arXiv:2304.05598v1 [cs.CC] 12 Apr 2023

用更少查询进行广义 Reed-Muller 码的最优测试

Dor Minzer* 凯·郑†

摘要

纠错码 $C \subseteq \Sigma^n$ 的局部测试器是指对给定字 $w \in \Sigma^n$ 进行 Q 次预言机查询，并决定接受或拒绝该字 w的测试器。最优局部测试器是具有完备性和最优可靠性这两项额外性质的局部测试器。完备性是指，如果 $w \in C$，测试器必须以概率 1 接受。最优可靠性是指，如果测试器以至少 $1-\varepsilon$的概率接受（其中 ε很小），那么 w必须在汉明距离上与某个码字 $c \in C$ 相距 $O(\varepsilon/Q)$。

我们证明，广义 Reed-Muller码存在具有 $Q = (3q)^{\lceil \frac{d+1}{q-1} \rceil + O(1)}$次查询的最优测试器。这里，对于素数幂 $q = p^k$，广义 Reed-Muller 码RM$[n, q, d]$由所有在 $\mathbb{F}_q$上的 n-元次数为 d 的多项式的取值组成。此前，尚无已知测试器能够达到这一查询复杂度；Haramaty、Shpilka 和 Sudan 提出的测试器 [21]（这是最优的），以及Ron-Zewi 和Sudan 提出的测试器 [33]（当时尚不知其是否最优），都需要$q^{\lceil \frac{d+1}{q-q/p} \rceil}$ 次查询。我们的测试器所达到的查询复杂度比幂为$p/(p-1)$的结果在多项式意义下更优；对于广义 Reed-Muller 码而言，这一查询复杂度几乎已经是可能达到的最佳值。

我们分析的测试器由 Ron-Zewi 和 Sudan 提出，并证明他们的基本测试器实际上是最优的。我们的方法更具一般性，还使我们能够证明一大类遵循 Ron-Zewi 和 Sudan 测试器形式的测试器都是最优的。该结果适用于所有仿射不变码的测试器（这些码不一定是广义 Reed-Muller 码）。

1 引言

1.1 Reed-Muller码的局部测试

Reed-Muller码是一种应用广泛的编码，在复杂性理论乃至更广泛的理论计算机科学中有许多应用。其中一个原因是，Reed-Muller码具有非常好的局部可测试性，这些性质对许多应用至关重要（例如，用于构造概率可检验证明）。本文的主要目标是为扩域上的Reed-Muller码提出查询复杂度更低的局部测试器，同时满足一种称为最优测试的更强可靠性概念。

在本文中，$p \in \mathbb{N}$是一个素数，$q = p^k$ 是一个素数幂，其中 k 应被视为中等大小（因此 q 显著大于 p）。对于次数参数 $d \in \mathbb{N}$ 和变量个数参数 $n \in \mathbb{N}$，Reed-Muller 码由所有次数为 d 的多项式f的求值向量组成：$\mathbb{F}_q^n \to \mathbb{F}_q$。也就是说，

$$\mathrm{RM}[n, q, d] = \left\{ (f(\vec{x}))_{\vec{x} \in \mathbb{F}_q^n} \mid f \colon \mathbb{F}_q^n \to \mathbb{F}_q \text{ is a polynomial of degree at most } d \right\}.$$

*数学系，麻省理工学院，美国剑桥。由斯隆研究学者奖学金、NSFCCF奖项2227876和NSF CAREER奖项2239160支撑。

†数学系，麻省理工学院，美国剑桥。获 NSF GRFP 资助。

当 $k > 1$时，RM$[n,q,d]$ 有时称为广义 Reed-Muller 码，以区别于素域情形；正如标题所示，我们的结果与这一情形最为相关。不过，为简便起见，以下我们仍将其称为 Reed-Muller 码。

稍微滥用一下记号，在指称码字时，我们不区分函数及其取值。也就是说，对于 $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$，我们只说 $f \in$ RM$[n,q,d]$ 当$\deg(f) \leqslant d$，并将 RM$[n,q,d]$ 的码字本身视为函数。谈到函数 f 的次数时，我们指的是将 f 写成多项式时的总次数。

给定邻近参数 $\delta > 0$，Reed-Muller 码的局部测试问题旨在设计一个随机测试器 $\mathcal{T}$，使其对给定函数 $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$ 进行 Q 次预言机查询（其中 Q 尽可能小），并满足：

1. Co. 完备性：如果 f 是次数至多为 d 的多项式，那么 $\mathcal{T}$ 以概率接受 1.

2. 可靠性：如果 f 与所有次数为 d 的多项式都相距至少 δ，那么测试器 $\mathcal{T}$ 至少以 $2/3$ 的概率拒绝。

局部测试。Reed-Muller 码有一种非常自然且经过充分研究的局部测试 [1, 24, 22, 21] ，称为t-仿射子空间测试。该测试起源于概率可验证证明的研究 [15, 3, 2, 34, 4, 32] （因为它与广为人知的平面对平面、平面对直线以及直线对点测试有关），也起源于Gowers一致性范数的理论 [16]。为了检查给定的函数 f 是否确实是低次数的，测试器随机抽取一个 t维仿射子空间 $U \subseteq \mathbb{F}_q^n$，对所有 $\vec{x} \in U$查询 $f(\vec{x})$，并检查所得的 t元函数 $f|_U$ 的次数是否至多为 d。显然，所进行的查询次数为 q^t；同样显然，该测试是完备的：如果 f 的次数至多为 d，那么测试器总是接受。至于可靠性，已知可以取 $t = \lceil \frac{d+1}{q-q/p} \rceil$ ，从而得到测试器具有一定的可靠性 [1],，也就是说，拒绝概率被一个正常数下界所约束（而不是至少为 $2/3$）。事实上，典型的局部测试结果表明，如果函数 f 与一个次数为 d 的函数的距离达到 δ，那么测试器以至少 $\varepsilon = \varepsilon(q,d,\delta) > 0$的概率拒绝它；这个量通常会随着各个参数的变化而趋于零。为了增强可靠性，依次重复测试器 $\theta(1/\varepsilon)$次，以获得 $2/3$ 的拒绝概率，从而得到一个查询复杂度为 $O(q^t/\varepsilon)$且可靠性至少为 $2/3$的测试器。

这类 Reed-Muller码测试器早已为人所知。事实上， [1] 中分析了 t 仿射子空间测试器，并证明基本测试器的拒绝概率至少为 $\varepsilon \geqslant \Omega(\delta/q^t)$，从而得到查询复杂度为 $O(q^{2t}/\delta)$ 的测试器。事实证明，这种可靠性分析并非最优；正如下文将要解释的，后续研究对 t 仿射子空间测试器给出了更好的分析。特别是，研究证明 t 仿射子空间测试器是一个最优测试器。

1.2 Reed-Muller码的最优测试

本文着重研究一种更强的测试概念，即最优测试。显然，如果测试器进行 Q 次查询，且邻近参数为 δ，那么拒绝概率至多为 $\min(1, Q\delta)$；事实上，这是区分一个 Reed-Muller 码字与一个在随机选取的 δ 比例输入上受到扰动的 Reed-Muller 码字的概率上界。如果测试器实现的查询次数与拒绝概率之间的权衡大致达到这一界限，就称其为最优测试器。很多时候，人们会满足于稍差一些、形式为 $c(q)\min(1, Q\delta)$ 的拒绝概率，其中函数 $c(q) > 0$ 仅取决于域的大小 q。我们也将此类结果称为最优测试结果。因此，理想情况下，我们希望测试器既能实现尽可能低的查询复杂度，又同时达到最优。

Reed-Muller码已知存在最优测试器。此类结果最初由 [10] 在 $\mathbb{F}_2$ 上证明。随后，人们在一般域 [21] 上确立了 Reed-Muller码的最优测试结果，并将其推广至仿射提升码这一更广泛的类别 [20]。在所有这些结果中，都分析了 t-仿射子空间测试（其中 t 按照上述方式选取），并证明它是一个最优测试器。我们还指出，对 [10, 21, 20] 的分析改进了 Reed-Muller码测试的查询复杂度。这些结果有重要应用，最值得一提的是，它们可用于构造具有许多接近 1 [8], 的特征值的小集合扩张图；此类图后来被用于改进 PCP 构造和积分间隙构造 [19, 12, 11, 23]。

从定量角度看，这些结果有两个缺点。首先，由于应用了密度 Hales-Jewett 定理， $c(q)$ 对域大小 q 的依赖呈塔式增长，因此结果主要适用于较小的域。其次，虽然他们的测试器在素域上的查询复杂度已达到最优（因为所需查询复杂度的下界由 RM$[n,q,d]$ 的对偶码的距离给出；当 q 为素数时，该距离为 q^t ），但对于大小为素数幂的域，尚不知其是否最优。这引出了两个自然的问题：平坦测试器在大域上是否确实表现较差（与小域相比）？ 在非素域（即扩域）上，是否存在查询复杂度更低的测试器?

在 [33] 中，设计了一种新的 Reed-Muller码局部测试器。该测试器的查询复杂度为$Q = \mathrm{poly}(q)(3q)^{\lceil \frac{d+1}{q} \rceil}$，比 q^t 上述结果小一个多项式量级（相差$\frac{p}{p-1}$的幂次）。这个测试器将在下文中称为稀疏 t-仿射子空间测试器，在本工作中发挥着至关重要的作用，并将在后续章节中介绍。

遗憾的是， [33] 中证明的稀疏 t-仿射子空间测试器的拒绝概率是一个 ε ，其值小于常数；将该测试器重复执行 $\Theta(1/\varepsilon)$ 次后，其查询复杂度最终大致与上述 t-仿射子空间测试器相同。这使得扩域上的 Reed-Muller码处境相当棘手：我们已知该码的局部刻画——也就是说，有一种基本测试器，能够以某个非忽略的概率拒绝与 Reed-Muller 码字相距较远的对象——但要将可靠性提升至常数，就会使查询复杂度退回到与 t-仿射子空间测试器相同的水平。

1.3 主要结 果：广义 Reed-Muller 码的最优查询高效测试器 s

本文的主要结果是对 [33] 的测试器进行新的改进分析。我们证明，该测试器的可靠性远优于 [33], 给出的保证；事实上，它还是一个最优测试器：

定理 1.1. 对所有素数 $p \in \mathbb{N}$ 和素数幂 $q = p^k$ ，存在一个测试器 $\mathcal{T}$，其查询复杂度为$Q \leqslant 3q^{p+O(1)}(3q)^{\lceil \frac{d+1}{q-1} \rceil}$；给定对函数 $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$ 的预言机访问，

1. 完备性：如果 f 的次数至多为 d，那么 $\mathcal{T}$ 以概率 1 接受。
2. 可靠性：如果 f 与次数为 d 的函数相距 δ，那么 $\mathcal{T}$ 以至少 $c(q)\min(1, Q\delta)$ 的概率拒绝，其中 $c(q) = {}^{1}\!/_{\text{多项式}(q)}$。

该测试使用参数 t（其中$\lceil \frac{d+1}{q-1} \rceil + t$类似于仿射子空间测试中的“维数”参数），而我们使用的 t 将为 $t = \max(p+2, 10)$。不过，我们要指出，给出的分析适用于所有 $t \geqslant \max(p+2, 10)$，并且我们选择这个特定的 t 是为了尽量降低查询复杂度。关于该参数的更多细节，请参见第 3.2 节。

所需查询复杂度的一个下界为 $q^{\lceil \frac{d+1}{q-1} \rceil}$。这一结论再次可通过考察广义 Reed-Muller 码的对偶码，并证明该数值就是其距离而得。因此，定理 1.1 在相差一个 $\mathrm{poly}(q)3^{\lceil \frac{d+1}{q-1} \rceil}$因子的范围内是紧的；当 q 较大时，与$q^{\lceil \frac{d+1}{q-1} \rceil}$相比，这个因子非常小，因此对于较大的域大小 q，我们的测试器所达到的查询复杂度基本上是最优的。

1.4 其他线性提升仿射不变码的最优测试

事实上，我们的技术适用范围更广，也适用于一类更广泛的码的测试器，这类码称为（线性）提升仿射不变码。这些码由 [17] 引入，并在[20, 31] 中证明可被最优测试。简单来说，我们证明，若这类码的任意测试器都能表示为若干多项式的乘积，且每个多项式都定义在常数个变量上，并且各多项式所用的变量互不相交，那么该测试器就是最优的。我们将在下文更详细地介绍这一结果，但完整讨论留待第 6 节。

码 $\mathcal{C} \subseteq \{f\colon \mathbb{F}_q^n \to \mathbb{F}_q\}$ 是线性的，当且仅当其码字构成一个线性子空间；若对于任意仿射变换 $T\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ 和 $f \in \mathcal{G}$，都有 $f \circ T \in \mathcal{G}$，则称其仿射不变，其中 $f \circ T$ 定义为函数 $f'\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$，满足对所有 $x \in \mathbb{F}_q^n$，$f'(x) = f(T(x))$。由于 $\mathcal{C}$ 是线性的，它有一个对偶码 $\mathcal{C}^\perp$，也由从 $\mathbb{F}_q^n \to \mathbb{F}_q$ 映射而来的函数组成；当且仅当对所有 $h \in \mathcal{C}^\perp$ 都有 $f \in \mathcal{C}$ $\langle f, h\rangle = 0$ 时，$f \in \mathcal{C}$ 成立，其中此内积是 f 和 h （在 $\mathbb{F}_q^n$ 上）的求值向量的标准点积。注意，也可以将 f 与仿射变换 $T\colon \mathbb{F}_q^k \to \mathbb{F}_q^n$ 对 $k < n$ 复合。此时，$f \circ T$ 是一个从 $\mathbb{F}_q^k \to \mathbb{F}_q$ 映射而来的函数，我们可以考虑由所有满足 $f \circ T$ 属于某个仿射不变基码 $\mathcal{G} \subseteq \{\mathbb{F}_q^k \to \mathbb{F}_q\}$ 的 $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$ 构成的码。这个码称为 $\mathcal{G}$ 的 n 维提升，定义如下：

$$\mathsf{Lift}_n(\mathcal{G}) = \{f : \mathbb{F}_q^n \to \mathbb{F}_q \mid f \circ T \in \mathcal{G} \text{ for all affine transformations } T : \mathbb{F}_q^k \to \mathbb{F}_q^n\}.$$

不难看出，$\mathsf{Lift}_n(\mathcal{G})$ 也具有仿射不变性且是线性的。假设我们想为 $\mathcal{C}$ 设计一个局部测试器，并且已知 $\mathcal{C} = \mathsf{Lift}_n(\mathcal{G})$，其中某个仿射不变的 $\mathcal{G}$ 如上所定义，且满足 $k \geqslant 10$。一种自然的测试如下：

1. 取 $\mathcal{H} \subseteq \mathcal{G}^\perp$。
2. 均匀随机地选取一个仿射变换 $T\colon \mathbb{F}_q^k \to \mathbb{F}_q^n$。
3. 当且仅当对所有 $h \in \mathcal{H}$，$\langle f \circ T, H\rangle = 0$ 时接受。

我们指出，并非每种 $\mathcal{H}$ 的选取都能得到局部测试器；事实上，有可能选取 $\mathcal{H}$，使得存在 $f \notin \mathcal{C}$，它们仍以概率 1 通过上述测试。我们的主要结果表明，当这种测试是局部测试，且 $\mathcal{H}$ 由特定形式的函数组成时，该测试器自动就是一个最优测试器。要得到显式的最优测试器，仍需找到这样一个作为局部测试器的 $\mathcal{H}$，但这并非本文的关注重点。

我们所需的 $\mathcal{H}$ 形式如下。设

$$H(x_1, \ldots, x_{k'}) = \left(\prod_{i=1}^{s} P_i(x_{m(i)}, \ldots, x_{m(i+1)-1})\right),$$

其中 $\mathrm{poly}(q) \geqslant k - k' \geqslant 0$，且 $m(i+1) - m(i) \leqslant t'$，对某个常数 t' 和所有 $1 \leqslant i \leqslant s-1$均成立。换言之，$H$ 是一个至多含有 k'个变量的多项式，其中某个 k' 与k相差不超过 q 的某个常数次幂；它可以分解为若干个多项式的乘积，每个多项式都只含常数个变量，且这些多项式的变量两两不相交。接下来，设 $\mathcal{M} \subsetneq \{\mathbb{F}_q^{k-k'} \to \mathbb{F}_q\}$是一个仿射不变码，$\overline{\mathcal{M}}$ 是 $\mathcal{M}^\perp$的一组基。最后，假设

$$\mathcal{H} = \{H(x_1, \ldots, x_{k'})M(x_{k'+1}, \ldots x_k) \mid M \in \mathcal{M}\}.$$

我们的定理表明：

定理 1.2. 假设 $\mathcal{H}$ 具有前面所述的形式，并假设使用 $\mathcal{H}$ 的前面所述测试是 $\mathcal{C} = \mathrm{Lift}_n(\mathcal{G})$ 的局部测试器。那么该局部测试器也是最优的。也就是说，

1. 完备性：如果 $f \in \mathcal{C}$，那么测试以概率 1 接受。

2. 可靠性：如果 f 与次数为 $\mathcal{C}$ 的多项式相距至少 δ，那么该测试以至少 $c(q)\min(1, Q\delta)$ 的概率拒绝，其中 $c(q) = \frac{1}{\mathrm{poly}(q)}$。

虽然我们的结果是针对提升的仿射不变码表述的，但取 $\mathcal{C} = \mathcal{G} = \mathrm{Lift}_k(\mathcal{G})$ 后，同样适用于仿射不变码。相比之下，文献 [31] 中针对提升的仿射不变码的最优测试结果，仅适用于 $\mathrm{Lift}_n(\mathcal{G})$ 的 k-仿射子空间测试；在 $\mathcal{C} = \mathcal{G}$ 的情况下，这已不再是“局部”测试，因为它会检查整个定义域。另一方面，对于 $\mathcal{C} = \mathcal{G}$ 的情况，仍可通过我们的结果实现局部性：构造一个具有稀疏支撑的、指定形式的集合 $\mathcal{H}$ 即可。

定理 1.2 给出了一种构造最优测试器的通用方法，从而推动了为一般仿射不变码确立最优测试结果这一任务。我们想强调两个留待未来研究的有趣方向。首先，值得探究还有哪些仿射不变码可以通过定理 1.2 进行分析。这可能为其他码带来新的最优测试结果，或者得到一类更一般的测试器，进而可以尝试用本文提出的工具（及其扩展）来分析。其次，值得将我们的技术加以扩展，以去除对 $\mathcal{H}$ 形式的要求（或许也可以在某种程度上放宽这一要求），并证明仿射不变码的任何局部测试都是最优的。

1.5 通过全局超契性实现最优测试

定理 1.1的证明与 [10, 21, 20]（其通过对 n进行归纳来完成）以及 [33] 的证明（其通过给出广义 Reed-Muller码的局部刻-画，并借助 [25], 提出的一般且强大的结果，将局部刻画转换为局部测试器）都非常不同。相反，我们的证明受到一种通过全局超契性 [31]建立此类结果的新方法的启发。

全局超契性是一种近期引入的工具，在研究非小集合扩张图时往往很有用。全局超契性的一个推论（在本质上与其等价）为图中所有边扩张与 1 保持一定距离的小集合提供了一种有用的刻画。对全局超契性的研究源于 2 对 2 游戏定理的证明 [29, 14, 13, 30], ，不过如今已知它对研究许多不同的问题都很有用（例如参见 [26, 27, 28, 31, 5,7, 6, 18]）。

下面，我们解释如何利用全局超契性方法证明局部可测试性结果。在第 1.6节中，我们解释如何将这一方法扩展到广义 Reed-Muller码的领域，以分析稀疏的 t-平坦测试器，并证明定理 1.1、1.2。

1.5.1 通过全局超契性对 Reed-Muller 码进行最优测试

在 [31], 中，作者将 Reed-Muller码的 t仿射子空间测试器的分析与仿射格拉斯曼图的扩张性质联系起来。这里，仿射格拉斯曼图是一个图，其顶点集由 $\mathbb{F}_q^n$中的所有t维仿射子空间组成；若两个顶点相交于一个 $t-1$ 维仿射子空间，则它们相邻。简而言之， [31] 的方法首先假设 t维仿射子空间测试器以至少 $1-\varepsilon$的概率接受 f

（将 ε 视为较小的量），然后证明测试器拒绝的 t维仿射子空间集合具有某种结构性结果：

$$S = \left\{ T \subseteq \mathbb{F}_q^n \mid \deg(f|_T) > d, T \text{ is a } t\text{-flat} \right\}.$$

具体而言，他们利用 [21] 中的一个引理证明，集合 S 在仿射格拉斯曼图中的扩张性质较差，并据此证明存在一个点 $x^\star \in \mathbb{F}_q^n$，使得当测试器选择一个包含 $x^\star$的子空间 T 时，几乎总是拒绝。这表明 f 在 $x^\star$ 处存在错误，应当进行修正；事实上，利用这一点， [31] 中设计了一种局部修正过程，证明可以改变 $x^\star$ 处 f的值，从而使接受概率增加 $q^{t-n-O(1)}$这一加性因子。重复这一论证，最终至多改变 f 在 $C(q) \cdot q^{-t}\varepsilon$ 比例的输入上的取值，并得到一个函数 f'，使测试器以概率 1 接受。这样的 f'次数至多为 d，因此可得 f 接近一个次数为 d 的多项式。

1.5.2 O通过全局超契性测试广义 Reed-Muller 码

尽管 [31] 的方法似乎更加稳健，因此有可能适用于分析更丰富的一类编码，但如何做到这一点并不完全显而易见。对于 t-仿射子空间测试器，可以将一个非常自然的图与该测试器关联起来，但在稀疏的 t-仿射子空间测试器的背景下（这正是我们所分析的测试器），这一点就远没有那么清晰。测试器所查询的输入模式不再是一个美观的子空间（但为了改进仿射子空间测试器的查询复杂度，这似乎是不可避免的）。

从高层次来看，我们证明了，解决这一问题的另一种方式是利用该码的对称变换，并在其上构造图。为此，我们必须将测试器视为“基本测试器”与该码对称变换群中的一个随机元素的复合。在我们的情形中，对称变换群是 $\mathbb{F}_q^n$ 上的仿射线性变换群，而事实证明，与对稀疏 t-仿射子空间测试器进行分析相关的图，就是所谓的仿射双线性方案图。

乍看之下，仿射线性变换似乎在本质上等同于仿射子空间（将仿射线性变换的像视为一个子空间），事实上，前一个图上的结果与后一个图上的结果之间确实存在许多联系。然而，仿射线性变换与仿射子空间之间的区别对我们至关重要。实际上，尽管两个仿射线性变换 A_1 和 A_2 可能具有相同的像，但测试器在选择 A_1 时与选择 A_2 时的表现却完全不同，因此我们必须在可靠性分析中充分利用这一差异。

1.6 我们的技术

本节将简要概述定理1.1证明所依据的技术。我们首先介绍 [33] 的稀疏$(s+t)$-仿射子空间测试器，然后以对称变换群的形式从一个略有不同的视角来审视它。之后，我们解释定理1.1 证明的总体策略，并说明与标准 t-仿射子空间测试器的分析相比，所面临的一些独特挑战。为便于表述，在本节余下部分我们聚焦于 $p = 2$ 的情形，并在第 2 节切换回一般的 p。

1.6.1 稀疏平坦测试器

[33]的稀疏平坦测试器构造始于以下观察。对于 $p = 2$ 情形，定义二元多项式 P： $\mathbb{F}_q^2 \to \mathbb{F}_q$ 通过

$$P(x_1, x_2) = \frac{-x_2^{q-1} + (x_1 + x_2)^{q-1}}{x_1} = \sum_{i=0}^{q-2} x_1^i x_2^{q-2-i}.$$

在 [33], 中，作者观察到 P 的以下两个关键性质，这使其有助于获得局部测试结果：

1. 稀疏支撑： P 的支撑大小至多为 $3q$；事实上，若 $x_1 + x_2 \neq 0$、 $x_1 \neq 0$ 和 $x_2 \neq 0$，则由费马小定理（$x_1 + x_2$）可得$^{q-1} = x_2^{q-1} = 1$ 和 $x_1 \neq 0$，因此 $P(x_1, x_2) = 0$。
2. 检测单项式 $x_1^{q-i} x_2^i$：考察 P 与单项式 M的内积，其定义为 $\langle P, M\rangle = \sum P(x_1, x_2)M(x_1, x_2)$。我们得到，若对 $i \in \{1, \ldots, q-1\}$ 有$M = x_1^{q-i} x_2^i$，则$_{x_1,\ x_2}\langle P, M\rangle \neq 0$。事实上，

$$\langle P, M\rangle = \sum_{j=0}^{q-2} \sum_{x_1} x_1^{q-i+j} \sum_{x_2} x_2^{q-2-j+i} = \sum_{j=0}^{q-2} (q-1)1_{q-i+j=q-1}(q-1)1_{q-2-j+i=q-1},$$

因此，我们只从 $j = i - 1$ 得到贡献，而且该贡献非零。对于任何其他单项式 M，类似的计算表明 $\langle P, M\rangle = 0$，因此，对函数 f与 P取内积，可以理解为检测 f 中是否存在某个形如 $x_1^{q-i} x_2^i$的单项式。

有鉴于此，下面给出稀疏测试器。文献 [33] 指出，要为广义 Reed-Muller 码设计局部测试器，只需设计一个检测器，判断某些典范单项式是否存在。令$d + 1 = s \cdot \frac{q}{2} + r$，其中 s 为偶数且 $r < q$，只需检测是否存在形如 $\prod_{i=1}^{s/2} x_{2i-1}^{q/2} x_{2i}^{q/2} \cdot \prod^{s+t} x_i^{e_i}$的单项式，其中 $\sum_{i=1}^{t} e_i \geqslant r$，且 t 为一个较小的常数（例如 $t = 10$）。利用上文中的 $P^{i=s+1}$，这类单项式的检测器可表示为

$$H_{e'}(x_1, \ldots, x_{s+t}) = P(x_1, x_2) \cdots P(x_{s-1}, x_s) \cdot M_{e'}(x_{s+1}, \ldots, x_{s+t}),$$

其中 $e' + e = (q-1, \ldots, q-1)$ 和 $M_{e'}(x_{s+1}, \ldots, x_{s+t}) = \prod_{i=s+1}^{s+t} x_i^{q-1-e_i}$。我们注意到， $H_{e'}$ 的次数大部分来自 P 的乘积，而次数中至多有 $t(q-1) - r$ 来自其余部分。由于 P的支撑相当稀疏，因此 $H_{e'}$ 的支撑也相当稀疏。更确切地说， $H_{e'}$的支撑大小至多为 $(3q)^{\frac{s}{2}+t}$，并且由于应将 t 视为较小，而 s 大致为 $2d/q$， $H_{e'}$ 的支撑大小大致为 $(3q)^{d/q}$。这带来了 $(3q)^{d/q}$ 的查询复杂度，比平坦测试器给出的 $q^{\lceil \frac{d}{q-q/p} \rceil} \approx q^{2d/q}$ 好二次方。

如前所述， [33] 中的可靠性分析依赖于来自 [25]的一个黑盒结果。他们设法证明，他们构造的检测器蕴含了一个具有相同查询复杂度的测试器，该测试器以 $\Omega((3q)^{-2(s/2+t)}\delta)$ 的概率拒绝那些与Reed-Muller 码字相差 δ的函数。要获得常数拒绝概率，必须将测试器重复 $(3q)^{2(s/2+t)}$ 次，这会大幅增加查询复杂度；更详细的讨论将在第 3 节中进行。

1.6.2 对称群视角

证明定理 1.1 的首要任务，是基于 [33] 中的思路设计一个测试器。这个测试器非常自然：

1. 随机选取一个仿射映射 $T\colon \mathbb{F}_q^{s+t} \to \mathbb{F}_q^n$；这里的 s 和 t 应当与上一节中的含义相同。我们要考察函数 $f \circ T$，但不会查询它的所有取值（事实上，查询所有取值就相当于 $(s+t)$-平坦测试器）。

2. 对于任意满足 $\sum_{i=1}^{t} q-1-e_i \geqslant r$ 的次数序列 $e = (e_{s+1}, \ldots, e_{s+t})$，取 H_e 并计算 $\langle f \circ T, H_e \rangle$。如果某个这样的次数序列对应的内积非零，则拒绝。否则，接受。

换言之，我们首先将 f 限制到一个随机的（$s+t$）维仿射子空间上，然后应用 [33] 的检测多项式。虽然我们会针对多个次数序列（最多到 q^t）进行测试，但我们将在第 3 节看到，H_e 的支撑在每种情况下都相同。因此，我们可以使用相同的 q^{s+t} 次查询来计算所有次数序列对应的内积。理解这个测试器的另一种方式是：我们利用 Reed-Muller码的对称变换群（仿射线性变换），测试器首先从该群中随机选取一个对称变换，取其限制，然后使用 [33] 的检测器。

1.6.3 仿射线性变换图及其分析

考虑到上述测试器，下一个问题是如何对其进行分析。在平坦测试器的情形下，我们有一个与测试器相关联的非常自然的图（仿射格拉斯曼图）。上述测试器似乎也与仿射子空间有关，因为仿射变换的像是一个仿射子空间；然而，二者之间存在一个关键且至关重要的区别。在上述测试器中，我们只会查看 f 在 Im(T)中少数几个位置处的值，因此，即使 T和 T' 具有相同的像，测试器对它们的表现也可能不同。这种缺乏对称性的特征对于测试的稀疏性至关重要，但也使得将一个图与该测试器关联起来的任务更加棘手。

为了对这个图的构造有一些直观认识，回想一下，在平坦测试器中，我们可以考虑适用于所有 t 的 t- 平坦测试器（不一定是最小的那个）。不同 t 对应的这些测试器之间的关系，在所有确立最优测试结果的工作中都起着关键作用。具体而言，我们知道，$(t+1)$-平坦测试器的拒绝概率至多是 q 倍的 t-平坦测试器的拒绝概率。稍后我们会详细说明这一性质（下文称为“影子引理”）。考察各种测试器的另一个好处是，我们可以通过在这些测试器之间进行上-下游走，自然而然地构造出仿射格拉斯曼图。要得到仿射格拉斯曼图的边，可以从一个 t-仿射子空间出发，向上走到一个包含它的 $(t+1)$-仿射子空间，然后再向下走到一个包含于该 $(t+1)$-仿射子空间中的 t-仿射子空间。那么，在稀疏平坦测试器的背景下，这种操作的恰当对应形式是什么?

