。次数在任意单项式集合 $\mathcal{I} \subseteq \mathcal{M}_m$ 上诱导出一个排序，即 $\mathcal{I} = \bigcup_{j=0}^{m} \mathcal{I}_j$，其中 $\mathcal{I}_j = \{f \in \mathcal{I} \mid \deg(f) = j\}$.

由于我们关注的是单项式在 $\mathbb{F}_2^m$ 中各元素上的求值，因此将 x_i 与 x_i^2 等同，并在环 $\mathrm{R}_m = \mathbb{F}_2[x_0, \ldots, x_{m-1}]/(x_0^2 - x_0, \ldots, x_{m-1}^2 - x_{m-1})$ 中进行运算。考虑上述理想的主要原因是，我们不希望在多项式或单项式相乘时携带无用的幂。解释多项式与码字之间的联系后，这一切都会清晰得多。现在，任意子集 $\mathcal{I} \subseteq \mathcal{M}_m$ 都构成一个 $(n = 2^m, k = |\mathcal{I}|)$ 单项式码 $\mathcal{C}$的生成集。该单项式码 $\mathcal{C}$ 作为线性码，是由将 $\mathcal{I}$ [5] 中的单项式求值所得、以行向量为基的张成空间所生成的向量子空间 $\mathcal{C}(\mathcal{I}) \subseteq \mathbb{F}_2^n$。也就是说，

$$\mathcal{C}(\mathcal{I}) = \mathrm{span}(\{\mathrm{ev}(f) \mid f \in \mathcal{I}\}),$$

其中，$\mathrm{ev}(f)$ 是通过对 $\mathbb{F}_2^m$ 中的所有二进制元素计算单项式 f 的值而得到的二进制向量，即。

$$\mathrm{ev}(f) \triangleq (\mathrm{ev}(f)(0,\ldots,0), \ldots, \mathrm{ev}(f)(1,\ldots,1)),$$

其中集合 $\mathbb{F}_2^m$ 按递减顺序排列（参见示例 1 中的 $m = 2$）。更确切地说，将条目 $\boldsymbol{i} = (i_0, \cdots, i_{m-1}) \in \mathbb{F}_2^m$ 排列，使最左侧的条目成为 $\boldsymbol{i}$ 的二进制表示中最低有效位（如条目索引所示），并按递减顺序对其排序。由于 $\mathrm{ev}(f)$ 是一个二进制向量，其汉明重量为 $\mathrm{w}(\mathrm{ev}(f))$，或简写为 $|f|_m$，有时也称为 f 的重量。对于任意 $f \in \mathcal{M}_m$，我们确有 $\mathrm{w}(\mathrm{ev}(f)) = 2^{m-\deg(f)}$. 。事实上，$\mathrm{ev}(f) = 1$ 的求值点由子集 $\{(f_0, \ldots\ldots, f_{m-1}) \in \mathbb{F}_2^m \mid \forall i \in \mathrm{ind}(f) f_i = 1\}$. 定义。该集合的基数为 $2^{m-|\mathrm{ind}(f)|} = 2^{m-\deg(f)}$，因为从 $\mathbb{F}_2$. 中有 $m - \deg(f)$ 个自由索引。

示例 1. 设 $m = 2$。所有单项式 $f \in \mathcal{M}_n = \{\mathbf{1}, x_0, x_1, x_0x_1\}$ 及其在 $\boldsymbol{G}_N$ 中对应行的评估 $\mathrm{ev}(f)$ 如下:

	$(i_0\ i_1)$:	11	01	10	00
$\mathbf{g}_0$	$\mathrm{ev}(x_0x_1)$	1	0	0	0
$\mathbf{g}_1$	$\mathrm{ev}(x_1)$	1	1	0	0
$\mathbf{g}_2$	$\mathrm{ev}(x_0)$	1	0	1	0
$\mathbf{g}_3$	$\mathrm{ev}(1)$	1	1	1	1

其中，例如，$f = x_0$ 的取值在所有 $(\mathbf{1}, i_2)$ $i_2 \in \{0,1\}$ 情况下均为 1，否则为 0。

由于函数 ev 在 R_m 和 $\mathbb{F}_2^n$ 之间定义了一个向量空间同构（见 [22] 中的推论 3,2,6），因此给定生成矩阵为 $\mathrm{G} = (\mathrm{g}_0 \cdots \mathrm{g}_k)^T$ 的单项式码 $\mathcal{C}(\mathcal{I})$，对于每一行 g_i（其中 $i \in [0,k)$），都存在一个单项式 $f \in \mathcal{I}$，使得 $\mathrm{ev}(f) = \mathrm{g}_i$。单项式码的最小距离因此为 [5]。

$$\min_{\mathbf{c}\in\mathcal{C}(\mathcal{I})} \mathrm{w}(\boldsymbol{c}) = \min_{f\in\mathcal{I}} \mathrm{w}(\mathrm{ev}(f)) = 2^{m-r^+(\mathcal{C})},$$

其中 $r^+(\mathcal{C}) = \max_{f\in\mathcal{I}} \deg(f)$。

根据上述形式体系，Reed-Muller 码$\mathcal{R}(r,m)$是单项式码

$$\mathcal{R}(r,m) \triangleq \mathrm{span}(\{\mathrm{ev}(f) \mid f \in \mathcal{M}_m, \deg(f) \leqslant r\}).$$

我们还需要定义多项式集合的和与积的概念。

定义 1. 给定两个多项式集合 $\mathcal{S}, \mathcal{T} \in \mathrm{R}_m$，它们的闵可夫斯基和为 $\mathcal{S} + \mathcal{T} = \{s + t \mid s \in \mathcal{S}, t \in \mathcal{T}\}$。此外，积定义为 $\mathcal{S} \cdot \mathcal{T} = \{s \cdot t \mid s \in \mathcal{S}, t \in \mathcal{T}\}$，其中 $+$和 $\cdot$ 分别表示多项式加法和乘法。

III. Decreasing monomial codes: the algebraic formalism behind polar codes

A. 极化码

码长为 $N = 2^n$ 的极化码基于二进制 Walsh-Hadamard 矩阵 $\mathrm{G}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$的 n次 Kronecker 幂构造，记为$(.)^{\otimes n}$，即 $\boldsymbol{G}_N = \mathrm{G}_2^{\otimes n}$，本文中我们将其

称为极化变换。我们将极化变换的各行记为 $\mathsf{g}_i, i=[N]$，即 $\boldsymbol{G}_N=[\mathsf{g}_0,\mathsf{g}_1,\cdots,\mathsf{g}_{N-1}]^T$，其中 $[\cdot]^T$ 中的算子 T 表示矩阵的转置。极化码的生成矩阵由 $\boldsymbol{G}_N$中的一组行构成。我们用 $\mathcal{A}$ 表示这些行的索引集合，并用 $\mathcal{C}(\mathcal{A})$表示由 $\boldsymbol{G}_N$ 中索引为 $\mathcal{A}$的行所生成的线性码。注意，$\mathcal{A}\subseteq[N]$。极化码的信息集 $\mathcal{A}$ 的刻画依赖于信道极化定理 [1] 以及合成信道可靠性的概念。码长为 $N=2^n$的极化码通过选取一组可靠性较高的索引 $i\in[0,N-1]$构成的集合 $\mathcal{A}$ 来构造 [1]。集合 $\mathcal{A}$ 中的索引用于信息比特，其余索引属于 $\mathcal{A}^c$，$[0,N-1]\setminus\mathcal{A}$ 的合成信道则用于传输已知值，默认值为 “0”，这些比特称为冻结比特。无论我们采用何种方法构造极化码的集合 $\mathcal{A}$，由索引 i表示的每个合成信道，记为 W_n^i，其中 $i\in\mathcal{A}$，其可靠性都必须高于 $\mathcal{A}^c$中的任何合成信道。

具有信息集 $\mathcal{A}$ 的极化码也可以视为单项式码 [22]，其中第 II-B 节讨论的单项式生成集 $\mathcal{I}\subset\mathcal{M}_n$ 与信息集 $\mathcal{A}$ 之间的关系如下：

$$\forall f\in\mathcal{I},\ \exists i\in\mathcal{A},\ \text{where } \operatorname{supp}(i)=[n]\setminus\operatorname{ind}(f). \quad (2)$$

因此，我们可以定义集合 $\mathcal{A}_{m-r}$，它等价于 $\mathcal{I}_r$，用于收集满足 $|\mathsf{supp}(i)|=m-r$ 的行索引，其中 $i\in\mathcal{A}_{m-r}$。本文中，对于极化码，我们采用 $m=n$，而对于一般的递减单项式码，则采用 m。矩阵 $\mathcal{G}_N=\begin{bmatrix}1&1\\0&1\end{bmatrix}^{\otimes n}$ 的各行表示在 $\mathbb{F}_2^n$ 上对单项式的所有可能求值。因此，i 与 f 之间的关系定义为

$$i=\sum_{j\in[n]\setminus\operatorname{ind}(f)}2^j. \quad (3)$$

根据（3），令 f由 $\mathsf{ind}(f)=[n]\setminus\mathsf{ind}(f)$ 定义的 $\boldsymbol{G}_N$的一行表示。例如，行 $f=x_4x_3x_1\to(00101)_2=5$ 等价于单项式 $f=x_2x_0\to(11010)_2=26$。我们可以交替使用 f 及其十进制等价形式。注意，由于简化多项式形式体系的优势，我们稍微偏离了极化码的通常约定，即在 $\boldsymbol{G}_2$的克罗内克积中使用。相反，我们使用 $\mathcal{G}_2=\begin{bmatrix}1&1\\0&1\end{bmatrix}$。很容易看出，这两个定义（我们的定义和传统定义）是等价的，它们只相当于重新排列码的位置。

B. 递减单项式码

首次在 [4] 中证明，极化码与 Reed-Muller码类似，属于一个称为递减单项式码的大型码族。此外，[5] 和 [23] 对单项式序进行了部分刻画，该单项式序在基于可靠性的子信道关系语境中被称为（通用）偏序。Reed-Muller码与极化码之间的基本代数关系超越了它们的单项式结构。众所周知，极化码和 Reed-Muller 单项式集合（$\mathcal{I}$）都遵循一种记作 $\preceq$的序关系，正如 [5] 和 [23] 中所示。

我们先定义单项式集合上的偏序。下面将建立同次数和不同次数的两个单项式f 和 g 之间的关系 $\preceq$ 和 $\preceq_w$。注意，$\preceq_w$ 中的“w”表示“弱”（如弱序中的弱）；与 $\preceq$ 相比，根据定义，任何一对满足关系 $f\preceq_w g$的单项式 f、g 也满足关系 $f\preceq g$。我们用“$|$”符号表示单项式之间的整除关系，即当且仅当 $\mathsf{ind}(f)\subseteq\mathsf{ind}(g)$ 时，$f|g$。自然地，两个单项式的最大公因单项式为 $\gcd(f,g)=h$，其满足 $\mathsf{ind}(h)=\mathsf{ind}(f)\cap\mathsf{ind}(g)$。

定义 2. 设 m 为正整数，且 f、$g\in\mathcal{M}_m$.那么，当且仅当 $f|g$. 时，$f\preceq_w g$。当 $\deg(f)=\deg(g)=s$时，若 $\forall\ 1\le\ell\le s\ \ i_\ell\le j_\ell$，则称 $f\preceq_{sh}g$，其中 $f=x_{i_1}\dots x_{i_s}$、$g=x_{j_1}\dots x_{j_s}$。

Define $f\preceq g$ iff $\exists g^*\in\mathcal{M}_m$ s.t. $f\preceq_{sh}g^*\preceq_w g$.

注 1。在 $\preceq$. 的定义中可能有 $g^*=g$。在这种情况下，如果 $f\preceq g$ 且 $\deg(f)=\deg(g)$，则有 $\preceq=\preceq_{sh}$.

