arXiv:2305.03493v1 [math.GT] 4 May 2023

RM(4, 8) 的覆盖半径

VAL´ERIE GILLOT 和 PHILIPPE LANGEVIN

Abstract. 我们提出一种有效的导数提升方法。导数提升是一种不变量，可用于给出 B(5, 6, 8) $= RM$(6, 8)/RM(4, 8) 的分类。其主要结论是证明 Reed-Muller RM(4, 8) 的覆盖半径等于 26。.

1. Boolean functions and classification

设 $\mathbb{F}_2$ 为阶为 2 的有限域。设 m 为正整数。我们用 $B(m)$ 表示布尔函数 f: $\mathbb{F}_2^m \to \mathbb{F}_2$ 的集合。 f 的汉明重量记为 wt (f)。每个布尔函数都有唯一的代数约化表示:

$$f(x_1, x_2, \dots, x_m) = f(x) = \sum_{S \subseteq \{1,2,\dots,m\}} a_S X_S, \quad a_S \in \mathbb{F}_2,\ X_S(x) = \prod_{s \in S} x_s.$$

f 的次数是代数形式中具有 S 且满足 $a_S = 1$ 的最大基数。 $f \neq 0$的赋值记作 val(f)，是满足 $a_S = 1$的S的最小基数。通常，val(0)为 ∞。我们用 $B(s, t, m)$表示赋值大于或等于 s 且次数小于或等于 t的布尔函数空间。注意，当 $s > t$时， $B(s, t, m) = \{0\}$。仿射一般线性群 AGL(m, 2)自然地从右侧作用于布尔函数。 $\mathfrak{s} \in$ AGL(m, 2)对布尔函数 f 的作用是 $f \circ \mathfrak{s}$，即应用的复合。模去次数小于 s的函数空间后，该群也作用于 $B(s, t, m)$。 $B(s, t, m)$的分类是~我们方法的先决条件。我们用 $B(s, t, m)$表示 $B(s, t, m)$的一个分类，即轨道代表元的集合。 $B(s, t, m)$的类数记作 n(s, t, m)。

2. Covering radius of Reed-Muller codes

一个 m 元 k 阶 Reed-Muller码的长度为 2^m，维数为$\sum_{i=0}^{k} \binom{m}{i}$，最小距离为 2^{m-k}。这些码字对应于在 $\mathbb{F}_2^m$上对次数小于或等于 k的布尔函数进行求值，我们将该码视为以下空间:

$$RM(k, m) = \{f \in B(m) \mid \deg(f) \leq k\}.$$

$\rho(k, m)$的覆盖半径是 $RM(k, m)$的 $\rho(k, m) = \max_{f \in B(m)} \mathrm{NL}_k(f)$，其中$\mathrm{NL}_k(f) = \min_{g \in RM(k,m)}$ wt $(f + g)$是 $f \in B(m)$的 k 阶非线性度。Reed-Muller码的经典参数（长度、维数和最小距离）很容易确定，并且它们都以 AGL(m, 2)作为自同构群。Reed-Muller码覆盖半径的经典结果见 [8, 第 800]页。我们来回顾一下这个简单但至关重要的引理:

Date: 2023年4月。本研究部分得到法国国家研究署（Agence Nationale de la Recherche）通过 SWAP 项目提供的资助，合同编号为 ANR-21-CE39-0012。

引理 1。

(i) $2\rho(k,m-1) \le \rho(k,m)$ (ii) $\rho(k-1, m-1) \le \rho(k,m)$ (iii) $\rho(k,m) \le \rho(k,m-1) + \rho(k-1,m-1)$

然而，大多数覆盖半径仍然未知。近期的结果是在 [4, 9] 情况下 $m = 7$获得的。因此，对于 $m \le 7$，所有覆盖半径均已知。对于 $m = 8$，大多数覆盖半径仍然未知。表 1 是表 [8,p. 802] 的更新版，其中包含对应于情况 $m = 7$、8 的最新结果。

TABLE 1. 编码理论手册的更新表格。

k	1	2	3	4	5	6	7	8
$\rho(k,8)$	120	$88^a - 96$	$50^b - 67^f$	$\mathbf{26}^c$	10	2	1	0
$\rho(k,7)$	56	40^d	20^e	8	2	1	0	

(a) 可以验证，$abd + bcf + bef + def + acg + deg + cdh + aeh + afh + bfh + efh + bgh + dgh$的二阶非线性度为 88；(b) 下界是由 $B(4,4,8)$ 的分类得出的推论，见 [3]；(c) 作为 [2] 中所得下界的推论，在本文中得出；(d) 参见 [9, 定理 11] 中的结果；(e) 参见 [4, 定理 1] 中的结果；(f) 是引理 1-(iii) 的推论。

