# 谱影：当通信复杂度遇上线性不变性测试

Swarnalipa Datta* Arijit Ghosh* Chandrima Kayal† Manaswi Paraashar‡ Manmatha Roy*

arXiv:2601.06828v1 [cs.DS] 11 Jan 2026

**摘要**

在这篇简短的论文中，我们首次在通信复杂度这一背景下研究线性同构测试问题。该问题是经典相等性问题在自然意义上的线性代数推广。给定布尔函数 $f$，$g$：$\mathbb{F}_2^n \to \{-1,+1\}$，Alice 和 Bob 需要判断 $f$ 和 $g$ 是否在输入变量的某个非奇异线性变换下等价，还是彼此相距甚远。由于该问题与组合电路设计、复杂性理论和密码学有着根本联系，因此已在多种计算模型中得到广泛研究，包括标准算法模型和性质测试框架。然而，尽管它具有广泛的意义，它在通信复杂度领域仍未得到探索，而本文正是针对这一空白展开研究。

我们的主要结果表明，输入函数的近似谱范数在决定该问题的通信复杂度方面起着核心作用。我们设计了一种简单的确定性协议，其通信成本关于近似谱范数呈多项式关系，并给出了几乎匹配的下界（相差至多一个二次因子）。在使用私有随机币的随机化情形下，我们提出了一种效率更高、同样简单的协议；与确定性情形相比，该协议对近似谱范数的依赖程度降低了一个二次量级。我们还证明，这种依赖关系基本上无法进一步改善。

这些结果表明，近似谱范数是通信复杂度框架下测试线性不变性的关键复杂度度量。作为核心技术要素，我们为近似谱范数较小的布尔函数建立了新的侏儒函数定理，这些定理在傅里叶分析和学习理论中或许也具有独立的研究价值。

## 1 引言

通信复杂度由 Yao [Yao79]，引入，研究两方（传统上称为 Alice 和 Bob）为计算一个输入分布在双方之间的函数所需的通信量。更具体地说，Alice 接收来自域 $D_1$ 的输入 $x$，Bob 接收来自域 $D_2$ 的输入 $y$，他们的目标是在尽量减少交换比特数的同时计算一个已知函数 $F$：$D_1 \times D_2 \to \{0,1\}$。这一模型在多种约束条件下得到了广泛研究，其中最受关注的是确定性协议：双方的消息完全由各自的输入和通信历史决定；以及随机化协议：这类协议可以使用共享随机性或私有随机性，并允许存在较小的错误概率，通常至多为 $1/3$。确定性通信复杂度与随机通信复杂度之间的区别至关重要，因为随机性往往能大幅降低通信成本，甚至带来指数级节省。

*印度统计研究所，加尔各答，印度
†巴黎西岱大学，法国国家科学研究中心，IRIF，巴黎，法国
‡印度理工学院海得拉巴分校，印度

若干经典问题在通信复杂度理论的发展中发挥了核心作用。相等性问题要求 Alice 和 Bob 判断他们的 $n$ 比特输入是否相同，它在确定性设置与随机化设置之间呈现出鲜明对比：任何确定性协议都需要 $\Theta(n)$ 比特，而随机化协议只需使用 $O(\log n)$ 比特即可解决该问题。集合不相交问题是另一个典型例子，因其随机通信复杂度很高，并且在证明理论计算机科学不同领域（例如流式处理和性质测试）中的若干下界时发挥了重要作用。其他重要问题还包括内积、间隙汉明距离、索引问题和指针追踪，每个问题都带来了独特的挑战与启示。理解各种复杂度度量之间的关系，例如长期悬而未决的对数秩猜想，仍是该领域最引人入胜的开放问题之一。