记号 $f\preceq_{sh}g$ 源于这样一个事实：可以通过对 f. 中的某些变量进行正向平移，从 f 得到 g。例如，$x_2x_3\preceq_{sh}x_2x_6$，因为 x_6 是将 x_3. 平移 3 个位置得到的

注意，变量之间存在链关系，即 $x_0\preceq x_1\preceq\cdots\preceq x_{m-1}.$。此外，$\preceq$ 是一种偏序关系，例如，x_3x_4 和 x_1x_5 关于 $\preceq$. 不可比较。本文研究的单项式集合都是递减单项式集。

定义3. 集合 $\mathcal{I}\subseteq\mathcal{M}_m$ 是递减的，当且仅当 ($f\in\mathcal{I}$ 和 $g\preceq f$) 蕴含 $g\in\mathcal{I}$。

如果我们将每个单项式 $f\in\mathcal{M}_n$ 映射到极化码背景下记为 W_n^f 的对应合成信道，那么可以根据信道可靠性建立任意一对合成信道之间的关系，如下所示：设 f 和 g 是满足 $f\preceq_w g$ 的两个单项式，则根据 [22, 命题3.3.29]，有 $W_n^g\preceq_d W_n^f$。这里，$\preceq_d$ 中的“d”表示信道 W_n^g 是信道 W_n^f 的退化。现在，由于极化码由单项式集合 $\mathcal{I}\subset\mathcal{M}_n$ 生成，若 $g\in\mathcal{I}$，则意味着 f 也属于 $\mathcal{I}$。

C. 置换群

将码 $\mathcal{C}$ 的码字映射为其他码字（即保持该码不变）的置换集合构成该码 $\mathcal{C}$ 的自同构群，记为 $\mathsf{Aut}(\mathcal{C})$。因此，置换 π 是码 $\mathcal{C}$ 的自同构，当且仅当对每个 $\boldsymbol{c}\in\mathcal{C}$，都有 $\pi(\boldsymbol{c})\in\mathcal{C}$。

$\mathbb{F}_2^m$ 上的双射仿射变换由一对 $(\mathrm{B}\ \boldsymbol{\varepsilon})$ 表示，其中 $\mathrm{B}=(b_{i,j})$ 是一般线性群 $\mathrm{GL}(m,2)$ 中的一个可逆矩阵，且 $\boldsymbol{\varepsilon}$ 属于 $\mathbb{F}_2^m$。$(\mathrm{B}\ \boldsymbol{\varepsilon})$ 对单项式 $g=\prod_{i\in\mathsf{ind}(g)}x_i$ 的作用记为 $(\mathrm{B}\ \boldsymbol{\varepsilon})\cdot g$，它将 g 中的每个变量 x_i 替换为一个变量 y_i，如

$$y_i=x_i+\sum_{j=0}^{i-1}b_{i,j}x_j+\varepsilon_i,$$

其中 $b_{i,j}$ 和 ε_i 属于 $\mathbb{F}_2$。这个新变量 y_i，实际上是一个线性形式（一个多项式，其中所有项的次数至多为 1）。此外，这个线性形式的最大变量是 x_i，因为其他变量相对于序关系 $\preceq$. 都小于 x_i

对于递减单项式码，采用一种下三角仿射变换，记作 LTA(m,2)，其中 B $\in$GL(m, 2) 是一个下三角二进制矩阵，且 $b_{i,\ i}=1$ 并且$b_{i,\ j}=0$ 当 $j>i$时。因此，下三角仿射群 LTA(m, 2) 可表示为以下从 $\mathbb{F}_2^m$到其自身的映射。

$$\boldsymbol{x}\to\mathbf{B}\boldsymbol{x}+\boldsymbol{\varepsilon},$$

其中，矩阵乘法表示线性映射，向量加法表示平移。对于递减单项式码的特殊子类，例如 Reed-Muller码，其完全置换群是已知的。事实上，一般仿射群是任意 $\mathcal{R}(r,m)$ 的完全置换群，其中 $1\le r<m-1$.

例 2. 令 $g=x_1x_4$，其中 $m=5$。那么映射 $\boldsymbol{x}\to\mathbf{B}\boldsymbol{x}+\boldsymbol{\varepsilon}$ 如下:

$$\begin{bmatrix}1&0&0&0&0\\b_{1,0}&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\b_{4,0}&b_{4,1}&b_{4,2}&b_{4,3}&1\end{bmatrix}\begin{bmatrix}x_0\\x_1\\x_2\\x_3\\x_4\end{bmatrix}+\begin{bmatrix}0\\\varepsilon_1\\0\\0\\\varepsilon_4\end{bmatrix}$$

LTA(m,2) 作用于一个单项式后得到的多项式集合，称为一个轨道。

定义 4. 单项式 f 在 LTA(m, 2) 作用下的轨道定义为以下多项式集合

$$\mathrm{LTA}(m,2)\cdot f=\{(\mathbf{B},\boldsymbol{\varepsilon})\cdot f\mid(\mathbf{B},\boldsymbol{\varepsilon})\in\mathrm{LTA}(m,2)\}.$$

由于 LTA(m, 2) 在 ev(f) 上的作用是一个置换，LTA(m, 2) $\cdot f$ 中的所有元素都具有相同的汉明重量。在估算递减单项式码的最小重量码字数量时，这一事实将很有用。

D. 最小重量码字

在着眼于较大重量之前，我们先回顾一下最小重量码字是如何计数的。本质上，[5] 中的作者利用 LTA(m,2) 在子集 $\mathcal{I}_r$上的作用，其中 r 是递减单项式集 $\mathcal{I}$中单项式的最大次数。问题在于，当我们考虑完整群 LTA(m, 2) 时，需要确定每个陪集首的稳定子子群。为实现这一目标，定义了 LTA(m, 2) 的一个特定子群。

定义 5（[5], [22]）。对于任意 $g\in\mathcal{M}_m$，定义 LTA(m, 2)$_g$ 为 (B $\boldsymbol{\varepsilon}$) $\in$LTA(m, 2) 的子群，其定义如下:

$$\varepsilon_i=0\text{ if }i\notin\mathrm{ind}(g)\quad\text{ and }\quad b_{ij}=\begin{cases}0\text{ if }i\notin\mathrm{ind}(g)\\0\text{ if }j\in\mathrm{ind}(g).\end{cases}$$

例 3. 令 $g=x_0x_1$，则根据定义，我们有 LTA(m, 2) $\cdot g=\{(x_0+\varepsilon_0)(x_1+a_{1,\ 0}x_0+\varepsilon_1)\mid\varepsilon_0$、$a_{1,\ 0}$、$\varepsilon_1\in\mathbb{F}_2\}$。完整群有 4 个不同元素，尽管 ε_0、$a_{1,\ 0}$，ε_1 可以在 $\{0,1\}$ 中取两个值，我们原本预期有 $2^3=8$ 个元素。四个重复元素使 g 保持不变量，即

$$(x_0+1)(x_1+x_0+1)=(x_0+1)(x_1+1)=x_0x_1+x_1+x_0+1,$$

$$(x_0+1)(x_1+x_0)=(x_0+1)x_1=x_0x_1+x_1,$$

$$x_0(x_1+x_0)=x_0(x_1+1)=x_0x_1+x_0,$$

$$x_0(x_1+x_0+1)=x_0x_1.$$

如上方蓝色高亮部分所示，由于 $0\in\mathrm{ind}(g)$，当$a_{1,\ 0}=1$ 时，所得多项式与群中的另一个多项式相同。回顾 $x_j^2=x_j$ 属于 $\mathbb{F}_2$。另一方面，子群 LTA(m,2)$_g$ 仅给出 2^2 个不同元素，因为根据定义 $a_{1,\ 0}=0$。该子群的元素为 (x_0+1)(x_1+1)、(x_0+1)x_1、x_0(x_1 +1) 和 x_0x_1。

注意，对于任意单项式 $g\in\mathcal{M}_m$，LTA(m,2)$_g$ 对子群中任意单项式 $f\in\mathcal{M}_m$ 的作用都是良定义的。此外，根据 LTA(m, 2)$_g$ 的定义，我们注意到，只有 g 中相对于 $\preceq$小于f 中变量的那些变量，才会在群作用中产生贡献。下面给出一个例子。

例4。取 $g=x_4$ 和 $f=x_0x_2$。那么

$$\mathrm{LTA}(m,2)_g\cdot f=\mathrm{LTA}(m,2)\cdot f.$$

如果令 $g=x_0x_4$ 和 $f=x_1x_2x_5$，那么 LTA(m, 2)$_g\cdot f$中的任意多项式都可以写成如下形式 ($x_1+\varepsilon_1$)($x_2+b_{2,\ 1}x_1+\varepsilon_2$)($x_5+b_{5,\ 3}x_3+b_{5,\ 2}x_2+b_{5,\ 1}x_1+\varepsilon_5$)。

这个子群的特别之处在于，它具有以下定理所述的两个重要性质。

定理1 ([5], [22])。令 $f\in\mathcal{M}_m$. 那么我们有

$$\mathrm{LTA}(m,2)\cdot f=\mathrm{LTA}(m,2)_f\cdot f.\tag{4}$$

此外，LTA(m, 2)$_f\cdot f$中不存在被多个群元素（恒等元除外）固定的多项式。

现在，我们来考察轨道 LTA(m, 2)$_f\cdot f$的大小，记为 |LTA(m, 2)$_f\cdot f$|。我们可以将 LTA(m,2)$_f$ 对 f 的作用分解为两个操作:

- 平移：单项式中的每个变量 x_i 都可以通过标量 $\varepsilon_i\in\mathbb{F}_2$ 平移为 $x_i+\varepsilon_i$。因此，次数为 deg(f) 的单项式 f，其平移数量等于所有变量可能取值的组合数，即 $2^{\deg(f)}$。
- 线性映射：每个变量 x_i 都可以映射为一个“新变量”（y_i），它是变量 x_j $j\in[i]\setminus f$ $y_i=x_i+$的线性组合，其中 $\sum_{j=0\ j\notin f}^{i-1}b_{i\ j}x_j$ ind( ) 作为 ,ind() ,。y_i中考虑的额外变量表示我们在 x_i. 上拥有的自由度。这将记作 $\lambda_f(i)=|\{j\in[i]\mid j\notin\mathrm{ind}(f)\}|$，并表示变量 x_i上的群作用中变量的最大数量。f 支撑集中的所有 x_i 上的自由变量总数为 $|\lambda_f(f)|=\sum_{i\in\mathrm{ind}(f)}\lambda_f(i)$。然后，总的可能数量。

支撑集 f 中所有变量的作用为 $2^{|\lambda_f|}$（因为我们定义在 $\mathbb{F}_2$ 上）。

一般而言，我们可以有 LTA$(m,2)_f \cdot g$，其中 f和 g可能不同。在这种情况下，我们有

$$|\lambda_f(g)| = \sum_{i \in \mathrm{ind}(g)} \lambda_f(i). \tag{5}$$

当 $g = f$ 时，我们将简化记号并使用 λ_f。因此，单项式 f 在 LTA$(m,2)$作用下的轨道基数为

$$|\mathrm{LTA}(m,2)_f \cdot f| = 2^{\deg(f)+|\lambda_f|} \tag{6}$$

例 5 展示了这一计数过程的运作方式。前述定理直接导出了一个高效的公式，用于计算最小重量码字的数量。假设我们有一个递减单项式集 $\mathcal{I}$，其最大次数单项式为 r，即 $\mathcal{I}_r$ 并不平凡。我们知道，$\mathcal{C}(\mathcal{I})$的任意最小重量码字的重量均为2^{m-r}；更重要的是，任何满足 w($\boldsymbol{c}$) $= 2^{m-r}$的 $\boldsymbol{c} \in \mathcal{C}(\mathcal{I})$都具有以下形式 $\boldsymbol{c} =$ ev$(y_1 \dots y_r)$，其中 y_i是线性无关形式，即 $y_i \in \mathrm{R}_m$，且 deg$(y_i) = 1$；对于任意索引 i，方程 $y_i = \sum_{1 \le j \le r,\ j \ne i} \varepsilon_j y_j$ 在 $\mathbb{F}_2$ 上只有一个解，即零向量 $\varepsilon_j = 0$。$\forall j$. 计数方法依赖于以下内容。

1) 任意单项式 $f \in \mathcal{I}_r$ 将在 LTA$(m,2)f$ 下定义一个轨道，其中所有多项式求值后均为最小重量码字；2) 我们知道如何计算轨道的基数|LTA$(m,2)_f \cdot f| =$ |LTA$(m,2)_f$|（根据定理1）；3) 对于任意一对单项式 f、$g \in \mathcal{I}_r$，轨道 LTA$(m,2)_f \cdot f$和 LTA$(m,2)_g \cdot g$互不相交。4) 最后 , 对所有单项式 $f \in \mathcal{I}_r$求和 .