我们还考虑 $RM(k,m)$ 到 $RM(t,m)$ 的相对覆盖半径 $\rho_t(k,m)$，

$$\rho_t(k,m) = \max_{f \in RM(t,m)} \mathrm{NL}_k(f) = \max_{f \in B(k+1,t,m)} \mathrm{NL}_k(f) \tag{1}$$

在论文 [2], 中，作者介绍了计算 $B(m)$ 中次数为 $m-3$ 的布尔函数到 Reed-Muller 空间 $RM(m-4,m)$ 的距离的方法。确定相对覆盖半径 $\rho_{m-3}(m-4, m)$ 很有用。尤其是，他们的结果 $\rho_5(4,8) = 26$ 是我们研究目的的一项里程碑：计算 $\rho(4,8)$。有必要确定 $\rho_6(4,8)$，但考虑到公式 (1)， $B(5,6,8) = 2^{84}$ 的基数过大，因此使用 $B(5,6,8)$ 的代表元集合

$$\rho_6(4,8) = \max_{f \in \widetilde{B}(5,6,8)} \mathrm{NL}_4(f).$$

因此，搜索空间缩减为 20748 个布尔函数。

我们确定覆盖半径 $\rho(4,8)$ 的策略如图 1 所示。它分为两部分。第一部分介绍用于获得 $B(5,6,8)$ 分类的工具：覆盖集、不变性和等价。第二部分~用于估算 $B(5,6,8)$ 中元素的 4 阶非线性度。

3. COVER SET AND CLASSIFICATION

~给定在AGL$(m,2)$作用下 $B(s,t,m)$ 的轨道代表元集合 $B(s,t,m)$，我们确定 $\rho_t(s-1,m)$：

$$\rho_t(s-1,m) = \max_{f \in B(s,t,m)} \mathrm{NL}_{s-1}(f) = \max_{f \in \widetilde{B}(s,t,m)} \mathrm{NL}_{s-1}(f).$$

~一般而言，确定一个 $B(s,t,m)$ 在计算上是一项困难的任务。因此，我们引入一个中间概念： $B(s,t,m)$ 的覆盖集是一个包含

$\sim B(s,t,m)$ 以及最终其他 $B(s,t,m)$ 函数的集合。为了从覆盖集中得到一个分类，我们需要一个消除同一轨道中函数的过程。首先，我们通过对 $B(s,t,m)$ 应用两个约化步骤，构造一个规模合理的覆盖集。任意布尔函数 $f \in B(m)$ 都可以写成$x_m g + h$，其中 $g, h \in B(m-1)$。特别地，

$$B(s,t,m) = \left\{ x_m g + h \mid g \in B(s-1,t-1,m-1),\ h \in B(s,t,m-1) \right\}. \tag{2}$$

引理 2（初始覆盖集）。该集合

$$B^{\dagger}(s,t,m) = \{ x_m g + h \mid g \in \widetilde{B}(s-1,t-1,m-1), h \in B(s,t,m-1) \} \tag{3}$$

$\widetilde{}$是 $B(s,t,m)$的覆盖集，其大小为 $\sharp B(s-1,t-1,m-1) \times \sharp B(s,t,m-1)$。

证明。元素 $\mathfrak{s} \in \mathrm{AGL}(m-1,2)$ 通过 $x_m g \circ \mathfrak{s} + h \circ \mathfrak{s}$ 作用于 f。 □

$\widetilde{}$引理 3（稳定子的作用）。设定 $g \in B(s-1,t-1,m-1)$。

(1) 对于 g 的稳定子中的所有 $\mathfrak{s} \in \mathrm{AGL}(m-1,2)$，函数 $x_m g + h$ 和 $x_m g + h \circ \mathfrak{s}$ 属于同一轨道。(2) 对于所有 $\alpha \in RM(1, m-1)$，函数 $x_m g + h$ 和 $x_m g + h + \alpha g$ 属于同一轨道。

其中，轨道对应于 $\mathrm{AGL}(m,2)$ 在 $B(s,t,m)$ 上的作用。

引理 4（第二覆盖集）。集合

$$B^{\ddagger}(s,t,m) = \bigsqcup_{g \in \widetilde{B}(s-1,t-1,m-1)} \left\{ x_m g + h \mid h \in \mathcal{R}(g) \right\}. \tag{4}$$

是一个大小为 $\sharp B^{\ddagger}(s,t,m) = \sum_{g \in \widetilde{B}(s-1,t-1,m-1)} \sharp \mathcal{R}(g)$ 的覆盖集。记 $\mathcal{R}(g)$ 为群在 $B(s,t,m-1)$ 上由变换 $h \mapsto h \circ \mathfrak{s}$ 和 $h \mapsto h + \alpha g$生成的作用所对应的一个轨道代表元集合。