在这些问题中，相等性问题因其简单性和基础性而尤为突出。在这一设定下，Alice 和 Bob 各自收到一个 $n$ 位的字符串 $x,\ y \in \{0,1\}^n$ 并必须判断$x = y$。任何确定性协议都需要 $\Omega(n)$ 个通信比特数，因为在最坏情况下，Bob 必须核验 Alice 输入的每一位。相比之下，随机化协议，尤其是使用公共随机币的协议，只需 $O(1)$ 比特，便可通过简单的指纹技术以高概率检测出不相等。在私有随机币模型中，目前已知的最佳协议需要$O(\log n)$ 比特 [Yao79], ，这反映了模拟共享随机性的代价。

在本文中，我们考虑相等性问题的一种自然的线性代数推广：Alice 和 Bob 的输入是布尔函数，而非比特串；相等性则放宽为在定义域的可逆线性变换下等价。形式上，给定布尔函数$f,\ g$：$\mathbb{F}_2^n \to \{-1,1\}$，若存在一个矩阵 $M \in \mathrm{GL}_n(\mathbb{F}_2)$，使得 $f$和 $g$线性同构，则称它们线性同构。

$$g(x) = f(Mx) \quad \text{for all } x \in \mathbb{F}_2^n.$$

这里，$\mathrm{GL}_n(\mathbb{F}_2)$ 表示域 $\mathbb{F}_2$ 上可逆 $n \times n$ 矩阵构成的群。

布尔函数的线性同构广泛应用于多个领域，包括高效组合电路的设计 [Cir03, Bem04, YTC+12]、纠错码的构造 [DN06, DRT01, Hou94], 以及密码协议 [CC07, DKS12]。Reed–Muller码是一个典型例子，它在输入变量的仿射变换下保持不变。这种对称性在快速译码算法的开发中发挥着关键作用，相关详细综述见 [ASY21, ASSY23]。线性同构问题也是多变量公钥密码学中的基础问题，其安全性往往依赖于判断两个多变量多项式系统是否在仿射／线性变换下等价这一问题的计算难度。该问题称为多项式同构问题，是若干密码方案的核心 [FP06]。

从计算的角度来看，线性同构问题仍以难解著称。即使两个布尔函数以析取范式等紧凑表示给出，判定它们是否线性同构仍然是 coNP-hard 的。该问题属于多项式层次的第二层 $\Sigma_2^p$，但目前尚不清楚它是否属于 coNP。Agrawal 和 Thierauf [AT00]证明，除非多项式层次坍缩到 $\Sigma_3^p$，否则该问题不是 $\Sigma_2^p$ -完全的。目前已知最高效的算法由 [Luk99], 提出，它将此任务归约为超图同构问题，运行时间为 $2^{O(n)}$ 。线性同构问题也在性质测试框架中得到研究。一项重要成果是，Wimmer 和 Yoshida [WY13] 证明，如果一个布尔函数的谱范数较小，那么只需使用关于已知函数谱范数的多项式数量级查询，就能高效测试该函数是否与一个未知函数线性同构，或与之相距甚远。该测试器只需要预言机访问未知函数的真值表。

然而，尽管线性同构问题具有基础性且应用广泛，它在通信复杂度领域却仍完全未被探索。在这项工作中，我们迈出了弥合这一空白的第一步。我们聚焦于通信复杂度设定下线性同构问题的以下间隙版本。

**定义 1.1**（$\mathsf{LinIso}_n$ 问题）。令 $\epsilon, \omega \geq 0$。*Alice* 和 *Bob* 分别获得布尔函数 $f, g : \mathbb{F}_2^n \to \{-1, 1\}$，并承诺以下两种情况之一成立：

$$\delta_{\mathcal{L}}(f, g) \leq \epsilon, \qquad or, \qquad \delta_{\mathcal{L}}(f, g) \geq \epsilon + \omega,$$

其中，$f$ 与 $g$ 之间的线性距离 $\delta_{\mathcal{L}}(f, g)$ 定义为

$$\delta_{\mathcal{L}}(f, g) := \min_{M \in \mathrm{GL}_n(\mathbb{F}_2)} \Pr_{x \in \mathbb{F}_2^n} [f(Mx) \neq g(x)] .$$