用于证明上述过程能够检索出所有最小重量码字的一个关键要素，是以下引理，该引理已在[22]中的命题 3.7.12 中得到证明。

引理 1. 设 $P = \prod_{j=1}^{l} y_j$ 是由 l 个线性无关形式 y_i 的乘积，且每个线性形式都具有最大变量 x_{i_j}。则 P可以写成 $P = \prod_{j=1}^{l} y_j^*$，其中 y_j 中的所有最大变量$x_{i_j^*}$ 两两不同。

注意，每个 $f \in \mathcal{I}_r$ 都表示陪集 $\mathcal{C}_{\tilde{f}}$ 的一个陪集首，而轨道表示这样一组核心行：它们与平衡行进行行组合后，能够得到最小重量码字 [24]。

例 5. 设 $m = 8$ 和 $\mathcal{I}$ 为一个递减单项式集，且 $r = 4$. 。假设 $f \in \mathcal{I}_r$ ={x_1x_0($x_3x_2, x_4x_2, x_5x_2, x_4x_3$)}，则下表展示了求重量为 w$_{min}$ 的码字总数（即 $|W_{\mathrm{w}_{\min}}|$）的过程。

ind(f)	{3, 2, 1, 0}	{4, 2, 1, 0}	{5, 2, 1, 0}	{4, 3, 1, 0}
($\lambda_f(3) \cdots, \lambda_f(0)$)	(0, 0, 0, 0)	(1, 0, 0, 0)	(2, 0, 0, 0)	(1, 1, 0, 0)
|LTA$(m,2)_f \cdot f$|	2^4	2^5	2^6	2^6
$\lvert W_{\mathrm{w}_{\min}} \rvert$	176			

IV. 重量为 1.5w$_{\min}$ 的码字的结构特性

我们将从回顾 Reed-Muller码的一项分类结果开始本节，这将构成.....的基础。

我们的重量枚举。Kasami 等人刻画了 [15] 中重量小于最小重量两倍的 Reed-Muller码码字，并推导出这些重量枚举的显式公式。

定理 2。 [25],[15,定理 1] 令 $r < m$ 和 $P \in \mathrm{R}_m$ 满足 deg$(P) \le r$，其中 $0 <$ w(ev$(P)| < 2^{m+1-r}$. 则P 仿射等价（可以使用仿射变换进行转换）于以下形式之一

1) $P = y_1 \dots y_{r-\mu}(y_{r-\mu+1} \dots y_r + y_{r+1} \dots y_{r+\mu})$ where $m \ge r+\mu, r \ge \mu \ge 3$
2) $P = y_1 \dots y_{r-2}(y_{r-1}y_r + \cdots + y_{r+2\mu-3}y_{r+2\mu-2})$ where $m - r + 2 \ge 2\mu, \mu \ge 2$.

在这两种情况下，y_i 都是线性无关形式，并且 w(ev(P)) $= 2^{m+1-r} - 2^{m+1-r-\mu}$.

例6. 设 $m = 9$ 和 $r = 3$. 。根据定理2中的条件，我们注意到 $3 \le \mu \le 3$（情况1）和 $4 \le 2\mu \le m - r + 2 = 8$，这意味着 $\mu \le 4$（情况2）。因此，有

<escape>• $P = y_1y_2y_3$ </escape>其给出了 w(ev(<escape>P</escape>)) <escape> = </escape>w$_{\min}$ <escape> $= 2^{9-3} =$</escape>64;

- $\mu = 2$（定理2中的情形2），$P = y_1(y_2y_3 + y_4y_5)$，且我们有 w(ev(P)) $= 2^7 - 2^{7-2} = 128 - 32 = 96$;
- $\mu = 3$（定理2中的情形1），$P = y_1y_2y_3 + y_4y_5y_6$ 并且我们有 w(ev(P)) $= 2^7 - 2^{7-3} = 128 - 16 = 112$;
- $\mu = 4$（定理2中的情形2），$P = y_1(y_2y_3 + y_4y_5 + y_6y_7)$, 且我们有 w(ev$(P)$) $= 2^7 - 2^{7-4} = 128 - 8 = 120$;

备注2。对于 Reed-Muller码，任意仿射变换都会整体保持该码；但对于一般的递减单项式码，这一性质不再成立。因此，对于递减单项式码，无法直接应用定理 2 来计数此类码字。

本文将把分析限制在情形 $\mu = 2$，这等价于重量为 1.5 w$_{\min}$. 的码字

推论1。设 $r < m$ 为正整数，满足 $r =$ max $_{\mathrm{ev}(P) \in \mathcal{C}}$ deg(P)。那么，任何重量为 1.5 w$_{\min}$ 的码字，在仿射变换下都等于 ev$(y_1 \dots y_{r-2}(y_{r-1}y_r + y_{r+1}y_{r+2}))$。

仔细观察推论1中多项式的形状，我们可以推断，任何重量为1.5 w$_{\min}$的码字都等于两个最小重量码字之和。事实上，$y_1 \dots \dots y_r$和 $y_1 \dots y_{r-2}y_{r+1}y_{r+2}$ 都定义了最小重量码字（作为 r 个线性无关形式的乘积），因此它们分别属于两个不同的轨道 LTA$(m,2)\cdot f$,LTA$(m,2) \cdot g$. 因此，我们的首要任务是理解这两个集合之和的结构。

回顾一下，作用于 f 上的子群 LTA$(m,2)f$ 生成的轨道与完整群作用 LTA$(m,2)$ 在

任意单项式 f. 上生成的轨道完全相同。由于这里涉及轨道的和与乘积，我们想了解在这种情况下子群性质如何保持。

引理2. 设 f、$g \in \mathcal{I}_r$ 和 $h =$ 的最大公约数为 f、$g \in \mathcal{M}_m$. 那么

$$\mathrm{LTA}(m,2)\cdot h\cdot\left(\mathrm{LTA}(m,2)\cdot\frac{f}{h}+\mathrm{LTA}(m,2)\cdot\frac{g}{h}\right)$$
$$=\mathrm{LTA}(m,2)_h\cdot h\cdot\left(\mathrm{LTA}(m,2)_f\cdot\frac{f}{h}+\mathrm{LTA}(m,2)_g\cdot\frac{g}{h}\right).$$

我们结果的证明可参见附录B。下面通过一个例子来说明这一分解的工作原理。

例7. 设 $h = x_0x_6$、$f/h = x_3x_2$ 和 $g/h = x_5x_1$.。多项式 $P = x_0(x_6 + x_2)\,((x_3 + x_0)x_2 + x_5(x_1 + x_0))$ 属于 LTA(m, 2)$\cdot h\cdot\left(\mathrm{LTA}(m,2)\cdot\frac{f}{h}+\mathrm{LTA}(m,2)\cdot\frac{g}{h}\right)$。展开乘积可得

$$\begin{aligned}P &= x_0(x_6+x_2)(x_3+x_0)x_2 + x_0(x_6+x_2)x_5(x_1+x_0)\\ &= x_0(x_6+x_2)(x_3+1)x_2 + x_0(x_6+x_2)x_5(x_1+1)\\ &= x_0(x_6+x_2)\left((x_3+1)x_2 + x_5(x_1+1)\right)\end{aligned}$$

因此，P $m\ 2_h\cdot h\cdot$ 是集合 $\left(m\ 2_f\cdot\frac{f}{h}+\ m\ 2_g\cdot\frac{g}{h}\right)$. LTA(,) LTA(,) LTA(,) 中的一个元素。

接下来，我们针对递减单项式码中重量为 1.5 $\mathrm{w}_{\min}$ 的码字提出一个分类定理。该结果在某种程度上相当于 Kasami 和 Tokuras 的分类定理：前者允许仿射变换，而这里的分类则允许来自 LTA(m,2) 的变换。

定理3. 设 $\mathcal{C}(\mathcal{I})$ 是一个递减单项式码，且 $r = \max_{f\in\mathcal{I}}\deg(f)$。那么，任意重量为 1.5 $\mathrm{w}_{\min}$ 的码字，例如 ev(P $\exists f\ g\in\mathcal{I}_r$ $P\in$ $m\ 2_h\cdot h\cdot$)，均满足，其中 $\left(m\ 2_f\cdot\frac{f}{h}+\ m\ 2_g\cdot\frac{g}{h}\right)$ $h =$ $f\ g$ LTA(,) LTA(,) LTA(,)，最大公约数为 gcd(,)，且 $\deg(h) = r-2$。

注意，该结果是构造性的，即给定一个重量为 1.5 $\mathrm{w}_{\min}$ 的码字$\boldsymbol{c} = \mathrm{ev}(P)$，可以计算出两个单项式 f, g，使得 P 属于它们在 LTA(m,2) 作用下的轨道的闵可夫斯基和。在下面的示例中，我们将说明如何给定 P 计算单项式 f, g （更多细节请参见附录 C 中定理的证明）。

例8. 设 $m = 9, r = 3$. 任意 $P \in \mathrm{R}_m$ 满足 $\mathrm{w}(\mathrm{ev}(P)) = 2^{9+1-3} - 2^{9+1-5} = 96 = 1.5\times 64 = 1.5\,\mathrm{w}_{\min}$。考虑以下情况。

1) 一个因子，所有互不相同的最大变量：
$P = (x_4 + x_0)x_2x_1 + (x_5 + x_1)(x_4 + x_0)x_3$。根据定理2，ev($P$)是一个1.5 $\mathrm{w}_{\min}$，因为将 P因式分解后，我们得到$P = (x_4 + x_0)(x_2x_1 + (x_5 + x_1)x_3)$，其形式为 $y_1(y_2y_3 + y_4y_5)$。只需将每个 y_i 中的最大变量附加上去，我们便可令 $f = x_4x_2x_1$、$g = x_5x_4x_3$，从而 $h =$ 最大公约数$(f, g) = x_4, f/h = x_2x_1, g/h = x_5x_3$.
2) 一个因子，四个互不相同的最大变量：
$P = (x_4 + x_0)(x_5 + x_2)x_1 + (x_5 + x_1)(x_4 + x_0)x_3$，一次因式分解后，与前一种情况一样，可得到定理 2 中所需的形式，$P = y_1(y_2y_3 + y_4y_5)$。然而，仅使用最大变量设置 f, g 并不可行。事实上，这会得到 $f = x_5x_4x_1$, $g = x_5x_4x_1$，而这并非定理 3 所述的形式。不过，按照定理 3 证明中的方法重新排列 P 中的各项，可得$P = (x_4 + x_0)((x_5 + x_1)(x_3 + x_1) + (x_2 + x_1)x_1)$。现在，在每个线性无关形式中取最大变量，可得到 $f = x_5x_4x_3$, $g = x_4x_2x_1$，这正是定理 3 所要求的。
3) 一个因子，三个互不相同的最大变量：
$P = (x_6 + x_0)(x_5 + x_4)(x_3 + x_1 + 1) + (x_5 + x_0)(x_6 + x_0)(x_3 + 1)$。事实上，根据定理 2，这对应一个重量为 1.5 $\mathrm{w}_{\min}$ 的码字，因为可以写成 $P = y_1(y_2y_3 + y_4y_5)$，其中 y_i 均为线性无关形式。如果我们只选取每个 y_1 中的最大变量（蓝色），就会得到 $f = g = x_6x_5x_3$，这实际上并无多大帮助。通过巧妙地处理这个多项式，可以得到 $P = (x_6 + x_0)((x_5 + x_0)x_1 + (x_4 + x_0)(x_3 + x_1 + 1))$, 由此可得 $f = x_6x_5x_1, g = x_6x_4x_3$，与定理 3 完全一致。

对于 Reed-Muller码，定理 2 与一般仿射群是刻画和计数重量小于 2 $\mathrm{w}_{\min}$ 的码字的两个主要要素。递减单项式码不具有完整的一般仿射群。因此，当我们研究递减单项式码时，我们的结果为理解此类码字的形成方式提供了第一步。

进一步地，我们将根据定理 3 确定 $\mathrm{LTA}(m,2)_h\cdot h\cdot(\mathrm{LTA}(m,2)_f\cdot\frac{f}{h}+\mathrm{LTA}(m,2)_g\cdot\frac{g}{h})$ 的基数。这里的主要挑战在于估计 $|\mathrm{LTA}(m,2)_{\frac{f}{h}+\ m\ 2_g\cdot\frac{g}{h}}|$. LTA(,) 显然，以下上界 [26] 成立 $|\mathrm{LTA}(m,2)\cdot f + \mathrm{LTA}(m,2)\cdot g| \trianglelefteq \mathrm{LTA}(m,2)\cdot f|\mathrm{LTA}(m,2)\cdot g|$. 然而，实际上并不总能达到该上界。我们先从一个例子开始。

例9. 令 $f = x_4x_2x_0$ 和 $g = x_3x_2x_1$. 那么，任意多项式 $P \in \mathrm{LTA}(m,2)\cdot f$和 $Q \in \mathrm{LTA}(m,2)\cdot g$都可以写成 $P = (\mathrm{A}\ \varepsilon)\cdot f$、$Q = (\mathrm{B}\ \gamma)\cdot g$，或者等价地

$$P = (x_4 + b_{4,3}x_3 + b_{4,1}x_1 + \varepsilon_4)(x_2 + b_{2,1}x_1 + \varepsilon_2)(x_0 + \varepsilon_0)$$
$$Q = (x_3 + a_{3,0}x_0 + \gamma_3)(x_2 + a_{2,0}x_0 + \gamma_2)(x_1 + a_{1,0}x_0 + \gamma_0)$$

其中标量为 $a_{i,j}, b_{i,j}, \varepsilon_i, \gamma_i \in \mathbb{F}_2$.