向上提升。上述讨论表明，可以为更高维度寻找上述测试器的类似版本，而向上步骤也有一个显而易见的自然对应：对于任意 $r \geqslant 0$，我们可以考察 $(s+t+r)$ 稀疏平坦测试器，其中随机选取一个仿射映射 $T\colon \mathbb{F}_q^{s+t+r} \to \mathbb{F}_q^n$，并像上文那样，对所有可行的度序列（但变量更多）执行测试器。因此，从 $(s+t)$ 稀疏平坦测试器开始，并将仿射映射 T 视为一个在 $\mathbb{F}_q$ 上、形如 $(n \times (s+t))$ 的矩阵，并带有仿射平移 $c \in \mathbb{F}_q^n$，我们可以通过随机选取向量 $w \in \mathbb{F}_q^n$，并考察与如下矩阵对应的仿射变换 A，来“向上”得到 $(s+t+1)$ 稀疏平坦测试器：该矩阵的列与 T的列相同，只是将w 追加为最后一列。与平坦测试器类似，不难发现，如果 $(s+t)$ 稀疏平坦测试器在选取 T时拒绝，那么 $(s+t+1)$ 稀疏平坦测试器在选取 A时也会拒绝。

向下进行。“向下进行”这一步同样简单，但要阐明其动机则稍微困难一些。受平坦测试器的启发，人们可能会想对 A 的列进行某种线性重排，然后“丢弃”其中一列。不过，这似乎行不通，因为这样做会导致一个 T'，其中性能表现

稀疏平坦测试器的性能似乎与 T“完全无关”（从其在 T' 中查看的点集通常与其在 T 中查看的点集不相交这一意义上而言）。

因此，向下时，我们希望采用一种方式，使 T' 和 T 在许多点上相等。一个自然的尝试是应用来自 R 的仿射变换：$\mathbb{F}_q^{s+t+1} \to \mathbb{F}_q^{s+t}$ 到 A，该变换固定一个余维 1 子空间。在这种情况下，输出 $T' = A \circ R$，并且 T' 在 R 所固定的余维 1 子空间上与 A 相等。另一方面，根据构造，T 也在一个余维 1 子空间上与 A 相等——具体来说，就是最后一个坐标等于 0 的子空间。因此，向下这一步之后，我们得到 T'，它在一个维数为 $s+t$ 的子空间上与 T 相等——在仍与 T 不同的前提下，这基本上是所能做到的最相似的情况。

换句话说，要从 $(s+t+1)$ 稀疏平坦测试器向下到 $(s+t)$ 稀疏平坦测试器，我们通过均匀且独立地选取 b_1、……、b_{s+t}、$b_{s+t+1} \in \mathbb{F}_q$，并取对应于如下矩阵的仿射变换 T'：其第 i 列为 $\mathsf{col}_i(T) + b_i \mathsf{col}_{s+t+1}(T)$，平移量为 $c + b_{s+t+1} u$。也就是说，我们删去最后一列，同时将它的一个随机倍数加到 T 的其他每一列上。

先上升再下降。将这两个操作拼接起来，就得到一个图，其顶点集为仿射线性变换 T：$\mathbb{F}_q^{s+t} \to \mathbb{F}_q^n$，其边与仿射格拉斯曼图在本质上非常相似；这个图称为双线性方案图。我们的分析核心依赖于 3 个组成部分：

1. 关联测试器的性能与该图上的扩张（影子引理），并证明测试器拒绝的 T 集合的边扩张至多为 $1 - 1/q$。2. 研究该图中扩张至多为 $1 - 1/q$ 的集合的结构，并证明它们必然具有某种强局部结构。3. 利用上述局部结构进行纠错论证，证明如果稀疏平坦测试器以较小的概率拒绝，那么 f 接近某个 Reed-Muller 码字。

1.6.4 影子引理

影子引理是一项断言 $(s+t+1)$ 测试器与 $(s+t)$ 测试器的拒绝概率之间存在关系的结果。

平坦测试器的影子引理。在平坦测试器的语境下，该引理断言，测试器拒绝的维数为 $(s+t+1)$ 的仿射子空间所占比例，至多为 q 乘以测试器拒绝的 $(s+t)$ 维仿射子空间所占比例。该结果名称的由来是：令 S 为测试器拒绝的 $(s+t)$ 维仿射子空间的集合，那么测试器拒绝的 $(s+t+1)$ 维仿射子空间集合恰好是 S 的上影：

$$S^{\uparrow} = \{A \subseteq \mathbb{F}_q^n \mid \mathsf{dim}(A) = s+t+1, \exists B \in S, B \subseteq A\}.$$

这意味着，平均而言，元素 $A \in S^{\uparrow}$ 的子集 $B \subseteq A$ 中有 $1/q$ 个属于 S；将仿射格拉斯曼图中的一条边视为一次上-下步，我们得到，从 S 出发的随机步到达 S 以外顶点的概率至多为 $1 - 1/q$。也就是说，S 的边扩张定义为

$$\Phi(S) = \frac{|\{e = (A, A') \in E \mid A, A' \in S\}|}{|\{e = (A, A') \in E \mid A \in S\}|},$$

至多为 $1 - \frac{1}{q}$。

稀疏平面测试器的影子引理。在稀疏平坦测试器的背景下，我们希望论证类似的结论也成立。为此，固定函数 $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$，我们定义

$$S = \{T\colon \mathbb{F}_q^{s+t} \to \mathbb{F}_q^n \mid \text{the sparse flat tester rejects when choosing } T\}.$$

由于上行和下行步骤之间存在不对称性，因此没有明确对应于 S 的上影的概念。不过，以下结论仍然成立：如果 $T \in S$，并且我们将某个向量 $u \in \mathbb{F}_q^n$ 追加到 T，以构成仿射映射 $R\colon \mathbb{F}_q^{s+t+1} \to \mathbb{F}_q^n$，那么稀疏（$s+t+1$）测试器会拒绝 R，因此定义.....是有意义的。

$$S^{\uparrow} = \{R\colon \mathbb{F}_q^{s+t+1} \to \mathbb{F}_q^n \mid \text{the sparse flat tester rejects when choosing } R\}.$$

我们证明，从 $R \in S^{\uparrow}$ 出发并向下移动至 $T'\colon \mathbb{F}_q^{s+t+1} \to \mathbb{F}_q^n$ 后，稀疏平坦测试器仍以至少 $1/q$ 的概率拒绝，因此 $T' \in S$。特别地，我们得出 $\mu(S^{\uparrow}) \leqslant q\mu(S)$（其中 $\mu(S)$ 表示 S 的大小与从 $\mathbb{F}_q^{s+t}$ 到 $\mathbb{F}_q^n$ 的仿射映射总数之比，而 $\mu(S^{\uparrow})$ 的定义类似）。利用与之前相同的推理，我们得出 $\Phi(S) \leqslant 1 - \frac{1}{q}$，其中这里的边扩张是相对于双线性方案图来测度的。

1.6.5 双线性方案图上的扩张

基于这样的理解：S 是一个小集合（因为我们假设稀疏平坦测试器以很小的概率拒绝），并且 $\Phi(S) \leqslant 1 - \frac{1}{q}$，下一个问题是，这意味着什么样的结构。在双线性方案图中，有这类集合的自然例子，它们类似于子空间背景下的缩入/缩出集合。粗略地说，有一类直观上应该与我们相关的例子，即缩入集合：

$$\mathcal{C}_{x^\star, y^\star} = \{T\colon \mathbb{F}_q^{s+t} \to \mathbb{F}_q^n \mid T(x^\star) = y^\star\}.$$

双线性方案图中还有其他扩张性较差的小集合示例，不过这些示例在当前语境下似乎“无关”。事实上，在证明我们的小集合 S 与这些其他示例都不相关之后（这种性质通常称为相对于线性部分上的缩出集和放大集合的伪随机性），我们利用全局超契性理论证明，必定存在 $x^\star$ 和 $y^\star$，使得 $\mu(S \cap \mathcal{C}_{x^\star,\ y^\star}) \geqslant (1 - o(1))\mu(\mathcal{C}_{x^\star,\ y^\star})$。换言之，稀疏的（$s+t$）平坦测试器在 $\mathcal{C}_{x^\star,\ y^\star}$ 内几乎总是拒绝。

我们指出，证明 S 与双线性方案中的任何其他非扩张集合都没有“相关性”颇为棘手，而本文当前的大量工作都致力于此。为此，我们必须借鉴 [31] 中的思想，并利用一个新的关系：在 a˜函数 f 上应用稀疏（$s+t$）平坦测试器，与在相关函数 f 上应用 t-平坦测试器之间的关系。由于构造这个相关函数在某种程度上较为技术性，我们将其详细讨论推迟到第 3.5 节。

1.6.6 通过局部修正完成证明

直观地说，S 能够在某个 $\mathcal{C}_{x^\star, y^\star}$ 内部稠密的唯一方式，就是我们从一个 Reed-Muller 码字 g开始，并在少量输入上对其进行扰动，其中 $y^\star$ 就是其中之一。确实，在这种情况下，对于所有 $T \in \mathcal{C}_{x^\star,\ y^\star}$ 以及测试器在扰动前检查的指数向量 e，我们都会有 $\langle g \circ T, H_e \rangle = 0$；而在 $y^\star$处改变 g 的值后，我们也会改变 $x^\star$处 $g \circ T$的值，从而破坏之前的等式。这一直觉表明，$y^\star$ 是一个应当修正 f 的点，以便更接近一个 Reed-Muller 码字，而我们证明事实确实如此。

当深入检查这一论证时，会出现几个困难。如果 $H_e(x^\star) = 0$，那么上述推理就会失效（因为 f 在 $y^\star$ 处的值会乘以 0）；然而，在这种情况下，认为 S 能在$\mathcal{C}_{x^\star,y^\star}$ 内部具有很高的密度是没有意义的（因为内积中包含的 f 的实质上唯一输入是 $f(y^\star)$，但无论如何它都会乘以 $H_e(x^\star) = 0$）。事实上，在我们的论证中，我们证明了如果 S 在 $\mathcal{C}_{x^\star,y^\star}$ 中具有很高的密度，那么必然有 $H_e(x^\star) \neq 0$。此外，我们证明了，对于 H_e的支撑中的所有 $x^\star$ 和 $x^{\star\prime}$，S 在 $\mathcal{C}_{x^\star,y^\star}$ 内部的密度与其在 $\mathcal{C}_{x^{\star\prime},y^\star}$ 内部的密度大致相同。最后这一步对于使分析得以进行至关重要，并且要求我们调整并强化来自 [31] 的技术。在这一步结束时，粗略地说，我们得出结论：每当测试器查询 f 在 $y^\star$ 处的值时，它以接近 1 的概率拒绝。

论证的最后一步是证明，我们可以将 f 在 $y^\star$ 处的值改掉，并使测试器的拒绝概率减少一个加法量 $\Theta(q^{s+t-n})$（该量与测试器查看 $y^\star$ 的概率成正比）。我们通过将问题归约到标准平坦测试器上的同一问题来实现这一点（该问题已在 [31] 中解决）。其思路是考察一个维数为 $s + t + 100$ 的稍大测试器，固定前 s 个坐标并让其余坐标变化，从而使该测试器成为标准平坦测试器的局部版本。

据此并迭代论证，我们最终得到一个函数 f'，它与 f 至多在 $\Theta(\varepsilon/q^{s+t-n})$ 比例的输入上不同（其中 ε 是原始拒绝概率），且以概率 1 通过测试。因此，f' 是一个 Reed-Muller 码字，所以 f 与某个 Reed-Muller 码字的距离为 $O(\varepsilon/Q)$。

2 预备知识

记号。对于整数 n，我们记 $[n] = \{1, \ldots, n\}$。对于素数幂 q，令 $\mathbb{F}_q$ 为大小为 q 的域，并用 $\mathbb{F}_q^* \subseteq \mathbb{F}_q$ 表示其中非零元素的集合。

2.1 域的基本事实

通篇滥用记号，我们将 Reed-Muller码 $\mathrm{RM}[n, q, d]$ 定义为定义在 $\mathbb{F}_q^n$上的函数集合，这些函数可以表示为次数至多为 d 的多项式。今后固定 d 并记

$$d + 1 = \ell \cdot p(q - q/p) + r = s(q - q/p) + r,$$

其中我们令 $s = \ell \cdot p$，且 $0 < r \leqslant p(q - q/p)$。

我们将需要一些基本事实。首先，众所周知，$\mathbb{F}_q^*$ 具有一个乘法生成元，我们通常将其记为 γ。下面的引理利用乘法生成元的存在性来估计关于$\mathbb{F}_q$的和。

引理 2.1. 对于任意素数幂 q和整数 $i \in \{0, \ldots, q - 1\}$,

$$\sum_{\alpha \in \mathbb{F}_q} \alpha^i = \begin{cases} -1, & \text{if } i = q - 1, \\ 0, & \text{otherwise}. \end{cases}$$

证明。如果 $i = q-1$，那么对于所有 $\alpha \neq 0$，$\alpha^i = 1$，而 $0^i = 0$。因此，该和是将 1相加 $q-1$ 次，这在 $\mathbb{F}_q$中为 -1。对于 $i \in \{1, \ldots, q - 2\}$，回忆一下，$\mathbb{F}_q^*$有一个生成元 γ。也就是说，$\mathbb{F}_q^* = \{1, \gamma, \ldots, \gamma^{q-2}\}$。由于 $\gamma^i \neq 1$，我们可以写出

$$\sum_{\alpha \in \mathbb{F}_q} \alpha^i = \sum_{j=0}^{q-2} (\gamma^i)^j = \frac{(\gamma^i)^{q-1} - 1}{\gamma^i - 1} = \frac{1 - 1}{\gamma^i - 1} = 0.$$

另一方面，如果 $i = 0$，那么引理左侧的和等于 $\sum_{\alpha\in\mathbb{F}_q} \alpha^0 = \sum_{\alpha\in\mathbb{F}_q} 1 = q = 0$。

□

2.2 域上的函数

给定两个函数 f, g: $\mathbb{F}_q^n \to \mathbb{F}_q$，我们用归一化汉明距离来度量它们之间的距离，即

$$\delta(f,g) = \Pr_{x\in\mathbb{F}_q^n}[f(x) \neq g(x)].$$

函数 f: $\mathbb{F}_q^n \to \mathbb{F}_q$到 Reed-Muller码 RM$[n,q,d]$的距离记为 $\delta_d(f)$，定义为 f 与某个函数 $g \in$ RM $[n,q,d]$之间的最小距离。也就是说，

$$\delta_d(f) = \min_{g\in\mathrm{RM}[n,q,d]} \delta(f,g) = \min_{g\in\mathrm{RM}[n,q,d]} \Pr_{x\in\mathbb{F}_q^n}[f(x) \neq g(x)].$$

对于两个函数 f, g: $\mathbb{F}_q^n \to \mathbb{F}_q$，定义它们的内积为

$$\langle f, g\rangle = \sum_{v\in\mathbb{F}_q^n} f(v)g(v).$$

显然，这个内积是双线性的。单项式是 $\mathbb{F}_q$上所有多项式的基本构成单元，以下记号将便于我们使用：

定义 1. 对于指数向量 $e \in \{0,\ldots,q-1\}^n$，我们定义单项式 $x^e = \prod_{i=1}^n x^e$ $_i{}^i$

下一个引理使我们能够计算单项式之间的内积：

引理 2.2. 对于 e、$e' \in \{0,\ldots,q-1\}^n$，我们有

$$\langle x^e, x^{e'}\rangle = \begin{cases} (-1)^n, & \textit{if } e+e' = (q-1,\ldots,q-1), \\ 0, & \textit{otherwise}. \end{cases}$$

证明。令 $e'' = e + e'$。根据定义

$$\langle x^e, x^{e'}\rangle = \sum_{(\alpha_1,\ldots,\alpha_n)\in\mathbb{F}_q^n} \prod_{i=1}^n \alpha_i^{e_i} = \prod_{i=1}^n \sum_{\alpha\in\mathbb{F}_q} \alpha^{e_i''}.$$

该结果由引理 2.1 得出。 □

2.3 仿射线性变换与仿射双线性方案

本节介绍仿射双线性方案，该方案在我们的论证中发挥着至关重要的作用。

定义 2。我们用 $\mathcal{T}_{n,\ell}$ 表示仿射变换 T: $\mathbb{F}_q^\ell \to \mathbb{F}_q^n$ 的集合。

每个仿射变换 $T \in \mathcal{T}_{n,\ell}$ 都由一个线性部分 $M \in \mathbb{F}_q^{n\times\ell}$和一个平移 $c \in \mathbb{F}_q^n$组成。我们采用记法 $T = (M, c)$，表示 T是满足条件 $Tx = Mx + c$（对 $x \in \mathbb{F}_q^\ell$成立）的仿射变换。换言之，M是 T 的线性部分，而 c是仿射平移。需要强调的是，仿射变换 $T \in \mathcal{T}_{n,\ell}$ 不一定是满秩的。

定义 3。集合 $S \subseteq \mathcal{T}_{n,\ell}$ 的密度定义为 $\mu_\ell(S) = \frac{|S|}{|\mathcal{T}_{n,\ell}|}$。

通常，如果上下文足够清楚，我们会省略下标 ℓ。我们的分析需要将仿射变换视为某个适当测试图的顶点。例如，对于（标准） t 仿射子空间测试，该图是仿射格拉斯曼图 AffGras(n, t)。图的顶点是 $\mathbb{F}_q^n$ 中所有 t 维仿射子空间；如果两个顶点 U_1 和 U_2 相交于一个 $(t-1)$ 维仿射子空间，即 $\dim(U_1 \cap U_2) = t-1$，则它们相邻。下面我们定义仿射变换上的一种类似图结构，称为仿射双线性方案图。

定义4。仿射双线性方案图，AffBilin(n, ℓ)，其顶点集为$\mathcal{T}_{n,\ell}$。两个顶点 T_1、$T_2 \in \mathcal{T}_{n,\ell}$ 当且仅当它们在一个 $\ell-1$ 维仿射子空间上相等时相邻相邻。该条件也可以写为 $\dim(\ker(T_1 - T_2)) \geqslant \ell - 1$。

用 $T_1 \sim T_2$ 表示邻接。我们指出，仿射格拉斯曼图可以通过将每个 $T_1 \in \mathcal{T}_{n,\ell}$ 与其像（即，在某种群运算下对集合 $\mathcal{T}_{n,\ell}$ 取闭包）视为相同而从仿射双线性方案中得到；然而，正如引言中所解释的，这一区别对我们至关重要。

2.4 仿射双线性方案中的扩张与伪随机性

我们将使用标准的边扩张概念，其定义如下。

定义 5. 对于正则图 $G = (V, E)$ 和顶点集 $S \subseteq V$，我们将 S 的边扩张定义为

$$\Phi(S) = \Pr_{\substack{u \in S \\ (u,v) \in E}} [v \notin S].$$

用文字来说， S 的边扩张是在 G 上进行随机游走时，一步之内离开它的概率。

我们将用 $\Phi_{n,\ell}$ 表示 AffBilin(n, ℓ) 上的边扩张。当从上下文中可以明确 n 和 ℓ 时，我们省略下标。在本文后文中，我们还将考虑仿射格拉斯曼图 AffGras(n, ℓ) 上的边扩张；稍微滥用记号，我们也用 $\Phi_{n,\ell}$ 表示该图上的边扩张，具体指哪个图将由上下文明确。

2.4.1 随机游走的向上-向下视角

考虑以下等价的两步过程，有助于我们对仿射双线性方案图中的$T_1 = (M_1, c_1) \in \mathcal{T}_{n,\ell}$ 进行邻居采样：

1. 向上：随机选择一个 $w \neq 0$。令 M' 为将 w 作为新列附加到 M_1后得到的矩阵，并且 $T' = (M', c) \in \mathcal{T}_{n,\ell+1}$.
2. 向下：随机选择一个 $R = (A, b) \in \mathcal{T}_{\ell+1,\ell}$，其中 A 的前 ℓ 行是单位矩阵， b 的前 ℓ 个元素均为 0，并且 A 的最后一行中的元素与 b 的最后一个元素中至少有一个非零。
3. 输出 $T_2 = T' \circ R$。

容易看出，对于 $T_2 = (M_2, c_2)$， M_2 的每一列都等于 M_1 中相应的列加上 w 的某个倍数，对于 c_2 和 c_1 也是如此。

2.4.2 仿射双线性方案中的非扩张集合

正如引言中所解释的，我们的证明将测试所拒绝的仿射变换集合 $\mathcal{S}$ 视为仿射双线性方案图中的顶点集合。我们证明， $\mathcal{S}$ 在该图中具有较小的边扩张，然后利用全局超契性来推导出关于$\mathcal{S}$结构的一些结论，而这反过来有助于进行局部纠正论证。

为了便于论证，我们必须先了解 AffBilin(n,ℓ) 中几个典型非扩张集合的结构。在仿射格拉斯曼图中，有以下几个例子：

- 放大： $\mathcal{D}_a = \{U \in \text{AffGras}(n,\ell) \mid a \in U\}$，其中 $a \in \mathbb{F}_q^n$。
- 缩出集： $\mathcal{D}_W = \{U \in \text{AffGras}(n,\ell) \mid U \subseteq W\}$，其中 $W \subseteq \mathbb{F}_q^n$ 是一个超平面。
- 线性部分上的放大： $\mathcal{D}_{a,\ \text{线性}} = \{U = z + V \in \text{AffGras}(n,\ell) \mid a \in V\}$，其中 $a \in \mathbb{F}_q^n$。
- 线性部分上的缩出集： $\mathcal{D}_{W,\ \text{线性}} = \{U = z + V \in \text{AffGras}(n,\ell) \mid V \subseteq W\}$，其中 $W \subseteq \mathbb{F}_q^n$ 是一个超平面。

不难看出，每个例子的扩张至多为 $1 - 1/q$；此外，简单计算可知，这些集合中每一个的密度都很小（如果 ℓ 远小于 n，且二者都趋于无穷大，则密度趋于零）。这些例子在 AffBilin(n,ℓ) 中也各有对应：

- 放大： $\mathcal{C}_{a,b} = \{T \in \mathcal{T}_{n,\ell} : \ T(a) = b\}$，其中 $a \in \mathbb{F}_q^\ell$ 和 $b \in \mathbb{F}_q^n$。
- 缩出集： $\mathcal{C}_{a^T,b,\beta} = \{(M,c) \in \mathcal{T}_{n,\ell} : \ a^T \cdot M = b,\ a^T \cdot c = \beta\}$，其中 $a \in \mathbb{F}_q^n, b \in \mathbb{F}_q^\ell$ 和 $\beta \in \mathbb{F}_q$。
- 线性部分上的放大： $\mathcal{C}_{a,b,\text{lin}} = \{(M,c) \in \mathcal{T}_{n,\ell} : \ M \cdot a = b\}$，其中 $a \in \mathbb{F}_q^\ell$ 和 $b \in \mathbb{F}_q^n$。
- 线性部分上的缩出集： $\mathcal{C}_{a^T,\ b,\ \text{lin}} = \{(M,c) \in \mathcal{T}_{n,\ \ell} : \ a^T \cdot M = b\}$，对于 a、 $\in \mathbb{F}_q^n$和$b \in \mathbb{F}_q^\ell$。