目标是判断上述两种情况中的哪一种成立；也就是说，计算函数

$$\mathsf{LinIso}_n(f, g) := \begin{cases} 1 & \text{if } \delta_{\mathcal{L}}(f, g) \leq \epsilon, \\ 0 & \text{if } \delta_{\mathcal{L}}(f, g) \geq \epsilon + \omega. \end{cases}$$

我们在两种标准模型下研究 $\mathsf{LinIso}_n$ 的通信复杂度。在确定性模型中，Alice 和 Bob 必须使用不含任何随机性的确定性协议，判断 $f$ 与 $g$ 是否线性同构，并使交换的比特数最少。在随机化模型中，双方可以使用私有随机性，且协议必须在所有输入上的成功概率至少为 $2/3$。我们的目标是理解在这些设定下求解 $\mathsf{LinIso}_n$ 的通信成本。

为了进一步展开讨论，我们先介绍布尔立方体上的傅里叶分析的一些基础概念。在 $\mathbb{F}_2^n$ 上进行傅里叶分析，为研究布尔函数的结构提供了一个自然且强大的框架。每个函数 $f : \mathbb{F}_2^n \to \mathbb{R}$ 都存在唯一的如下形式的表示

$$f(x) = \sum_{\alpha \in \mathbb{F}_2^n} \widehat{f}(\alpha) \chi_\alpha(x),$$

其中，特征函数 $\chi_\alpha(x) = (-1)^{\langle \alpha,\ x \rangle}$ 是利用 $\mathbb{F}_2^n$ 上的标准内积定义的奇偶函数。与布尔函数相关的一个核心解析量是其谱范数，定义为

$$\|\widehat{f}\|_1 := \sum_{\alpha \in \mathbb{F}_2^n} |\widehat{f}(\alpha)|,$$

该范数在理解布尔函数的复杂性、可学习性和结构性质方面发挥着关键作用 [KM93, TWXZ13, STlV17, GTW21]。为了在我们的语境中刻画近似性，我们考虑近似谱范数，它量化了布尔函数能否逐点地由一个谱范数较小的实值函数进行近似。对于 $\gamma \geq 0$，函数 $f$ 的 $\gamma$-近似谱范数定义为

$$\|\widehat{f}\|_{1,\gamma} := \inf \left\{ \|\widehat{g}\|_1 : g : \mathbb{F}_2^n \to \mathbb{R},\ \text{and } \forall x \in \mathbb{F}_2^n,\ |f(x) - g(x)| \leq \gamma \right\}.$$

这一量推广了谱范数，且可能显著更小，反映了在逐点误差有界的情况下，$f$ 在傅里叶域中的可压缩性。近似谱范数也在量子查询复杂度和通信复杂度方面有重要应用，凸显了它在不同计算模型中的相关性 [BT22, BS21]。

## 1.1 我们的贡献

我们研究确定性和随机化协议下 LinIso$_n$ 问题的通信复杂度。首先考察使用公共随机币的随机化协议。当 $\epsilon = 0$ 和 $\omega > 0$时，问题 LinIso$_n(f,\ g)$ 存在一种高效的公共随机币随机化协议，所需通信比特数仅为 $O(1)$。其核心思路是将 $f$ 和 $g$ 的真值表视为 $\{-1,1\}^{2^n}$中的向量。Alice（不与 Bob 交互）计算一个非奇异矩阵 $A \in \mathbb{F}_2^{n\times n}$，使得 $f \circ A$ 的真值表按字典序最小。类似地，Bob 独立地为 $g$计算一个非奇异矩阵 $B$ 。如果 $f$ 和 $g$ 线性同构，那么$f \circ A = g \circ B$，问题便归结为检验这些变换后函数的相等性。使用标准的公共随机币随机化协议即可完成此操作，所需通信比特数为 $O(1)$（见 [KN97，第 3]章）。然而，当 $\epsilon > 0$时，对于该问题的容错版本，目前尚无此类高效的随机化协议。