轨道的基数为 $|\mathrm{LTA}(m,2)\cdot f| = 2^{3+(2+1+0)} = 2^6$ 和 $|\mathrm{LTA}(m,2)\cdot g| = 2^{3+(1+1+1)} = 2^6$。因此，我们有

$$|\mathrm{LTA}(m,2)\cdot f + \mathrm{LTA}(m,2)\cdot g| \le 2^{12}.$$

然而，在这个例子中，由于存在碰撞，上界无法达到。我们将碰撞定义如下：

定义6. 碰撞：任意一对不同的多项式$P, P^* \in \mathrm{LTA}(m,2)\cdot f$ 和 $Q, Q^* \in \mathrm{LTA}(m,2)\cdot g$，其中$P \ne P^*, Q \ne Q^*$，若它们产生相同的和，即 $P + Q = P^* + Q^*$，则会发生碰撞。

碰撞的一个例子是 $P=(x_4+x_3)x_2x_0, Q=x_3x_2x_1$和 $P^*=x_4x_2x_0, Q^*=x_3x_2(x_1+x_0)$。注意，在例9中，我们只需在每个单项式中插入一个来自另一个单项式的变量，就能为 $x_4x_2x_0+x_3x_2x_1$生成一个不变量。但并非总能这样做。

我们需要定义两个单项式的碰撞数。

定义7. 设 $f = x_{i_1}x_{i_2}$和 $g = x_{j_1}x_{j_2}$满足 $\gcd(f,g) = 1$ 和 $i_2 > j_2.$，则 f 和g 的碰撞度为

$$\alpha_{f,g} = \begin{cases} 0 & i_2 > i_1 > j_2 > j_1 \\ 1 & i_2 > j_2 > i_1 > j_1 \\ 2 & i_2 > j_2 > j_1 > i_1 \end{cases}.$$

对于任意给定的一对 (P,Q)，满足 $P \in \mathrm{LTA}(m,2) \cdot f$且$q \in \mathrm{LTA}(m,2) \cdot g$，数量 $\alpha_{f,g}$ 将使我们能够统计任意固定的一对多项式会产生多少次碰撞。事实上，正如我们将要证明的，对于给定的一对单项式 $f,g.$，该参数恰好等于发生碰撞时需要满足的独立线性方程的数量。因此，f 和 g 的结构与该参数之间存在联系是很自然的。

例10. 我们分别考虑两种情况

- $i_2 > j_2 > j_1 > i_1$ with $f = x_6x_2, g = x_5x_3$, which imply $\alpha = 2$. For $P = (x_6 + x_4 + 1)(x_2 + x_1) \in \mathrm{LTA}(m,2)\cdot f$ and $Q = (x_5+x_4+x_2)(x_3+x_2+x_0+1) \in \mathrm{LTA}(m,2)\cdot g$. We can create two non-trivial distinct pairs P^*, Q^*
  - $P^* = (x_6 + x_4 + x_3 + x_2 + x_0)(x_2 + x_1)$ and $Q^* = (x_5 + x_4 + x_1)(x_3 + x_2 + x_0 + 1)$
  - $P^* = (x_6 + x_5 + x_3 + x_2 + x_1 + x_0)(x_2 + x_1)$ and $Q^* = (x_5 + x_4 + x_1)(x_3 + x_1 + x_0 + 1)$
- $i_2 > j_2 > i_1 > j_1$ with $f = x_4x_2, g = x_3x_0$. We obtain that $f + g = (x_4 + x_0)x_2 + (x_3 + x_2)x_0$.

参数 $\alpha_{f,g}$ 为何重要? 主要是因为它能帮助我们统计有多少多项式被重复计数。

命题1. 设 $\mathcal{I} \subseteq \mathcal{M}_m$ 为递减单项式集，且 $f = x_{i_1}x_{i_2}$ 和 $g = x_{j_1}x_{j_2}$ 满足 $\gcd(f,g) = 1$，以及 $i_2 > j_2.$，则

$$|\mathrm{LTA}(m,2)\cdot f + \mathrm{LTA}(m,2)\cdot g| = \frac{|\mathrm{LTA}(m,2)\cdot f| \times |\mathrm{LTA}(m,2)\cdot g|}{2^{\alpha_{f,g}}}, \quad (7)$$

该结果的证明见附录D。

到目前为止，我们已经刻画了不同轨道的闵可夫斯基和的基数，但仍有最后一个问题尚未回答。乘积 $\mathrm{LTA}(m,2)_h \cdot h \cdot \left(\mathrm{LTA}(m,2)_f \cdot \frac{f}{h} + \mathrm{LTA}(m,2)_g \cdot \frac{g}{h}\right)$. 的基数是多少? 答案相当明显：乘积集的基数等于各集合基数的乘积。

引理 3. 设 $\mathcal{I}$ 是一个递减集合，满足 $r = \max_{f\in\mathcal{I}} \deg(f)$，且 f、$g \in \mathcal{I}_r$ 满足 $h = \gcd(f,g)$，使得 $\deg(h) = r-2.$。那么

$$|\mathrm{LTA}(m,2)_h \cdot h \cdot \left(\mathrm{LTA}(m,2)_f \cdot \frac{f}{h} + \mathrm{LTA}(m,2)_g \cdot \frac{g}{h}\right)| = |\mathrm{LTA}(m,2)_h \cdot h| \times |\left(\mathrm{LTA}(m,2)_f \cdot \frac{f}{h} + \mathrm{LTA}(m,2)_g \cdot \frac{g}{h}\right)| \quad (8)$$

V. 1.5$w_{\min}$ 重量码字的计数公式

我们此前已经证明，任何具有单项式集合 $\mathcal{I}$ 且最大次数单项式为 $r = \max_{f\in\mathcal{I}} \deg(f)$ 的递减单项式码，当且仅当存在次数为 r 的单项式（记这样的一对单项式为 (f,g)），使得它们共享 $r-2$ 个变量，即 $\deg(\gcd(f,g)) = r-2.$ 时，才会包含重量为 1.5 $w_{\min}$ 的码字。例如，最大次数单项式为 $x_0x_1x_2$、$x_0x_1x_3$ 的递减单项式码不会包含重量为 1.5 $w_{\min}$ 的码字，而最大次数变量为 $x_0x_1x_2$、$x_0x_1x_3$、$x_0x_2x_3$、$x_0x_1x_4$ 的码则会包含重量为 1.5 $w_{\min}$ 的码字，因为码字对 $(x_0x_1x_4, x_0x_2x_3)$ 具有次数为 $r-2=1$ 的公因子 x_0。

因此，由定理3可推得以下结论。

推论 2. 设 $\mathcal{I}$ 是满足 $r = \max_{f\in\mathcal{I}}(\deg(f))$ 的递减单项式集。那么我们有

$$W_{1.5\,w_{\min}} = \bigcup_{\substack{f,g\in\mathcal{I}_r \\ h=\gcd(f,g)\in\mathcal{I}_{r-2}}} \mathrm{LTA}(m,2)_h \cdot h \cdot \left(\mathrm{LTA}(m,2)_f \cdot \frac{f}{h} + \mathrm{LTA}(m,2)_g \cdot \frac{g}{h}\right) \quad (9)$$

接下来，我们将证明，对于不同的单项式对 (f,g)、(f^*, g^*)，它们定义的多项式集互不相交。从某种意义上说，我们将最小重量码字中轨道互不相交这一性质转移到了 1.5 $w_{\min}$.

命题 2. 设 $\mathcal{I}$ 是递减单项式集，且 (f,g)、$(f^*,g^*) \in \mathcal{I}_r \times \mathcal{I}_r$ 满足 $(f,g) \neq (f^*,g^*)$，并且 $\deg(h) = \deg(h^*) = r-2$，其中 $h = \gcd(f,g)$ 且 $h^* = \gcd(f^*,g^*)$。那么，集合 $\mathrm{LTA}(m,2)_h \cdot h \cdot (\mathrm{LTA}(m,2)_f \cdot \frac{f}{h} + \mathrm{LTA}(m,2)_g \cdot \frac{g}{h})$ 和 $\mathrm{LTA}(m,2)_{h^*} \cdot h^* \cdot (\mathrm{LTA}(m,2)_{f^*} \cdot \frac{f^*}{h^*} + \mathrm{LTA}(m,2)_{g^*} \cdot \frac{g^*}{h^*})$ 互不相交。

现在我们已掌握三项要素，将它们结合起来，就能得到任意递减单项式码中 1.5$w_{\min}$ 重量码字的闭式公式，从而隐含地得到极化码和 Reed–Muller 码的相应公式。让我们回顾这些要素，然后陈述结果。

- 任意1.5$w_{\min}$ 重量码字都是某个多项式的求值结果，该多项式属于两个轨道的闵可夫斯基和（定理3）
- 两个不同的次数为 r 的单项式生成不同的轨道（命题 2）
- 我们知道如何计算轨道的 Minkowski 和的基数（命题1）

定理 4. 设 $\mathcal{I}$ 是一个递减单项式集，且 $r = \max_{f\in\mathcal{I}} \deg(f)$。

$$|W_{1.5\,\mathrm{w}_{\min}}| = \sum_{\substack{f,g\in\mathcal{I}_r \\ h=\gcd(f,g)\in\mathcal{I}_{r-2}}} 2^{r+2+|\lambda_h|+|\lambda_f(\frac{f}{h})|+|\lambda_g(\frac{g}{h})|-\alpha_{\frac{f}{h},\frac{g}{h}}} \tag{10}$$

where $\frac{f}{h} = x_{i_1}x_{i_2}, \frac{g}{h} = x_{j_1}x_{j_2}$ with $i_2 > j_2$.

定理 4 中提出的用于统计重量为 $1.5\mathrm{w}_{\min}$ 的码字的闭式表达式，可以通过一个简单的过程实现。附录 A 中提供了一个实现方程 (10) 的 MATLAB 脚本。请注意，由于存在嵌套循环，该过程的复杂度为 $O(|\mathcal{I}_r|^2 \cdot r)$ 量级。[27]中提供了 MATLAB 脚本。

示例 11. 考虑极化码 (128,64)，将其视为递减单项式码，其中 $m = 7$ 和 $r = 4.$。令 $\mathcal{I}_r$ 为次数为 4 的单项式集合，其定义如下:

$$x_0x_1x_2x_3,\ x_0x_1x_2x_4,\ x_0x_1x_3x_4,$$

$$x_0x_2x_3x_4,\ x_1x_2x_3x_4,\ x_0x_1x_2x_5,\ x_0x_1x_3x_5$$

等价于 $\mathcal{A}_{m-r} = \{112, 104, 100, 98, 97, 88, 84\}$，作为 $\boldsymbol{G}_N$ 的行索引。表 I 列出了所有具有次数为 $r-2=2$ 的公因子 h 的单项式组合及其对应的基数。惩罚项用于计入碰撞，即不应重复计数的相同码字。“总计”列由所有子群的基数与惩罚项相乘得到。

示例 12。以示例 11 中的极化码 (128,64) 为例。由于极化码的构造取决于信道，因此可以通过缩小集合 $\mathcal{I}_r$ （或等效地，使用任意构造方法调整设计 SNR [28]）来改进该码。表 II 从上到下展示了设计 SNR 分别为 = 0、3、6 和 8 时对应的集合 $\mathcal{A}_{m-r}$。注意，当 $\mathcal{A}_{m-r} = \{112, 104\}$，或等效地当 $\mathcal{I}_r = \{x_0x_1x_2x_3, x_0x_1x_2x_4\}$ 时，公因子 $x_0x_1x_2$ 的次数为 $3 > r-2$，不满足存在重量为 $1.5\mathrm{w}_{\min}$的码字的条件。因此，不存在重量为 $1.5\mathrm{w}_{\min}$ 的码字。此外，通过改变设计 SNR，我们正从极化码转向 Reed-Muller码。

作为较长码的一个例子，我们取极化码 (2048,1024)，其中 $m = 11$。表 II 的最后两行给出了采用设计信噪比 = 2 和 3（底部）构造的该码的枚举结果。由于重量为 $\mathrm{w}_{\min}$ 和 $1.5\mathrm{w}_{\min}$ 的码字枚举取决于集合 $\mathcal{I}_r$，因此减小该集合的基数可以同时减少这两种枚举数量。表 II 展示了这一点。