同样可以验证，这里的每个例子在 AffBilin(n,ℓ) 中的扩张至多为 $1 - 1/q$。我们的论证需要证明，从某种意义上说，这些例子穷尽了 AffBilin(n,ℓ) 中所有边扩张至多为 $1 - 1/q$ 的小顶点集合。为此，我们首先定义伪随机性的概念。直观地说，若集合 S 相对于某个例子（例如缩入集）是伪随机的，就意味着 S 与$\mathcal{C}_{a,\ b}$们的相关性很弱，也就是说，S 在这类集合中的密度仍然很小。更精确地说：

定义 6. 设 $\mathcal{S} \subseteq \mathcal{T}_{n,\ \ell}$，并设 $\xi \in [0,1]$。

1. 我们称 $\mathcal{S}$ 关于缩入是 ξ-伪随机的，如果对于每个 $a \in \mathbb{F}_q^\ell$ 和 $b \in \mathbb{F}_q^n$，都有

$$\mu(\mathcal{S}_{a,b}) := \Pr_{T \in \mathcal{C}_{a,b}}[T \in \mathcal{S}] \leqslant \xi.$$

2. 我们称 $\mathcal{S}$ 关于缩出是 ξ-伪随机的，如果对于每个 $a \in \mathbb{F}_q^n$、 $b \in \mathbb{F}_q^\ell$和 $\beta \in \mathbb{F}_q$，都有

$$\mu(\mathcal{S}_{a^T,b,\beta}) := \Pr_{T \in \mathcal{C}_{a^T,b,\beta}}[T \in \mathcal{S}] \leqslant \xi.$$

3. 如果对于每个 $a \in \mathbb{F}_q^\ell$ 和 $b \in \mathbb{F}_q^n$，都有.....，我们就称 $\mathcal{S}$ 关于线性部分上的缩入是 ξ-伪随机的。

$$\mu(\mathcal{S}_{a,b,\text{lin}}) := \Pr_{T \in \mathcal{C}_{a,b,\text{lin}}}[T \in \mathcal{S}] \leqslant \xi.$$

4. 如果对于每个 $a \in \mathbb{F}_q^n$、$b \in$ 和 $\mathbb{F}_q^\ell$，都有.....，我们就称 $\mathcal{S}$ 关于线性部分上的缩出集是 ξ-伪随机的。

$$\mu(\mathcal{S}_{a^T,b,\mathrm{lin}}) := \Pr_{T \in \mathcal{C}_{a^T,b,\mathrm{lin}}}[T \in \mathcal{S}] \leqslant \xi.$$

通常，全局超契性结果表明，一个扩张被限制在远离1 的小集合不可能是伪随机的（其中伪随机性的概念与此相同，但稍微复杂一些；例如参见 [13, 29]）。然而，对于编码理论中的结果，似乎需要一种有所不同（但又密切相关）的结果 [31]。直观地说，在这类结果中，对集合 $\mathcal{S}$ 的扩张所作的假设要强得多，粗略地说，它断言 $\mathcal{S}$ 的扩张几乎“尽可能小”。作为这一强假设的交换条件，人们通常会要求关于集合 $\mathcal{S}$的非伪随机性的更强结论。例如，在 [31] 中证明了：一个顶点集合 $\mathcal{S}$，其扩张至多为 $1 - 1/q$，并且相对于上述三类例子是高度伪随机的，则它相对于第四类必定是高度非伪随机的，其含义是它几乎包含这样一个集合的副本。对于我们的目的，我们需要关于 AffBilin(n, ℓ)的一个类似陈述，即以下陈述：

定理 2.1。如果$\mathcal{S} \subseteq \mathcal{T}_{n,\ \ell}$ 满足

1. $\mu(\mathcal{S}) \leqslant \xi$，2. $\mathcal{S}$ 关于缩出、在线性部分上的缩出以及在线性部分上的缩入是 ξ-伪随机的，

3. $1 - \Phi(\mathcal{A}) \geqslant \frac{1}{q}$.

那么存在$a \in \mathbb{F}_q^\ell$ 和$b \in \mathbb{F}_q^n$，使得 $\mu(\mathcal{S}_{a,\ b}) \geqslant 1 - \ ^1\!/_{(q-1)^2} - \frac{q^3}{q-1}\left(4q^{-\ell} + 867\xi^{1/4}\right)$，其中 $\mu(\mathcal{S}_{a,\ b})$是 $\mathcal{S}$ 在$\mathcal{C}_{a,\ b}$中的密度。

证明。证明通过归约到仿射格拉斯曼图上的一个类似结果来完成，使用了来自 [9], 的思想，详细内容推迟到附录 A。 □

3 Reed-Muller 码的局部测试器

现在我们正式介绍稀疏平坦测试和完整平坦测试。虽然我们主要关注稀疏测试，但有时将问题归约到完整测试会便于分析。

3.1 t-仿射子空间测试器与内积视角

从整体上看，t-仿射子空间测试和平坦稀疏（$s + t$）测试都可以用以下方式描述：

1. 限制：随机选择一个 $T \in \mathcal{T}_{n,\ t}$ 其中维数 t 取适当值。

2. 对限制进行局部测试：检查 t 元函数 $f \circ T$ 是否确实具有 d 次数。如果是，则接受；否则拒绝。

两种测试的区别在于步骤 2 中如何进行“检查”。最直接的检查方法是在 $\mathbb{F}_q^t$ 中的所有点上查询 $f \circ T$，插值出 $f \circ T$，并检查其次数。事实上，这正是 t- 仿射子空间测试的定义。在这种情况下，很容易看出测试结果只取决于 T 的像；这是因为对于任意满秩 $A \in \mathcal{T}_{t,\ t}$，$f \circ T \circ A$ 和 $f \circ T$ 的次数相同。因此，t- 仿射子空间测试可以改写成大家熟悉的形式如下：

1. 随机选择一个 t-仿射子空间 $U \subseteq \mathbb{F}_q^n$。

2. 当且仅当 $\deg(f|_U) \leqslant d$ 时接受。

然而，还有其他方法可以尝试测试 $f \circ T$ 的次数是否至多为 d。其中一种方法是利用引理 2.2，通过计算内积来检查 f 中是否存在某些高次单项式。一种简单的做法如下：

如果接受 and only if $\langle f \circ T, x^e \rangle = 0$ for all $e \in \{0, \ldots, q-1\}^t$ such that $\sum_{i=1}^t q - 1 - e_i > d$.

根据引理 2.2，不难看出，该条件等价于 $\deg(f \circ T) \leqslant d$。此外，显然，计算所有内积都需要查询某个所用 x^e 的支撑中的每个点；本例中，该对象是 $\mathbb{F}_q^t$。因此，与所有这些单项式求内积并不能降低查询复杂度。

事实证明，还有一些更巧妙的“测试多项式”选择（并非单项式），能够据此设计出一种查询效率更高的内积测试。[33] 运用了这一思路，提出了稀疏的（$s+t$）仿射子空间测试，我们将在下一小节正式介绍。

3.2 稀疏 $(s+t)$-仿射子空间测试

我们对稀疏 $(s+t)$-仿射子空间的介绍与 [33], 中的略有不同，而这种观点对于我们的分析是必要的。回忆一下，我们写作 $d+1 = s\cdot(q-q/p)+r$，其中 s 可被 p 整除，且 $0 < r \leqslant p(q-q/p)$。对于向量 $x = (x_1, \ldots, x_p)$ 和集合 $I \subseteq \{1, \ldots, p\}$，记作 $x_I = \sum_{i \in I} x_i$。定义 p 元多项式

$$P(x_1, \ldots, x_p) = \frac{\sum_{I \subseteq [p-1]} (-1)^{|I|+1} (x_I + x_p)^{q-1}}{x_1 \cdots x_{p-1}}.$$

对于任意度序列 $e = (e_1, \ldots, e_t) \in [q]^t$，定义

$$M_e(x_1, \ldots, x_t) = \prod_{i=1}^t x_i^{e_i}, \qquad H_e(x) = \left(\prod_{i=1}^{s/p} P(x_{p(i-1)+1}, \ldots, x_{pi}) \right) M_e(x_{s+1}, \ldots, x_{s+t}).$$

稀疏 $(s+t)$-仿射子空间测试器的工作方式如下：

1. 随机选取一个仿射变换 $T\colon \mathbb{F}_q^n \to \mathbb{F}_q^{s+t}$。

2. Accept if and only if, $\langle f \circ T, H_e \rangle = 0$ for all $e \in \{0, \ldots, q-1\}^t$ such that $\sum_{i=1}^t e_i \leqslant t(q-1) - r$.

回忆一下，我们将参数 t 设为 $t = \max(p+2, 10)$。从本质上说，t 只需足够大，使得步骤 2 中的度序列能够涵盖次数最高为 $r+q-1$ 的单项式。

我们将满足步骤 2 中不等式的度序列 e 称为有效度序列。由于 d 始终固定，有效度序列的概念在全文中也不会改变。因此，若对于某个有效的 e，有 $\langle f \circ T、 H_e \rangle \neq 0$，我们称 T拒绝 f，或称 $f \circ T$ 被拒绝。否则，我们称 T接受 f，或称 $f \circ T$被接受。我们将测试器拒绝的 T's 构成的集合定义为 $\mathcal{S}_t$：

$$\mathcal{S}_t = \left\{ T \in \mathsf{AffBilin}(n, s+t) \mid \langle f \circ T, H_e \rangle \neq 0 \text{ for some } e \in \{0, \ldots, q-1\}^t \text{ such that } \sum_{i=1}^t e_i \leqslant t(q-1) - r \right\}, \tag{1}$$

并令 $\mathrm{rej}_{s+t}(f)$ 表示测试拒绝的概率。显然，我们有 $\mathrm{rej}_{s+t}(f) = \mu_{s+t}(\mathcal{S}_t)$

3.3 假设 n 足够大

本节我们将说明，不失一般性，我们可以假设 $n \geqslant s+t+100$。事实上，我们可以将一个 n 元函数 f 视为某些 N 个变量上的函数，其中 $N = O(n)$ 足够大。将此函数记为 $g\colon\ \mathbb{F}_q^N \to \mathbb{F}_q$，并对任意 $a \in \mathbb{F}_q^n, b \in \mathbb{F}_q^{N-n}$，定义为 $g(a,b) = f(a)$。我们证明$\delta(f, \mathrm{RM}[n,q,d]) = \delta(g, \mathrm{RM}[N,q,d])$，这意味着我们可以将测试视为在 g 上进行，同时仍使定理 1.1 中的 δ 为 $\delta(f, \mathrm{RM}[n,q,d])$。

Lem命题 3.1. 令 f 和 g 如上所定义。则 $\delta(f, \mathrm{RM}[n,q,d]) = \delta(g, \mathrm{RM}[N,q,\quad d])$.

证明。我们首先证明 $\delta(f,\mathrm{RM}[n,q,d]) \geqslant \delta(g, \mathrm{RM}[N,q,d])$。假设 $h\colon\ \mathbb{F}_q^n \to \mathbb{F}_q$是次数为 d的函数，使得 $\delta(f, h) = \delta(f,\mathrm{RM}[n,q,d])$。将 h扩展为 N个变量的函数（方式与定义 g相同），记为 h'。令 $h'(\cdot,b)$表示这样一个 N元函数，其中最后 $N-n$ 个变量均被设为$b \in \mathbb{F}_q^{N-n}$。类似地定义 $g(\cdot,b)$。注意，对于任意 b，$h'(\cdot,b) = h$，$g(\cdot,b) = f$。于是我们有

$$\delta(h',g) = \mathop{\mathbb{E}}_{b\in\mathbb{F}_q^{N-n}} \left[\delta\left(h'(\cdot,b), g(\cdot,b)\right)\right] = \mathop{\mathbb{E}}_{b\in\mathbb{F}_q^{N-n}} [\delta(h,f)] = \delta(f, \mathrm{RM}[n,q,d]).$$

由于 hi s的次数为 d，h' 也是如此，因此上述内容意味着 $\delta(f, \mathrm{RM}[n,q,d]) \geqslant \delta(g, \mathrm{RM}[2n,q,d])$.

对于另一个方向，假设 h' 是次数为 d 的 N 元函数，满足 $\delta(g, \mathrm{RM}[N,q,d])$ =$\delta(g,h')$。沿用上文的记号，我们有waswo

$$\mathop{\mathbb{E}}_{b\in\mathbb{F}_q^{N-n}} [\delta\left(g(\cdot,b), h'(\cdot,b)\right)] = \delta(g,h') = \delta(g, \mathrm{RM}[N,q,d]).$$

因此，存在一个 b 的选择，使得

$$\delta\left(f, h'(\cdot,b)\right) = \delta\left(g(\cdot,b), h'(\cdot,b)\right) = \delta(g, \mathrm{RM}[N,q,d]).$$

由于 h' 是 d 次的，因此 $h'(\cdot,b)$ 也必须是 d 次的，所以由上述不等式可得 $\delta(f, \mathrm{RM}[n,q,d])$ 6$\delta(g,$ $\mathrm{RM}[N,q,d])$，证明完毕。 □

利用这个引理，我们总可以将测试视为在 g 上进行，而不是在 f 上进行，并证明稀疏的 $s+t$-仿射子空间测试以至少 $c(q)\min(1, Q\delta(g, \mathrm{RM}[N,q,d]))$ 的概率拒绝。其中 Q 是查询次数，而 $c(q)$ 是某个 ^{1} $_{\mathrm{poly}(q)}$。由于这些参数都不依赖于 N，~~我们可以~~使用上面的引理，得到该拒绝概率与 $c(q)\min(1, Q\delta(f, \mathrm{RM}[n,q,d]))$ 相同。

此后我们假设 $n \geqslant s+t+100$。这一假设很有帮助，因为它使我们能够界定来自 $\mathbb{F}_q^n \to \mathbb{F}_q^{s+t}$ 的非满秩仿射变换的数量，正如下文的注释所述。

注 3.2. $\mathcal{T}_{n,\ s+t}$ 中非满秩的比例至多为 $q^{100}{}^{1}$ $_{(q-1)}$。对于任意~~的 $a \in$~~ $\mathbb{F}_q^{s+t}$、$b \in \mathbb{F}_q^n$，在给定 $Ta = b$ 的条件下，$\mathcal{T}_{n,\ s+t}$ 中非满秩的比例也满足同样的界。为此，注意到我们可以将 M 的线性部分非满秩的概率上界为

$$\sum_{i=0}^{s+t} \frac{q^{i-1}}{q^n} \leqslant \frac{q^{s+t}-1}{(q-1)q^n} \leqslant \frac{1}{q^{100}(q-1)}.$$

对于第二部分，请注意，以 $Ta = b$ 为条件不会改变这一估计，因为我们仍然可以均匀地随机选择线性部分，并设置仿射平移，使得 $Ta = b$。

3.4 稀疏平坦测试器的一些基本事实

我们现在收集 t 关于稀疏平坦测试器的一些基本事实，这些事实对于我们的分析是必要的 s.

3.4.1 基本可靠性性质

我们首先描述为什么这个测试器有效。本文的阐述将是不完整的，重点关注分析所必需的最基本性质；更多细节请参阅附录 B 或 [33] 以获取更多细节。

考虑单项式 $x^{e'}$，对于 $e' \in \{0,\dots,q-1\}^{s+t}$，使得 $\langle x^{e'}, H_e(x)\rangle \neq 0$ 对某个 $e \in \{0,\dots,q-1\}^t$ 成立，使得 $\sum_{i=1}^{t} e_i \leqslant t(q-1) - r$，且 $t \geqslant p+2$。根据引理 2.1，这些单项式 $x^{e'}$ 必须满足：

- $e'_{p(i-1)+1} + \cdots + e'_{pi} = p \cdot (q - q/p)$ for $1 \leqslant i \leqslant \frac{s}{p}$
- $e'_{s+1} + \cdots + e'_{s+t} \geqslant r$.

更一般地，我们可以将与 H_e 的任意内积明确表示如下。

引理 3.3。对于 $f(x) = \sum_{a\in\{0,\dots,q-1\}^n} C_a x^a$，以及 $e \in \{0,\dots,q-1\}^t$，我们有

$$\langle f, H_e\rangle = \sum_{e'} D_{e'} C_{e'},$$

其中，$D_{e'}$ 是取决于 H_e 的系数的常数，求和遍历同时满足上述第一个条件以及对 $1 \leqslant i \leqslant t$ 而言的 $e'_{s+i} + e_i = q-1$ 的 e'。

证明。我们有

$$\langle x^{e'}, H_e\rangle = \left(\prod_{i=1}^{s/p} \sum_{\alpha_1,\dots,\alpha_p\in\mathbb{F}_q} \alpha_1^{e'_{p(i-1)+1}} \cdots \alpha_p^{e'_{pi}} P(\alpha_1,\dots,\alpha_p)\right) \sum_{\beta_1,\dots,\beta_t\in\mathbb{F}_q^t} \beta_1^{e'_{s+1}+e_1} \cdots \beta_t^{e'_{s+t}+e_t}.$$

由引理 2.2 可知，对于每个 i，我们有

$$\sum_{\alpha_1,\dots,\alpha_p\in\mathbb{F}_q} \alpha_1^{e'_{p(i-1)+1}} \cdots \alpha_p^{e'_{pi}} P(\alpha_1,\dots,\alpha_p) \neq 0,$$

仅当单项式 $x_1^{q-1}\cdots x_p^{q-1}$ 出现在 $x_1^{e'_{p(i-1)+1}} \cdots x_p^{e'_{pi}} P(x_1,\dots,x_p)$ 中时。由于 P 的次数为 $q-p$，只有在 $e'_{p(i-1)+1} + \cdots + e'_{pi} = p\cdot(q-q/p)$ 的情况下才可能如此。同样，

$$\sum_{\beta_1,\dots,\beta_t\in\mathbb{F}_q^t} \beta_1^{e'_1+e_1} \cdots \beta_t^{e'_t+e_t} \neq 0,$$

当且仅当对每个 $1 \leqslant i \leqslant t$ 都有 $e'_i + e_i = q-1$。 □

由引理 3.3 可知，T 只有在 $\deg(f\circ T) > d$ 时才会拒绝 f，因为在这种情况下，f 没有任何满足上述条件的单项式。因此，如果 f 确实是次数 d，那么它以概率 1 被接受。但如果函数 f 的次数超过 d，稀疏平坦测试器是否必然会以正概率拒绝它？利用典范单项式已在 [33] 中证明了这一点。由于我们将需要这一事实，而且为了使本文自成一体，我们在附录 B 中给出证明。

定理 3.4. 函数 f 通过稀疏 $(s+t)$-仿射子空间测试的概率为 1，当且仅当 f 的次数至多为 d。

证明。详见附录 B。 □

3.4.2 稀疏性

顾名思义，稀疏平坦测试器的下一个重要特点是查询复杂度低。注意，测试所需的查询次数与测试多项式 H_e 的支撑大小成正比，而下一个引理表明，对于步骤 2 中 $\mathbb{F}_q^t$ 的任意 e， $H_e(x)$ 都具有稀疏支撑。此外，无论选择哪个 e，这个支撑都相同。因此，计算 $\langle f \circ T、 H_e \rangle$ 时，无需查询 $f \circ T$ 定义域中的所有 q^{s+t} 个点。

引理 3.5。 P 的支撑大小至多为 $(2^{p-1}+p-1)q^{p-1}$，且包含于集合

$$\left(\bigcup_{i=1}^{p-1}\{x_i=0\}\right)\cup\left(\bigcup_{I\subset[p-1]}\{x_I+x_p=0\}\right).$$

其中， $\{x_I=x_p\}$ 表示由 $x_I=x_p$ 给出的超平面。

证明。假设 x 不在所述集合中。那么在 P 的表达式中，根据费马小定理，每一项 $(x_I+x_p)^{q-1}=1$。此外，分母非零，因此直接计算可得 $P(x)=0$。 □

引理 3.6. 对于任意 $e\in\{0,\dots,q-1\}^t$，我们有

$$\operatorname{supp}(H_e)\subseteq\prod_{i=1}^{s/p}\operatorname{supp}(P)\times\mathbb{F}_q^t,$$

证明。由于 $H_e(x)=\left(\prod_{i=1}^{s/p}P(x_{p(i-1)+1},\dots,x_{pi})\right)\prod_{j=1}^{t}x_{s+j}^{e_j}$，结论显然成立。 □

下文中，我们令 $\operatorname{supp}(H)=\bigcup_{e\in\{0,\dots,q-1\}^t}\operatorname{supp}(H_e)$。对于任意 T，稀疏 $s+t$-仿射子空间测试只需查询 $\operatorname{supp}(H)$ 中的点上的 $f\circ T$，从而得到以下查询复杂度上界。

引理 3.7. 稀疏 $s+t$-仿射子空间测试的查询复杂度至多为 $(3q)^{\frac{d+1}{q}}q^t$。由于我们可以选择任意 $t\geqslant p+2$，查询复杂度最低可达 $(3q)^{\frac{d+1}{q}}q^{p+2}$

证明。根据引理 3.6，我们可以界定 $\prod_{i=1}^{s/p}\operatorname{supp}(P)\times\mathbb{F}_q^t$ 的大小。根据引理 3.5，

$$|\operatorname{supp}(P)|\leqslant(2^{p-1}+p-1)q^{p-1},$$

so

$$\left|\prod_{i=1}^{s/p}\operatorname{supp}(P)\times\mathbb{F}_q^t\right|\leqslant((2^{p-1}+p-1)q^{p-1})^{s/p}q^t\leqslant(3q)^{s(p-1)/p}q^t,$$

其中我们用到了这一事实：$(2^{p-1}+p-1)^{1/p}\leqslant 3$。此外，$s\leqslant\frac{d+1}{q-q/p}$，因此

$$(3q)^s q^t\leqslant(3q)^{\frac{d+1}{q}}q^t.$$ □

3.5 建立稀疏平坦测试器与平坦测试器之间的联系

在本节中，我们描述一种将稀疏（$s+t$）-仿射子空间测试解释为 t-仿射子空间测试的方法。这一关系将在后文发挥作用，因为它使我们能够借用来自 [31] 对 t-仿射子空间测试的分析中的技术。

固定一个仿射变换 $A \in \mathcal{T}_{n,\ s+\ell}$ 其中 $\ell > t$，并令 $\mathrm{Res}_{s,\ \ell,\ t}$ 表示如下形式的仿射变换集合 (R, b):

$$R = \begin{bmatrix} I_s & 0 \\ 0 & R' \end{bmatrix}, b = \begin{bmatrix} 0 \\ b' \end{bmatrix}, \tag{2}$$

其中 $R' \in \mathbb{F}_q^{\ell \times t}, b' \in \mathbb{F}_q^{\ell}$。我们将 $\mathrm{Res}_{s,\ \ell,\ t}$ 中的仿射变换称为限制。换言之，将A 与 $\mathrm{Res}_{s,\ \ell,\ t}$ 中的一个随机 (R, b) 复合，相当于保留前 s 列，并将其余列随机化。如下文所述，这使我们能够将 $(s+t)$-稀疏测试视为在 f 的某个受限类型函数上嵌入了t-平坦测试器。

更确切地说，注意到我们可以通过选择 $A \in \mathcal{T}_{n,\ s+\ell}$，再从 $\mathrm{Res}_{s,\ \ell,\ t}$ 中均匀随机选取一个限制$B = (R, b) \in$，并输出 $T = A \circ B$，来采样 $T \in \mathcal{T}_{n,\ s+t}$。在引理 3.8 和 3.9 中，我们证明测试结果“完全取决于” $b' + \mathrm{Im}(R') = \mathrm{Im}((R', b'))$。为此，在固定 A 后，我们定义 $\tilde{f}$: $\mathbb{F}_q^{\ell} \to \mathbb{F}_q$ 如下:

$$\tilde{f}(\beta_1, \ldots, \beta_\ell) = \sum_{\alpha \in \mathbb{F}_q^s} f \circ A(\alpha, \beta_1, \ldots, \beta_\ell) \prod_{i=1}^{s/p} P(\alpha_{p(i-1)+1}, \ldots, \alpha_{pi}).$$

此外，对于 $B = (R, b) \in \mathrm{Res}_{s,\ell,t}$，令 $\mathrm{fl}(B) \subseteq \mathbb{F}_q^{\ell}$ 为由 $b' + \mathrm{Im}(R')$ 给出的 t-仿射子空间。下面的引理~给出了拒绝 $f \circ T$ 的稀疏平坦测试器与在$b' + \mathrm{Im}(R')$ 上拒绝 f 的（标准）平坦测试器之间的关系。

~引理3.8。对于任意 $B \in \mathrm{Res}_{s,\ \ell,\ t}$，$A \circ B$ 当且仅当 $\deg(f|_{\mathrm{fl}(B)}) \geqslant r$ 时拒绝 f。

证明。将 $B = (R, b)$ 写成 (2) 的形式，并令 B'： $\mathbb{F}_q^t \to \mathbb{F}_q^{\ell}$ 为由 (R', b') 给出的仿射变换。回顾一下，$A \circ B$ 拒绝当且仅当

$$\langle f \circ A \circ B, H_e \rangle = \langle \tilde{f} \circ B, H_e \rangle \neq 0.$$

对于某个 $e \in \{0, \ldots, q-1\}^t$，使得 $\sum_{i=1}^t e_i \leqslant t(q-1) - r$。对于任意 e，我们可以将右侧的这个内积改写如下。

$$\begin{aligned}
\langle f \circ A \circ B, H_e \rangle &= \sum_{\alpha \in \mathbb{F}_q^s, \beta \in \mathbb{F}_q^t} (f \circ A \circ B(\alpha, \beta)) \cdot \prod_{i=1}^{s/p} P(\alpha_{p(i-1)+1}, \ldots, \alpha_{pi}) \beta^e \\
&= \sum_{\beta \in \mathbb{F}_q^t} \left(\sum_{\alpha \in \mathbb{F}_q^s} f(\alpha, B'(\beta)) \cdot \prod_{i=1}^{s/p} P(\alpha_{p(i-1)+1}, \ldots, \alpha_{pi}) \right) \cdot \beta^e \\
&= \sum_{\beta \in \mathbb{F}_q^t} \tilde{f} \circ B'(\beta) \cdot \beta^e \\
&= \langle \tilde{f} \circ B', x^e \rangle.
\end{aligned}$$

然而，$\langle \tilde{f} \circ B', x^e \rangle \neq 0$ 当且仅当 $\tilde{f} \circ B'$ 包含单项式 $x_1^{q-1-e_1} \cdots x_t^{q-1-e_t}$。由此可知，~$A \circ B$ 拒绝当且仅当 $\deg(f \circ B') \geqslant r$。最后，由于多项式的次数在 ~ 仿射变换下保持不变，因此这等价于 $\deg(f|_{\mathrm{fl}(R)}) \geqslant r$。 □

我们指出，引理 3.8 尤其意味着，稀疏的 $s+t$-仿射子空间测试在任何只影响最后 t个坐标的仿射变换下都保持不变。特别地，我们得到：

引理 3.9. 对任意 $B \in \mathrm{Res}_{s,t,t}, T \circ B$， f拒绝当且仅当 T拒绝 f。

˜证明。我们对 $\ell = t$ 和 $A = T$ 应用引理 3.8。然后，应用 B 不会改变 f 的次数，结论便得证。 □

固定 $A \in \mathcal{T}_{n,s+\ell}$ 后，这条引理使我们可以将稀疏（$s+t$）-仿射子空间测试的其余部分，即选择一个限制 $B \in \mathrm{Res}_{s,\ell,t}$，视为在 $f = f \circ A$ 上进行的 t- 仿射子空间测试。令 $\ell = t + 100$，我们可以将稀疏 $s + t$- 仿射子空间测试描述如下。

1. 随机选择一个 $A \in \mathcal{T}_{n,s+t+100}$。

2. 执行 ˜对根据上述内容定义的 $t + 100$ 元函数执行标准的 t-仿射子空间测试 e.