现在我们转向本文的主要贡献：分析该问题在确定性协议和私有随机币随机化协议下的情形。给定函数 $f,\ g\colon \mathbb{F}_2^n \to \mathbb{R}$，定义

$$t := \min\left\{\left\lceil \|\widehat{f}\|_{1,1/3}\right\rceil, \left\lceil \|\widehat{g}\|_{1,1/3}\right\rceil\right\}.$$

下文总结的主要结果，针对这项任务的通信复杂度，基于近似谱范数 $t$ 给出了近乎紧的界。具体而言，我们证明，当 $t$ 较小时，存在简单高效的协议。然而，正如本文所示，即使对于使用私有随机币的随机化协议，对 $t$ 的依赖也不可避免。

**定理 1.2** (确定性通信复杂度)。 设 *Alice* 和 *Bob* 分别持有布尔函数 $f$ 和 $g$，并令 $\delta_{\mathcal{L}}(f,g)$ 表示它们的线性距离。那么：

*(a)* 存在一个确定性协议，可以判定是否

$$\delta_{\mathcal{L}}(f,g) \le \epsilon \quad or \quad \delta_{\mathcal{L}}(f,g) \ge \epsilon + \omega$$

使用至多 $O(t^4\log^2(1/\omega))$ 个通信比特数。

（*b*）此外，任何使用 $\epsilon = 0$ 和 $\omega = 1/20$ 解决上述问题的确定性协议，至少必须通信 $\Omega(t^2)$ 个比特。

现在我们将注意力转向随机化设置。我们证明，当参与方可以使用私有随机性时，在非容错设置下，存在一种用于 LinIso$_n(f,g)$ 的高效通信协议。与确定性情形相比，该协议实现了关于近似谱范数的多项式通信成本，并且对这一参数的依赖改善了二次方。此外，我们证明，即使在随机化私有硬币模型中，对近似谱范数的依赖也是不可避免的，这不同于公共硬币设置的情形。

**定理 1.3**（随机通信复杂度）。 设 $f$ 和 $g$ 分别是由 *Alice* 和 *Bob* 持有的布尔函数，并令 $\delta_{\mathcal{L}}(f,g)$ 表示它们的线性距离。则：

（*a*）存在一种私有硬币随机化协议，可以判定

$$\delta_{\mathcal{L}}(f,g) = 0 \quad or \quad \delta_{\mathcal{L}}(f,g) \ge \omega$$

使用至多 $O\left(\frac{t^2}{\omega^3}\right)$ 个通信比特。

*(b)* 此外，对于上述问题，任何满足 $\omega = 1/20$ 的私有随机币随机化协议，其通信量至少为 $\Omega(\log t)$ 比特。

我们的结果表明，当参与的布尔函数具有较小的近似谱范数时，线性同构问题存在高效的通信协议。在确定性和随机化（私有硬币）两种设置下，我们都得到了对近似谱范数呈多项式依赖的上界，并证明这种依赖不可避免。一个仍然引人关注的开放问题是：较小的近似谱范数是否刻画了唯一一类能够高效解决该问题的函数。

### 1.2 论文结构

本文其余部分安排如下。第2节研究线性同构问题的确定性通信复杂度。我们首先给出一种高效的确定性协议，其通信成本关于输入函数的近似谱范数呈多项式依赖，随后证明一个与之几乎匹配的下界。第3节转向随机化设置。我们首先指出，在公开硬币模型中，该问题可以通过常数通信解决，随后提出一种高效的私有硬币协议，使其对近似谱范数的依赖降低为原来的二次量级。我们还推导出相应的下界，表明这种依赖基本上是紧的。最后，第4节简要讨论我们研究结果的意义，并提出若干有待未来研究的开放问题。