VI. 通过 $\boldsymbol{G}_N$-行组合构造 $1.5\mathrm{w}_{\min}$ 重量码字

在本节中，我们展示前几节讨论内容对通过组合特定的成对重量为 $\mathrm{w}_{\min}$ 的码字来形成重量为 $1.5\mathrm{w}_{\min}$ 的码字所产生的影响。如 [31], [32], 所示，极化码 $\mathcal{C}(\mathcal{A})$ 的重量为 $\mathrm{w}_{\min}$ 的码字形成于由一行引导的陪集中。$\mathbf{g}_i, i \in \mathcal{A}_{m-r}$。然而，重量为 $1.5\mathrm{w}_{\min}$ 的码字是通过组合不同陪集的重量为 $\mathrm{w}_{\min}$ 的码字生成的。因此，让我们首先如下定义陪集:

定义 8. 陪集：我们可以将一个极化码划分为 $|\mathcal{A}|$个互不相交的陪集 $\mathcal{C}_i(\mathcal{A}) = \mathbf{g}_i + \mathcal{C}(\mathcal{A} \setminus [0, i])$，它们属于其子码$\mathcal{C}(\mathcal{A} \setminus [0, i])$，其中 $i \in \mathcal{A}$，$\mathbf{g}_i$ 是极化变换 $\boldsymbol{G}_N$ 的第 i 行，即

$$\mathcal{C}_i(\mathcal{A}) \triangleq \left\{ \mathbf{g}_i \oplus \bigoplus_{h\in\mathcal{H}_i} \mathbf{g}_h \colon \mathcal{H}_i \subseteq \mathcal{A} \setminus [0, i] \right\} \subseteq \mathcal{C}(\mathcal{A}). \tag{11}$$

请注意，由行 f 引领的陪集可视为置换群 LTA(m, 2)$_f$ 对 f 的作用。由于每个陪集 $\mathcal{C}_i(\mathcal{I})$ 中码字的重量为 [24]

$$\mathrm{w}(\mathbf{g}_i \oplus \bigoplus_{j\in\mathcal{H}_i} \mathbf{g}_h) \geq \mathrm{w}(\mathbf{g}_i), \tag{12}$$

其中 $\mathcal{H}_i \subseteq [i+1, N-1]$，对于任意 $i \notin \mathcal{A}_{m-r}$，码$\mathcal{C}(\mathcal{A})$ 中位于陪集 $\mathcal{C}_i(\mathcal{A})$ 内的码字重量都将大于 $\mathrm{w}_{\min}$。因此，对于 $\mathrm{w}_{\min}$ 重量码字，我们只考虑陪集 $\mathcal{C}_i, i \in \mathcal{A}_{m-r}$。

将 $\boldsymbol{G}_N$ 中在陪集 $\mathcal{C}_{\bar{f}}$ 内形成 $\mathrm{w}_{\min}$ 重量码字的核心行索引收集在集合 $\mathcal{K}_{\bar{f}}$ 中，定义如下

$$\mathcal{K}_{\bar{f}} = \{i \in \mathcal{A}_{m-r} \setminus [0, \bar{f}] \colon |\operatorname{ind}(i) \setminus \operatorname{ind}(\bar{f})| = 1\},$$

和 $|\mathcal{K}_{\bar{f}}| = \deg(f) + |\lambda_f|$。回顾 f 与 $\bar{f}$ 之间的关系: f 的二进制表示是 f 的二进制表示的按位取反。假设有两个 $\mathrm{w}_{\min}$ 重量码字 $\boldsymbol{c}_{\bar{f}}$ 和 $\boldsymbol{c}_{\bar{g}}$，分别等价于 ev(P) 和 ev(Q), 其中 $P \in$ LTA(m, 2)$_f \cdot f$ 且 $Q \in$ LTA(m, 2)$_g \cdot g$。码字$\boldsymbol{c}_{\bar{f}}$ 由下式生成

$$\boldsymbol{c}_{\bar{f}} = \mathbf{g}_{\bar{f}} \oplus \bigoplus_{j\in\mathcal{J}} \mathbf{g}_j \oplus \bigoplus_{m\in\mathcal{M}(\mathcal{J})} \mathbf{g}_m. \tag{13}$$

其中，$\mathcal{J} \subseteq \mathcal{K}_{\bar{f}}$ 和 $\mathcal{M}$（$\mathcal{J}$）定义为一组附加行，用于得到 $\mathrm{w}(\boldsymbol{c}_{\bar{f}}) = \mathrm{w}_{\min}$，若 $\mathrm{w}\left(\mathbf{g}_{\bar{f}} \oplus \bigoplus_{j\in\mathcal{J}} \mathbf{g}_j\right) > \mathrm{w}_{\min}$（见[32]）。码字 $\boldsymbol{c}_{\bar{g}}$ 的构造方式类似。

要通过将 $\boldsymbol{c}_{\bar{f}}$ 和 $\boldsymbol{c}_{\bar{g}}$ 相加得到一个 $1.5\mathrm{w}_{\min}$-重量码字，即 $\mathrm{w}(\boldsymbol{c}_{\bar{f}} \oplus \boldsymbol{c}_{\bar{g}}) = 1.5\,\mathrm{w}_{\min}$，码字 $\boldsymbol{c}_{\bar{f}}, \boldsymbol{c}_{\bar{g}}$ 必须满足以下条件:

$$|\operatorname{ind}(\boldsymbol{c}_{\bar{f}}) \cap \operatorname{ind}(\boldsymbol{c}_{\bar{g}})| = \frac{1}{4}\,\mathrm{w}_{\min}\,.$$

这些码字存在于陪集 $\mathcal{C}_{\bar{f}}$ 和 $\mathcal{C}_{\bar{g}}$ 中，其中

$$|\operatorname{ind}(\bar{g}) \setminus \operatorname{ind}(\bar{f})| = 2. \tag{14}$$

这等价于推论1，即每一项中都有两个不同的变量，分别为 $y_{r-1}y_r$ 和 $y_{r+1}y_{r+2}$。为使不同陪集中的每一对码字都满足此条件，我们需要将每个陪集中可选的码字限制为在 $|\operatorname{ind}(f) \cap \operatorname{ind}(g)| = r-2$ 个共享变量上相匹配的码字。这会将码字的选择范围从 $2^{|\mathcal{K}_{\bar{f}}|}$缩小到$2^{|\mathcal{K}_{\bar{f}}|-(r-2)}$，位于 $\mathcal{C}_{\bar{f}}$中，或者位于 $\mathcal{C}_{\bar{g}}$中。也就是说，我们不能随意组合来自这些陪集的任意一对 $\mathrm{w}_{\min}$-码字，而是必须使它们相匹配。就每个陪集中的行组合而言，这意味着坐标 $\operatorname{ind}(f) \cap$

$\bar{f},\bar{g}$	ind(f), ind(g)	ind(h)	ind($\frac{f}{h}$)	ind($\frac{g}{h}$)	$\lvert\mathrm{LTA}(m,2)_h \cdot h\rvert$	<escape>$\lvert\mathrm{LTA}(m,2)_{\frac{f}{h}} \cdot \frac{f}{h}$</escape>	$\lvert\mathrm{LTA}(m,2)_g \cdot \frac{g}{h}\rvert$	惩罚项	总计
104, 84	$[0,1,2,4],[0,1,3,5]$	$[0,1]$	$[2,4]$	$[3,5]$	2^{2+0+0}	2^{2+0+1}	2^{2+1+2}	2^{-1}	512
100, 88	$[0,1,3,4],[0,1,2,5]$	$[0,1]$	$[3,4]$	$[2,5]$	2^{2+0+0}	2^{2+1+1}	2^{2+0+2}	2^{-2}	256
98, 88	$[0,2,3,4],[0,1,2,5]$	$[0,2]$	$[3,4]$	$[1,5]$	2^{2+0+1}	2^{2+1+1}	2^{2+0+2}	2^{-2}	512
98, 84	$[0,2,3,4],[0,1,3,5]$	$[0,3]$	$[2,4]$	$[1,5]$	2^{2+0+2}	2^{2+1+1}	2^{2+0+2}	2^{-2}	1024
97, 88	$[1,2,3,4],[0,1,2,5]$	$[1,2]$	$[3,4]$	$[0,5]$	2^{2+1+1}	2^{2+1+1}	2^{2+0+2}	2^{-2}	1024
97, 84	$[1,2,3,4],[0,1,3,5]$	$[1,3]$	$[2,4]$	$[0,5]$	2^{2+1+2}	2^{2+1+1}	2^{2+0+2}	2^{-2}	2048

表 I 示例 11 中给出的极化码 (128,64) 枚举示意，其中 $A_{1.5\,\mathrm{w}_{\min}} = |W_{1.5\,\mathrm{w}_{\min}}| = 5376$。

$\mathcal{A}_{m-r}$	m	r	$\mathrm{w}_{\min}$	$A_{\mathrm{w}_{\min}}$	$A_{1.5\,\mathrm{w}_{\min}}$	Ref.
$\{112,104,100,98,97,88,84\}$	7	4	8	688	5376	
$\{112,104,100,98,88\}$	7	4	8	304	768	
$\{112,104\}$	7	4	8	48	0	[14]
$\{120,116,\cdots,23,15\}$	7	3	16	94488	74078592	[29]
$\{1920,1856,\cdots,1680\}$	11	7	16	11648	215040	[30]
$\{1920,1856\}$	11	7	16	384	0	

表 II 示例 12 中讨论的码 (128,64) 和 (2048,1024) 的 $A_{1.5\,\mathrm{w}_{\min}}$ 上码构造（即集合 $\mathcal{A}$）的影响。我们的结果与所提供参考文献中的结果一致。

每个陪集的行索引的二进制表示中的 ind(g) 都应与其他陪集中的行相匹配。

例13. 设我们考察极化码 (128,64) 中的陪集 $\mathcal{C}_{84}$ 和 $\mathcal{C}_{104}$，其中 $m=7$、$r=4$。注意，行 g_{104} 和 g_{84} 分别被视为重量为 $\mathrm{w}_{\min}$ 的码字，且 $\mathrm{ind}(f)\cap\mathrm{ind}(g) = \{0,1\}$。由于条件 (14) 对 $f=104$、$\bar{g}=84$ 成立，因此 $\mathrm{w}(\mathrm{g}_{104}\oplus\mathrm{g}_{84}) = 1.5\,\mathrm{w}_{\min}$。现在，我们将行 $85=(1010101)_2\in\mathcal{K}_{84}$ 加到 g_{84} 中，以在陪集 $\mathcal{C}_{84}$ 中形成另一个重量为 $\mathrm{w}_{\min}$ 的码字。然而，要与 g_{104}, 组合形成重量为 $1.5\,\mathrm{w}_{\min}$ 的码字，我们还必须将行 $105=(1101001)_2\in\mathcal{K}_{104}$ 纳入陪集$\mathcal{C}_{104}$。注意，两个陪集各行在坐标 0、1 处的二进制数字（蓝色高亮）相匹配，因此 $\mathrm{w}((\mathrm{g}_{104}\oplus\mathrm{g}_{105})\oplus(\mathrm{g}_{84}\oplus\mathrm{g}_{85})) = 1.5\mathrm{w}_{\min}$。

因此，由 $\mathcal{C}_{\bar{f}}$中一个和 $\mathcal{C}_{\bar{g}}$中一个组成的每一对重量为 $_{\min}$的码字组合所产生的重量为 $1.5\,\mathrm{w}_{\min}$的码字数量，至多为$A_{1.5\,\mathrm{w}_{\min}}\{\bar{f},\bar{g}\}\le 2^{|\mathcal{K}_{\bar{f}}|}\times 2^{|\mathcal{K}_{\bar{g}}|}\times 2^{-(r-2)}$。此外，当 $\mathcal{K}_{\bar{f}}\cap\mathcal{K}_{\bar{g}}\neq\emptyset$时，我们会得到多个相同的码字，这等同于定义6中的碰撞。

例14。我们取 $f,\bar{g}$为22，$25\in\mathcal{A}_{m-r}$用于极化码(32,16)，其中 $m=5,r=2$。由于 $\mathcal{K}_{\bar{f}}\cap\mathcal{K}_{\bar{g}}=\{26,28\}$，行$\mathrm{g}_{26}$ 和g_{28} 参与了陪集 $\mathcal{C}_{22}$ 和 $\mathcal{C}_{25}$中$\mathrm{w}_{\min}$-重量码字的形成，例如，$\mathcal{C}_{22}$ 中的 $\mathrm{w}(\mathrm{g}_{22}\oplus\mathrm{g}_{26}) = \mathrm{w}_{\min}$ 以及 $\mathcal{C}_{25}$中的$\mathrm{w}(\mathrm{g}_{25}\oplus\mathrm{g}_{26}) = \mathrm{w}_{\min}$。因此，如果将码字$(\mathrm{g}_{22}\oplus\mathrm{g}_{26})\oplus\mathrm{g}_{25}$ 和$\mathrm{g}_{22}\oplus(\mathrm{g}_{25}\oplus\mathrm{g}_{26})$视为不同码字，就会产生重复计数，而它们实际上并不不同。