这种对测试的看法将使我们能够借鉴一些来自 t-仿射子空间测试的概念和事实，下面我们将介绍该测试。首先，我们正式定义仿射子空间的上影。

定义 7. 对于一个 ℓ-仿射子空间集合 S，将其上影定义如下。

$$S^{\uparrow} = \{V \mid \dim(V) = \ell + 1, \exists U \in S, U \subseteq V\}.$$

下述影子引理在 [10] 中给出，并在对 [31]的分析中得到广泛使用。该引理也将在我们的分析中发挥作用，因此我们将其记录如下。

Lem引理 3.10。对于一个函数 f，令 S 为满足$\deg(f|_U) > d$ 的 ℓ 维仿射子空间 U。那么，

$$\mu(S^{\uparrow}) \leqslant q\mu(S),$$

其中，测度分别取自 $(\ell + 1)$-仿射子空间和 ℓ-仿射子空间的集合。

我们还可以为仿射变换定义一个类似的上影概念，这与刚刚介绍的稀疏平坦测试器的视角相符。

定义 8. 对于一个仿射变换集合 $\mathcal{S} \subseteq \mathcal{T}_{n,s+\ell}$，定义

$$\mathcal{S}^{\uparrow} = \{T \in \mathcal{T}_{n,s+\ell+1} \mid \exists R \in \mathrm{Res}_{s+\ell+1,s+\ell}, T \circ R \in \mathcal{S}\}$$

我们需要以下关于仿射变换集合的上影的简单结论。

引理 3.11. 对于一个仿射变换集合 $\mathcal{S} \subseteq \mathcal{T}_{n,s+\ell}$,

$$\mu(\mathcal{S}^{\uparrow}) \geqslant \mu(\mathcal{S}).$$

证明。我们可以先采样 $T$by，再采样 $T' \in \mathcal{T}_{n,\ s+\ell+1}$ 然后选择一个限制 $R \in \mathrm{Res}_{s+\ell+1,\ s+\ell}$并输出 $T = T' \circ R$。只有当 $T' \in \mathcal{S}^{\uparrow}$ 时，我们才能得到 $T \in \mathcal{S}$，因此结论成立。 □

4 定位潜在错误

我们现在开始证明定理 1.1。回顾一下， $\mathcal{S}_t = \{T \in \mathcal{T}_{n,s+t} \mid T$ 拒绝 $f\}$ 定义于 (1)，且 $\mathrm{rej}_{s+t}(f) = \mu_{s+t}(\mathcal{S}_t)$；为简便起见，我们记作 $\varepsilon = \mu_{s+t}(\mathcal{S}_t)$。本节将证明，若 $\varepsilon \leqslant q^{-M}$（其中 M 是一个待确定的较大绝对常数），则我们可以找到 f 的一个潜在错误输入 $x^\star$，也就是说，只要所选测试多项式的支撑中含有 $x^\star$，稀疏平坦测试器几乎总是拒绝。

我们首先检验集合 $\mathcal{S}_t$ 满足定理 2.1 的条件。

4.1 仿射双线性方案中 $\mathcal{S}_t$ 的边扩张

我们首先证明 $\mathcal{S}_t$的扩张上界。对于矩阵 M 和列向量 v v，令$[M, v]$ 表示将 v 作为附加列追加后的矩阵。考虑以下在 AffBilin$(n, s+t)$ 中采样一条边的过程。

1. 均匀随机选择 $T_1 = (M, c) \in \mathcal{T}_{n,s+t}$ 。
2. 在满足 $v \neq 0$ 的条件下，均匀随机选择 $v \in \mathbb{F}_q^n$，并令 $T' = ([M, v], c)$.
3. 选择一个形如 $R = [I_{s+t}, w]^T$ 的均匀随机矩阵 $R \in \mathbb{F}_q^{(s+t+1)\times(s+t)}$，以及一个均匀随机的 $b \in \mathbb{F}_q^{s+t+1}$，使得 b 中前 $s+t$ 个元素为零。
4. 设置 $T_2 = T' \circ (R, b)$。

下面的引理将使我们能够证明 $\mathcal{S}_t$ 的扩张性较差。它取代了 [31] 中的“影子”引理。

引理4.1。设 $G: \mathbb{F}_q^{s+t} \to \mathbb{F}_q$ 为任意多项式，并设 $T = (M, c)$ 是一个 $s+t$-仿射变换，使得 $\langle f \circ T, G\rangle \neq 0$。固定在步骤 2中选取的 $v \in \mathbb{F}_q^n$，并令 $T' = ([M, v], c)$。然后，

$$\Pr_{(R,b)}[\langle f \circ T' \circ (R, b), G\rangle \neq 0] \geqslant \frac{1}{q},$$

其中， R 是根据步骤 3 进行采样的。

证明。令 $w = (w_1, \ldots, w_{s+t})$ 为 R 的最后一行，并令 b_{s+t+1} 为 b 的最后一个条目。均匀随机选择 (R, b) 等价于在 $\mathbb{F}_q$ 中均匀随机选择 β 和每个 α_i 。为得到该结果，我们将 $\langle f \circ T' \circ R, G\rangle$ 视为这些随机值的函数，并应用 Schwartz-Zippel 引理。

函数 $f \circ T' \circ (R, b)$ 可以通过将 $(s+t+1)$ 元变量函数 $\tilde{f}$ 与 (R, b) 复合得到。然后，$f \circ T' \circ (R, b)$ 就是 $(s+t)$ 元函数

$$\left(f \circ T' \circ (R, b)\right)(x_1, \ldots, x_{s+t}) = \tilde{f}\left(x_1, \ldots, x_{s+t}, \sum_{i=1}^{s+t} w_i x_i + b_{s+t+1}\right).$$

根据引理 3.3， $\langle f \circ T' \circ (R, b)\ G\rangle$ 是 f的系数的某个线性组合，但这些系数是 $w_1, \ldots, w_{s+t}$, b_{s+t+1} 的多项式，总次数至多为 $q-1$，因为 f 可以写成一个各变量次数至多为 $q-1$的多项式。因此，$\langle f \circ T' \circ R, G\rangle$ 是一个多项式，其

$w_1, \ldots, w_{s+t}, b_{s+t+1}$ 的总次数至多为 $q-1$。此外，该多项式非零，因为令 $w_1 = \cdots = w_{s+t} = b_{s+t+1} = 0$ 时，其值为

$$\langle f \circ T, G \rangle \neq 0.$$

由 Schwartz-Zippel 引理可得 $\Pr_{(R,b)}[\langle f \circ T' \circ R, G \rangle \neq 0] \geqslant \frac{1}{q}$。 □

作为一个直接推论，我们得到，拒绝的仿射变换集合的扩张性很差。

引理 4.2。拒绝 $f, \mathcal{S}_t$ 的 $s+t$-仿射变换集合满足

$$1 - \Phi(\mathcal{S}_t) \geqslant \frac{1}{q}.$$

其中扩张是在 AffBilin$(n, s+t)$ 中进行的。

证明。固定 $T_1 \in \mathcal{S}_t$，并在 AffBilin$(n, s+t)$ 中选择与 T_1 相邻的 T_2。根据假设，存在某个有效的 e 和 H_e，使得 $\langle f \circ T_1, H_e \rangle \neq 0$。由于可以按照本节开头所述的过程选择 T_2，我们可以将引理 4.1 应用于 $G = H_e$,

$$\Pr_{T_2}[\langle f \circ T_2, H_e \rangle \neq 0] \geqslant \frac{1}{q}.$$

因此 $1 - \Phi(\mathcal{S}_t) \geqslant \frac{1}{q}$。 □

4.2 关于缩出和线性部分上的缩出集的伪随机性

接下来，我们证明 t 集合 $\mathcal{S}_t$ 相对于缩出集以及线性部分上的缩出而言是伪随机的。

引理4.3。集合 $\mathcal{S}_t$ 关于缩出集和线性部分上的缩出集是 $q\mu(\mathcal{S}_t)$-伪随机的。

证明。我们给出针对缩出集的证明。针对线性部分上的缩出集的论证非常相似。

固定一个缩出 $\mathcal{C}_{a^T,b,\beta}$ 记 $\mu_{a^T,b,\beta}(\mathcal{S}_t)$ 为 $\mathcal{S}_t$ 在 $\mathcal{C}_{a^T,b,\beta}$ 中的测度，即 $\frac{|\mathcal{S}_t \cap \mathcal{C}_{a^T,b,\beta}|}{|\mathcal{C}_{a^T,b,\beta}|}$。固定任意一个 v 使得 $a^T \cdot v \neq 0$。首先均匀随机地选择 $(M, c) \in \mathcal{C}_{a^T,b,\beta}$，然后根据步骤3和4 并取 v 选择 (M', c')，从而抽取一个 $(s+t)$-仿射变换。也就是说，如果第 i 个 M 列为 M_i，那么 M' 的第 i 列为 $M_i + \alpha_i v$，且对于 $\mathbb{F}_q$ 中均匀随机的 $\alpha_i' s$ 和 α_0，仿射平移为 $c' = c + \alpha_0 v$。根据引理 4.1，如果 $T_1 \in \mathcal{S}_t \cap \mathcal{C}_{a^T,b,\beta}$，那么以至少 $1/q$ 的概率有 $T_2 \in \mathcal{S}_t$，因此

$$\Pr[T_2 \in \mathcal{S}_t] \geqslant \frac{\mu_{a^T,b,\beta}(\mathcal{S}_t)}{q}.$$

另一方面，注意到 T_2 的分布在 $\mathcal{T}_{n,\ s+t}$ 上是均匀的。事实上，固定一个 $T = (M', c') \in \mathcal{T}_{n,\ s+t}$ 并令 M_i' 表示 M' 的第 i 列。那么，得到 $T_2 = T$ 的唯一方式就是选择，

$$\alpha_i = \frac{a^T M_i' - b_i}{a^T v} \text{ for } 1 \leqslant i \leqslant n, \quad \text{and} \quad \alpha_0 = \frac{a^T c' - \beta}{a^T v},$$

且 $(M, c) \in \mathcal{C}_{a^T,\ b,\ \beta}$ 使得

$$M_i = M_i' - \alpha_i v \text{ for } 1 \leqslant i \leqslant n, \quad \text{and} \quad c = c' - \alpha_0 v.$$

由于 T_2 在 $\mathcal{T}_{n,\ s+t}$上均匀分布，我们有

$$\mu(\mathcal{S}_t) \geqslant \Pr[T_2 \in \mathcal{S}_t] \geqslant \frac{\mu_{a^T,b,\beta}(\mathcal{S}_t)}{q},$$

因此 $\mu_{a^T,\ b,\ \beta}(\mathcal{S}_t) \leqslant q\mu(\mathcal{S}_t)$。由于这对所有缩出集都适用，结论得证。对于线性部分上的缩出集，也可以采用类似的论证。

□

4.3 关于线性部分上缩入的伪随机性

接下来我们将证明关于线性部分上缩入的伪随机性。论证会更加复杂。特别地，我们利用其与 t-仿射子空间测试的关系，将该命题的证明归约为仿射格拉斯曼图上的类似命题。随后，我们使用与 [31] 类似的思想证明该命题。形式化地说，本节将证明：

引理 4.4。集合 $\mathcal{S}_t$ 是关于线性部分上缩入的 $tq^{162}\varepsilon$ 伪随机的 $C_{a,\ b,\ \mathrm{lin}}$。

我们先给出一些定义。对于一个长度大于 s 的任意向量 a，令 $a_{[s]}$ 表示这样一个向量：其前 s 个坐标等于 a，其余坐标均为 0。令 $a|_{[s]}$ 表示将向量 a 限制在其前 s 个坐标上所得的向量。对于矩阵 $M \in \mathbb{F}_q^{n\times(s+\ell)}$，记

$$\mathrm{Im}_a(M) = \{Ma' \mid a' \in \mathbb{F}_q^{\ell}, a'|_{[s]} = a|_{[s]}, a' \neq a'_{[s]}\}.$$

换言之，$\mathrm{Im}_a(M)$ 是由满足以下条件的元素构成的像：这些元素与 a 在前 s 个坐标上相同，并且在其余坐标上不全为 0。

由于测试引入的不对称性，我们需要根据 a 的 0 模式采用不同的论证。首先，我们将通过直接论证证明，对于线性部分上的缩入，$\mathcal{S}_t$ 是伪随机的，$C_{a,\ b,\ \mathrm{lin}}$，其中$a \neq a_{[s]}$。然后，我们将通过归约到这种情形，证明对于线性部分上的任意缩入，$\mathcal{S}_t$ 都是伪随机的。

引理 4.5。集合 $\mathcal{S}_t$ 对于线性部分上的缩入 $C_{a,\ b,\ \mathrm{lin}}$（其中$a \neq a_{[s]}$）是 $q^{161}\varepsilon$ 伪随机的。

引理 4.5 的证明需要一些准备工作和辅助陈述，接下来我们将予以介绍。固定引理中的 a、b，并假设 $\mathcal{S}_t$ 在 $\mathcal{C}_{a,\ b,\ \mathrm{lin}}$ 中的分数大小为 α，也就是说，

$$\frac{\mu(\mathcal{S}_t \cap \mathcal{C}_{a,b,\mathrm{lin}})}{\mu(\mathcal{C}_{a,b,\mathrm{lin}})} = \alpha.$$

考虑另一个 $a' \in \mathbb{F}_q^{s+t}$使得$a'_{[s]} = a_{[s]}$，且$a' \neq a'_{[s]}$。换言之，$a'$ 在其前 s 个坐标中等于 a，并且在其后 t 个坐标中非零。存在一个可逆矩阵 R，其前 s 行和列构成单位矩阵，I_s，使得 $Ra' = a$。与 R 复合给出了集合 $\mathcal{C}_{a,b,\mathrm{lin}}$ 和 $\mathcal{C}_{a',b,\mathrm{lin}}$ 之间的一个双射。此外，根据引理3.9，$(M, c) \in \mathcal{S}_t$ 当且仅当 $(M \cdot R, c) \in \mathcal{S}_t$。因此，对于满足 $a'_{[s]} = a_{[s]}$的任意 a'，以及 $a' \neq a'_{[s]}$，有

$$\frac{\mu(\mathcal{S}_t \cap \mathcal{C}_{a',b,t})}{\mu(\mathcal{C}_{a',b,t})} = \frac{\mu(\mathcal{S}_t \cap \mathcal{C}_{a,b,t})}{\mu(\mathcal{C}_{a,b,t})} = \alpha.$$

换句话说， $\mathcal{S}_t$ 在满足 $b \in \mathrm{Im}_a(M)$ 的 (M, c) 集合中具有分数大小 α，因此我们定义

$$\mathcal{D}_{a,b,\ell} = \{(M, c) \in \mathcal{T}_{n,s+\ell} \mid b \in \mathrm{Im}_a(M)\}.$$

我们可以通过首先选择 $(M, c) \in \mathcal{D}_{a,b,t+100}$，然后均匀地随机选择 $(R, b) \in \mathrm{Res}_{s,t+100,t}$，并输出 $(M', c') = (M, c) \circ (R, v) = (M \cdot R, c + Mv)$（条件为 $M \cdot R \in \mathcal{D}_{a,b,t}$），来采样一个 $(M', c') \in \mathcal{D}_{a,b,t}$。由于 $(M', c') \in \mathcal{S}_t$ 的概率为 α，且只有在 $(M, c) \in \mathcal{S}_t^{\uparrow 100}$ 时才可能发生，因此我们得到

$$\frac{\mu(\mathcal{S}'_b)}{\mu(\mathcal{D}_{a,b,s+t+100})} \geqslant \alpha,$$

其中 $\mathcal{S}'_b = \mathcal{S}_t^{\uparrow 100} \cap \mathcal{D}_{a,b,t+100}$。回顾一下，$\mathcal{S}_t^{\uparrow}$ 是 $(s+t+1)$-仿射变换的集合，T，对于这些变换，存在一个限制 R 使得 $T \circ R \in \mathcal{S}_t$，而 $\mathcal{S}_t^{\uparrow 100}$ 是将同一操作应用 100 次。

下面的引理表明，可以固定该测试的前 s 列，使得拒绝概率仍然很小：

引理 4.6。存在 $(M, c) \in \mathcal{S}'_b$，使得均匀随机地选择 $(R, v) \in \mathrm{Res}_{t+100,t}$ 并设定 $M' = M \cdot R, c' = c + Mb$，我们有

$$\Pr_{B=(R,b)\in \mathrm{Res}_{s,t+100,t}}[(M, c) \circ B \in \mathcal{S}_t \mid b \notin \mathrm{Im}_a(M')] \leqslant \frac{2}{\alpha}\varepsilon.$$

证明。均匀地选择一个在 $(M, c) \in \mathcal{S}'_b$ 条件下的满秩 $(s+t+100)$-仿射变换 (M, c)，然后均匀地选择一个 $(R, v) \in \mathrm{Res}_{s,t+100,t}$，并设置 $(M', c') = (M, c) \circ R$。在本证明的其余部分，所有概率均依据此分布。定义以下事件。

- $E_1 = \{(M', c') \in \mathcal{S}_t\}$。
- $E_2 = \{(M, c) \in \mathcal{S}'_b\}$.
- $E_3 = \{b \notin \mathrm{Im}_a(M')\}$.
- $E_4 = \{b \in \mathrm{Im}_a(M)\}$.

首先，我们注意到

$$\Pr[E_1 \mid E_3 \wedge E_4] = \Pr[E_1 \mid E_3],$$

因此，

$$\Pr[E_1 \wedge E_3 \mid E_4] = \Pr[E_1 \mid E_3 \wedge E_4] \cdot \Pr[E_3 \mid E_4] \leqslant \Pr[E_1 \mid E_3].$$

由此我们可以得出

$$\begin{aligned}
\Pr_{(M',c')=(M,c)\circ R}[E_1 \mid E_2 \wedge E_3] &= \frac{\Pr[E_1 \wedge E_3 \wedge E_4]}{\Pr[E_2 \wedge E_3]} \\
&= \frac{\Pr[E_1 \wedge E_3 \mid E_4]\Pr[E_4]}{\Pr[E_2 \wedge E_3]} \\
&\leqslant \frac{\Pr[E_1 \mid E_3]\Pr[E_4]}{\Pr[E_2 \wedge E_3]} \\
&= \frac{\Pr_{(M',c')}[E_1 \mid E_3]}{\Pr[E_2 \mid E_4]\Pr[E_3 \mid E_2]},
\end{aligned}$$

这里我们利用了 $E_2 \wedge E_4 = E_2$ 这一事实，因此 $\mathbf{Pr}[E_2]/\mathbf{Pr}[E_4] = \mathbf{Pr}[E_2 \mid E_4]$。

注意到最后一个分数的分子至多为 ε，而分母至少为 $\alpha/2$，因此该概率至多为 $2\varepsilon/\alpha$。所以，存在 $(M,c) \in \mathcal{S}'_b$，使得在给定该 (M,c) 的条件下，关于 $R \in \mathsf{Res}_{s,t+100,t}$ 的概率 $(M,c) \circ R \in S$ 至多为 $2\varepsilon/\alpha$。

□

固定此 (M,c)后，剩余的测试图现在位于$\mathsf{Res}_{s+t+100,s+t}$，并且同构于$\mathsf{AffBilin}(t+100,t)$。此外，根据引理3.8，我们可以仅关注由 $b' + \mathsf{Im}(R')$ 给出的仿射子空间，其中 $(R,b) \in \mathsf{Res}_{s,t+100,t}$。这使我们能够定义 $\tilde{f}\colon \mathbb{F}_q^{t+100} \to \mathbb{F}_q^t$，如第 3.5 节中所做的那样：

$$\tilde{f}(\beta_1,\ldots,\beta_{t+100}) = \sum_{\alpha \in \mathbb{F}_q^s} f \circ A(\alpha,\beta_1,\ldots,\beta_{t+100}) \prod_{i=1}^{s/p} P(\alpha_{p(i-1)+1},\ldots,\alpha_{pi}).$$

根据引理 3.8，我们现在使用针对 f 的标准 t-仿射子空间测试。$b \notin \mathsf{Im}_a(M \cdot R)$的条件转化为：$t$-仿射子空间 $U \subseteq \mathbb{F}_q^{t+100}$不包含点 $w \in \mathbb{F}_q^{t+100}$，等于 a'的最后 $t+100$ 个坐标，其中 a' 是满足 $Ma' = b$ 的唯一点。

翻译引理 4.6 得到

$$\Pr_{B=z+A \in \mathsf{AffGras}(t+100,t)}[\deg(\tilde{f}|_B) \geqslant r \mid w \notin A] \leqslant \frac{2}{\alpha}\varepsilon.$$

这与 [31, 命题 3.4], 证明开头给出的结果相同，其余论证也如其中所述。令

$$\mathcal{B} = \{B = z + A \in \mathsf{AffGras}(t+100,t) \mid w \notin A, \deg(\tilde{f}|_A) \geqslant r\}.$$

引理 4.7。集合 $\mathcal{B}$ 非空。

证明。由于我们选择了 $(M,c) \in \mathcal{S}'_b$，至少存在一个限制 B，使得 $(M,c) \circ B$拒绝 f，因此存在一个 t 维仿射子空间，在其上 f 的次数大于 r。由此可知，若随机抽取一个 t 维仿射子空间$z + A = B'' \subseteq B'$，则 $\deg(f|_{B''}) \geqslant r$ 的概率至少为 $1/q$。然而，若 $\mathcal{B}$ 为空，则只有当 $w \in A$ 时，$\deg(f|_{B''}) \geqslant r$。在这种情况下，$w \in A$ 的概率至多为

$$\frac{q^t - 1}{q^{t+1} - 1} < \frac{1}{q}.$$

因此 $\mathcal{B}$ 非空。 □

现在我们开始证明引理 4.5。

证明♀♀♀ 引理 4.5。由引理 4.7 $\mathcal{B}$ 非空，因此必定存在一个 $t+40$ 仿射子空间 W，使得t
♀♀♀

$$\mathcal{B}_W = \{B \in \mathcal{B} \mid B \subseteq W\}.$$

非空。令 μ_W表示 $\mathsf{AffGras}(W,t)$ 上的均匀测度。此图同构于 $\mathsf{AffGras}(t{+}40,t)$，但底空间 $\mathbb{F}_q^{t+40}$被视为 W。我们首先声称，由于 $\mu_W(\mathcal{B}_W) > 0$，它必定至少为 q^{-100}。否则，$0 < \mu_W(\mathcal{B}_W) < q^{-100}$。然而，仅凭其大小，$\mathcal{B}_W$就相对于缩入和线性部分上的缩入是伪随机的。事实上，任何缩入或线性部分上的缩入的测度都已经是 q^{-40}，因此 $\mathcal{B}_W$ 只能包含一个 q^{-60} 的比例。此外，通过类似的论证，$\mathcal{B}_W$ 相对于缩出和其线性部分上的缩出也是伪随机的。

根据引理 4.3。最后，通过与引理 4.2 类似的论证， $1-\Phi_W(\mathcal{B}_W) \geqslant \frac{1}{q}$。综上，这与定理 A.1 矛盾，因此我们得出 $\mu_W(\mathcal{B}_W) \geqslant q^{-100}$。

因此，存在 W 使得 $\mu_W(\mathcal{B}_W) \geqslant q^{-100}$。固定这样一个 W，并在给定 $w \notin V$ 的条件下，采样一个均匀的 $t+99$-仿射子空间 $Y = u+V \subseteq z+A$，再采样一个均匀的 $t+60$-仿射子空间 $A_2 \subseteq Y$，并考虑 $A_2 \cap W$。我们可以将W视为由 60 个线性无关的线性方程 $\langle h_1, x\rangle = c_1, \ldots, \langle h_{60}, x\rangle = c_{60}$ 定义。也就是说， W 是满足这 60 个方程的 $\mathbb{F}_q^{t+100}$ 的子空间。同样， A_2 由 39 个线性方程的限制给出， $\langle h'_1, x\rangle = c'_1, \ldots, \langle h'_{39}, x\rangle = c'_{39}$。99 个线性方程全部线性无关的概率至少是

$$\prod_{j=0}^{38} \frac{q^{99}-q^{60+j}}{q^{99}} \geqslant e^{-2\sum_{j=1}^{\infty} q^{-j}} \geqslant e^{-4/q}.$$

当所有 99 个 li 相邻的方程线性无关，因此 $A_2 \cap W$ 在 AffGras(W,t) 上均匀分布。因此 ，

$$\Pr[A_2 \cap W \in \mathcal{B}_W] \geqslant e^{-4/q} q^{-100}.$$

若 $A_2 \cap W \in \mathcal{B}_W$，则 $A_2 \in \mathcal{B}_Y^{\uparrow 60}$，其中上影是相对于 AffGras$(Y,t)$ 取的，因此可得

$$E_Y[\mu_Y(\mathcal{B}_Y^{\uparrow 60})] \geqslant e^{-4/q} q^{-100}.$$

然而，根据引理 3.10,

$$\mu_Y(\mathcal{B}_Y^{\uparrow 60}) \leqslant q^{60}\mu_Y(\mathcal{B}_Y),$$

因此综合起来可得

$$E_Y[\mu_Y(\mathcal{B}_Y)] \geqslant e^{-4/q} q^{-160}.$$

最后请注意，左侧至多为这样的概率：在满足 $w \notin A$ 的均匀 $B = x + A \subseteq \mathbb{F}_q^{t+100}$ 中， $f|_B$ 的次数大于 r。根据假设，此概率至多为 $\frac{2}{\alpha}\varepsilon$，因此

$$\alpha \leqslant e^{-4/q} q^{160} 2\varepsilon. \qquad \square$$

现在我们可以证明引理 4.4 了。

引理 4.4 的证明。我们证明集合 $\mathcal{S}_t$ 相对于线性部分 $C_{a,\ b,\ \mathrm{lin}}$ 上的缩入是 $tq^{198}\varepsilon$伪随机的，对任意 $a \in \mathbb{F}_q^{s+t}$均成立。