$\widetilde{}$证明。对于每个 $g \in B(s-1,t-1,m-1)$，应用引理 3 到覆盖集 (3)。 □

为了确定 $\rho_6(4,8)$，初始覆盖集为 $B^{\dagger}(5,6,8) = \widetilde{B}(4,5,7) \times \sim B(5,6,7)$。分类 $B(4,5,7)$ 在 [3], 中得到，其基数为 179，因此 $\sharp B^{\dagger}(5,6,8)$ 是 $179 \times 2^{28} \approx 2^{35.5}$。

应用引理 4，我们得到一个大小为 $3828171 \approx 2^{21.9}$ 的覆盖集。它已经$\widetilde{}$已知 $\sharp B(5,6,8) = 20748$，轨道代表元集合的确定是下一节的主题。我们的方法基于不变量工具和等价算法。

4. Invariant

根据前一节关于 $B(5,6,8)$ 的结果，我们必须从 3828171 个函数中提取 20748 个轨道代表元。在 $\mathrm{AGL}(m,2)$ 的作用下，处于同一轨道中的两个元素 f、$f' \in B(s,t,m)$ 称为等价，记作 $f \sim^{m}_{s,t} f'$，这意味着存在 $\mathfrak{s} \in \mathrm{AGL}(m,2)$，使得 $f' \equiv f \circ \mathfrak{s} \bmod RM(s-1,m)$。对于任意集合 X，不变性 $j\colon B(s,t,m) \to X$ 满足 $f \sim^{m}_{s,t} f' \implies j(f) = j(f')$。如果 $j(f) = j(f')$ 且 $f \not\sim^{m}_{s,t} f'$，我们称存在碰撞。

我们回顾一下，布尔函数 f 沿方向 v 的导数 $\mathrm{d}_v f$ 是由 $\mathbb{F}_2^m \ni x \mapsto \mathrm{d}_v f(x) = f(x+v) + f(x)$ 定义的映射。在特定情形 $f \in B(s,t,m)$ 下，我们将导数定义为

$$\mathrm{Der}_v f \equiv \mathrm{d}_v f \mod RM(s-2,m).$$

该导数是 $B(s-1,t-1,m)$ 的一个元素，我们考虑如下映射：

$$\begin{aligned} F\colon B(s,t,m) &\longrightarrow \widetilde{B}(s-1,t-1,m)^{\mathbb{F}_2^m} \\ f &\longmapsto \widetilde{\mathrm{Der}_{\cdot} f}, \end{aligned}$$

引理 5. 设 $f \in B(m)$，$\mathfrak{s} \in \mathrm{AGL}(m,2)$。考虑线性部分 $A \in \mathrm{GL}(m,2)$ 和 $a \in \mathbb{F}_2^m$ $\mathfrak{s} = (A,a)$ 的仿射部分，$\mathfrak{s}(x) = A(x) + a$，则有 $F(f \circ \mathfrak{s}) = F(f) \circ A$。

证明。注意 $\mathfrak{s}(x+y) = A(x+y) + a = \mathfrak{s}(x) + A(y)$。对于 $x, v \in \mathbb{F}_2^m$, $f \in B(m)$

$$\begin{aligned} \mathrm{d}_v(f \circ \mathfrak{s})(x) &= f \circ \mathfrak{s}(x+v) + f \circ \mathfrak{s}(x) \\ &= f(\mathfrak{s}(x) + A(v)) + f \circ \mathfrak{s}(x) \\ &= (\mathrm{d}_{A(v)} f) \circ \mathfrak{s}(x) \end{aligned}$$

模 $RM(s-2,m)$ 化简后，我们有 $\widetilde{\mathrm{Der}_v(f \circ \mathfrak{s})} \equiv \widetilde{(\mathrm{Der}_{A(v)} f)} \circ \mathfrak{s}$，因此 $\widetilde{\mathrm{Der}_v(f \circ \mathfrak{s})} = \widetilde{\mathrm{Der}_{A(v)} f}$，从而 $F(f \circ \mathfrak{s}) = F(f) \circ A$。 □

引理 6（不变性）。对于所有 $v \in \mathbb{F}_2^m$，将 $f \in B(s,t,m)$ 映射到 $F(f)(v)$ 的取值分布的应用 $J\mathrm{mapping}$，是一个不变性。

证明。考虑 $f, f' \in B(s,t,m)$、$\mathfrak{s} \in \mathrm{AGL}(m,2)$，使得 $f' \equiv f \circ \mathfrak{s} \mod RM(s-1,m)$（即 $f \sim_{s,\ t}^{m} f'$）。应用引理 5，我们得到 $F(f') = F(f) \circ A$。□