因此，将存在 $2^{|\mathcal{K}_{\bar{f}}\cap\mathcal{K}_{\bar{g}}|}$ 个冗余码字，并且我们需要通过将它们扣除来避免碰撞

$$A_{1.5\,\mathrm{w}_{\min}}\{\bar{f},\bar{g}\} = 2^{|\mathcal{K}_{\bar{f}}|+|\mathcal{K}_{\bar{g}}|-(r-2)-|\mathcal{K}_{\bar{f}}\cap\mathcal{K}_{\bar{g}}|}. \quad (15)$$

注意到，式 (15) 等价于式 (10) 中的求和项。

示例15。令 $f,\bar{g}$为 $22,25\in\mathcal{A}_{m-r}$，对于极化码 (32,16)，其中 $m=5,r=2$。注意到 $|\mathrm{ind}(\bar{g})\setminus\mathrm{ind}(f)| = |\{0,3,4\}\setminus\{1,2,4\}| = 2$，$\mathcal{K}_{22}=\{23,26,28,30\}$，且 $\mathcal{K}_{25}=\{26,27,28,29\}$。由于 $\mathrm{ind}(g)\cap\mathrm{ind}(f) = \{0,3\}\cap\{1,2\}=\emptyset$，因此我们有 $A_{1.5\,\mathrm{w}_{\min}}\{f,\bar{g}\} = 2^4\times 2^4\times 2^{-2} = 64$。注意，由于对于 $\mathcal{A}_{m-r}$ 中的每一对，我们都有 $r=2$ 和$|\mathrm{ind}(\bar{g})\setminus\mathrm{ind}(f)|=2$，因此条件 $\mathrm{ind}(h)=\mathrm{ind}(g)\cap\mathrm{ind}(f)=\emptyset$始终成立。作为另一个示例，令 $f,\bar{g}$为 104, $84\in\mathcal{A}_{m-r}$，对于极化码 (128,64)，其中 $m=7,r=4$ （参见表 I 的第 1 行）。由于 $|\mathcal{K}_{104}|=5$, $|\mathcal{K}_{84}|=7$，且 $\mathcal{K}_{104}\cap\mathcal{K}_{84}=\{112\}$, 因此$A_{1.5\,\mathrm{w}_{\min}}\{104,84\} = 2^5\times 2^7\times 2^{-2}\times 2^{-1} = 512$。

VII. 结论

本文提出了一个框架，用于刻画重量小于 $2\mathrm{w}_{\min}$ 的递减单项式码码字。具体而言，我们给出了 $1.5\,\mathrm{w}_{\min}$-重量码字计数的闭式表达式。我们还展示了如何通过组合一对 $\mathrm{w}_{\min}$-码字来构造 $1.5\mathrm{w}_{\min}$-重量码字。结果表明，$1.5\mathrm{w}_{\min}$-重量码字的数量仅取决于最高次数单项式。

参考文献

[1] E. Arıkan，《信道极化：一种为对称二元输入无记忆信道构造容量逼近码的方法》，IEEE 信息论汇刊，第55卷第7期，第3051–3073页，2009年7月。[2] 3GPP，《3GPP TSG RAN WG1 #87 v1.0.0最终报告》，技术报告，2016年11月，美国里诺。[在线]。可访问：http://www.3gpp. org / ftp /tsg % 20ran / WG1 % 20RL1 / TSGR1 % 2087 / Report / Final % 20Minutes%20report%20RAN1%5C%2387% 20v100.zip。[3] S. Lin 和 D. J. Costello，《差错控制编码》，第2版，Pearson，上萨德尔里弗：Prentice Hall，2004年，第395–400页。[4] M. Bardet、J. Chaulet、V. Dragoi、A. Otmani 和 J.-P. Tillich，《基于极化码的 McEliece 公钥密码体制的密码分析》，载于《后量子密码学》，第9606卷，2016年，第118–143页。[5] M. Bardet、V. Dragoi、A. Otmani 和 J.-P. Tillich，《基于新多项式形式体系的极化码代数性质》，载于2016年 IEEE 国际信息论研讨会（ISIT），2016年，第230–234页。[6] M. Mondelli、S. H. Hassani 和 R. L. Urbanke，《次线性复杂度的极化码构造》，IEEE 信息论汇刊，第65卷第5期，第2782–2791页，2019年。

[7] Y. Li、H. Zhang、R. Li、J. Wang、W. Tong、G. Yan 和 Z. Ma，《极化码的完整仿射自同构群》，载于2021年 IEEE 全球通信大会（GLOBECOM），2021年，第01–06页。[8] M. Geiselhart、A. Elkelesh、M. Ebada、S. Cammerer 和 S. t Brink，《Reed-Muller码的自同构集成译码》，IEEE 通信汇刊，第69卷第10期，第6424–6438页，2021年10月。[9] M. Geiselhart、A. Elkelesh、M. Ebada、S. Cammerer 和 S. ten Brink，《论极化码的自同构群》，2021年 IEEE 国际信息论研讨会（ISIT），2021年7月，第1230–1235页。[10] C. Pillet、V. Bioglio 和 I. Land，《用于自同构集成译码的极化码》，IEEE 信息论研讨会（ITW），第2021卷，第1–6页，2021年10月。[11] ——，《用于极化码译码的自同构分类》，载于 ICC 2022——IEEE 国际通信大会，2022年5月，第110–115页。[12] K. Ivanov 和 R. L. Urbanke，《对称码的极化类译码效率》，IEEE 通信汇刊，第70卷第1期，第163–170页，2022年1月。[13] K. Ivanov 和 R. Urbanke，《极化码并无大量仿射自同构》，载于2022年 IEEE 国际信息论研讨会（ISIT），2022年6月，第2374–2378页。[14] H. Yao、A. Fazeli 和 A. Vardy，《计算极化码重量分布的确定性算法》，arXiv 预印本，2020年。arXiv：2102.07362v1。[15] T. Kasami 和 N. Tokura，《论 Reed-Muller码的重量结构》，信息论汇刊，第16卷第6期，第752–759页，1970年11月。[16] T. Kasami、N. Tokura 和 S. Azumi，《论 Reed-Muller码中小于2.5d的重量的重量枚举》，《信息与控制》，第30卷第4期，第380–395页，1976年。[17] Z. Liu、K. Chen、K. Niu 和 Z. He，《极化码的距离谱分析》，载于 IEEE 无线通信与网络会议（WCNC），第2014卷，第490–495页，2014年。[18] M. Valipour 和 S. Yousefi，《论极化码的概率重量分布》，IEEE 通信快报，第17卷，2123，2013 11，2120 no. pp. –。[19] Q. Zhang、A. Liu 和 X. Pan，《一种改进的极化码重量分布概率计算方法》，IEEE 通信快报，第21卷第12期，第2562–2565页，2017年。[20] M. P. C. Fossorier 和 S. Lin，《用于最近陪集译码的——u—u+v—构造码的重量分布》，载于 IEEE 信息论汇刊，第43卷第3期，第1028–1030页，1997年5月。[21] R. Polyanskaya、M. Davletshin 和 N. Polyanskii，《极化码连续消除译码的重量分布》，IEEE 通信汇刊，第68卷第12期，第7328–7336页，2020年12月。[22] V. F. Dragoi，《一种解决密码学和编码理论中算法问题的代数方法》，博士论文，Normandie Universit´é，2017年。[23] C. Sch¨urch，《极化码合成信道的偏序》，载于2016年 IEEE 国际信息论研讨会（ISIT），巴塞罗那，2016年，第220–224页。[24] M. Rowshan、S. H. Dau 和 E. Viterbo，《错误系数降低的 Polar/PAC 码》，预印本，2021年。arXiv：2111.088435。[25] N. J. Sloane 和 E. R. Berlekamp，《二阶 Reed-Muller码的重量枚举式》，IEEE 信息论汇刊，第 16， 6， 745 751, no. pp. – T. Tao 和 V. H. Vu，《加法[26]组合学》，第1版。剑桥 pp. 112-178：剑桥大学出版社，2006年。[27] [在线]。可访问：https://github.com/mohammad-rowshan/closed-form-weight-enumeration-of-polar-codes。[28] H. Vangala、E. Viterbo 和 Y. Hong，《AWGN 信道极化码构造的比较研究》，2015年。arXiv：1501 . 02473。[29] M. Sugino、Y. Ienaga、N. Tokura 和 T. Kasami，《（ 128，64 ） Reed-Muller 码的重量分布（通信）》，IEEE 信息论汇刊，第17卷第5期，第627–628页，1971年9月。[30] B. Li、H. Shen 和 D. Tse，《一种适用于带循环冗余校验极化码的自适应连续消除列表译码器》，IEEE 通信快报，第16卷第12期，第2044–2047页，2012年。[31] M. Rowshan、S. Hoang Dau 和 E. Viterbo，《降低极化码的错误系数数》，载于2022年 IEEE 信息论研讨会（ITW），2022年，第249–254页。DOI：10.1109/ITW54588.2022. 9965852。[32] M. Rowshan 和 J. Yuan，“PAC 码的最小重量码字快速枚举”，2022年，第255–260页。DOI：10 . 1109 / ITW54588.2022.9965901。

附录 A
用于枚举重量为 $w_{\min}$ 和 $1.5w_{\min}$ 的码字的 MATLAB 脚本

以下清单展示了 MATLAB™函数 weight enum，用于枚举前两个最小重量码字。所需输入为非冻结比特的坐标集合 $\mathcal{A}$，以及 $n = \log_2(N)$，其中 N为码长。值得注意的是，集合 $\mathcal{A}$中的元素必须按升序排列。这一点至关重要，因为确定 $\alpha_{\frac{f}{h},\ \frac{g}{h}}$的条件取决于 f和 g的顺序，详见定理10。函数首先从集合 $\mathcal{A}$中提取最高次数单项式，并将其存储在集合 $\mathcal{A}_{m-r}$中（第2行和第3行）。接下来，在两个嵌套的 for 循环中，函数找出集合 $\mathcal{A}_{m-r}$中的所有不同单项式对，分别命名为 f和 g，其最大公约数（GCD）的次数为 $r-2$。利用 (6)、(10) 以及表示 (5) 的 lambda 函数，计算并返回 $w \in \{w_{\min}$ 和 $1.5\ w_{\min}\}$ 对应的 A_w。

```
函数 [w,A_w] = 重量_enum(A,n) r = max(sum(~(dec2bin(A)-'0'),2)); Amr =A(find(sum(~(dec2bin(sort(A))-'0'),2)==r)) Amr_sub = Amr; w=zeros(1,2); A_w=zeros(1,2); ... w(1)=2^(n-r); w(2)=1.5*w(1); 对于 i = Amr f = find(~(reverse(dec2bin(i,n))-'0')); A_w(1) = A_w(1) + 2^(r+lambda(f,f)); Amr_sub(Amr_sub==i) = []; 对于 j = Amr_sub g =find(~(reverse(dec2bin(j,n))-'0')); h =intersect(f,g); 如果 length(h)==r-2 foh = setdiff(f,h); goh = ... setdiff(g,h); alpha = 1*(foh(2)>goh(2) & ... goh(2)>foh(1)) + ...1*(goh(1)>foh(1)); A_w(2) = A_w(2) + 2^(r+2 +... lambda(h,h) +lambda(f,foh) ...+ lambda(g,goh) - alpha); 结束 结束 结束 结束 函数轨道 = lambda(f,g) 轨道 = 0; 对于 i = g 轨道 = 轨道 +length(setdiff([1:i-1],f)); 结束 结束
```

附录B 引理2的证明

证明：考虑一个元素 $P \in \mathrm{LTA}(m, 2)^{h} \cdot h \cdot \left(m2^{f \cdot \frac{f}{h}} + m2^{g \cdot \frac{g}{h}}\right)$. LTA(,) LTA(,) 根据 LTA( ) 和 LTA(,) 的定义，我们有 $P \in m2^{\cdot h \cdot} \left(m2^{\cdot \frac{f}{h}} + m2^{\cdot \frac{g}{h}}\right)$. LTA(,) LTA(,) LTA(,) 反过来，选取一个元-