如果 $a \neq a_{[s]}$，那么根据引理 4.5，我们就完成了证明，因此不妨设 $a = a_{[s]}$，这意味着 a 在其前 s 个坐标之外均为零。显然， a必须至少有一个非零坐标，否则 $a=0$ 和 $C_{a,\ b,\ \mathrm{lin}}$ 要么是 $\mathcal{T}_{n,\ s+t}$ 的全部（如果 $b=0$），要么为空集（如果 $b \neq 0$）。前一种情况由 $\mu(\mathcal{S}_t) \leqslant q^{-M}$这一假设不可能发生，而后一种情况显然成立。不失一般性，设 $a_1 = \alpha \neq 0$。

对于每个 $T \in \mathcal{S}_t \cap C_{a,\ b,\ \mathrm{lin}}$，都存在满足 $\sum_{i=1}^{t} e_i \leqslant t(q-1) - r$ 的 $e \in \{0,\ldots,q-1\}^t$，使得 $\langle f \circ T, H_e\rangle \neq 0$。此外，由于 $r>0$，必然存在某个“特殊索引” i，使得 $e_i < q-1$。取所有 $T \in \mathcal{S}_t \cap C_{a,\ b,\ \mathrm{lin}}$ 中出现次数最多的特殊索引，不失一般性地设其为 1。因此，对于至少 $1/t$ 的 $T \in \mathcal{S}_t \cap C_{a,\ b,\ \mathrm{lin}}$，存在某个 e，使得 $\langle f \circ T, H_e\rangle \neq 0$、 $e_1 < q-1$，且 $\sum_{i=1}^{t} e_i \leqslant t(q-1) - r$。令 $\mathcal{A}$ 表示这些变换的集合。

考虑映射 F_β： $\mathbb{F}_q^{s+t} \to \mathbb{F}_q^{s+t}$，它将 x_{s+1} 变为 $x_{s+1} + \beta x_1$，并保持所有其他坐标不变。也就是说，

$$F_\beta(x_1,\ldots,x_{s+t}) = (x_1,\ldots,x_s, x_{s+1}+\beta x_1, x_{s+2},\ldots,x_{s+t}).$$

对于任意 $T \in \mathcal{A}$，我们断言

$$\Pr_{\beta \in \mathbb{F}_q}\left[\langle f \circ T \circ F_\beta, H_e\rangle \neq 0\right] \geqslant \frac{2}{q},$$

其中 e 是t 指数向量，使得 $e_1 < q-1$、$\sum_{i=1}^{t} e_i \leqslant t(q-1) - r$，且 $\langle f \circ T$、$H_e\rangle \neq 0.$

事实上，$\langle f \circ T \circ F_\beta$、$H_e\rangle$ 是 $f \circ T \circ F_\beta$ 的系数的线性组合，而 $f \circ T \circ F_\beta$ 是关于 β 的多项式。实际上，根据引理 2.2，它是那些单项式的系数的线性组合，其中 x_{s+1} 的次数为 $q-1-e_1 > 0$。然而，在 $f \circ T \circ F_\beta$ 的每个单项式中，β 的次数与 x_{s+1} 的次数之和至多为 $q-1$，因此可知，对 $\langle f \circ T \circ F_\beta$、$H_e\rangle$ 有贡献的系数在 β 中的次数至多为 $q-2$。因此，$\langle f \circ T \circ F_\beta$、$H_e\rangle$ 是关于 β 的次数至多为 $q-2$ 的多项式。最后，该多项式非零，因为它在 $\beta = 0$ 处取值非零。由此，根据 Schwartz-Zippel 引理可得该不等式。

特别地，这意味着对于每个 $T \in \mathcal{A}$，都存在一个非零的 β，使得 $\langle f \circ T \circ F_\beta, H_e\rangle \neq 0$，我们选择 $\beta^\star$ 为其中最常见的 β（注意，$\beta^\star \neq 0$ 这一事实正是我们需要概率为 $2/q$ 而非 $1/q$ 的原因）。因此，对于 $\mathcal{A}$ 中至少 $2/q$ 的变换，都有 $T \circ F_{\beta^\star} \in \mathcal{S}_t$。令 $a' = F_\beta^{-1}(a)$，则对于至少 $2/q$ 比例的 $T \in \mathcal{A}$，都有$T \circ F_{\beta^\star} \in \mathcal{C}_{a',\,b,\,\text{线性}} \cap \mathcal{S}_t$；又由于 $F_{\beta^\star}$ 是一个双射，故可得

$$\frac{1}{t}\mu(\mathcal{S}_t \cap \mathcal{C}_{a,b,\mathrm{lin}}) \leqslant \mu(\mathcal{A}) \leqslant \frac{q}{2}\mu(\mathcal{S}_t \cap \mathcal{C}_{a',b,\mathrm{lin}}).$$

最后，注意到 $a' \neq a'_{[s]}$，因为其 $(s+1)$ 坐标按设计即为非零。应用引理 4.5 可得$\mu(\mathcal{S}_t \cap \mathcal{C}_{a',\,b,\,\text{线性}}) \leqslant q^{161}\varepsilon\mu(\mathcal{C}_{a',\,b,\,\text{线性}})$；又由于 $\mu(\mathcal{C}_{a',\,b,\,\text{线性}}) = \mu(\mathcal{C}_{a,\,b,\,\mathrm{lin}})$，结合上述结果可得

$$\frac{\mu(\mathcal{S}_t \cap \mathcal{C}_{a,b,\mathrm{lin}})}{\mu(\mathcal{C}_{a,b,\mathrm{lin}})} \leqslant tq^{162}\varepsilon. \qquad \square$$

5 修正错误并迭代

根据前面小节的结果，以及假设 $\mu(\mathcal{S}_t) \leqslant q^{-M}$，可以得出 $\mathcal{S}_t$ 满足以下性质：

1. $\mu(\mathcal{S}_t) \leqslant q^{-M}$
2. $1 - \Phi(\mathcal{S}_t) \geqslant \frac{1}{q}$.
3. $\mathcal{S}_t$ 关于线性部分上的缩出和缩出集是 q^{1-M}-伪随机的。
4. $\mathcal{S}_t$ 关于线性部分上的放大是 tq^{162-M}-伪随机的。

由于我们取 $t \geqslant 10$，由定理 2.1，结合 $\xi = tq^{162-M}$ 和 $\ell = s + t$，可知存在一对 a、b，使得

$$\mu_{a,b}(\mathcal{S}_t) = \frac{\mu(\mathcal{S}_t \cap \mathcal{C}_{a,b})}{\mu(\mathcal{C}_{a,b})} \geqslant 1 - \frac{1}{(q-1)^2} - \frac{1}{q^6} - 2000tq^{200}q^{-M/4}, \tag{3}$$

对于足够大的 M。

我们该如何利用这些信息？换句话说，(3) 告诉我们，$\mathcal{S}_t$ 在将 a 变换为 b的变换上是稠密的，这表明点 b 是 f 的一个错误点，我们应当修正它，从而提高测试的接受概率。此外，按理说，这种改变应当影响所有源自 $\mathcal{C}_a$ 中变换的测试，b。

然而，仔细考察后会发现，只有在 $a \in \mathrm{supp}(H)$ 时，这些测试才会受到影响；否则，在我们执行的测试中，值 $f(T(a)) = f(b)$ 会乘以 0，因此改变 f 在 b 处的值根本不会影响测试。因此，要使上述策略奏效，我们必须证明 (3) 对某一对 a, b 成立，且其中 a 属于 $\mathrm{supp}(H)$。

引理 5.1。存在 $a \in \mathrm{supp}(H)$ 和 $b \in \mathbb{F}_q^n$，使得 $\mu_{a,b}(\mathcal{S}_t) \geqslant 1 - {}^{1}\!/_{(q-1)^2} - \frac{1}{q^6} - 2000tq^{200}q^{-M/4}$。

一旦证明了这一引理，我们就能够证明，在 $\mathcal{C}_{a,b}$ 中，b 处的修正可以降低测试的拒绝概率；然而，要证明测试器是最优的，我们需要通过一次修正修复更大比例的测试。具体来说，我们需要能够修复满足 $T(a) = b$ 的测试，对任意 $a \in \mathrm{supp}(H)$ 都成立。为了使这一论证成立，我们必须证明 $\mathcal{S}_t$ 在 $\bigcup_{a \in \mathrm{supp}(H)} \mathcal{C}_{a,b}$ 中是稠密的。

引理 5.2. 如果存在一个 $a \in \mathrm{supp}(H)$，使得 $\mu_{a,b}(\mathcal{S}_t) \geqslant 1 - {}^{1}\!/_{(q-1)^2} - \frac{1}{q^6} - 2000tq^{200}q^{-M/4}$，那么 $\mathcal{S}_t$ 的密度至少为 $\geqslant 1 - {}^{1}\!/_{(q-1)^2} - \frac{1}{q^6} - {}^{1}\!/_{q^{100}(q-1)^2} - 2000tq^{200}q^{-M/4} - q^{-M/2}$，其中 $\cup_{a \in \mathrm{supp}(H)} \mathcal{C}_{a,b}$。

换言之，$\cup_{a \in \mathrm{supp}(H)} \mathcal{C}_{a,b}$ 是满足以下条件的（$s+t$）-仿射变换的集合：T 对于某个 $a \in \mathrm{supp}(H)$，$Ta = b$。在接下来的两个小节中，我们将证明引理5.1和5.2。证明这些引理之后，如何进行修正将变得显而易见，我们也将很快完成定理 1.1 的证明。两个引理的证明方式相似，因此我们首先给出一个将在两个证明中使用的一般引理。设 $g : \mathbb{F}_q^{\ell+100}$ 是一个任意多项式，设 d 是一个次数参数，设 ν 表示 $\mathbb{F}_q^{\ell+100}$ 中 ℓ-仿射子空间上的均匀测度，并设 $b \in \mathbb{F}_q^{\ell+100}$ 是一个任意点。定义以下两个集合：

$$\mathcal{A} = \{U \mid \dim(U) = \ell, \deg(f|_U) > d, b \in U\},$$

$$\mathcal{B} = \{U \mid \dim(U) = \ell, \deg(f|_U) > d, b \notin U\}.$$

保持 ε 和 M（这个较大的绝对常数）与我们所定义的一致，使得 $q^{M/2}O(\varepsilon) < q^{-M/2}$ 很小。我们将使用以下结果，该结果是对 [31] 的第 3.2 节中结果的扩展：

引理 5.3。保持 g、d、b 和 $\mathcal{B}$ 的定义与上文相同，并假设 $\ell \geqslant \max(\lceil \frac{d+1}{q-q/p} \rceil, 4)$。如果 $\nu(\mathcal{B}) \leqslant q^{M/2}O(\varepsilon)$，那么 $\mathcal{B} = \emptyset$。此外，存在一个值 γ，将 $g(b)$ 改为 γ 后，$\nu(\mathcal{A}) = 0$。

由这两点可知，将 $g(b)$ 的值改为后，$\deg(g) \leqslant d$ γ.

证明。证明推迟到 C 节。 □

5.1 引理 5.1 的证明

为证明引理 5.1，我们说明 $\mathcal{S}_t$ 相对于支撑之外的缩入是伪随机的，因此 (3) 中找到的缩入必定位于 H 的支撑中。具体而言，我们说明：

引理 5.4。 对于任意 $a \notin \mathrm{supp}(H)$ 以及任意 $b \in \mathbb{F}_q^n$，$\mu_{a,b}(\mathcal{S}_t) < 1 - {}^{1}\!/_{(q-1)^2} - \frac{1}{q^6} - 2000tq^{200}q^{-M/4}$.

我们开始证明引理 5.4，并反设该引理不成立。也就是说，假设存在 $a \notin \mathrm{supp}(H)$，使得 $\mu_{a,b}(\mathcal{S}_t) \geqslant 1 - {}^{1}\!/_{(q-1)^2} - \frac{1}{q^6} - 2000tq^{200}q^{-M/4}$。由于 $a \notin \mathrm{supp}(H)$，存在 p 个连续坐标 $(a_{pi+1}, \ldots, a_{pi+p-1}) \notin \mathrm{supp}(P)$。为方便起见，我们将坐标的顺序调换，使这些坐标成为最后的 p 个坐标。因此，对于 $e \in \{0, \ldots, q-1\}^t$，多项式 $H_e(x)$ 现在为，

$$H_e(x_1, \ldots, x_{s+t}) = \left(\prod_{i=1}^{s/p-1} P(x_{p(i-1)+1}, \ldots, x_p) \right) x_{s-p+1}^{e_1} \cdots x_{s-p+t}^{e_t} P(x_{s+t-p+1}, \ldots, x_{s+t}).$$

使用仿射变换 T 的测试会检查，对于所有有效的 e，是否有 $\langle f \circ T, H_e \rangle = 0$，其中 H_e 如上所定义。以这种方式重新排列变量会改变支撑，因此我们的假设 $a \notin \mathrm{supp}(H)$ 不失一般性地变为 $(a_{s+t-p+1}, \ldots, a_{s+t}) \notin \mathrm{supp}(P)$，这会让我们之后的记号稍微简单一些（这也是重新排列变量的唯一原因）。我们将再次采样一个更大的仿射变换，并选取一个限制来得到一个 $T \in \mathcal{T}_{n,\ s+t}$，不过这次的限制会略有不同。我们要求这些限制为满秩，并固定 T的前 $s+t-p$ 列/坐标，而不是像之前那样固定前 s 列/坐标。令 $\mathrm{Res}_{s+t-p,\ p+102,\ p}$ 由以下形式的仿射变换（R, b）组成：

$$R = \begin{bmatrix} I_{s+t-p} & 0 \\ 0 & R' \end{bmatrix}, b = \begin{bmatrix} 0 \\ b' \end{bmatrix}, \tag{4}$$

其中 $R' \in \mathbb{F}_q^{(p+102)\times p}$是满秩的，且 $b' \in \mathbb{F}_q^{p+102}$。对于 $B = (R, b) \in \mathrm{Res}_{s+t-p,\ p+102,\ p}$ 这种形式，令 $\mathrm{fl}(B) = b' + \mathrm{Im}(R')$。此外，对于仿射变换 T，定义 $\mathrm{Im}_a(T) = \{Tx : \ x_{[s+t-p]} = a_{[s+t-p]}\}$，其中回想一下，$a_{[s+t-p]}$ 是将前 $s+t-p$ 个坐标以外的所有坐标都设为零后的 a。按如下方式采样一个 $T \in \mathcal{T}_{n,\ s+t}$：

1. 选择一个满秩的 $A \in \mathcal{T}_{n,\ s+t+102}$，使得 $b \in \mathrm{Im}_a(A)$。
2. 选择 $B \in \mathrm{Res}_{s+t-p,\ p+102,\ p}$。
3. 输出 $T = A \circ B$。

选定 A 之后，A 的线性部分/仿射平移的前 $s+t-p$ 列/坐标便固定了，而其余部分则与某个随机限制复合。因此，一旦 A 固定，就存在唯一的 $x^\star$ 使得 $Ax^\star = b$，且只有当 $Ba = x^\star$ 时才可能有 $Aa = b$。特别地，这仅在 $x^\star \in \mathrm{Im}(B)$ 时发生；按照设计，这个 $x^\star$ 满足 $x^\star_{[s+t-p]} = a_{[s+t-p]}$。令 $z^\star \in \mathbb{F}_q^{p+102}$ 为 $x^\star$ 的最后 $p+102$ 个坐标，则 $Ta = b$ 仅当 $z^\star \in \mathrm{fl}(B)$ 时成立。令 μ_A 表示 $\mathrm{Res}_{s+t-p,\ p+102,\ p}$ 中的测度。定义

$$\mathcal{R}_A = \{B \mid A \circ B \text{ rejects}, z^\star \notin \mathrm{fl}(B)\}.$$

如果在如上选择 A 并构造 $z^\star$ 后，我们再以 $z^\star \notin \mathrm{fl}(B)$ 为条件，那么 $A \circ B$ 在 $\mathcal{T}_{n,s+t}$ 中服从在满秩变换上的均匀随机分布，且其像不包含 b。因此，$\mathbb{E}_A[\mu_A(\mathcal{R}_A)] \leqslant O(\varepsilon)$，并且以至少 $1/2$ 的概率，我们有 $\mu_A(\mathcal{R}_A) \leqslant O(\varepsilon)$。

另一方面，在选择 A 后，如果我们均匀地选择 B 使得$A \circ B \in \mathcal{C}_{a,b}$，则关于 T 的分布在满秩$T \in \mathcal{C}_{a,b}$ 上是均匀的。根据注 3.2，在 $\mathcal{C}_{a,b}$ 中不是满秩的仿射变换所占的比例至多为 $q^{100}{}^{-1}{}_{(q-1)}$，并且根据我们的假设，拒绝变换的集合在 $\mathcal{C}_{a,b}$ 中是稠密的。因此，简单的平均论证表明，在满秩 $T \in \mathcal{C}_{a,b}$ 中拒绝的变换所占的比例也很大，尤其严格大于 $1/2$。因此，以严格大于 $1/2$ 的概率，在 A中至少存在一个 B，使得 $A \circ B$ 是满秩的并且拒绝。

因此，存在一个满秩$A \in \mathcal{T}_{n,\ s+t+102}$ 使得以下两点成立：

- $\mu_A(\mathcal{R}_A) \leqslant O(\varepsilon)$,
- 存在一个 $B^\star$，使得$T = A \circ B^\star \in \mathcal{C}_{a,\ b}$ 是满秩的并且拒绝。

固定这个 A，并保持 $x^\star$、$z^\star$ 和 $\mathcal{R}_A$ 的定义不变。现在我们来说明这如何导出矛盾。思路是应用引理 5.3，并论证存在一个点，我们可以在该点进行修正，使得对于所有可能的 B，$A \circ B$ 都会被接受，尤其是对于 $B^\star$。由于我们假设支撑之外的缩入具有较高的拒绝概率，我们将证明修正是在一个未被查看的点处进行的。

被测试 $A \circ B^\star$。这两条事实合在一起构成矛盾，因为在不属于点集 $(A \circ B^\star)(\alpha)$ 的点处改变 f，对于 $\alpha \in \mathrm{supp}(H)$，不会改变测试 $A \circ B^\star$ 的结果。然而，为了应用引理 5.3，我们需要一个类似于 $\mu_A(\mathcal{R}_A) \leqslant O(\varepsilon)$ 的陈述，但针对的是仿射子空间集合，而非仿射变换集合。为此，我们将尝试论证 $B \in \mathcal{R}_A$ 的 $\mathrm{fl}(B)$ 集合也很小。

我们开始进行形式化论证。第一步是定义一个类似于引理3.8中的辅助多项式。假设 T 因 $\langle f \circ T、\ H_e \rangle \neq 0$ 而拒绝，对于一个固定的有效 e。利用这个 e，定义 $\tilde{f}$： $\mathbb{F}_q^{p+102} \to \mathbb{F}_q$ 如下

$$\tilde{f}(\beta) = \sum_{\alpha \in \mathbb{F}_q^{s-p+t}} f \circ A(\alpha_1, \ldots, \alpha_{s-p+t}, \beta) \left(\prod_{i=1}^{s/p-1} P(\alpha_{p(i-1)+1}, \ldots, \alpha_{pi}) \right) \alpha_{s-p+1}^{e_1} \cdots \alpha_{s-p+t}^{e_t}.$$

对于任意 $B = (R, b) \in \mathrm{Res}_{s+t-p,p+102,p}$ 按照公式（4）写出，很容易检查 th at

$$\langle f \circ A \circ B, H_e \rangle = \langle \tilde{f} \circ (R', b'), P \rangle,$$

˜因此，在固定 A 后，我们可以将测试视为在 f 上进行，并使用变换 $(R', b') \in \mathcal{T}_{p+102,\ p}$。
˜根据定理 3.4，如果 $\deg(f) < q(p-1)$，那么对于所有 $B' = (R', b') \in \mathcal{T}_{p+102,\ p}$，都有 $\langle f \circ (R', b')\ P \rangle = 0$。这引出了以下事实：

$$B \text{ can only reject if } \deg(\tilde{f}|_{\mathrm{fl}(B)}) \geqslant q(p-1).$$

这个事实类似于引理 3.8，不过我们只有一个方向。也就是说，当 $\deg(f|_{\mathrm{fl}(B)}) \geqslant q(p-1)$ 时，并非总是 B ˜拒绝，因为对 f 的测试只检查与 P 的内积，而不是检查所有次数至多为 $q-p$ 的单项式。

利用这一事实，我们现在可以将 $\mu_A(\mathcal{R}_A)$与不包含 $z^\star$˜ 且满足 $\deg(f|_{\mathrm{fl}(B)}) \geqslant q(p-1)$的 p-仿射子空间 $\mathrm{fl}(B)$ 集合的测度联系起来。定义 p-仿射子空间集合，

$$\mathcal{B}_A = \{\mathrm{fl}(B) \mid \deg(\tilde{f}_{\mathrm{fl}(B)}) \geqslant q(p-1), z^\star \notin \mathrm{fl}(B)\} \subseteq \mathsf{AffGras}(p+102, p).$$

˜等价地， $\mathcal{B}_A$ 是所有 p-仿射子空间 U 不包含 $z^\star$ 且满足 $\deg(f)|_U \geqslant q(p-1)$的集合。

为了分析这个集合的分数大小，我们可以通过选择一个 p-仿射子空间，然后为该仿射子空间选择一组基，来选择 (R', b')。更正式地说，在固定 A 的情况下，

选择 $B \in \mathrm{Res}'_{p+102,\ p}$ 使得 $z^\star \notin \mathrm{fl}(B)$，并根据公式（4）写出 B。

2.选择$T \in \mathcal{T}_{p,\ p}$，并将$(R', b')$ 替换为 $(R', b') \circ T$。将所得限制记为 $B' \in \mathrm{Res}'_{p+102,\ p}$。

3. 输出 B'.

我们声称，如果 initi ˜ally $\deg(f|_{\mathrm{fl}(B)}) \geqslant q(p-1)$时，则输出的 B' 以至少 $1/q$的概率拒绝 .

˜引理 5.5. 假设 $\deg(f|_{\mathrm{fl}(B)}) \geqslant q(p-1)$。那么在第二步中， B' 以至少 $1/q$ 的概率在 $M \in \mathcal{T}_p$ 中$_p$ 拒绝。也就是说， $\langle f \circ B', P \rangle \neq 0$。

˜证明。将 B 写成公式（4）的形式。则假设 $\deg(f|_{\mathrm{fl}(B)}) \geqslant q(p-1)$ 等价于˜$\deg(f \circ (R', b')) \geqslant q(p-1)$。

均匀随机地选择一个满秩 T，并考虑

$$\langle \tilde{f} \circ (R', b') \circ T, P \rangle = \langle \tilde{f} \circ (R', b'), P \circ T^{-1} \rangle.$$

˜由于 $\deg(f \circ (R', b')) \geqslant q(p-1)$，引理 B.5 表明，至少存在一种可逆$T$的取值，从而存在一个 T^{-1}，使得上述表达式非零。因此，我们可以将 $\langle \tilde{f} \circ (R', b')\ P \circ T^{-1} \rangle$ 视为关于 T^{-1} 各项的非零多项式。由于 P 的次数至多为 $q-p$，内积$\langle \tilde{f} \circ (R', b')\ P \circ T^{-1} \rangle$ 是关于 T^{-1} 各项的非零多项式，总次数至多为 $q-p$。由 Schwartz-Zippel 引理，对 T^{-1} 的各项取值，$\langle \tilde{f} \circ (R', b')\ P \circ T^{-1} \rangle \neq 0$的概率至少为 p/q。由于 T^{-1} 必须可逆，我们需要排除不可逆的各项取值，但这至多占 ($p-1$)/q $1/q$ $T \in \mathcal{T}_{p\,p}$ R' b' $\circ T$) 的比例。总的来说，我们仍然得到：以至少 的概率，，，(,) 拒绝 f。 □

令 ν_A 表示 AffGras($p+102, p$) 上的均匀测度，引理 5.5 意味着 $\nu_A(\mathcal{B}_A) \leqslant 6q\mu_A(\mathcal{R}_A)$。现在我们已经接近可以应用引理 5.3 了，但 $\mathcal{B}_A$ 是由 p-维仿射子空间组成的集合，而引理 5.3 只适用于由维数至少为 4 的仿射子空间组成的集合。因此，在 $p = 2, 3$ 这两种情形下，我们无法使用该引理。不过有一个简单的补救办法：考察 $\mathcal{B}_A$ 的上影

Le 引理 5.6。设 $\mathcal{B}'_A = \{U' \mid \dim(U') = p+2, z^\star \notin U', \deg(f|_{U'})\} \geqslant q(p-1)\}$。那么 ，

$$\nu(\mathcal{B}'_A) \leqslant q^2 \nu_A(\mathcal{B}_A),$$

其中 ν 是 AffGras($p+102, p+2$) 上的均匀测度。

证明。注意到 $\mathcal{B}'_A \subseteq \mathcal{B}_A^{\uparrow 2}$。事实上，对于任意 $U' \in \mathcal{B}'_A$，必定存在一个 p-维仿射子空间 $U \subseteq U'$，使得˜$\deg(f|_U) \geqslant q(p-1)$。由于 $z^\star \notin U'$，可得 $z^\star \notin U$，进而得到 $U \in \mathcal{B}_A$。然后对引理 3.10 应用两次即可得到结论。 □

现在，我们通过应用引理 5.4 并导出矛盾来完成证明。

引理5.4的证明。根据引理 5.6，$\nu(\mathcal{B}'_A) \leqslant q^2 \nu_A(\mathcal{B}_A) \leqslant q^3 O(\varepsilon)$。现在可以应用引理5.3，其中 $\ell = p+2$、次数参数 $q(p-1) - 1$，以及特殊点 $z^\star$。引理5.3 的条件得到满足，因为 $p+2 \geqslant \max(\lceil \frac{q(p-1)}{q-q/p} \rceil, 4)$且 $q^3 O(\varepsilon) \leqslant q^{M/2} O(\varepsilon)$。由引理 5.3可知，$\mathcal{B}'_A$为空，并且˜ ˜ 存在一个值 γ，使得将 $f(z^\star)$改为 γ后，有$\deg(f) \leqslant p(q-1)$。特别地，必有˜ $\langle f \circ A \circ B^\star, H_e \rangle = 0$，或者等价地，$\langle f \circ (R^\star, b^\star)\ P \rangle = 0$，其中$(R^\star, b^\star)$ 是 $B^\star$ 按照 (4) 写出时的非恒等部分。

回顾点 $z^\star$ 的定义：固定 A 后，$x^\star \in \mathbb{F}_q^{s+t+102}$ 是满足 $Ax^\star = b$ 的唯一点，而 $z^\star \in \mathbb{F}_q^{p+102}$ 是 $x^\star$ 的最后 $p+102$ 个坐标。由于 $B^\star$ 满足 $A \circ B^\star \in \mathcal{C}_{a,\ b}$，我们有 $(A \circ B^\star)(a) = b$，因此 $B^\star a = x^\star$。令 a' 为 a 的最后 $p+102$ 个坐标，则有 $(R^\star, b^\star)(a') = z^\star$。然而，根据假设，$a' \notin \mathrm{supp}(P)$，并且由于 $(R^\star, b^\star)$ 满秩，对于任意 $\alpha \in \mathrm{supp}(P)$，都有 $(R^\star, b^\star)(\alpha) \neq z^\star$。现在我们看到了矛盾所在。在改变 $f(z^\star)$ 的取值˜ 后，我们突然得到

$$\langle \tilde{f} \circ (R^\star, b^\star), P \rangle = \sum_{\alpha \in \mathrm{supp}(P)} \tilde{f}\left((R^\star, b^\star)(\alpha)\right) \cdot P(\alpha) = 0.$$

˜然而，由于我们只改变了 $f(z^\star)$ 的值，上述求和中的各项均未改变，因此这个内积仍应非零。因此，集合 $\mathcal{S}_t$ 不可能在任何 $\mathcal{C}_{a,b}$ 中稠密，其中 $a \notin \mathrm{supp}(H)$。 □

5.2 引理 5.2 的证明

我们已经证明，存在一个 $a^\star \in \mathrm{supp}(H)$ 和 $b \in \mathbb{F}_q^n$，使得

$$\mu_{a^\star,b}(\mathcal{S}_t) \geqslant 1 - \frac{1}{(q-1)^2} - \frac{1}{q^6} - 2000tq^{200-M/4}.$$

利用这一点，我们将推导出引理 5.2，该引理指出集合 $\mathcal{S}_t$ 在 $\cup_{v\in\mathrm{supp}\,(H)}\mathcal{C}_{v,b}$ 中稠密。

令 $\mathcal{U}_{s+t}$ 表示满足 $\deg(f|_U) > d$ 的 $(s+t)$-仿射子空间集合 U，并令 ν 表示 $(s+t)$-仿射子空间集合上的均匀测度。我们通过以下方式采样 $T \in \mathcal{C}_{a^\star,b}$：首先选择一个包含 b 的 $(s+t)$-仿射子空间 U，然后选择满足条件 $Ta^\star = b$ 且其像为 U 的 T。这一过程的关键在于，选定 U 后，得到的 T 只有在 $\deg(f|_U) > d$ 时才会拒绝。形式化地，

1. 选择一个包含 b 的随机 $(s+t)$-仿射子空间 U，以及一个随机基 $U =$，使其张成空间为 $\mathrm{span}(u_1,\ldots,u_{s+t}) + u_0$。令 $T' = (M', u_0)$，其中 M' 的第 i 列为 u_i。根据假设，对于某个 $x \in \mathbb{F}_q^{s+t}$，$T'(x) = b$。
2. 选 择任意一个矩阵 $B \in \mathcal{T}_{s+t,\ s+t}$ 使得 $Ba^\star = x$，并输出 $T = (M' \cdot B, u_0 \qquad\qquad)$.