## 2 确定性设置

确定性通信复杂度研究的是：在双方（Alice 和 Bob）遵循确定性协议的前提下，为了计算一个输入由双方分持的函数，他们需要交换的最少比特数。其目标是确定精确计算该函数所需的最坏情况通信成本，且不使用随机性，也不允许出现错误。本节将介绍一种在此设置下高效通信的线性同构判定协议，并给出一个与之几乎匹配的下界。

在继续之前，我们引入以下记号来表示两个函数$f$，$g$之间的距离：$\mathbb{F}_2^n \to \{-1,+1\}$:

$$\delta(f,g) := \Pr_{x\in\mathbb{F}_2^n}[f(x)\neq g(x)] = \frac{|\{x\in\mathbb{F}_2^n : f(x)\neq g(x)\}|}{2^n}.$$

我们定义符号函数 sign：$\mathbb{R}\to\{-1,+1\}$，规定当 $x\geq 0$ 时，$\mathrm{sign}(x)=+1$，否则 $\mathrm{sign}(x)=-1$。

### 2.1 高效的确定性通信协议

现在我们证明定理 1.2 的上界部分。如前所述，Alice 和 Bob 获得布尔函数 $f$，$g$：$\mathbb{F}_2^n\to\{-1,1\}$，并承诺以下两种情况之一成立：

$$\delta_{\mathcal{L}}(f,g)\leq\epsilon \quad \text{or} \quad \delta_{\mathcal{L}}(f,g)\geq\epsilon+\omega.$$

任务是区分这两种情况。我们给出一个能够解决该问题的确定性协议，详见算法 1。

我们首先证明一个关于近似谱范数较小的布尔函数的结构引理。这可以视为 Bruck and Smolensky [BS92] 关于具有较小近似谱范数的函数的经典结果的一种近似类比。

**引理 2.1** (近似谱采样)。 设 $f:\ \mathbb{F}_2^n \to \{-1,1\}$ 是一个布尔函数，且 $\gamma \in [0,1)$。那么，对每个 $\delta > 0$，都存在一个子集 $\mathcal{S} \subseteq \mathbb{F}_2^n$ 和一个布尔函数 $F:\ \mathbb{F}_2^n \to \{-1,1\}$，使得：

- $|\mathcal{S}| = O\left(\|\widehat{f}\|_{1,\gamma}^2 \cdot \underline{\frac{1}{1-\gamma()^2}} \cdot \text{对数}(1/\delta)\right)$,
- $F(x) = \text{符号}\left(\sum_{\alpha\in\mathcal{S}} a_\alpha \chi_\alpha(x)\right)$ 其中系数 $a_\alpha \in \{\pm 1\}$ 为某些系数，
- $\delta(f,\ F) \le \delta$。

在本引理的证明中，我们将使用以下集中不等式。

**定理 2.2** (霍夫丁不等式)。 设 $X_1, X_2, \ldots, X_n$ 是相互独立的随机变量，且对所有 $i \in [n]$，$a_i \le X_i \le b_i$ 均成立。定义 $S_n :\ = \sum_{i=1}^n X_i$ 以及 $\mu :\ = \mathbb{E}[S_n]$。那么，对于任意 $t > 0$，有

$$\Pr[\,|S_n - \mu| \ge t\,] \le 2\exp\left(-\frac{2t^2}{\sum_{i=1}^n (b_i - a_i)^2}\right).$$

本引理的证明采用 Haviv 和 Regev [HR16, 引理 3.1]，的方法，他们改编了 Bruck and Smolensky [BS92] 的论证。

引理 *2.1* 的证明。令 $h:\ \mathbb{F}_2^n \to \mathbb{R}$ 为一个实值函数，使得对于所有 $x \in \mathbb{F}_2^n$，都有$\lnot|f(x) - h(x)| \le \gamma$，且 $\|h\|_1 = \|f\|_{1,\ \gamma}$。我们将 $h$ 表示为其傅里叶展开：

$$h(x) = \sum_{\alpha\in\mathbb{F}_2^n} \widehat{h}(\alpha)\chi_\alpha(x) = \|\widehat{h}\|_1 \cdot \sum_{\alpha\in\mathbb{F}_2^n} \left(\frac{|\widehat{h}(\alpha)|}{\|\widehat{h}\|_1} \cdot \operatorname{sign}\left(\widehat{h}(\alpha)\right)\chi_\alpha(x)\right)$$