元素 $P \in \mathrm{LTA}(m,2)\cdot h\cdot\left(\mathrm{LTA}(m,2)\cdot\frac{f}{h}+\mathrm{LTA}(m,2)\cdot\frac{g}{h}\right)$。因此我们有

$$
\begin{aligned}
P=&\prod_{i\in\mathrm{ind}(h)}(x_i+\sum_{j<i,j\notin\mathrm{ind}(h)}b_{i,j}x_j+\varepsilon_i)\times\\
&\prod_{i\in\mathrm{ind}(\frac{f}{h})}(x_i+\sum_{j<i,j\notin\mathrm{ind}(\frac{f}{h})}b_{i,j}x_j+\varepsilon_i)\\
&+\prod_{i\in\mathrm{ind}(h)}(x_i+\sum_{j<i,j\notin\mathrm{ind}(h)}b_{i,j}x_j+\varepsilon_i)\times\\
&\prod_{i\in\mathrm{ind}(\frac{g}{h})}(x_i+\sum_{j<i,j\notin\mathrm{ind}(\frac{g}{h})}b_{i,j}x_j+\varepsilon_i)
\end{aligned}
$$

$$
\begin{aligned}
P=&\prod_{i\in\mathrm{ind}(h)}(x_i+\sum_{j<i,j\notin\mathrm{ind}(h)}b_{i,j}x_j+\varepsilon_i)\times\\
&\prod_{i\in\mathrm{ind}(\frac{f}{h})}(x_i+\sum_{j<i,j\notin\mathrm{ind}(f)}b^*_{i,j}x_j+\varepsilon^*_i)\\
&+\prod_{i\in\mathrm{ind}(h)}(x_i+\sum_{j<i,j\notin\mathrm{ind}(h)}b_{i,j}x_j+\varepsilon_i)\times\\
&\prod_{i\in\mathrm{ind}(\frac{g}{h})}(x_i+\sum_{j<i,j\notin\mathrm{ind}(g)}b^*_{i,j}x_j+\varepsilon^*_i)
\end{aligned}
$$

其中 $b^*_{i,\ j}$ 按照命题 3.7.3 的证明中所述由 [22] 得到（见引理 1）。 ■

附录 C 定理 3 的证明

证明：根据定理 2，任何满足 $\mathrm{w}(\mathrm{ev}(P)) = 1.5\,\mathrm{w}_{\min}$ 的码字 $\mathrm{ev}(P)$，在仿射变换 $P = y_1\dots y_{r-2}(y_{r-1}y_r + y_{r+1}y_{r+2})$ 下均可得到。

直接推论由 LTA(m,2) 的定义和定理 2 得出。

对于逆向蕴含，考虑一个码字 $\mathrm{ev}(P)$，其中 $P = y_1\dots y_{r-2}(y_{r-1}y_r + \cdots + y_{r+2\mu-3}y_{r+2\mu-2})$。$[y_1\dots y_{r-2}y_{r-1}y_r]$、…、$[y_1\dots y_{r-2}y_{r+2\mu-3}y_{r+2\mu-2}]$ 中的最大变量均互不相同（见引理 1）。因此，我们可以构造 $h = x_{i_1}\dots x_{i_{r-2}}$ 和 $f/h = x_{i_{r-1}}x_{i_r}$、…、$g/h = x_{i_{r+1}}x_{i_{r+2}}$。注意，虽然 i_1、$\dots i_{r-2}$ 两两互不相同，但指标 i_{r-1}、i_r、i_{r+2} 不一定两两互不相同。下面证明存在一个仿射变换，使得这些指标也两两互不相同。假设 f/h 和 g/h 至少共享一个最大变量。形式上，我们可以将 $P_1 \in \mathrm{LTA}(m,2)_f \cdot f/h$ 写为 $P_1 = (x_{i_1} + v_{i_1})(x_{i_2} + v_{i_2})$，将 $P_2 \in \mathrm{LTA}(m,2)_g \cdot g/h$ 写为 $P_2 = (x_{j_1} + z_{j_1})(x_{j_2} + z_{j_2})$，其中 v_{i_1}、v_{i_2}、z_{j_1}、z_{j_2} 均为线性函数，其最大变量严格小于对应指标，并且至少存在一个指标 i_l 等于某个指标 j_l.。此外，我们有 $i_1 < i_2$ 和 $j_1 < j_2$.。于是，我们得到以下几种情况。

- $i_1 = j_1$ 和 $i_2 > j_2$. 然后

$$
\begin{aligned}
P_1+P_2&=(x_{i_1}+v_{i_1})(x_{i_2}+v_{i_2})+(x_{i_1}+z_{i_1})(x_{j_2}+z_{j_2})\\
&=(x_{i_1}+v_{i_1})(x_{i_2}+v_{i_2}+x_{j_2}+z_{j_2})\\
&\quad+(x_{j_2}+z_{j_2})(v_{i_1}+z_{i_1})\\
&\in \mathrm{LTA}(m,2)_f\cdot f/h+\mathrm{LTA}(m,2)_{g^*}\cdot g^*/h,
\end{aligned}
$$

其中 $g^*/h = x_{j_1^*}x_{j_2}$，其中 $j_1^* = \max\{l \mid x_l \in v_{i_1} + z_{i_1}\}$.。由于 $j_1^* < i_1$，这意味着四个指标 i_1、i_2、j_1^*、j_2 两两不同。此外，j_1^* 存在，因为 $v_{i_1} \neq z_{i_1}$ 且 $v_{i_1} \neq 1 + z_{i_1}$。若 $v_{i_1} = z_{i_1}$，则 $P_1 + P_2$ 是两个线性形式的乘积，因此 $\mathrm{ev}(P)$ 是一个最小重量码字，这与我们的假设矛盾。若 $v_{i_1} = 1+z_{i_1}$，则 P_1+P_2 的重量将是 P_1 重量的 2 倍，这意味着 P 的重量严格大于 $1.5\,\mathrm{w}_{\min}$，与假设矛盾。

- $i_1 = j_2$. Then

$$
\begin{aligned}
P_1+P_2&=(x_{i_1}+v_{i_1})(x_{i_2}+v_{i_2})+(x_{j_1}+z_{j_1})(x_{i_1}+z_{i_1})\\
&=(x_{i_1}+v_{i_1})(x_{i_2}+v_{i_2}+x_{j_1}+z_{j_1})\\
&\quad+(x_{j_1}+z_{j_1})(v_{i_1}+z_{i_1})\\
&\in \mathrm{LTA}(m,2)_f\cdot f/h+\mathrm{LTA}(m,2)_{g^*}\cdot g^*/h,
\end{aligned}
$$

其中 $g^*/h = x_{j_1}x_{j_2^*}$，$j_2^* = \max\{l \mid x_l \in v_{i_1} + z_{i_1}\}$。这里，我们可能有 $j_2^* = j_1$，但在这种情况下，由于 $(x_{j_1} + z_{j_1})(v_{i_1} + z_{i_1})$ 是线性形式的乘积，根据引理 1，可以将其改写为最大变量互不相同的形式，这一事实便完成了此情形的证明。此外，与前一种情况一样，j_2^* 存在。

- $i_1 = j_1$，且 $i_2 = j_2$.。于是

$$P_1 + P_2 = (x_{i_1} + v_{i_1})(x_{i_2} + v_{i_2}) + (x_{i_1} + z_{i_1})(x_{i_2} + z_{i_2})$$

由于 $v_{i_1} \neq z_{i_1}$（或者等价地说，$\mathrm{ev}(P)$ 不是一个最小重量码字），且 $v_{i_2} \neq z_{i_2}$，我们有

$$P_1 + P_2 = (x_{i_2} + z_{i_2})(z_{i_1} + v_{i_1}) + (z_{i_2} + v_{i_2})(x_{i_1} + v_{i_1}).$$

和式中的两项分别具有最大变量 $x_{i_2}x_{j_1^*}$ 和 $x_{j_2^*}x_{i_1}$，其中 $j_1^* = \max\{l \mid x_l \in v_{i_1} + z_{i_1}\}$，且 $j_2^* = \max\{l \mid x_l \in v_{i_2} + z_{i_2}\}$.。如果这四个指标两两不同，证明便完成了。否则，请参见前面的条目。

■

附录D 命题1的证明

令 $f = x_{i_1}x_{i_2}$ 和 $g = x_{j_1}x_{j_2}$，其中最大公约数 $(f,g) = 1$ 且 $i_2 > j_2$，并且 $P = (\mathrm{B}\ \varepsilon)\cdot f, P = (\mathrm{B}^*, \varepsilon^*)\cdot f, Q = (\mathrm{A}\ \gamma)\cdot$

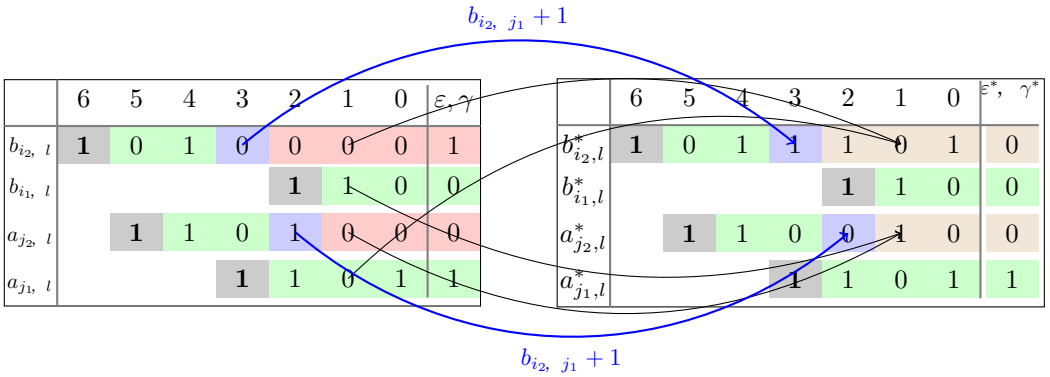

图1 命题1在 $i_2 > j_2 > j_1 > i_1$ 且有 $f = x_6x_2$、$g = x_5x_3$. 的情况下的应用。对于 $P = (x_6 + x_4 + 1)(x_2 + x_1) \in \text{LTA}(m, 2) \cdot f$ 以及 $Q = (x_5 + x_4 + x_2)(x_3 + x_2 + x_0 + 1) \in \text{LTA}(m, 2)$，我们可以构造一个非平凡的不同对 P^*、Q^*，其中 $P^* = (x_6 + x_4 + x_3 + x_2 + x_0)(x_2 + x_1)$ 和 $Q^* = (x_5 + x_4 + x_1)(x_3 + x_2 + x_0 + 1)$。颜色的含义如下：灰色单元格表示支撑集中的变量索引，绿色单元格表示 $b^*_{i,\ j} = b_{i,\ j}$ 或 $a^*_{i,\ j} = a_{i,\ j}$，蓝色单元格表示 $b^*_{i,\ j} = 1 + b_{i,\ j}$ 或 $a^*_{i,\ j} = 1 + a_{i,\ j}$，棕色单元格由红色单元格及其对应的绿色单元格组合得到；也就是说，$b^*_{i_2,\ l} = b_{i_2,\ l} + a_{j_1,\ l}$ 以及 $a^*_{j_2,\ l} = a_{j_2,\ l} + b_{i_1,\ l}$。

$g, Q^* = (\mathrm{A}^*, \gamma^*) \cdot g$. 根据 LTA$(m, 2)$ 的定义以及碰撞的定义，我们有

$$\begin{aligned}
&(x_{i_2} + \sum_{l<i_2, l\neq i_1} b_{i_2,l}x_l + \varepsilon_{i_2})(x_{i_1} + \sum_{l<i_1} b_{i_1,l}x_l + \varepsilon_{i_1}) \\
&- (x_{i_2} + \sum_{l<i_2, l\neq i_1} b^*_{i_2,l}x_l + \varepsilon^*_{i_2})(x_{i_1} + \sum_{l<i_1} b^*_{i_1,l}x_l + \varepsilon^*_{i_1}) \\
&= (x_{j_2} + \sum_{l<j_2, l\neq j_1} a_{j_2,l}x_l + \gamma_{j_2})(x_{j_1} + \sum_{l<j_1} a_{j_1,l}x_l + \gamma_{j_1}) \\
&- (x_{j_2} + \sum_{l<j_2, l\neq j_1} a^*_{j_2,l}x_l + \gamma^*_{j_2})(x_{j_1} + \sum_{l<j_1} a^*_{j_1,l}x_l + \gamma^*_{j_1})
\end{aligned} \tag{16}$$

由于 x_{i_2} 是最大变量，提取 x_{i_2} 的系数可得

$$x_{i_1} + \sum_{l<i_1} b_{i_1,l}x_l + \varepsilon_{i_1} = x_{i_1} + \sum_{l<i_1} b^*_{i_1,l}x_l + \varepsilon^*_{i_1}.$$