容易验证，此过程从 $\mathcal{C}_{a^\star,\ b}$ 中均匀采样；并且如前所述，只有当 $\deg(f|_U) > d$ 时，T 才可能拒绝，这引出了以下观察：

注 5.7。

$$1 - \frac{1}{(q-1)^2} - \frac{1}{q^6} - 2000tq^{200-M/4} \leqslant \mu_{a^\star,b}(\mathcal{S}_t) \leqslant \nu_b(\mathcal{U}_{s+t}),$$

其中 ν_b 表示缩入 $\mathcal{D}_b$（仿射格拉斯曼图上的）中的密度。

利用关于 $\mathcal{U}_{s+t}$ 的这些信息，我们现在尝试应用引理 5.3。按如下方式采样一个满秩 $T \in \cup_{v\in\mathrm{supp}(H)}\mathcal{C}_{v,\ b}$：

1. 均匀随机地选择一个包含 b 的 $(s+t+100)$-维仿射子空间 V。
2. 均匀随机地选择 $U \subseteq V$，使得 $b \in U$。
3. 选择基表示 $U = \mathrm{span}(u_1,\ldots,u_{s+t}) + u_0$，并输出 $T = (M, u_0)$，其中 M 的第 i 列为 u_i，条件是对于某个 $v \in \mathrm{supp}(H)$，有 $Tv = b$。

选定 V 后，回顾以下两个集合，

$$\mathcal{A}_V = \{U \subseteq V \mid \dim(U) = s+t, \deg(f|_U) > d, b \in U\},$$

$$\mathcal{B}_V = \{U \subseteq V \mid \dim(U) = s+t, \deg(f|_U) > d, b \notin U\},$$

并令 ν_V 表示包含于 V 中的 $s+t$-维仿射子空间上的测度。

于是 $\mathbb{E}_V[\nu_V(\mathcal{A}_V)] \geqslant 1 - \frac{1}{(q-1)^2} - \frac{1}{q^6} - 2000tq^{200-M/4}$，因此以至少 $1 - \frac{1}{(q-1)^2} - \frac{1}{q^6} - 2000tq^{200-M/4}$ 的概率，我们有 $\nu_V(\mathcal{A}_V) > 0$。另一方面，$\mathbb{E}_V[\nu_V(\mathcal{B}_V)] = O(\varepsilon)$，因此以至少 $1 - q^{-M/2}$ 的概率，我们有 $\nu_V(\mathcal{B}_V) \leqslant q^{-M/2}O(\varepsilon)$。综上，这意味着概率至少为

$$1 - \frac{1}{(q-1)^2} - \frac{1}{q^6} - 2000tq^{200-M/4} - q^{-M/2},$$

V 同时满足 $\nu_V(\mathcal{A}_V) > 0$ 和 $\nu_V(\mathcal{B}_V) \leqslant q^{M/2}O(\varepsilon)$。

假设选择了这样一个 V，且上述条件成立。现在我们可以应用引理5.3，证明步骤 3中可以选择的任何T 现在都必须拒绝。这将确立所需的结果：一个随机的 $T \in \cup_{v\in\mathrm{supp}(H)}\mathcal{C}_{v,b}$ 以接近 1 的概率拒绝。

根据引理 5.3，存在一个值 γ，使得将 $f(b)$ 改为 γ 后，$\deg(f|_V) \leqslant d$。必有 $\gamma \neq f(b)$，因为 $\nu_V(\mathcal{A}_V) > 0$。令 f'为将 f在 b处的值改动后的函数。那么，对于上述描述的任意 T，对每个有效的 e，我们都有 $\langle f'\circ T, H_e\rangle = 0$。由于 T是满秩的，因此至多有一个点映射到 b，且该点是某个 $v \in \mathrm{supp}(H)$，所以我们有

$$\langle f'\circ T, H_e\rangle - \langle f\circ T, H_e\rangle = H_e(v)(f(b) - f'(b)) \neq 0.$$

因此，对于每个有效的 e $\langle f\circ T, H_e\rangle \neq \langle f'\circ T, H_e\rangle$，特别是，$T$拒绝 f。

引理 5.2 的证明。按照上述过程对一个满秩 $T \in \cup_{v\in\mathrm{supp}(H)}\mathcal{C}_{v,\ b}$ 进行抽样，前面的论证表明，对于以至少 $1 - \frac{1}{(q-1)^2} - \frac{1}{q^6} - 2000tq^{200-M/4} - q^{-M/2}$ 的概率抽取的 $(s+t+100)$-仿射子空间，步骤 3 中输出的 T会拒绝。由此可知，在满足 $Tv = b$ 对某个 $a \in \mathrm{supp}(H)$ 成立的满秩变换 T 集合中，$\mathcal{S}_t$的密度至少为 $1 - \frac{1}{(q-1)^2} - \frac{1}{q^6} - 2000tq^{200-M/4} - q^{-M/2}$。由于非满秩变换仅占 $\cup_{v\in\mathrm{supp}(H)}\mathcal{C}_{v,\ b}$ 中所有变换的 $\frac{1}{q^{100}(q-1)}$，根据注 3.2，我们再减去一个 $\frac{2}{q^{100}(q-1)}$，便得到所需结果。 □

5.3 迭代论证

回顾一下，$\mathrm{rej}_{s+t}(f)$ 表示随机选取的 $T \in \mathcal{T}_{n,s+t}$ 拒绝 f的概率。根据引理 5.3，对于至少 $9/10$ 个 $T \in \cup_{v\in\mathrm{supp}(H)}\mathcal{C}_{v,b}$，存在一个值 γ，使得将 $f(b)$ 的值改为 γ后，T接受 f。因此，存在一个 f'，使得 f'除 b 外在所有点上都与 f 相同，并且

$$\Pr_T[T \text{ rejects } f \mid \exists v \in \mathrm{supp}(H), T(v) = b] \leqslant 1 - \frac{9}{10q}.$$

命题 5.8. 若 $0 < \mathrm{rej}_{s+t}(f) < q^{-M}$且 $t = O(p)$，则存在一个点 $z \in \mathbb{F}_q^n$和一个函数 f'，使得 f除 b 外在所有点上都相同，并且

$$\mathrm{rej}_{s+t}(f') \leqslant \mathrm{rej}_{s+t}(f) - \frac{|\mathrm{supp}(H)|}{q^n C(q)},$$

其中 $C(q) = O(q)$。

证明。根据引理 5.2，存在 b，使得

$$\Pr_T[T \text{ rejects } f \mid \exists v \in \mathrm{supp}(H), T(v) = b] \geqslant 1 - \frac{1}{(q-1)^2} - \frac{1}{q^6} - \frac{2}{q^{100}(q-1)} - 2000tq^{200-M/4} - q^{-M/2}.$$

根据上述讨论，存在一个 f'，使得 f'除 b外在所有点上都与 f相同，并且

$$\Pr_T[T \text{ rejects } f \mid \exists v \in \mathrm{supp}(H), T(v) = b] \leqslant 1 - \frac{9}{10q}.$$

另一方面，显然，对于满足 $T(v) \neq b$ 的 T，对所有 $v \in \mathrm{supp}(H)$ 都成立时，对 $f\circ T$ 和 $f'\circ T$ 进行测试的结果相同，因为在计算 $\langle f\circ T、 H_e\rangle$ 所需的点上，f 和 f' 完全相同。

并且，对于任意 e，$\langle f' \circ T、H_e \rangle$。由于 $|_{\mathrm{supp}(\frac{H|}{q^n})}$ 表示 $b \in \{T(v) \mid v \in \mathrm{supp}(H)\}$ 的概率，直接计算可得

$$\begin{aligned}
&\mathrm{rej}_{s+t}(f') \\
&\leqslant \mathrm{rej}_{s+t}(f) - \frac{|\mathrm{supp}(H)|}{q^n}\left(1 - \frac{1}{(q-1)^2} - \frac{1}{q^6} - \frac{2}{q^{100}(q-1)} - 2000tq^{200-M/4} - q^{-M/2} - \left(1 - \frac{9}{10q}\right)\right) \\
&\leqslant \mathrm{rej}_{s+t}(f) - \Omega\left(\frac{|\mathrm{supp}(H)|}{q^n q}\right).
\end{aligned}$$

□

最后，我们可以完成定理 1.1 的证明。

定理 1.1 的证明。由命题 5.8，当 $\mathrm{rej}_{s+t}(f) > 0$ 时，我们可以改变 f 在一个点处的值，并将拒绝概率降低 $\Omega\left(|_{\mathrm{supp}(\frac{H|}{q^n q})}\right)$。当拒绝概率~~为 0 时~~，该函数的次数必定至多为 d，因此，

$$\delta_d(f)q^n \leqslant O\left(\frac{\mathrm{rej}_{s+t}(f)}{|\mathrm{supp}(H)|}q^n q\right)$$

这意味着

$$\mathrm{rej}_{s+t}(f) \geqslant \Omega\left(\frac{|\mathrm{supp}(H)|}{q}\delta_d(f)\right).$$

□

6 基于其他局部表征的最优测试

在证明稀疏平坦测试是最优测试时，我们最低限度地依赖了 H_e的结构。因此，将我们的方法加以扩展，并为能够给出局部刻画的其他多项式证明最优测试结果，并不困难。本节中我们将重新使用变量 s and r，因此它们不再指代之前的定义。令 $P\colon\ \mathbb{F}_q^k \to \mathbb{F}_q$ 为如下形式的多项式

$$P(x_1, \ldots, x_k) = \prod_{i=1}^{s} P_i(x_{m(i)}, \ldots, x_{m(i+1)-1})).$$

其中 $m(1) = 1$，$m(s) = k+1$，$m(i+1) - m(i) \leqslant t'$，对于每个 $1 \leqslant i \leqslant s-1$ 以及某个较小常数 t'。换言之，H 是一个 k 元多项式，它是少量变量上的多项式的乘积，其中每个此类多项式的变量彼此不相交。最后，令 $\mathcal{M} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$为任意非空的仿射不变多项式集合，并假设 $t = \mathrm{poly}(q)$。定义

$$\mathcal{E} = \{e \in \{0, \ldots, q-1\}^t \mid \prod_{i=1}^{t} x_i^{q-1-e_i} \notin \mathcal{M}\}.$$

注意，$(q-1, \ldots, q-1) \notin \mathcal{E}$。众所周知，任意多项式仿射不变集合都由该族中至少一个多项式所包含的单项式张成，参见 [25], ; 附录 B 对这一事实作了详细阐述。结合引理 3.3 可知，$g\colon\ \mathbb{F}_q^t \to \mathbb{F}_q$ 属于 $\mathcal{M}$，当且仅当对于每个 $(e_1, \ldots, e_t) \in \mathcal{E}$，都有 $\langle g, \prod_{i=1}^t x_i^{e_i} \rangle = 0$。与第 1.4 节中的描述相比，$\{\prod_{i=1}^t x_i^{e_i} \mid e \in \mathcal{E}\}$ $\mathcal{M}^\perp$ 是 的显式基。

利用 H 和指数向量属于 $\mathcal{E}$ 的单项式，我们可以定义一种类似于稀疏平坦测试器的测试。对于 $e \in \mathcal{E}$，定义

$$H_e(x_1, \ldots, x_{k+t}) = P(x_1, \ldots, x_k) \prod_{i=1}^{t} x_{k+i}^{e_i},$$

令 $\mathcal{F}_n(H) = \{f\colon \mathbb{F}_q^n \to \mathbb{F}_q \mid \forall T \in \mathcal{T}_{n,\,k}、\ \langle f \circ T、\ H_e\rangle = 0、\ \forall e \in \mathcal{E}\}$。显然，$\mathcal{F}_n(H)$ 是仿射不变的，并具有以下自然测试器：

1. 均匀随机地选择 $T \in \mathcal{T}_{n,\,k}$。

2. 如果对于任意 $e \in \mathcal{E}$，$\langle f \circ T、\ H_e\rangle \neq 0$，则拒绝；否则接受。

令 $\mathsf{supp}(H) = \cup_{e\in\mathcal{E}} \mathsf{supp}(H_e) = \mathsf{supp}(P) \times \mathbb{F}_q^t$。显然，测试器进行的查询次数为 $Q = |\mathsf{supp}(H)|$，尽管我们并不关心这一数值。本节余下部分的目标是证明该测试器是最优的。由此，通过使用具有上述规定形式的稀疏支撑的 P 构造局部刻画，可以为一般仿射不变码获得查询复杂度更低的最优测试器，这与 [33]中对广义 Reed-Muller 码所做的工作类似。

定理 6.1。上述测试器对于 $\mathcal{F}_n(H)$ 是最优的。也就是说，对于任意 $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$，

$$\mathrm{rej}(f) \geqslant c(q) \min(1, Q\delta(f, \mathcal{F}_n(H))),$$

其中，$\mathsf{rej}(f)$ 是测试器拒绝 f 的概率，$c(q) = {}^{1}\!/_{\mathrm{poly}(q)}$，~~$Q =$~~ $|\mathsf{supp}(H)|$ 是测试器执行的查询次数，而 $\delta(f, \mathcal{F}_n(H))$ 是 f 与 $\mathcal{F}_n(H)$ 中某个成员之间的最小相对汉明距离。

我们将采用相同的策略：先定位一个潜在错误，然后纠正该错误并重复迭代。令 $\mathcal{S}$ 表示 $\mathcal{T}_{n,\,k+t}$ 中被拒绝的测试集合，并假设对于某个 M，有 $\mu(\mathcal{S}) \leqslant q^{-M}$，其中 $M > 10t'$ 且 $q^M \geqslant t$。

在进入证明之前，我们先介绍一个见于 [31] 的引理。回顾引言中提升仿射不变码的定义。根据设计，$\mathcal{F}_n(\mathcal{H})$ 是一个提升的仿射不变码。令 $\mathcal{F} = \mathcal{F}_{k+t}(H)$，不难看出

$$\mathcal{F}_n(H) = \mathsf{Lift}_n(\mathcal{F}).$$

由于 我们可以将 $\mathcal{F}_n(H)$ 视为一种提升码，因此可以应用来自 [31 的以下引理].

引理 6.1. 设 $g\colon \mathbb{F}_q^{k'+1} \to \mathbb{F}_q$ 是一个满足 $g \notin \mathsf{Lift}_{k'+1}(\mathcal{F})$ 的多项式，并假设 $k' \geqslant k$。那么，

$$\Pr_U[g|_U \notin \mathsf{Lift}_{k'}(\mathcal{F})] \geqslant \frac{1}{q},$$

其中概率取自超平面 $U \subset \mathbb{F}_q^{k'+1}$。如果该不等式是紧的，并且满足 $g|_U \notin \mathsf{Lift}_{k'}(H)$ 的超平面集合 U 具有如下形式

$$\{U \mid x^\star \in U\},$$

对于某个点 $x^\star$，那么存在一个函数 g'，它在除 $x^\star$ 之外的所有点上都等于 g，使得 $g' \in \mathcal{F}_{k+i+1}(H)$。

该引理将在本节的分析中发挥引理 C.2 的作用。

定位潜在错误 为了定位错误，我们将再次证明 $\mathcal{S}$ 在某个缩入上是稠密的。由于我们已经假设 $\mathcal{S}$ 的测度很小，这一步要求我们证明，相对于缩出集、线性部分上的缩出集以及线性部分上的缩入，$\mathcal{S}$ 的扩展性很差且具有伪随机性。

引理 6.2。集合 $\mathcal{S}$ 具有以下性质：

- $\mu(\mathcal{S}) \leqslant q^{-M}$
- $\Phi(\mathcal{S}) \leqslant 1 - 1/q$
- $\mathcal{S}$ 关于线性部分上的缩出和缩出集是 $q\mu(\mathcal{S})$-伪随机的。
- $\mathcal{S}$ 关于线性部分上的放大是 $tq^{162}\varepsilon$-伪随机的。

其中， μ 是集合 $\mathcal{T}_{n,\ k+t}$ 中的测度。

第一项根据假设成立。第二项和第三项可分别用与引理 4.1 和 4.3 中完全相同的论证证明。

第四项的证明也采用与 Reed-Muller码 情形类似的方法，但由于这一论证更为复杂，我们将回顾相关步骤。

考虑对线性部分 $\mathcal{C}_{a,\ b,\ \mathrm{lin}}$进行缩入。我们可以假设 $a \neq 0$，否则该集合要么为空，要么为 $\mathcal{T}_{n,\ k}$。我们仍然分两种情况：一种是 a 的最后 t 个坐标中至少有一个非零，另一种是它们全为零。第一种情况可以完全按照引理 4.5 的方式证明。对于后一种情况，回想一下，根据假设 $(q-1, \ldots, q-1) \notin \mathcal{E}$。因此，从第一种情况归约到后一种情况（损失因子为 tq）的过程，与引理 4.4 的证明完全相同。

我们再次可以通过先选择一个满秩 $A \in \mathcal{T}_{n,k+t+100}, B \in \mathrm{Res}_{k+t+100,k}$，再输出 $A \circ B = T$ 来采样一个变换。此处 $\mathrm{Res}_{k,t+100,t}$ 是由满足以下条件的仿射变换 (R, b) 构成的集合：

$$R = \begin{bmatrix} I_k & 0 \\ 0 & R' \end{bmatrix}, b = \begin{bmatrix} 0 \\ b' \end{bmatrix}, \tag{5}$$

其中 $R' \in \mathbb{F}_q^{(t+100)\times t}$ 满秩且 $b' \in \mathbb{F}_q^{t+100}$。称 (R', b') 为 $B = (R, b)$ 的非平凡部分，并令 $\mathrm{fl}(B) = \mathrm{Im}(R', b')$。

沿用第 4.3 节中的相同设定，我们可以找到 A，使得以下两条性质成立：

- $b \in \mathrm{Im}^{a_{[k]}}(A)$
- 存在 $B \in \mathrm{Res}_{k,t+100,t}$，使得 $A \circ B \in \mathcal{S}$
- $\Pr_B[A \circ B \in \mathcal{S} \mid b \notin \mathrm{Im}^{a_{[k]}}(M \circ R)] \leqslant \frac{2}{\alpha}\varepsilon$.

固定这个 A，定义

$$\tilde{f}(\beta_1, \ldots, \beta_{t+100}) = \sum_{\alpha} f \circ A(\alpha, \beta_1, \ldots, \beta_{t+100}) P(\alpha).$$

那么，对于任何将 $B' = (R', b') \in \mathcal{T}_{t+100,t}$ 作为其非平凡部分的限制 B，以及任何 t 元单项式 x^e，我们有

$$\langle f \circ A \circ B, H_e \rangle = \langle \tilde{f} \circ B', x^e \rangle.$$

˜由此可知，当且仅当 $f|_{b'+\mathrm{Im}(R')} \in \mathcal{M}$ 时， $B = (R, b)$ 拒绝 f。

根据构造， $Ax^\star = b$存在某个 $x^\star \in \mathbb{F}_q^{k+100}$，使得 $x^\star$ 在其前 k 个坐标上等于 a。那么$b \in \mathrm{Im}^{a_{[k]}}($ $A \circ B)$ 等价于 $z^\star \in \mathrm{Im}(R')$，其中 $z^\star$ 是 $x^\star$的最后 $t+100$ 个坐标

令 $\mathcal{R}_A = \{$ ˜$(R', b') \in \mathcal{T}_{t+100,t} \mid f|_{b'+\mathrm{Im}(R')}\, z^\star \in \mathrm{Im}(R')\}$, 我们可以将上面的第三项翻译为

$$\Pr_B[A \circ B \in \mathcal{S} \mid b \notin \mathrm{Im}_{a_{[k]}}(M \circ R)] = \mu_A(\mathcal{R}_A) \leqslant \frac{2}{\alpha}\varepsilon,$$

其中 μ_A 是 $\mathrm{Res}_{k,\ t+100,\ t}$中的测度。定义

$$\mathcal{B}_A = \{b' + \mathrm{Im}(R') \mid (R', b') \in \mathcal{R}_A\}.$$

按照引理 4.7 中相同的论证， $\mathcal{B}_A$ 非空。最后，我们可以使用与引理 4.5 相同的证明（只是用引理 6.1 的第一部分而不是引理 3.10 来界定上影的大小），以证明 $\alpha \leqslant 2e^{-4/q}\varepsilon q^{160} \leqslant \varepsilon q^{161}\varepsilon$。这表明 $\mathcal{S}$ 关于 $\mathcal{C}_{a,\ b,\ \mathrm{lin}}$ 是 $\varepsilon q^{161}\varepsilon$-伪随机的，其中 a 的最后 t 个坐标之一非零。若不然，由于 $(q-1,$ $\ldots, q-1) \notin \mathcal{E}$，我们可以执行与引理 4.4 中相同的归约，以证明 $\mathcal{S}$ 关于线性部分上的每个缩入都是 $tq^{162}\varepsilon$-伪随机的。

总之，这就证明了引理 6.2，使我们能够利用定理 2.1 和 $\xi = tq^{162-M}$ 及$\ell = s + t$。由于我们取 $t \geqslant 10$，定理 2.1 意味着 $\mathcal{S}$ 在某个缩入$\mathcal{C}_{a,b}$上的密度至少为$1 - \quad {}^{1}{}_{(q-1)}$ ${}_2 - \frac{1}{q^6} - 2000tq^{200-M/4}$。以下固定这个缩入，并记作$\mathcal{C}_{a^\star,b}$。

点 $a^\star$ 属于 H 的支撑。接下来我们证明必有 $a^\star \in \mathrm{supp}(H)$。我们将用到下面这个引理，它与引理 5.3 相同，只是针对当前的设定。正如引理 5.3 的设定中那样，令 $g\colon \mathbb{F}_q^{\ell+100}$为任意多项式，令 ν 表示 $\mathbb{F}_q^{\ell+100}$ 中 ℓ-维仿射子空间上的均匀测度，并令 $b \in \mathbb{F}_q^{\ell+100}$为任意一点。再令 $\mathcal{G} \subseteq \{\mathbb{F}_q^N \to \mathbb{F}_q\}$ 为任意仿射不变码。

定义以下两个集合:

$$\mathcal{A} = \{U \mid \dim(U) = \ell, g|_U \notin \mathsf{Lift}_\ell(\mathcal{G}), b \in U\},$$

$$\mathcal{B} = \{U \mid \dim(U) = \ell, g|_U \notin \mathsf{Lift}_\ell(\mathcal{G}), b \notin U\}.$$

保持 ε 和 M （大的绝对常数）与我们定义的一致，使得 $q^{M/2}O$（ε） $< q^{-M/2}$ 很小。我们将使用以下结果，这是对 [31]中第 3.2 节结果的扩展:

引理 6.3. 保持以上定义的记号，并假设 $\ell \geqslant \max(N,4)$。如果 $\nu(\mathcal{B}) \leqslant q^{M/2}O(\varepsilon)$，那么$\mathcal{B} = \emptyset$。此外，存在一个值 γ，使得将 $g(b)$ 改为 γ后， $\nu(\mathcal{A}) = 0$

证明。该引理的证明与引理5.3 的证明相同，不过我们援引引理 6.1，而不是引理 C.2。

□

按照引理 5.4 证明中的相同步骤，这个引理几乎立即表明，必定有 $a^\star \in \mathrm{supp}(H)$。为反证起见，假设 $a^\star \notin \mathrm{supp}(H)$，且其坐标组 $(a^\star_{m(i)}, \ldots, a^\star_{m(i+1)-1}) \notin \mathrm{supp}(P_i)$。根据假设， P_i 是一个关于$t'' \leqslant t'$的 t'' 元多项式。令

$$\mathcal{F}_{t''}(P_i) = \{g : \mathbb{F}_q^{t''} \to \mathbb{F}_q \mid \langle g \circ T, P_i\rangle = 0, \forall T \in \mathcal{T}_{t'',t''}\}.$$

我们同样可以找到一个辅助多项式 $\tilde{f}\colon \mathbb{F}_q^{t''+102} \to \mathbb{F}_q$ 以及一个特殊点 $z^\star \in \mathbb{F}_q^{t''}$，使得以下条件成立:

- $\mu(\mathcal{R}) \leqslant O(\varepsilon)$，其中 $\mathcal{R} = \{B \in \mathcal{T}_{t''+102,t''} \mid \langle \tilde{f} \circ B, P_i \rangle \neq 0, z^\star \notin \mathrm{Im}(R)\}$，且 μ 是$\mathcal{T}_{t''+102}$的测度,t''。
- 存在一个满秩仿射变换 $B^\star \in \mathcal{T}_{t''+102,\ t''}$ 使得 $\langle f \circ B^\star, P_i \rangle \neq 0$,
- $z^\star \notin \{B^\star(v) \mid v \in \text{支撑}(P_i)\}$.