让我们利用 f 在（2）中的分解，观察 $f \in RM(t,m)$ 沿 e_m 方向的导数；对于 $(y, y_m) \in \mathbb{F}_2^{m-1} \times \mathbb{F}_2$ 以及 $e_m = (0,1) \in \mathbb{F}_2^{m-1} \times \mathbb{F}_2$，我们得到：

$$\begin{aligned} \mathrm{d}_{e_m} f(y, y_m) &= f((y, y_m) + (0,1)) + f(y, y_m) \\ &= x_m(y, y_m + 1) g(y) + x_m(y, y_m) g(y) + h(y) + h(y) \\ &= (y_m + 1) g(y) + y_m g(y) \\ &= g(y) \end{aligned}$$

它不过是关于 x_m 的偏导数。因此，g 是一个以 $m-1$ 个变量构成、次数小于或等于 $t-1$ 的布尔函数。对于沿任意方向 v 的导子，这一事实通常成立。布尔函数 $f \in B(m)$ 是 v-周期的，当且仅当 $f(x+v) = f(x)\ \forall x \in \mathbb{F}_2^m$。$v$-周期布尔函数在任意 $T(x) = x + \theta(x)v$ 类型的换位 $T \in \mathrm{GL}(m,2)$ 的作用下保持不变，其中 v 是线性形式 θ 的核中的元素。

对于 v 的任意补充 E_v，v-周期函数 $f \in B(m)$ 的限制 $f|_{E_v}$ 是一个以 $m-1$ 个变量为自变量的函数。注意，对于 $f \in B(s,t,m)$，$\mathrm{Der}_v f$ 是 v-周期的，其在 E_v 上的限制是一个以 $m-1$ 个变量为自变量、次数小于或等于 $t-1$ 的布尔函数。

引理 7. 设 f、$g \in B(m)$ 是两个 v-周期布尔函数。若 f 在 $B(m)$ 中等价于 g，则对于 v 的任意补充E_v，$f|_{E_v}$ 在 $B(m-1)$ 中等价于 $g|_{E_v}$。

证明。如果 f和 g在 $B(m)$ 中等价，则存在 $\mathfrak{s}=(A,a)$ 使得 $f\circ\mathfrak{s}=g$。平移的情形显然成立。我们可以假设 $a=0$ 是线性部分 A, $f\circ A=g$ 的作用。由于 g 是 v-周期的，g 被任意换位$T=x+\theta(x)v$ 固定，其中 v 属于线性形式 θ 的核:

$$\forall x\in\mathbb{F}_2^m,\quad g(T(x))=g(x+\theta(x)v)=g(x)$$

我们将 P表示为沿 v方向的 $\mathbb{F}_2^m$在 E_v 上的投影（$P(e+v)=e$），

$$\forall x\in\mathbb{F}_2^m,\quad g(x)=g(T(x))=f(AT(x))=f(PAT(x)).$$

注意，$AT(x)=A(x)+\theta(x)A(v)$。我们将确定 $\theta(A^{-1}(v))$，使得 $\ker PAT\cap E_v=\{0\}$。这意味着对于 $x\in E_v\setminus\{0\}$, $AT(x)\notin\{0,v\}$。令$x\in\mathbb{F}_2^m$满足 $AT(x)=\lambda v$ 且 $\lambda\in\mathbb{F}_2$。

$$\begin{aligned}&A(x)+\theta(x)A(v)=\lambda v\\&x+\theta(x)v=\lambda A^{-1}(v)\\&\theta(x)+\theta(x)\theta(v)=\lambda\theta(A^{-1}(v))\quad\theta(x)=\lambda\theta(A^{-1}(v))\\&x=\lambda(A^{-1}(v)+\theta(A^{-1}(v))v)\end{aligned}$$

需要考虑两种情况:

- $v\in A(E_v)$: $A^{-1}(v)\neq v$，我们可以固定 $\theta(A^{-1}(v))=1$。因此，$x=\lambda(A^{-1}(v)+v)$。

$$x=\lambda(A^{-1}(v)+v)\quad\lambda=\begin{cases}0,\ x=0\\1,\ x\notin E_v\end{cases}$$

- $v\notin A(E_v)$: $A^{-1}(v)\notin E_v$，我们可以固定 $\theta(A^{-1}(v))=0$。因此，$x=\lambda A^{-1}(v)$，我们得到 $x=0$ 当 $\lambda=0$ 时，以及 $x\notin E_v$ 当 $\lambda=1$时

$$x=\lambda A^{-1}(v)\quad\lambda=\begin{cases}0,\ x=0\\1,\ x\notin E_v\end{cases}$$

在这两种情况下，我们得到 $x=0$ 当 $\lambda=0$ 时，以及 $x\notin E_v$ 当 $\lambda=1$时。因此，PAT在 E_v上的限制是一个自同构，故 $f|_{E_v}$在$B(m-1)$中等价于 $g|_{E_v}$。□