这意味着

$$\begin{aligned}
&(\sum_{l<i_2, l\neq i_1} (b_{i_2,l} - b^*_{i_2,l})x_l + \varepsilon_{i_2} - \varepsilon^*_{i_2})(x_{i_1} + \sum_{l<i_1} b_{i_1,l}x_l + \varepsilon_{i_1}) \\
&= Q - Q^*.
\end{aligned} \tag{17}$$

若我们处于 $i_2 > i_1 > j_2$. 的情形，那么 x_l 要么是最大变量（在第一项的第一个因子中），要么 x_{i_1} 是最大变量（在第一项的第二个因子中）。无论哪种情况，我们都可推得 $Q - Q^* = 0$，这意味着 $\mathrm{A} = \mathrm{A}^*$，且进一步不存在可能的碰撞。因此，在这种情况下，闵可夫斯基和 LTA$(m, 2) \cdot f +$ LTA$(m, 2) \cdot g$ 具有最大基数。

如果属于 $i_2 > j_2 > i_1$. 这种情况 $i_2 > j_2 > i_1$.，并且我们认为下一个最大变量是 x_l（出现在第一项中），则有 $j_2 < l < i_2$ 我们得到 $b_{i_2,l} = b^*_{i_2,l}$，对所有此类指标均成立。这意味着我们有

$$\begin{aligned}
&(\sum_{l\leq j_2, l\neq i_1} (b_{i_2,l} - b^*_{i_2,l})x_l + \varepsilon_{i_2} - \varepsilon^*_{i_2})(x_{i_1} + \sum_{l<i_1} b_{i_1,l}x_l + \varepsilon_{i_1}) \\
&= Q - Q^*.
\end{aligned} \tag{18}$$

如果下一个最大变量是 x_{j_2}，则有两种情况，$b_{i_2,\ j_2} - b^*_{i_2,j_2} = 0$ 以及 $b_{i_2,j_2} - b^*_{i_2,j_2} = 1$.

A）情形 $b_{i_2,\ j_2} - b^*_{i_2,\ j_2} = 0$。最后一个方程变为

$$\begin{aligned}
&(\sum_{l<j_2, l\neq i_1} (b_{i_2,l} - b^*_{i_2,l})x_l + \varepsilon_{i_2} - \varepsilon^*_{i_2})(x_{i_1} + \sum_{l<i_1} b_{i_1,l}x_l + \varepsilon_{i_1}) \\
&= Q - Q^*.
\end{aligned} \tag{19}$$

提取 x_{j_2} 的系数可得

$$x_{j_1} + \sum_{l<j_1} a_{j_1,l}x_l + \gamma_{j_1} = x_{j_1} + \sum_{l<j_1} a^*_{j_1,l}x_l + \gamma^*_{j_1}.$$

这意味着

$$\begin{aligned}
&(\sum_{l<j_2, l\neq i_1} (b_{i_2,l} - b^*_{i_2,l})x_l + \varepsilon_{i_2} - \varepsilon^*_{i_2})(x_{i_1} + \sum_{l<i_1} b_{i_1,l}x_l + \varepsilon_{i_1}) \\
&= (\sum_{l<j_2, l\neq j_1} (a_{j_2,l} - a^*_{j_2,l})x_l + \gamma_{j_2} - \gamma^*_{j_2})(x_{j_1} + \sum_{l<j_1} a_{j_1,l}x_l + \gamma_{j_1}).
\end{aligned} \tag{20}$$

为了使方程（20）成立，我们需要

- $b_{i_2,\ l} = b^*_{i_2,\ l}$ 对于 $j_1 < l < j_2$
- $a_{j_2,\ l} = a^*_{j_2,\ l}$ 对于 $i_1 < l < j_2$
- $b_{i_2,j_1} - b^*_{i_2,j_1} = 1$
- $a_{j_2,i_1} - a^*_{j_2,i_1} = 1$
- $b_{i_2,\ l} - b^*_{i_2,\ l} = a_{j_1,\ l}$ 对于 $l < j_1$
- $a_{j_2,\ l} - a^*_{j_2,\ l} = b_{i_1,\ l}$ 对于 $l < i_1$
- $\varepsilon_{i_2} - \varepsilon^*_{i_2} = \gamma_{j_1}$
- $\gamma_{j_2} - \gamma^*_{j_2} = \varepsilon_{i_1}$

由于这些已涵盖所有可能的系数，因此本情况到此结束。

B）情形 $b_{i_2,j_2} - b^*_{i_2,j_2} = 1$。我们有

$$(x_{j_2}+\sum_{l<j_2,l\neq i_1}(b_{i_2,l}-b^*_{i_2,l})x_l+\varepsilon_{i_2}-\varepsilon^*_{i_2})(x_{i_1}+\sum_{l<i_1}b_{i_1,l}x_l+\varepsilon_{i_1}) = Q - Q^*. \quad (21)$$

提取 x_{j_2} 的系数可得

$$x_{i_1}+\sum_{l<i_1}b_{i_1,l}x_l+\varepsilon_{i_1} = \sum_{l<j_1}(a_{j_1,l}-a^*_{j_1,l})x_l+\gamma_{j_1}-\gamma^*_{j_1}.$$

该方程成立的条件只有 $i_1 < j_1$. 。若此条件成立，则可推得

$$\begin{aligned} a_{j_1,l} - a^*_{j1,l} &= 0,\ for\ i_1 < l < j_1 \\ a_{j_1,i_1} - a^*_{j1,i_1} &= 1, \\ a_{j_1,l} - a^*_{j1,l} &= b_{i_1,l},\ for\ l < i_1 \\ \gamma_{j_1} - \gamma^*_{j_1} &= \varepsilon_{i_1}. \end{aligned}$$

此外，我们还可推得

$$\begin{aligned} &(x_{j_2}+\sum_{l<j_2,l\neq i_1}(b_{i_2,l}-b^*_{i_2,l})x_l+\varepsilon_{i_2}-\varepsilon^*_{i_2})(x_{i_1}+\sum_{l<i_1}b_{i_1,l}x_l+\varepsilon_{i_1}) \\ &= (x_{j_2}+\sum_{l<j_2,l\neq j_1}a_{j_2,l}x_l+\gamma_{j_2})(x_{j_1}+\sum_{l\leq i_1}a_{j_1,l}x_l+\gamma_{j_1}) \\ &-(x_{j_2}+\sum_{l<j_2,l\neq j_1}a^*_{j_2,l}x_l+\gamma_{j_2})(x_{j_1}+\sum_{l\leq i_1}a_{j_1,l}x_l+\gamma_{j_1}) \\ &-(x_{j_2}+\sum_{l<j_2,l\neq j_1}a^*_{j_2,l}x_l+\gamma_{j_2})(x_{i_1}+\sum_{l<i_1}b_{i_1,l}x_l+\varepsilon_{i_1}) \end{aligned} \quad (22)$$

由此可得

$$\begin{aligned} &(\sum_{l<j_2,l\neq i_1}(b_{i_2,l}-b^*_{i_2,l})x_l+\varepsilon_{i_2}-\varepsilon^*_{i_2}-\sum_{l<j_2,l\neq j_1}a^*_{j_2,l}x_l-\gamma_{j_2}) \\ &\qquad\times(x_{i_1}+\sum_{l<i_1}b_{i_1,l}x_l+\varepsilon_{i_1}) \\ &=(\sum_{l<j_2,l\neq j_1}(a_{j_2,l}-a^*_{j_2,l})x_l+\gamma_{j_2}-\gamma^*_{j_2})(x_{j_1}+\sum_{l\leq i_1}a_{j_1,l}x_l+\gamma_{j_1}) \end{aligned} \quad (23)$$

注意，在前一个方程中，不能有 x_l ，且 $l > j_1$ 为最大变量；也就是说，我们需要有$a_{j_2,\ l} = a^*_{j_2,\ l}$ ，其中 $l > i_1$ ；并且$b_{i_2,\ l} - b^*_{i_2,\ l} - a^*_{j_2,\ l} = 0$ ，其中 $l > j_1$. 。与前一种情况一样，我们可以确定一组使方程 (23) 成立的条件。

- $b_{i_2,j_1} - b^*_{i_2,j_1} = 1$
- $a_{j_2,i_1} - a^*_{j_2,i_1} = 1$
- $b_{i_2,l} - b^*_{i_2,l} = a_{j_1,l} - a^*_{j_2,l}$ for $l < j_1$
- $a_{j_2,l} - a^*_{j_2,l} = b_{i_1,l}$ for $l < i_1$
- $\varepsilon_{i_2} - \varepsilon^*_{i_2} = \gamma_{j_1} - \gamma_{j_2}$
- $\gamma_{j_2} - \gamma^*_{j_2} = \varepsilon_{i_1}$

由于所有可能的系数都已出现，此情况到此结束。

继续讨论这些情形：当 $i_2 > i_1 > j_2$ 没有碰撞时，当 $i_2 > j_2 > j_1 > i_2$ 我们有两个限制条件时，以及当 $i_2 > j_2 > i_1 > j_1$ 我们只有一个限制条件时。每个限制条件都是关于两个自由变量（$b_{i_2,\ j_2}$、 $b^*_{i_2,\ j_2}$）的方程 $\mathbb{F}_2$，因此，每个限制条件产生 2 个可能的解，由此我们可以得到所需的结果。换句话说，变量$b_{i_2,\ j_2}$ 是 B 中的一个自由变量，使我们能够计算每个元素对应的不变量数量。

附录 E 引理 3 的证明

反设存在多项式$H, H^* \in \text{LTA}(m, 2)_h \cdot h$和 P, $P^* \in \text{LTA}(m, 2)_f \cdot \frac{f}{h} + \text{LTA}(m, 2)_g \cdot \frac{g}{h}$，满足 $H \neq H^*$和 $P \neq P^*$，使得 $HP = H^*P^*$。由于 h 是由 P 和 P^* 中均未出现的变量构成的乘积，从 HP和 H^*P^* 中提取 h 的系数可得$P = P^*$. 。但这与我们的假设矛盾，证明完毕。

附录 F 命题 2 的证明

证明：反设两个集合之间存在公共多项式 P 。由于 P 属于 $\text{LTA}(m, 2)_h \cdot h \cdot (\text{LTA}(m, 2)_f \cdot \frac{f}{h} + \text{LTA}(m, 2)_g \cdot \frac{g}{h})$，这意味着 P 中的最大单项式为 $f + g$ （根据 $\text{LTA}(m, 2)$ 的定义）。又由于 P属于 $\text{LTA}(m, 2)^*_h \cdot h^* \cdot (\text{LTA}(m, 2)_{f^*} \cdot \frac{f^*}{h^*} + \text{LTA}(m, 2)_{g^*} \cdot \frac{g^*}{h^*})$，这意味着 P中的最大单项式为 $f^* + g^*$。因此， $f + g = f^* + g^*$. 。两个和不可能都等于零，因为 $f \neq g$ 且 $f^* \neq g^*$. 。因此，我们必须有 $(f, g) = (f^*, g^*)$ 或 $(f, g) = (g^*, f^*)$，证明完毕。 ■

附录 G 定理 4 的证明

证明：首先， $W_{1.5\,\mathrm{w_{min}}}$ 的基数可以计算为对所有满足 $\deg(h) = r - 2$ 且 $f = hx_{i_1}x_{i_2}$ 的可能 h，求和 $|\text{LTA}(m, 2)_h \cdot h| \times |(\text{LTA}(m, 2)_f \cdot x_{i_1}x_{i_2} + \text{LTA}(m, 2)_g \cdot x_{j_1}x_{j_2})|$。其次，回顾 $|\text{LTA}(m, 2)_h \cdot g| = 2^{\deg(g)+|\lambda_h\ (g)|}$以及$|\text{LTA}(m, 2)_h \cdot h| = 2^{\deg(h)+|\lambda_h|}$。结合命题 1 可得 $|(\text{LTA}(m, 2)_f \cdot x_{i_1}x_{i_2} + m\ 2\ _g \cdot x_{j_1}x_{j_2}| = |m\ 2\ _f \cdot x_{i_1}x_{i_2}| \times |m\ 2\ _g \cdot x_{j_1}x_{j_2}| \times 2^{\alpha \frac{f}{h} \frac{g}{h}}$

$\text{LTA}(,))\ (\text{LTA}(,)\,\text{LTA}(,))$。因此，每个轨道的基数为 $2^{r-2+|\lambda_h|} \times 2^{2+|\lambda_f\ (\frac{f}{h})|+2+|\lambda_g\ (\frac{g}{h})|-\alpha \frac{f}{h},\ \frac{g}{h}}$，证毕。 ■