利用第一个事实，我们还可以界定以下 t''-仿射子空间集合的测度,

$$\mathcal{B} = \{U \in \mathsf{AffGras}(t''+102, t'') \mid f|_U \in \mathcal{F}_{t''}(P_i), z^\star \in U\}.$$

引理 6.4. 设 g 是一个 t''元多项式，满足 $g \notin \mathcal{F}_{t''}(P_i)$。那么，对 $T \in \mathcal{T}_{t'',\ t''}$，以至少 $\frac{1}{q^{t''}}$的概率有 $\langle g \circ T, P_i \rangle \neq 0$。

证明。随机选取 T后，我们可以将 $\langle g \circ T, P_i \rangle$ 视为关于 T各项的多项式。由于 $g \notin \mathcal{F}_{t''}(P_i)$，必定存在某个取值 T使该多项式的值非零，因此 $\langle g \circ T, P_i \rangle$ 是关于 T各项的非零多项式。由于 g 的各个变量的次数至多为 $q-1$，由施瓦茨-齐佩尔引理可知，以至少 $\frac{1}{q^{t''}}$的概率有 $\langle g \circ T, P_i \rangle \neq 0$。□

令 ν 表示 $\mathsf{AffGras}(t''+102, t'')$ 中的测度。我们可以通过先选取一个不包含 $z^\star$ 的 $U \in \mathsf{AffGras}(t''+102, t'')$，再选取像包含于 U 的 B，来选择 $B \in \mathcal{T}_{t''+102,\ t''}$，使得 $z^\star \notin \mathrm{Im}(B)$。引理 6.4 结合假设 $\mu(\mathcal{R}) \leqslant O(\varepsilon)$ 可推出

$$\frac{1}{q^{t''}} \nu(\mathcal{B}) \leqslant \mu(\mathcal{R}).$$

因此，我们有 $\nu(\mathcal{B}) \leqslant q^{t''} O(\varepsilon)$，并且根据引理 6.3，$\nu(\mathcal{B}^{\uparrow^4}) \leqslant q^{t''+4} O(\varepsilon) \leqslant q^{M/2} O(\varepsilon)$。接着，我们可以将引理 6.3 应用于 $\mathcal{G} = \mathcal{F}_{t''}(P_i)$ 和特殊点 $z^\star$，从而得到一个值 γ，使得在改变 $f(z^\star)$ 后，$\tilde{}$，我们有:

$$\tilde{f}|_{U'} \in \mathsf{Lift}_{t''+4}(\mathcal{F}_{t''}(P_i)), \quad \text{for all } t''+4\text{-flats } U' \text{ containing } z^\star.$$

$\tilde{}$ $\tilde{}$这也意味着，对于所有 t''-仿射子空间 $U \ni z^\star$，都有 $f|_U \in \mathcal{F}_{t''}(P_i)$；但请注意，改变 $f(z^\star)$ 的值不会影响测试的值

$$\langle \tilde{f} \circ B^\star, P_i \rangle \neq 0,$$

由于上面的第三项。因此，我们得到矛盾，由此可知 $a^\star \in \mathrm{supp}(H)$。

在 H 的支撑内的所有放大上稠密。证明 $\mathcal{S}$ 在 $\mathcal{C}_{a^\star,b}$ 和 $a^\star \in \mathrm{supp}(H)$ 内的密度至少为 $1 - \frac{1}{(q-1)^2} - 2000tq^{200-M/4}$ 后，我们可以使用与引理 5.2 的证明中相同的论证，说明 $\mathcal{S}$ 的密度至少为

$$1 - \frac{1}{(q-1)^2} - \frac{2}{q^{100}(q-1)} - 2000q^{200+t-M/4} - q^{-M/2},$$

在 $\cup_{v \in \mathrm{supp}(H)} \mathcal{C}_{v,b}$ 内。我们可以通过先选择一个包含 b 的 $k+t+100$-仿射子空间 V，再选择一个包含 b 的 $k+t$-仿射子空间 $U \subseteq V$，最后在满足 $\mathrm{Im}(T) = U$ 和 $Ta = b$ 的条件下输出 T，来选择 $T \in \mathcal{C}_{a^\star,b}$。

使用相同的抽样和平均论证，我们得到：对于 $k+t+100$-维仿射子空间 V，以下结论以至少 $1 - \frac{1}{(q-1)^2} - 2000q^{200+t-M/4} - q^{-M/2}$ 的概率成立:

- $\nu_V(\mathcal{A}_V) > 0$，其中 $\mathcal{A}_V = \{U \subseteq V \mid \dim(U) = k, f|_U \notin \mathcal{F}_{k+t}(H)\ b \in U\}$，
- $\nu_V(\mathcal{B}_V) \leqslant q^{M/2}O(\varepsilon)$，其中 $\mathcal{B}_V = \{U \subseteq V \mid \dim(U) = k, f|_U \notin \mathcal{F}_{k+t}(H)\ b \notin U\}$，

应用引理 6.3，结合 $\mathcal{G} = \mathcal{F}_{k+t}(H)$ 和 $g = f|_V$，我们得到存在一个值 γ，使得将 $f(b)$的值改为 γ 后，$\nu_V(\mathcal{A}_V) = 0$。根据上面的第一项，$\gamma \neq f(b)$。因此，在改变 $f(b)$ 的值之前，对于所有满秩 $B \in \mathcal{T}_{k+t+100,k+t}$，只要 $B(v) = b$ 对某个 $v \in \mathrm{supp}(H)$，我们必有 $\langle f|_V \circ B, H\rangle \neq 0$。减去非满秩变换所占的比例后，我们可以得出 $\mathcal{S}$ 的密度至少为

$$1 - \frac{1}{(q-1)^2} - \frac{2}{q^{100}(q-1)} - 2000q^{200+t-M/4} - q^{-M/2},$$

在 $\cup_{v\in\mathrm{supp}(H)}\mathcal{C}_{v,\ b}$。

纠正误差并迭代 最后，我们可以像第 5.3 节中那样纠正错误并进行迭代。对于至少 $9/10$ 个 $T \in \mathrm{supp}_{v\in\mathrm{supp}(H)}\mathcal{C}_{v,\ b}$，存在一个值 γ，使得将 $f(b)$ 的值改为 γ 后，T 接受 f。因此，存在一个 f'，它在除 b 之外的所有点上都与 f 相同，并且

$$\Pr_T[T \text{ rejects } f \mid \exists v \in \mathrm{supp}(H), T(v) = b] \leqslant 1 - \frac{9}{10}q.$$

由与引理 5.8 相同的计算可得

$$\mathrm{rej}(f') \leqslant \mathrm{rej}(f) - \frac{|\mathrm{supp}(H)|}{q^n C(q)},$$

对于某个 $C(q) = O(q)$，我们可以得出

$$\mathrm{rej}(f) \geqslant \Omega\left(\frac{|\mathrm{supp}(H)|}{q}\delta(f, \mathcal{F}_n(H))\right).$$

参考文献

[1] Noga Alon、Tali Kaufman、Michael Krivelevich、Simon Litsyn 和 Dana Ron。Reed-Muller 码的测试。IEEE信息论汇刊，51(11)：4032–4039，2005年。[2] Sanjeev Arora、Carsten Lund、Rajeev Motwani、Madhu Sudan 和 Mario Szegedy。证明验证与近似问题的困难性。ACM学报，45(3)：501–555，1998年。[3] Sanjeev Arora 和 Shmuel Safra。证明的概率检查：NP 的一种新刻画。ACM学报，45(1)：70–122，1998年。[4] Sanjeev Arora 和 Madhu Sudan。改进的低次数测试及其应用。《组合学》，23(3)：365–426，2003年。[5] Mitali Bafna、Boaz Barak、Pravesh K. Kothari、Tselil Schramm 和 David Steurer。在经过认证的小集合扩张器上进行唯一游戏。载于 STOC '21：第53届年度 ACM SIGACT计算理论研讨会，线上活动，意大利，2021年6月21日至25日，第1629–1642页，2021年。

[6] Mitali Bafna、Max Hopkins、Tali Kaufman 和 Shachar Lovett。高维扩张器：特征值剥离、伪随机性与唯一游戏。载于《2022年 ACM-SIAM离散算法研讨会论文集》，SODA 2022，线上会议／美国弗吉尼亚州亚历山德里亚，2022年1月9日至12日，第1069–1128页，2022年。[7] Mitali Bafna、Max Hopkins、Tali Kaufman 和 Shachar Lovett。高维扩张器上的超收缩性。载于 STOC '22：第54届年度 ACM SIGACT计算理论研讨会，意大利罗马，2022年6月20日至24日，第185–194页，2022年。[8] Boaz Barak、Parikshit Gopalan、Johan H˚astad、Raghu Meka、Prasad Raghavendra 和 David Steurer。让长码变得更短。SIAM计算杂志，44(5)：1287–1324，2015年。[9] Boaz Barak、Pravesh Kothari 和 David Steurer。短码图中的小集合扩张与 2-至-2 猜想。载于第10届理论计算机科学创新会议论文集，ITCS 2019，2021年1月10日至12日，美国加利福尼亚州圣迭戈，2019年。[10] Arnab Bhattacharyya、Swastik Kopparty、Grant Schoenebeck、Madhu Sudan 和 David Zuckerman。Reed-Muller 码的最优测试。载于第51届年度 IEEE计算机科学基础研讨会论文集，FOCS 2010，2010年10月23日至26日，美国内华达州拉斯维加斯，第488–497页，2010年。[11] Irit Dinur 和 Venkatesan Guruswami。通过低次长码构造概率可验证证明及受限超图着色的困难性。载于第54届年度 IEEE计算机科学基础研讨会，FOCS 2013，2013年10月26日至29日，美国加利福尼亚州伯克利，第340–349页，2013年。[12] Irit Dinur、Prahladh Harsha、Srikanth Srinivasan 和 Girish Varma。使用低次长码的去随机化图乘积结果。载于第32届理论计算机科学国际研讨会，STACS 2015，2015年3月4日至7日，德国加兴，第275–287页，2015年。[13] Irit Dinur、Subhash Khot、Guy Kindler、Dor Minzer 和 Muli Safra。关于格拉斯曼图中非最优扩张的集合。载于第50届年度 ACM SIGACT计算理论研讨会论文集，STOC 2018，美国加利福尼亚州洛杉矶，2018年6月25日至29日，第940–951页，2018年。[14] Irit Dinur、Subhash Khot、Guy Kindler、Dor Minzer 和 Muli Safra。迈向 2-至-1 游戏猜想的证明？载于第50届年度 ACM SIGACT计算理论研讨会论文集，STOC 2018，美国加利福尼亚州洛杉矶，2018年6月25日至29日，第376–389页，2018年。[15] Uriel Feige、Shafi Goldwasser、L´aszl´o Lov´asz、Shmuel Safra 和 Mario Szegedy。交互式证明与近似团的困难性。ACM学报，43(2)：268–292，1996年。[16] William T Gowers。Szemer´edi 定理的新证明。《几何与泛函分析》GAFA，11(3)：465–588，2001年。[17] Alan Guo、Swastik Kopparty 和 Madhu Sudan。通过提升得到的新型仿射不变码。载于第4届理论计算机科学创新会议论文集，ITCS '13，美国纽约州纽约，2013年，第529–540页。计算机协会。[18] Tom Gur、Noam Lifshitz 和 Siqi Liu。高维扩张器上的超收缩性。载于 STOC '22：第54届年度 ACM SIGACT计算理论研讨会，意大利罗马，2022年6月20日至24日，第176–184页，2022年。

[19] Venkatesan Guruswami、Prahladh Harsha、JohanH˚astad、Srikanth Srinivasan和Girish Varma。通过低次长码实现超多对数级超图着色困难性。SIAM计算杂志，46(1):132–159，2017。[20] Elad Haramaty、Noga Ron-Zewi和Madhu Sudan。提升码的绝对可靠测试。《计算理论》，11:299–338，2015。[21] Elad Haramaty、AmirShpilka和Madhu Sudan。小素域上多元多项式的最优测试。SIAM计算杂志，42(2):536–562，2013。[22] Charanjit S. Jutla、Anindya C. Patthak、AtriRudra和David Zuckerman。素域上的低次多-项式测试。《随机结构与算法》，35(2):163–193，2009。[23] Daniel M. Kane和RaghuMeka。用于多项式Lipschitz函数的PRG及其在最稀疏割中的应用。载于《计算理论研讨会会议录》，STOC'13，美国加利福尼亚州帕洛阿尔托，2013年6月1日至4日，第1–10页，2013年。[24] Tali Kaufman和Dana Ron。一般域上的多项式测试。SIAM计算杂志，36(3):779–802，2006。[25] Tali Kaufman和Madhu Sudan。代数性质测试：不变性的作用。载于《第40届ACM计算理论年度研讨会论文集》，STOC 2008，加拿大不列颠哥伦比亚省维多利亚，2008年5月17日至20日，第403–412页，2008年。[26] PeterKeevash、NoamLifshitz、Eoin Long和Dor Minzer。全局函数的超收缩性与尖锐阈值。arXiv预印本arXiv:1906.05568，2019年。[27] PeterKeevash、NoamLifshitz、Eoin Long和DorMinzer。码的禁交集。arXiv预印本arXiv:2103.05050，2021年。[28] Peter Keevash、NoamLifshitz和DorMinzer。关于交错群中最大的无积子集。arXiv预印本arXiv:2205.15191，2022年。[29] SubhashKhot、DorMinzer和Muli Safra。关于独立集、2对2游戏和格拉斯曼图。载于《第49届ACMSIGACT计算理论研讨会论文集》，STOC 2017，加拿大魁北克省蒙特利尔，2017年6月19日至23日，第576–589页，2017年。[30] SubhashKhot、Dor Minzer和MuliSafra。格拉斯曼图中的伪随机集合具有近乎完美的扩张。载于《第59届IEEE计算机科学基础研讨会论文集》，FOCS 2018，法国巴黎，2018年10月7日至9日，第592–601页，2018年。[31] DorMinzer和Tali Kaufman。由全局超收缩性得到的改进最优测试结果。载于《第63届IEEE计算机科学基础研讨会论文集》，FOCS2022，美国科罗拉多州丹佛，2022年10月31日至11月3日。[32] Ran Raz和Shmuel Safra。次常数错误概率的低次测试，以及NP的次常数错误概率PCP刻画。载于《第29届ACMSIGACT计算理论研讨会论文集》，STOC 1997，美国得克萨斯州埃尔帕索，1997年5月406日，第475–484页，1997年。[33] Noga Ron-Zewi和Madhu Sudan。广义Reed-Muller码测试查询复杂度的新上界。《计算理论》，9(25):783–807，2013年。

[34] Ronitt Rubinfeld 和 Madhu Sudan。多项式的鲁棒刻画及其在程序测试中的应用。SIAM计算杂志，25(2):252–271，1996年。

定理 2.1 的证明

现在我们证明定理 2.1。首先需要证明以下结果，这是定理 2.4] 的一个略微变体：[31,

定理 A.1. 设 $\mathcal{A} \subseteq \mathsf{AffGras}(n+\ell, \ell)$ 满足

1. $\mu(\mathcal{A}) \leqslant \xi$,
2. $\mathcal{A}$ 关于超平面、其线性部分上的超平面以及其线性部分上的点是 ξ-伪随机的。

3. $1 - \Phi(\mathcal{A}) \geqslant \frac{1}{q} - \delta$.

那么存在一个点 $x \in \mathbb{F}_q^n$，使得 $\mu(\mathcal{A}_x) \geqslant 1 - q^2\left(4q^{-\ell} + 867\xi^{1/4} + \frac{\delta}{q-1}\right)$。

T

测度、扩张和伪随机性均相对于 $\mathsf{AffGras}(n+\ell, \ell)$ 而定义，$\mu(\mathcal{A}_x)$ 表示 $\mathcal{A}$ 在 $\mathsf{AffGras}(n+\ell, \ell)$ 中包含点 x 的子集里的分数大小。

为了说明仿射双线性方案图中也成立类似结果，我们重述 [9]中的步骤，以建立与仿射格拉斯曼图的联系，然后应用定理 A.1。为此，定义以下单射 $\varphi\colon \mathcal{T}_{n,\ \ell} \to \mathcal{V}_{n+\ell,\ \ell}$。令 $\{e_1, \ldots, e_\ell\} \in \mathbb{F}_q^\ell$ 为标准基。对于长度分别为 ℓ_1 和 ℓ_2 的两个列向量 v 和 w，我们将 $(v, w)^T$ 表示为通过垂直拼接 v 和 w 得到的长度为 $\ell_1 + \ell_2$ 的列向量。同样地，令 $[v^T, w^T]$ 为通过水平拼接 v 和 w 得到的长度为 $\ell_1 + \ell_2$ 的列向量。

对于仿射变换 $(M, c) \in \mathcal{T}_{n,\ell}$，其中 M 的列为 $v_1, \ldots, v_\ell$，我们定义 $\varphi((M, v)) = (0, c)^T +$ 张成空间$((e_1, v_1)^T, \ldots, (e_\ell, v_\ell^T))$。显然，该映射是单射。此外，$\varphi$ 的像是满足将 V 投影到前 ℓ 个坐标后为满秩的所有 ℓ-维仿射子空间 $V \subseteq \mathbb{F}_q^{n+\ell}$。

映射 φ 保留边，几乎保留扩张，并将$\mathsf{AffBilin}(n, \ell)$ 中的规范非扩张集合映射到 $\mathsf{AffGras}(n+\ell, \ell)$ 中的对应集合。

引理A.2. 如果 $T_1, T_2 \in \mathcal{T}_{n,\ell}$ 在 $\mathsf{AffBilin}(n, \ell)$ 中相邻，那么 $\varphi(T_1)$ $\varphi(T_2)$在$\mathsf{AffGras}(n+\ell, \ell)$ 中相邻。反之，如果 $V_1, V_2 \in V_{n,\ell}$ 在 $\mathsf{AffGras}(n+\ell, \ell)$ 中相邻，且二者都在 φ 的像中，那么$\varphi^{-1}(V_1)$ $\varphi^{-1}(V_2)$ 在 $\mathsf{AffBilin}(n, \ell)$ 中相邻。

证明。对于第一个方向，假设 T_1 和 T_2 分别由 (M_1, c_1) 和 (M_2, c_2) 给出。令 M_1'' 为将 I_ℓ 和 M 纵向拼接得到的 $(n+\ell) \times n$ 矩阵，并令 c_1'' 为将长度为 ℓ 的零向量与 c_1 纵向拼接得到的长度为 $n+\ell$ 的向量。类似地定义 M_2'' 和 c_2''。注意，$\varphi(T_1)$ 由仿射变换 $T_1'' = (M_1'', c_1'')$ 的列像给出，而 $\varphi(T_2)$ 由仿射变换 $T_2'' = (M_2'', c_2'')$ 的列像给出。因此，要证明边得以保持，只需证明 T_1'' 和 T_2'' 的列像的交集维数为 $\ell - 1$。确实，$T_1'' - T_2'' = (M_1'' - M_2'', c_1'' - c_2'')$，并且由于 $M_1'' - M_2''$ 和 $c_1'' - c_2''$ 在前 ℓ 行中都全为零，因此 $\dim(\ker(T_1'' - T_2'')) = \dim(\ker(T_1 - T_2)) = \ell - 1$。因此，$\dim(\mathrm{Im}(T_1'' - T_2'')) = 1$ 且 $\dim(\varphi(T_1) \cap \varphi(T_2)) = \ell - 1$。

在逆向方向，设 $U, V \in \mathcal{V}_{n+\ell,\ell}$ 其中$\dim(U \cap V) = \ell - 1$。记 $U = u_0 +$ 张成空间$(u_1, \ldots, u_\ell)$ 和 $V = v +$ 张成空间 $(v_1, \ldots, v_\ell)$，其中 $u_i = (e_i, u_i')^T$, $v_i = (e_i, v_i')^T$, $u_0 = (0, u_0')^T$,

以及 $v_0 = (0, v_0')^T$。令 M_1 为列为 u_i 的矩阵，令 M_2 为列为 v_i 的矩阵。根据假设，仿射变换 $T_1 = (M_1, u_0)$ 和 $T_2 = (M_2, v_0)$ 的像的交集的维数为 $\ell - 1$。我们断言，这意味着 T_1 和 T_2 实际上在一个 $\ell - 1$ 维子空间上相等。事实上，如果 $T_1(a) = T_2(b)$ 对于 $a, b \in \mathbb{F}_q^\ell$，那么考察前 ℓ 个坐标可推出 $a = b$。因此，T_1、T_2 在$\mathrm{Im}(T_1) \cap \mathrm{Im}(T_2)$ 的 $\ell - 1$ 维原像上相等。最后，由于 $\varphi^{-1}(U)$ 和 $\varphi^{-1}(V)$ 分别由将 T_1 和 T_2 投影到最后 n 个坐标所得，$\dim(\ker(\varphi^{-1}(U) - \varphi^{-1}(V))) = \ell - 1$，结论得证。 □

引理 A.3. 设 $V_1 \in \mathcal{V}_{n+\ell,\ell}$ 属于 φ的像。那么，它的邻居中至少有 $1 - 1/q$ 的比例也属于 φ的像。

证明. 回顾一下，若将 V投影到其前 ℓ个坐标后得到满秩矩阵，则 V属于 φ 的像。固定$V_1 \in \mathcal{V}_{n+\ell,\ell}$，使其属于 φ的像。可以按如下方式采样得到 V_1 的一个邻居：均匀随机地选取一个点 $v_0 \in V$和 ℓ 个线性无关方向 $v_1, \ldots, v_\ell$，使得 $V_1 = v_0 +$张成空间 $\mathrm{span}(v_1, \ldots, v_\ell)$；再在 $\mathrm{span}(v_1, \ldots, v_\ell)$之外均匀随机地选取一个 v_ℓ'，并令 $V_2 = v_0 +$为 $\mathrm{span}(v_1, \ldots, v_{\ell-1}, v_\ell')$。由于 V_1属于 φ的像，将 $v_1, \ldots, v_\ell$投影到前 ℓ个坐标后得到满秩矩阵。同理，若将 v_ℓ'投影到其前 ℓ个坐标后，与 $v_1, \ldots, v_{\ell-1}$投影到前 ℓ个坐标所得的向量线性无关，则 V_2属于 φ 的像。该条件成立的概率恰为 $1 - 1/q$，证毕。 □

引理 A.4. 如果 $S \subseteq \mathcal{T}_{n,\ell}$ 满足 $1 - \Phi(S) = \eta$，那么 $\varphi(S)$ 满足 $1 - \Phi'(\varphi(S)) \geqslant \eta(1 - 1/q)$，其中 Φ和 Φ' 分别是 $\mathrm{AffBilin}(n, \ell)$ 和 $\mathrm{AffGras}(n + \ell, \ell)$ 中的扩张。

证明。这直接由前面的两个引理得出。根据引理A.3，$1 - 1/q$ 比例的 $\varphi(S)$的邻居也在 φ 的像中，并且根据假设和引理A.2 η，这些邻居中有 $1 - 1/q$ 比例也在 $\varphi(S)$中。结论得证。 □

引理 A.5。映射 φ 是以下集合对之间的双射：

- $\mathcal{C}_{a,b}$ 以及 $\mathcal{D}_v \cap \mathrm{Im}(\varphi)$ 对于 $v = [a, b]^T$。
- $\mathcal{C}_{a,b,\text{线性}}$ 和 $\mathcal{D}_{v,\text{线性}} \cap \mathrm{Im}(\varphi)$对于 $v = [a, b]^T$.
- $\mathcal{C}_{a^T,\ b,\ \beta}$ 以及 $\mathcal{D}_W \cap \mathrm{Im}(\varphi)$，其中 W由 $\langle [-b^T, a^T], x \rangle = \beta$ 给出。
- $\mathcal{C}_{a^T,\ b,\ \beta,\ \mathrm{lin}}$ 以及 $\mathcal{D}_{W,\ \mathrm{lin}} \cap \mathrm{Im}(\varphi)$，其中 W由 $\langle [-b^T, a^T], x \rangle = \beta$ 给出。

证明。我们展示缩入和缩出的情形。其余两种情形类似。

放大：任取一个任意的 $T = (M, c) \in \mathcal{C}_{a,\ b}$并令 let $M' = [I_\ell, M]^T$和 $c' = [0, c]^T$。容易验证 $M'a + c' = [a, b]^T$。由于 T是任意的，这就证明了双射的前半部分。

为完成此情形的证明，我们必须证明 $\mathrm{Im}(\varphi)$ 中的任意仿射子空间都会被映射到。取这样的一个仿射子空间 U。由于 $U \in \mathrm{Im}(\varphi)$，我们可以将其写为 $U = c' + \mathrm{span}(u_1, \ldots, u_\ell)$，其中 u_i 的前 ℓ 个坐标等于 e_i，而 c' 的前 ℓ 个坐标全为 0。存在 u_i 的各项与 c' 的唯一线性组合，其和为 v；考察前 ℓ 个坐标可知，必有 $v = c' + a_1 u_1 + \cdots + a_\ell u_\ell$，其中 a_i 是 a 的第 i 个坐标。令 M 为矩阵，其第 i 列由 u_i 的最后 n 个元素给出，并令 c 为 c' 的最后 n 个元素。因此，$U = \varphi((M, c))$，且 $Ma = b$。

缩出集：任取一个 $T = (M, c) \in \mathcal{C}_{a^T,b,\beta}$，并设其列为 $v_1, \ldots, v_{\ell_0}$ 则$\varphi(T) = c' +$张成空间$(v_0', \ldots, v_\ell')$，其中 $c' = [0, c]^T$且 $v_i' = [e_i, v_i]^T$对 $1 \leqslant 1 \leqslant \ell$成立。令 $h = [-b^T, a^T]$为长度为 $\ell + n$ 的行向量，其前 ℓ 个元素为 b^T，最后 n 个元素为 a^T。根据构造，$\langle h, v_i' \rangle = 0$

且 $\langle h, c\rangle = \beta$。因此， $\varphi(T)$ 包含于由 $\langle h, x\rangle = \beta$ 给出的超平面中。由于 T 是任意的，可知 $\varphi(\mathcal{C}_{a^T,b,\beta})$ $\subseteq W$，其中 W 是由 $\langle h, x\rangle = \beta$ 给出的超平面。

对于该双射的另一个方向，取任意 $z + V \in \mathcal{D}_{W,\mathrm{lin}} \cap \mathrm{Im}(\varphi)$，令 (M, c) 为其在 φ 下的原像，并设 W 由 $\langle h, x\rangle = 0$ 给出（注意， W 必须是一个线性子空间，因为它包含 V，而 V 是一个线性子空间）。令 b 为 h 的前 ℓ 个坐标的负值，并令 a 为 h 的后 n 个坐标。由此可得 $a^T M = b$。 □

借助这些引理 因此，我们可以得到 AffBilin$(n, \ell$ 中扩张性较差集合的所需刻画。).