~通过对 $B(s-1,t-1,m)$ 的元素编号，$F(f)$ 的取值属于 $\mathbb{N}$。我们可以考虑它的傅里叶变换 $\widehat{F}(f)(b)=\sum_{v\in\mathbb{F}_2^m}F(f)(v)(-1)^{b\cdot v}$。对于 $A\in\mathrm{GL}(m)$, ^关系 $F(f')=F(f)\circ A$变为 $F(f')\circ A^*=F(f)$，其中 A^*是 A 的伴随。我们将 J记为与 $F(f)$ 的取值分布对应的不变性，并将∽J记为与 $F(f)$ 的取值分布对应的不变性。这些不变性 J^和 J 由 [1]引入。在我们的语境中，不变性 J 比 J更具区分性。引理 7 的应用使我们可以考虑 $B(s-1,t-1,m-1)$ 中的导函数，而不是 $B(s-1,t-1,m)$。

注 1. 为了使算法 *Invariant* 更高效，我们需要优化对 $B(4,5,7)$ 中元素的类判定 ~。$B(5,5,7)$ 中只有 4 个类。我们通过确定代表元，预先计算 $B(5,5,7)$ 的完整分类

$\{r_1, r_2, r_3, r_4\}$ 集合 $B(5, 5, 7)$ 的代表元、每个代表元的稳定子群 $\{S_1, S_2, S_3, S_4\}$ 以及一个横截集。对于每个稳定子群，我们在内存中保存该稳定子群 S_i 作用于 $B(4, 4, 7)$ 所得轨道的描述。利用键 $h \circ \mathfrak{s} + r_i$ 的查找表，可以通过一个代表元 $r_i \sim_{5,\ 5}^{7} h$ 和一个横截集元素 $\mathfrak{s} \in \mathrm{AGL}(7)$ 来确定 $h \in B(4, 5, 7)$ 中元素所属的类，其中 $h \circ \mathfrak{s} \equiv r_i$ 模 $RM(4, 7)$。

共有 $B(4,5,7)$ 类 data 这些数据大约需要 32 GB 的内存。

Listing 1. 不变性

```
不变量算法( f, s, t,              m )
{   // f 属于 B(s,t,m)
    对于 每个 v 在 F_2^m
        g← d_v f
        h ←g|_{E_v}
        F[v] ←类( h, s−1, t−1, m−1 )
    返回 FourierTransform(F )
}
```

将不变性 J 应用于覆盖集 $B^{\ddagger}(5,6,8)$ 的 3828171 个布尔函数后，可以发现 20694 种分布，这意味着存在 54 次碰撞。在同一集合上，不变性 J 取 20742 个值：仅存在 6 次碰撞。在下一节中，我们将介绍一种等价算法，用于检测并解决这些碰撞。

5. Equivalence

在本节中，我们只研究空间 $B(t-1, t, m)$，即特殊情形 $s = t - 1$。考虑 J，它是与 $F(f)$ 的取值分布对应的不变性。两个取值分布不同的函数 f、$f' \in B(t-1, t, m)$ 不等价。在情形 $f \sim_{t-1,\ t}^{m} f'$ 下，分布相同，并且存在 $A \in \mathrm{GL}(m, 2)$，使得

$$F(f') = F(f) \circ A \quad \text{and} \quad \widehat{F}(f') \circ A^* = \widehat{F}(f). \tag{5}$$

A 的存在并不能保证这些函数等价。这样的 A 称为候选项，必须补上仿射部分 $a \in \mathbb{F}_2^m$，才能得出等价的结论。对于 $f \in RM(t, m)$ 和 $x \in \mathbb{F}_2^m$，

$$\begin{aligned} \mathrm{d}_{u,v} f(x) &= \mathrm{d}_v(\mathrm{d}_u f)(x) \\ &= \mathrm{d}_u(f(x+v) + f(x)) \\ &= f(x+u+v) + f(x+u) + f(x+v) + f(x) \\ &= f(x+u+v) + f(x) + f(x+u) + f(x) + f(x+v) + f(x) \\ &= \mathrm{d}_{u+v} f(x) + \mathrm{d}_u f(x) + \mathrm{d}_v f(x) \end{aligned}$$

$\mathrm{d}_{u,\ v} f$ 的次数小于或等于 $t-2$，对 $RM(t-2, m)$ 取模后，我们得到

$$\mathrm{d}_{u+v} f(x) + \mathrm{d}_u f(x) + \mathrm{d}_v f(x) \equiv 0.$$

集合 $\Delta(f) = \{\mathrm{d}_v f \bmod RM(t-2, m) \mid v \in \mathbb{F}_2^m\}$ 是 $B(t-1, t-1, m)$ 的一个子空间。

引理 8（候选检查）。设 f, f' 属于 $B(t-1,t,m)$。考虑一个候选 $A \in \mathrm{GL}(m)$。存在 $a \in \mathbb{F}_2^m$，使得 $f' \equiv f \circ (A,a) \bmod RM(t-2,m)$，当且仅当 $f' \circ A^{-1} + f \in \Delta(f)$。

证明。若 $f' \equiv f \circ (A,a) \bmod RM(t-2,m)$，则存在 $r \in RM(t-2,m)$，使得对所有 $x \in \mathbb{F}_2^m$

$$
\begin{aligned}
f'(x) &= f \circ (A,a)(x) + r(x) = f(A(x)+a) + r(x) \\
f' \circ A^{-1}(x) &= f(x+a) + r(x) \\
f' \circ A^{-1}(x) + f(x) &= f(x+a) + f(x) + r(x) \\
(f' \circ A^{-1} + f)(x) &= \mathrm{d}_a f(x) + r(x)
\end{aligned}
$$

因此 $f' \circ A^{-1} + f \in \Delta(f)$。反过来，对于 $f' \circ A^{-1} + f \in \Delta(f)$，存在 $a \in \mathbb{F}_2^m$，使得 $f' \circ A^{-1} + f \equiv \mathrm{d}_a f \bmod RM(t-2,m)$。存在 $r \in RM(t-2,m)$，使得对所有 $x \in \mathbb{F}_2^m$，$(f' \circ A^{-1} + f)(x) = \mathrm{d}_a f(x) + r(x)$。通过以相反顺序重复计算，我们得到 $f' \equiv f \circ (A,a) \bmod RM(t-2,m)$。□

根据引理 8，可以推导出一个算法 CandidateChecking(A,f,f')，当且仅当存在一个元素 $a \in \mathbb{F}_2^m$，使得 $f' \equiv f \circ (A,a) \bmod RM(t-\widehat{\ }\widehat{\ }2,m)$ 时返回 true，否则返回 false。给定满足 $J(f) = J(f')$ 的 $f, f' \in B(t-1,t,m)$，算法 Equivalent(f,f',iter)[1] 分两个阶段测试 f 和 f' 在 $RM(t-2,m)$ 模下是否在 AGL$(m,2)$ 的作用下等价：

$\widehat{\ }$(1) 最多确定迭代次数个候选项 $A^* \in \mathrm{GL}(m)$，使得 $F(f') \circ A^* = \backsim F(f)$

(2) 对每个候选项 A^*，调用候选检查 (A,f,f')。

该算法最终会得到以下三个值之一：

等价$(f,f',\text{iter}) = \begin{cases} \text{不等价，已测试所有可能的 } A\text{，因此} f \not\sim^m_{t-1,t} f'\text{；等价，存在一个}(A,a)\text{来证明} f \sim^m_{t-1,t} f'\text{；未定} \end{cases}$

义，迭代次数过小，无法得出结论。

LISTING 2. 在AGL$(m,2)$作用下，$B(t-1,t,m)$中的等价

```
等价判定算法(f, f', 迭代次数)
{   // f、f' 是 B(t-1,t,m) 中给定的元素
    // 满足条件 Ĵ(f') = Ĵ(f)
    // 返回等价或不等价或未定义
    s ← AGL(m) 的随机元素
    f ← f ∘ s
    基 ←(b1, ..., bn) 是 F2^m 的一组基
    旗标 ←不等价
    // 确定 A*属于 GL(m)
    A*(0) ←0
    搜索(1,基 )
    返回旗标
}
```

[1]参数 `iter` 根据具体情况从 1024 变化到 2^{23}

LISTING 3. 搜索

```
搜索算法(i, 基)
{   // 基 =(b_1, .. ., b_n)          F_2^m的基
    // i 是 {1,2,... 中基元素的索引,                m}
    如果( i  >m )
        // A*在 GL(m) 中已完全构造
        // 检查 F_2^m 中是否存在 a
        如果 候选检查(A,f,f')
            旗标 ←等价
            返回
        iter ←迭代次数 − 1
        如果 ( 迭代次数 < 0)
            旗标 ←未定义
            返回
    else
        // ∀x ∈ ⟨b_1、 . . .、 b_{i−1}⟩、 F̂ (f′) ∘ A* (x) = F̂(f)(x)
        // 继续构造 A*
        对于 每个 y, 遍历 F_2^m
            如果 Admissible(y,i) 且 ( 旗标 = NotEquiv )
                搜索(i+1,基)
```

算法 Admissible(y,i) 检查在 $\langle b_1, \ldots, b_{i-1}, b_i\rangle$ 上继续构造 A^* 的可能性，并设置 $A^*(x + b_i) := A^*(x) + y$ 对所有 $x \in \langle b_1, \ldots, b_{i-1}\rangle$。然后，如果 $\forall x \in \langle b_1, \ldots, b_{i-1}, b_i\rangle$, $F(f')\circ A^*(x) = F(f)(x)$，该函数返回 true；否则返回 false。