定理 2.1的证明。假设 $\mathcal{S}$ 满足定理 2.1的条件，并令 $\mathcal{A} = \varphi(\mathcal{S}) \subseteq$ AffGras$(n+\ell, \ell)$。以下用 Φ 和 μ 分别表示 AffGras$(n + \ell, \ell)$ 中的扩张和测度。由引理 A.4 可知， $1 - \Phi(\mathcal{A}) \geqslant \frac{1}{q} - \frac{1}{q^2}$。由引理 A.5 可知， $\mathcal{A}$ 关于超平面、其线性部分上的超平面以及其线性部分上的点也是 ξ-伪随机的。最后，由于 φ 是一个单射，显然 $\mu(\mathcal{A}) \leqslant \xi$。由引理 A.1 可知，存在一个点 v 使得

$$\frac{|\mathcal{A} \cap \mathcal{D}_v|}{|\mathcal{D}_v|} \geqslant 1 - q^2 \left(4q^{-\ell} + 867\xi^{1/4} + \frac{1}{q^{100}(q-1)}\right).$$

根据引理 A.5，存在一个缩入（在仿射双线性方案图中）$\mathcal{C}_{a,\ b}$ 使得 $\varphi^{-1}(\mathcal{A} \cap \mathcal{D}_v) = \mathcal{S} \cap \mathcal{C}_{a,\ b}$，因此 $|\mathcal{S} \cap \mathcal{C}_{a,\ b}| = |\mathcal{A} \cap \mathcal{D}_v|$。最后， $\frac{|\mathcal{C}_{a\ b}|}{|\mathcal{D}_v|}$, 表示从 $\mathcal{D}_v$ 中随机选取的仿射子空间在限制到其前 ℓ 个坐标时不满秩的概率。该概率至多为 $1 - 1/q$。事实上，可以通过选择 $\mathcal{D}_v$ 个线性无关向量 v_1、……、 v_ℓ，并令仿射子空间为 $v +$ 张成空间$(v_1$、……、 $v_\ell)$，来选取 $\mathcal{D}_v$ 中的一个仿射子空间。假设前 $\ell - 1$ 个向量的选取使得它们限制到前 ℓ 个坐标后线性无关，那么 v_ℓ 也满足这一性质的概率为 $1 - 1/q$。由此可得

$$\frac{|\mathcal{S} \cap \mathcal{C}_{a,b}|}{|\mathcal{C}_{a,b}|} \geqslant \frac{q}{q-1}\left(1 - q^2\left(4q^{-\ell} + 867\xi^{1/4} + \frac{1}{q^{100}(q-1)}\right)\right) \geqslant 1 - \frac{1}{(q-1)^2} - \frac{q^3}{q-1}\left(4q^{-\ell} + 867\xi^{1/4}\right).$$

□

B 刻画 RM$[n, q, d]$ 的典范单项式

本节给出定理 3.4 的证明，说明任何以概率 1 通过测试的多项式，其次数都是 d。该证明隐含于 [33], 中，但由于我们提出的测试器形式不同，为使论述完整，我们仍给出证明。

写作 $d+1 = \ell \cdot p(q - q/p) + r$，其中 $1 \leqslant r \leqslant p(q - q/p)$，并令 $s = \ell \cdot p$。首先，注意我们的测试器会检测以下形式的单项式：

$$\left(\prod_{i=1}^{s} x_i^{q-q/p}\right) \prod_{j=1}^{p+2} x_{s+j}^{e_j}, \tag{6}$$

对于满足 $\sum_{j=1}^{t} e_j \geqslant r$ 的任意$(e_1, \ldots, e_t)$。事实上，对于满足 $\sum_{j=1}^{t} e_j \geqslant r$的 $(e_1, \ldots, e_t)$，令 $e' = (q-1-e_1, \ldots, q-1-e_t)$，并考虑 $H_{e'}(x_1, \ldots, x_{s+t})$ 的扩张。利用卢卡斯定理，不难看出， $H_{e'}(x_1, \ldots, x_{s+t})$ 的扩张包含单项式 $\left(\prod_{i=1}^{s} x_i^{q/p-1}\right) \prod_{j=1}^{t} x_{s+j}^{q-1-e_j}$，因此根据引理 3.3，(6) 中的任意规范单项式都会被拒绝。

令 $\mathcal{G}$ 为以概率 1 通过稀疏 $s + t$-仿射子空间测试的函数族。本节将证明：

引理 B.1. 若 f 以概率 1 通过稀疏-$s+t$-仿射子空间测试，则 $f \in \mathrm{RM}[n,q,d]$。等价地，$\mathcal{G} = \mathrm{RM}[n,q,d]$

这个引理的一个方向显然成立。若 $\deg(f) \leqslant d$，则 f 以概率 1 通过。另一个方向相当于证明 $\mathcal{G} \subseteq \mathrm{RM}[n,q,d]$。为此，我们实际上将证明其逆否命题：若 $\deg(f) \geqslant d+1$，且 $f \in \mathcal{G}$，则式 (6) 中的某个典范单项式必定属于 $\mathcal{G}$。这就构成矛盾，并由此证明 $\mathcal{G} \subseteq \mathrm{RM}[n,q,d]$。

在开始证明之前，我们需要用到 [25] 中关于仿射不变多项式族的以下两个事实。对于多项式族 $\mathcal{F}$，令 $\mathrm{supp}(\mathcal{F})$ 表示至少出现在其中一个多项式中的单项式集合。第一个事实指出，这些单项式构成 $\mathcal{F}$ 的一组基。

引理 B.2（单项式提取引理 [25]）。若 $\mathcal{F}$ 是一个仿射不变多项式族，则 $\mathcal{F} = \mathrm{span}(\mathrm{supp}(\mathcal{F}))$。

第二个事实表明，仿射不变多项式族中出现的单项式具有 p 影闭性质。对于两个整数 a、$b \in \{0,\dots,q-1\}$，令 $a = \sum_{i=0}^{k-1} p^i a_i$ 和 $b = \sum_{i=0}^{k-1} p^i b_i$ 为它们的 p 进制表示（回忆 $q = p^k$）。若 $a_i \leqslant b_i$ 对 $i = 0, \dots, k-1$ 均成立，则称 a 属于 b 的 p阴影，并记为 $a \leqslant_p b$。接着，对于两个指数向量 $e = (e_1, \dots, e_n)$ 和 $e' = (e'_1, \dots, e'_n)$，若对每个 i都有 $e_i \leqslant_p e'_i$，则称 $e \leqslant_p e'$。仿射不变多项式族具有以下影闭性质。

引理B.3。令 $\mathcal{F} =$ 张成空间($\mathrm{supp}(\mathcal{F})$) 为一个仿射不变的多项式族。如果 $e \leqslant_p e'$ 并且$e' \in \mathrm{supp}(\mathcal{F})$，那么 $e \in \mathrm{supp}(\mathcal{F})$ 也成立。

最后，我们还需要以下结论，它将使我们能够从一个 $\mathcal{F}$ 单项式转到另一个次数相同、但各个次数的分布有所变化的单项式。

引理 B.4。假设 $x^e \in \mathcal{F}$ 并且假设 $m \leqslant_p e_2$。那么单项式 $x^{e'} \in \mathcal{F}$，其中 $e' = (e_1 + m、 e_2 - m、 e_3、 ...、 e_n)$。

证明。令 T为仿射变换 $T(x) = (x_1, x_1 + x_2, x_3, \dots, x_n)$。那么，

$$x^e \circ T = x_1^{e_1}(x_1+x_2)^{e_2} \prod_{j=3}^{n} x_j^{e_j} = \left(\sum_{i=0}^{d_2} \binom{d_2}{i} x_1^{e_1+i} x_2^{e_2-i} \right) \prod_{j=3}^{n} x_j^{e_j}.$$

根据卢卡斯定理以及假设 $m \leqslant_p e_2$, $\binom{d_2}{m} \neq 0$属于 $\mathbb{F}_q$，因此 $x^e \circ T = x_1^{e_1}(x_1+x_2)^{e_2} \prod_{j=3}^{n} x_j^{e_j}$包含单项式 $x^{e'}$。结论由引理 B.2 得出。

□

有了这三个引理，我们可以开始证明引理 B.1。反设 $\deg(f) > d$，利用上述引理，我们将证明这意味着某个典范单项式属于 $\mathcal{F}$。然而，这是不可能的，因为式 (6) 中的所有单项式都被恒等式 $T = I$ 拒绝。

引理 B.1 的证明。设 $\mathcal{F}$ 为以概率 1 通过稀疏 $s+t$-仿射子空间测试的多项式族。为导出矛盾，假设 $f \in \mathcal{F}$ 和 f 含有一个次数为 $d' > d$ 的单项式。令 $x^e = \prod_{i=1}^{n} x_i^{e_i}$ 为这样的单项式，并令 ℓ 为满足 $e_1 + \cdots + e_\ell > d$ 的最小索引。于是 $(e_1, \dots, e_\ell, 0, \dots, 0) \leqslant_p e$，因此 $\prod_{i=1}^{\ell} x_i^{e_i} \in \mathcal{F}$，且

$$d+1 \leqslant \sum_{i=1}^{\ell} e_i \leqslant d + q - 1 = s(q - q/p) + r + q - 1.$$

我们将证明，这个单项式会使某个典范单项式属于 $\mathcal{F}$。首先，我们声称存在一个单项式 $x^{e'}$，使得对于 $i = 1, \ldots, s$，有 $e'_i \geqslant q - q/p$。定义

$$c(e) = \sum_{i=1}^{s} \max(0, (q - q/p) - e_i).$$

如果 $c(e) = 0$，那么 e 就具有所需的形式。如果 e 不具有所需的形式，那么存在 $i \leqslant s$ 使得 $e_i < q - q/p$。否则，以下情况必有一种成立：

- 存在 $j > s$ 使得 $e_j > 0$，此时我们只需找到某个 $p^m \leqslant_p e_j$，并应用引理 B.4，以单项式 $x_i^{e_i+p^m} x_j^{e_j-p^m}$ 替换 $x_i^{e_i} x_j^{e_j}$，
- 存在 $j \leqslant s$ 使得 $e_j > q - q/p$。在这种情况下，我们可以找到 p^m 使得 $e_j - p^m \geqslant q - q/p$，并应用引理 B.4，以单项式 $x_i^{e_i+p^m} x_j^{e_j-p^m}$ 替换 $x_i^{e_i} x_j^{e_j}$。

在任一情况下，我们都可以找到另一个单项式 $x^{e'}$ 使得 $x^{e'} \in \mathcal{F}$，且 $c(e') < c(e)$。重复这一过程，我们最终必能找到所需的单项式，使得 $c(e) = 0$。

现在，稍微滥用一下记号，令 x^e 表示这个单项式。我们有，$d+1 \leqslant \sum_{i=1}^{n} e_i \leqslant d+q-1 = s(q-q/p) + r + q - 1$ 且 $e_i \geqslant q - q/p$ 适用于 $1 \leqslant i \leqslant s$。现在我们可以基本沿用相同的论证，将次数中超过 $q - q/p$ 的部分移至 $e_{s+1}, \ldots, e_{s+t}$。剩余部分至多为

$$d + q - 1 - s(q - q/p) = r + q - 1 \leqslant p(q - q/p) + q - 1,$$

减去后剩余的次数，因此我们可以运用上述论证进行移位，直到每个次数 $e_{s+1}, \ldots, e_{s+t-1}$ 都至少为 $q - q/p$。这样剩余次数至多为 $q - 1$，我们只需将其移至 e_{s+t}即可。

□

引理 B.5. 设 $g\colon \mathbb{F}_q^p \to \mathbb{F}_q$ 满足 $\deg(g) \geqslant q(p-1)$。那么存在满秩仿射变换 $T_1, T_2 \in \mathcal{T}_{p,\ p}$，使得：

1. $g \circ T_1$ 包含一个单项式$\prod_{i=1}^{p} x_i^{e_i}$，其满足 $q - q/p \leqslant e_i \leqslant q - 1$ 对于所有 $i \in [p]$。
2. $\langle g \circ T_2, P \rangle \neq 0$.

证明。为证明引理的第一部分，我们采用与引理B.4的证明类似的思路。假设 g 包含一个单项式 $\prod_{i=1}^{p} x_i^{e'_i}$，并假设 $m \leqslant_p e'_2$。考虑满秩仿射变换 $T_\alpha(x) = (x_1, \alpha x_1 + x_2, x_3, \ldots, x_p)$（对于 $\alpha \in \mathbb{F}_q$）以及 $g \circ T_\alpha$中 $x_1^{e'_1+m} x_2^{e'_2-m} \prod_{i=3}^{p} x_i^{e'_i}$ 的系数。不难看出，该系数是关于 α 的非零多项式，因此存在一个 α，使得 $g \circ T_\alpha$ 包含单项式 $x_1^{e'_1+m} x_2^{e'_2-m} \prod_{i=3}^{p} x_i^{e'_i}$。由于 T_α 是一个满秩仿射变换，我们可以反复应用这样的变换，从而得到一个满秩 $T_1 \in \mathcal{T}_{p,\ p}$，使得 $g \circ T_1$ 包含一个满足 $q - q/p < e_i \leqslant q - 1$ 的单项式 $\prod_{i=1}^{p} x_i^{e_i}$，从而证明引理的第一部分。

令 T_1 为第1部分中的变换，并令 $g' = g \circ T_1$，使得 g' 包含一个单项式 $\prod_{i=1}^{p} x_i^{e_i}$，且具有 $q - q/p < e_i \leqslant q - 1$。对于 $a \in \mathbb{F}_q^p$，令 T_a 为满足 $T_a(x) = (x_1 + a_1, \ldots, x_p + a_p)$的满秩仿射变换，并考虑内积

$$\langle g' \circ T_a, P \rangle,$$

作为关于 a 的多项式。回顾一下，P 包含单项式 $\prod_{i=1}^{p} x_i^{q/p-1}$。由于 g' 包含单项式$\prod_{i=1}^{p} x_i^{e_i}$，且 $q - q/p < e_i \leqslant q - 1$，因此存在一项 $\prod_{i=1}^{p} a_i^{e_i - (q-q/p)}$，其系数非零，并且该项无法被任何其他单项式抵消。因此，$\langle g' \circ T_a, P \rangle$ 是关于 a 的非零多项式，并且存在一个 $a \in \mathbb{F}_q^p$ 使得 $\langle g' \circ T_a, P \rangle \neq 0$。这就证明了引理的第二部分。 □

C 引理 5.3 的证明

在本节中，我们给出引理 5.3 的证明。这本质上与 [31, 命题 3.5] 相同，仅作了细微修改。回顾一下：g： $\mathbb{F}_q^{\ell+100}$是任意多项式，d 是任意次数参数，$b \in \mathbb{F}_q^{\ell+100}$是任意点。我们在 AffGras($\ell+100, \ell$) 中进行讨论。用 ν 表示所有 ℓ-仿射子空间上的均匀测度，用 ν_b 表示 b上的缩入的均匀测度。提及缩入、线性部分上的缩入等时，我们指的是仿射格拉斯曼图中的相应版本。我们有以下两组 ℓ-仿射子空间，

$$\mathcal{A} = \{U \mid \dim(U) = \ell, \deg(g|_U) > d, b \in U\},$$
$$\mathcal{B} = \{U \mid \dim(U) = \ell, \deg(g|_U) > d, b \notin U\},$$

以及 $\nu(\mathcal{B}) \leqslant q^{M/2}O(\varepsilon)$。我们将证明引理 5.3 的以下较弱形式，然后解释为什么它可以推出完整的引理 5.3。

引理 C.1. 若 $\nu(\mathcal{B}) \leqslant q^{M/2}O(\varepsilon)$，则 $\mathcal{B} = \emptyset$。此外，存在一个值 γ，使得将 $f(b)$ 改为 γ 后，$\nu_b(\mathcal{A}) \leqslant 1 - \frac{1}{q}$。

在证明该引理之前，我们先解释它为何能推出引理 5.3。假设引理 C.1 成立，设将 $g(b)$ 的值改为 γ 后得到的函数为 g'，并考虑由满足 $\deg(g'|_U) > d$ 的 ℓ-维仿射子空间 $\mathcal{U}$ 构成的集合。为导出矛盾，假设 $\mathcal{U}$ 非空。我们记录关于 $\mathcal{U}$ 的一些事实，

1. $\mathcal{U} \subseteq \mathcal{D}_b = \{U \mid \dim(U) = \ell, b \in U\}$。2. $\nu_V(\mathcal{U}) \leqslant q^{-100}$。3. $\Phi(\mathcal{U}) \leqslant 1 - \frac{1}{q}$。
4. $\nu_V(\mathcal{U})$ 关于线性部分上的缩出和缩出集是 q^{-99} 伪随机的。5. $\nu_V(\mathcal{U})$ 关于线性部分上的放大是 q^{-100} 伪随机的。

第一项由假设引理 C.1 得出。第二项由第一项以及对包含 b 的 ℓ 个仿射子空间所占比例的界得出。第三项和第四项可由与引理 4.2 和 4.3 相同的论证得出。最后，第五项再次由第一项以及以下事实得出：对于线性部分上的任意缩入，从该集合中随机选取的一个 ℓ 维仿射子空间包含点 b 的概率至多为 q^{-100}。

将 $\xi = q^{-100}$ 代入定理 A.1，可得 $\mathcal{U}$ 在某个缩入中的密度至少为 $1 - q^2(867q^{-25} + q^{-\ell}) > 1 - 1/q$，这里用到了事实 $\ell \geqslant 4$。只有一个缩入中 $\mathcal{U}$ 的密度可能非零，那就是 b 上的缩入。然而，这与以下假设矛盾：改变 $g(b)$ 的值后，$\nu_b(\mathcal{A}) \leqslant 1 - \frac{1}{q}$。简言之，我们已经证明，在这种设定下，如果某项修正导致某个缩入内的拒绝概率降至 $1 - 1/q$ 以下，那么拒绝概率实际上必须为 0。

我们现在给出引理 C.1 的证明。该证明需要以下结果，该结果在 [5, 31], 中也被使用过，并在引言中被称为影子引理。

引理 C.2. 令 $d \in \mathbb{N}$ 为一个次数参数，且 $k \geqslant \lceil \frac{d+1}{q - q/p} \rceil$。那么对于任意 $f\colon \mathbb{F}_q^{k+1} \to \mathbb{F}_q$:

1. *If* $\deg(f) > d$, *then* $\varepsilon_{k,d}(f) \geqslant \frac{1}{q}$.

2. 若 $d < \deg(f) < (k+1)(q-1)$，则 $\varepsilon_{k,\,d}(f) > \frac{1}{q}$。

其中，$\varepsilon_{k,d}(f)$ 和 $\varepsilon_{k+1,d}(f)$ 分别表示在限制 f 的次数大于 d 的 k-仿射子空间和 $k+1$-仿射子空间所占的比例。

在 [31] 中，本引理用于证明拒绝平坦的集合是不扩张的，这与本文中的引理4.2类似。不过，该引理还有另一个用途，这一点在其第二项中有所陈述。就我们而言，第二项表明，如果 $f|_V$的次数大于 d，并且对于超平面 $U \subseteq V$中多于 $1/q$ 个的超平面，我们还有 $\deg(f|_U) > d$，那么 $f|_V$不可能包含次数最大的单项式。在本节中，我们将使用参数为 $d = d$ 和 $k = \ell$的引理 C.2。注意，根据假设，$\ell \geqslant \lceil \frac{d+1}{q-q/p} \rceil$。

我们的第一个目标是证明 $\mathcal{B} = \emptyset$。首先，在给定 $b \notin W$的条件下，均匀地取一个 $(\ell+40)$-仿射子空间 W 均匀。令

$$\mathcal{B}_W = \{B \subseteq W \mid B \in \mathcal{B}\},$$

and 在 AffGras(W, ℓ) 中工作——包含于 W 中的 ℓ 维仿射子空间所构成的仿射格拉斯曼图 .

令 μ_W 和 Φ_W 分别表示 AffGras(W, ℓ)中的测度和扩张。我们断言，要么$\mu_W(\mathcal{B}_W) = 0$，要么 $\mu_W(\mathcal{B}_W) \geqslant q^{-100}$。否则，$0 < \mu_W(\mathcal{B}_W) < q^{-100}$，且 $\mathcal{B}_W$关于线性部分上的放大和放大是 q^{-60}伪随机的。通过与引理4.3类似的论证，我们得到 $\mathcal{B}_W$关于线性部分上的缩出集和缩出集是 q^{-98} 伪随机的；通过与引理 4.1 类似的论证，我们得到 $1 - \Phi_W(\mathcal{B}_W) \geqslant 1/q$。然而，这与定理 A.1 矛盾，因此我们得出结论：要么 $\mu_W(\mathcal{B}_W) = 0$，要么 $\mu_W(\mathcal{B}_W) \geqslant q^{-100}$。

引理 C.3. $\mathcal{B} = \emptyset$.

证明。否则我们可以找到一个 W，使得 $\mu_W(\mathcal{B}_W) \geqslant q^{-100}$。固定这样一个 W，并在以 $b \notin Y$ 为条件的情况下均匀采样一个 $\ell+99$-仿射子空间 Y，以及一个均匀的 $\ell+60$-仿射子空间 $A_2 \subseteq Y$。现在考虑 $A_2 \cap W$。我们可以将 W 看作由60 个线性无关的线性方程 $\langle h_1, x\rangle = c_1, \ldots, \langle h_{60}, x\rangle = c_{60}$定义。也就是说，$W$ 是 $\mathbb{F}_q^{\ell+100}$中满足这 60个方程的子空间。同样，A_2 由 39个线性方程的限制给出，即 $\langle h'_1, x\rangle = c'_1, \ldots, \langle h'_{39}, x\rangle = c'_{39}$。所有 99 个线性方程线性无关的概率至少为

$$\prod_{j=0}^{38} \frac{q^{99} - q^{60+j}}{q^{99}} \geqslant e^{-2\sum_{j=1}^{\infty} q^{-j}} \geqslant e^{-4/q},$$

且 $A_2 \cap W$在 AffGras(W, ℓ) 上均匀分布。因此，

$$\Pr[A_2 \cap W \in \mathcal{B}_W] \geqslant e^{-4/q} q^{-100}.$$

如果 $A_2 \cap W \in \mathcal{B}_W$，那么 $A_2 \in \mathcal{B}_Y^{\uparrow 60}$，其中上影是相对于 AffGras$(Y, \ell)$ 取的，因此可得

$$\mathop{\mathbb{E}}_{Y}[\mu_Y(\mathcal{B}_Y^{\uparrow 60})] \geqslant e^{-4/q} q^{-100}.$$

另一方面，由引理 C.2 可得，

$$\mathop{\mathbb{E}}_{Y}[\mu_Y(\mathcal{B}_Y^{\uparrow 60})] \leqslant q^{60} \mathop{\mathbb{E}}_{Y}[\mu_Y(\mathcal{B}_Y)] \leqslant 2q^{60}\mu(\mathcal{B}_V) \leqslant 2q^{60+M/2} O(\varepsilon).$$

根据假设 $\varepsilon < q^{-M}$，综上可得，

$$q^{-M/2} \geqslant \frac{1}{C(q) q^{-160}},$$

对于某个常数 $C(q)$。当 M 足够大时，这就产生了矛盾。 □

现在我们完成引理 C.1 的证明，由此也证明了引理 5.3。

引理 5.3 的证明。固定一个包含 b 的 ℓ-维仿射子空间 U。我们将证明，存在一个值 γ，将 $g(b)$ 的值改为 γ 后，会得到定义在 U 上的一个次数为 r 的函数。证明这一事实，并在所有 ℓ-维仿射子空间上选取最常见的 γ，即可证明引理 C.1；根据前面的讨论，这又能证明引理 5.3。

假设 $\deg(g|_U) > d$，否则令 $\gamma = g(b)$ 即可得证。取一个 $\ell+1$-维仿射子空间 $U' \supset U$，并令 $g' = g|_{U'}$，且令 $M(x) = 1_{x \neq b}$，定义在 U' 上。注意到 $M(x)$ 含有次数为 $(\ell+1)(q-1)$ 的单项式，因此存在某个值 γ，使得 $\gamma M(x) + g'(x)$ 的次数严格小于 $(\ell+1)(q-1)$。证明对于这个 γ，$\deg(\gamma M(x) + g'(x)) \leqslant d$，即可完成证明。

由于我们已经证明，对于任何不包含点 b 的 ℓ-维仿射子空间，都有 $\deg(g|_{U'}) \leqslant d$，这意味着在任何不包含 b 的 ℓ-维仿射子空间上，$\gamma M(x) + g'(x)$ 的次数也至多为 d。这是因为限制在这类仿射子空间上时，$\gamma M(x) + g'(x)$ 等于 g 的限制再加上某个常数多项式。由于 g 的限制次数至多为 d，所以 $\gamma M(x) + g'(x)$ 的次数也至多为此值。因此，只有当限制在包含 b 的 ℓ-维仿射子空间上时，$\gamma M(x) + g'(x)$ 的次数才可能大于 d。然而，这至多占包含于 U' 中的 ℓ-维仿射子空间的 $1/q$ 比例。结合 $\deg(\gamma M(x) + g'(x)) < (\ell+1)(q-1)$，可由引理 C.2 推得 $\deg(\gamma M(x) + g'(x)) \leqslant d$。 □