6. DETERMINATION OF $\rho(4, 8)$

我们确定 $\rho(4, 8)$的策略各个步骤总结于1。

```
算法 非线性度(k,m,f,迭代次数,limit )
{
    G ←RM(k,m) 的生成矩阵
    当( 迭代次数 > 0 )
        对于( i = 0 ; i < k; i++ )
        do {
            p =随机( n )
        <escape>} 当 ( 非 G[i][p] )</escape>
        对于( j = i+1 ; j < k; j++ )
            if ( G[j][p] )
            G[j] ←G[j] 异或 G[i]
        if ( f[ p ] )
            f ←f 异或 G[i]
        w =权重( f )
        如果 ( w <= 限制 )
            返回 真
    iter ←迭代次数 − 1
    返回 假
}
```

该算法通过随机高斯消元，在 $RM(k,m)$ 的一个陪集内生成低重量码字。为了确定覆盖半径 $\rho_6(4,8)$ 和 $\rho(6,8)$，我们必须估计 $B(8)$ 中某些函数的 4 阶非线性度。我们使用非线性度概率算法三次：

(1) 检查 $B(5,6,8)$ 中是否不存在 4 阶非线性度大于或等于 28 的函数；(2) 提取 $B(5,6,8)$ 中 4 阶非线性度大于或等于 26 的两个函数 $\{f,g\}$；(3) 证明函数 $\{f+\delta_a, g+\delta_a\}$ 的 4 阶非线性度不大于或等于 27。

6.1. 计算 $\rho_6(4,8)$。回顾一下，

$$\rho_6(4,8) = \max_{f\in\widetilde{B}(5,6,8)} \mathrm{NL}_4(f) = \max_{f\in\widetilde{B}(5,6,8)} \min_{g\in RM(4,8)} \mathrm{wt}\,(f+g).$$

我们对 $B(5,6,8)$ 应用非线性度算法，以确认所有这些函数的 4 阶非线性度都小于或等于 26。利用结果 $\rho_5(4,8) = 26$，根据 [2], 可得 $\rho_6(4,8) = 26$。

6.2. 计算 $\rho(4,8)$。已知 $\rho(6,8) = 2$，并根据先前得到的结果 $\rho_6(4,8) = 26$，可得

$$\rho(4,8) \le \rho_6(4,8) + \rho(6,8) = 28.$$

再次应用非线性度算法，从 $B(5,6,8)$ 中剔除了 20746 个 4 阶非线性度小于 26 的函数。经过这一过程，还剩下两个函数：

$$f = abcef + acdef + abcdg + abdeg + abcfg + acdeh + abcfh \\ + bdefh + bcdgh + abegh + adfgh + cefgh$$

and

$$g = abcdeh + abcdf + abcef + abdeg + bcefh + adefh + bcdgh + acegh + abfgh$$

我们找到了文中提到的余三次函数 f [2], ，其次数为 5，4 阶非线性度为 26。另一个函数 g 的次数为 6，其非线性度很可能为 26，且确定小于或等于 26。现在，我们将证明，在 $B(8)$ 中不存在 4 阶非线性度等于 28 的布尔函数。为此，只需检验是否存在满足 $\mathrm{NL}_4(h) = 27$ 的函数 h；这样的 h 具有奇数重量，因此其次数为 8。对于 $a \in \mathbb{F}_2^m$，我们用 δ_a 表示狄拉克函数，当且仅当 $x = a$ 时，$\delta_a(x) = 1$。每个布尔函数都可以表示为狄拉克函数之和 $f(x) = \sum_{\{a|f\ (a)\ =1\}} \delta_a(x)$。$\delta_a$ 的多项式形式为：

$$\delta_a(X_1, X_2, \ldots, X_m) = (X_1 + \bar{a}_1)(X_2 + \bar{a}_2)\cdots(X_m + \bar{a}_m) \tag{6}$$

其中 $\bar{a}_i = a_i + 1$。

引理 9. 奇权函数与 $RM(m-2,m)$ 的距离为 1。

证明。我们将 X_i 记为次数为 $m-1$ 且包含除X_i之外所有变量的单项式项。考虑一个奇权函数 $h \in B(m)$，其次数为 m，因此

$$h(X_1, X_2, \ldots, X_m) = X_1X_2\ldots X_m + \bar{a}_1\widetilde{X_1} + \cdots + \bar{a}_m\widetilde{X_m} + r(x)$$

其中 $\deg(r) \leq m-2$。由（6）还可得

$$\delta_a(X_1, X_2, \ldots, X_m) = X_1X_2 \ldots X_m + \bar{a}_1\widetilde{X_1} + \cdots + \bar{a}_m\widetilde{X_m} + r'(x)$$

其中 $\deg(r') \leq m-2$。我们得到 $h \equiv \delta_a \bmod RM(m-2, m)$。狄拉克函数的权重为 1，因此 h 到 $RM(m-2, m)$ 的距离为 1。□

将算法 NonLinearity 第三次应用于由 256 个狄拉克函数映射得到的集合 $\{f, g\}$，可以证明不存在非线性度为 4 阶且大于或等于 27 的奇权函数。这意味着在 $B(8)$ 中不存在非线性度为 4 阶且大于或等于 27 的函数，因此我们得到 $\rho(6, 8) = 26$。第二次和第三次应用算法 NonLinearity 需要 569713 次迭代。

~注 2. 使用不变性方法和 *equivalent*算法提取 $B(5, 6, 8)$ 的 20748 个等价类需要数周的计算时间（等价性测试）

备注 3。平均需要迭代 565252 次，以估计布尔函数的 4 阶非线性度。使用 48 个处理器检查非线性度，总运行时间约为一天。

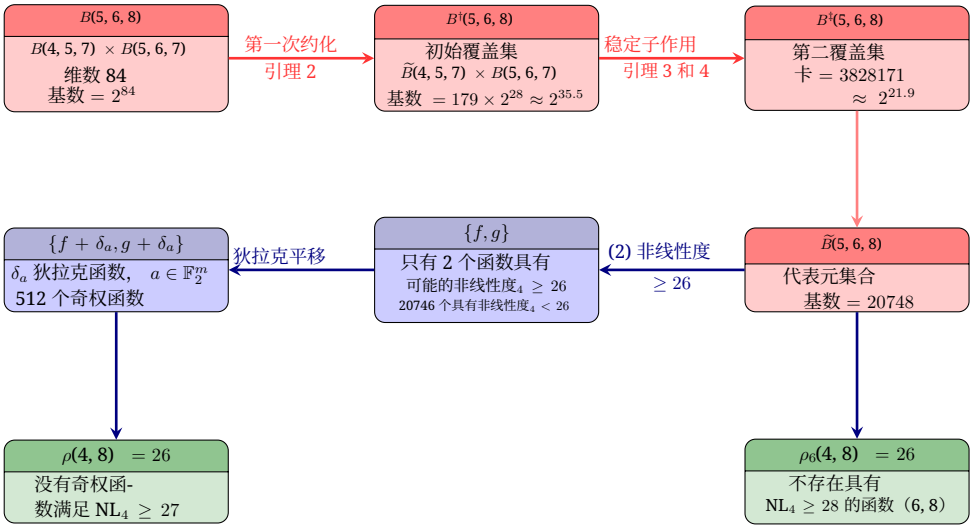


FIGURE 1. 计算 $\rho(4, 8)$ 的策略

7. 结论

我们已经从$B(5, 6, 8)$的分类中确定了 $RM(4, 8)$的覆盖半径。如何应用我们的方法来获得8个变量的二阶和三阶Reed-Muller码的覆盖半径，并不显而易见。然而，我们相信，我们的方法能够帮助改进这些未解决情形的下界。

References

[1] ´Eric Brier 和 Philippe Langevin。

9 ITW 变

2003 179

量布尔三次型的分类。，–182，2003年。[2] Randall Dougherty、R. Daniel Mauldin 和 Mark Tiefenbruck。Reed-Muller码 $RM(m-4,m)$在 $RM(m-3,m)$中的覆盖半径。

IEEE Trans. Inform. Theory，68(1):560–571，2022年。[3] 八变量布尔四次型的分类 Philippe Langevin、Gregor Leander。北约和平与安全科学系列D：信息与通信安全

Boolean Functions in Cryptology and Information Security (18) 139–147，2005年。[4] J. Gao、H. Kan、Y. Li 和 Q. Wang。三阶Reed-Muller码 rm(3, 7) 的覆盖半径为20。 *submitted to IEEE IT*，2023年。[5] Val´erie Gillot 和 Philippe Langevin。Reed-Muller码的某些陪集的分类。

`https://hal-univ-tln.archives-ouvertes.fr/hal-03834481`，2022年。[6] Val´erie Gillot 和 Philippe Langevin。$B(s,t,7)$的分类。

`http://langevin.univ-tln.fr/project/agl7/aglclass.html`，2022年。[7] Val´erie Gillot 和 Philippe Langevin。RM(4, 8)的覆盖半径。`http://langevin.univ-tln.fr/project/agl8`，2022年。[8] Pless、V. S.、Huffman、W. C. 和 Brualdi、R. A.《编码理论手册》。第I、II卷，北荷兰出版社，阿姆斯特丹，1998年[9] Qichun Wang。Reed-Muller码 RM(2, 7)的覆盖半径为40。 *Discrete Math.*，342 12 111625，7，2019年 ( ): 。

Email address: `valerie.gillot@univ-tln.fr`*Email address*: `philippe.langevin@univ-tln.fr`Imath, université de Toulon