这启发了一种自然的基于采样的近似策略。定义 $\mathcal{D}$ 在 $\mathbb{F}_2^n$ 上的分布如下：对于所有 $\alpha \in \mathbb{F}_2^n$,

$$\Pr_{\mathcal{D}}[\alpha] = \frac{|\widehat{h}(\alpha)|}{\|\widehat{h}\|_1}.$$

注意到

$$h(x) = \mathop{\mathbb{E}}_{\alpha\sim\mathcal{D}}\left[\|\widehat{h}\|_1 \cdot \operatorname{sign}\left(\widehat{h}(\alpha)\right)\chi_\alpha(x)\right]$$

独立采样 $\alpha_1, \ldots, \alpha_T \sim \mathcal{D}$，其中

$$T = O\left(\|\widehat{h}\|_1^2 \cdot \frac{1}{\beta^2} \cdot \log(1/\delta)\right).$$

定义经验近似器：

$$\widetilde{h}(x) = \frac{\|\widehat{h}\|_1}{T}\sum_{i=1}^T \operatorname{sign}(\widehat{h}(\alpha_i))\chi_{\alpha_i}(x).$$

根据霍夫丁不等式（定理 2.2），该近似器满足：

$$\Pr_{x\in\mathbb{F}_2^n}\left[\,|h(x) - \widetilde{h}(x)| > \beta\,\right] \le \delta.$$

令 $\beta := \frac{1-\alpha}{10}$，并定义 $D := \left\{x \in \mathbb{F}_2^n \colon |h(x) - \widetilde{h}(x)| \leq \beta\right\}$，。现在，对所有 $x \in D$，应用三角不等式：

$$|f(x) - \widetilde{h}(x)| \leq |f(x) - h(x)| + |h(x) - \widetilde{h}(x)| \leq \beta + \gamma < 1.$$

由于 $f(x) \in \{-1, 1\}$，这意味着

$$\operatorname{sign}(\widetilde{h}(x)) = f(x).$$

~定义最终假设 $F(x) := \operatorname{sign}(h(x))$。那么，对于所有 $x \in D$，我们都有 $F(x) = f(x)$，因此

$$\delta(f, F) = \Pr_{x \in \mathbb{F}_2^n}[f(x) \neq F(x)] \leq \delta.$$

证明至此完成。 □

现在我们给出定理 1.2 (a) 的证明。

定理 *1.2 (a)* 的证明。 该定理的证明源于对算法 1 的分析。

**正确性**。 我们首先回顾一下，三角不等式对线性距离同样成立。也就是说，对于任意 $f$、$g$、$h$：$\mathbb{F}_2^n \to \{\pm 1\}$，我们有：

$$\delta_{\mathcal{L}}(f, h) + \delta_{\mathcal{L}}(h, g) \geq \delta_{\mathcal{L}}(f, g).$$

现在我们分析两种可能的情况：

- **情况 1：** 假设 $\delta_{\mathcal{L}}(f, g) \leq \epsilon$。那么，根据线性距离的三角不等式，

$$\delta_{\mathcal{L}}(F, g) \leq \delta_{\mathcal{L}}(f, g) + \delta_{\mathcal{L}}(f, F) \leq \epsilon + \frac{\omega}{4}.$$

- **情况 2：** 假设 $\delta_{\mathcal{L}}(f, g) \geq \epsilon + \omega$。那么，

$$\delta_{\mathcal{L}}(F, g) \geq \delta_{\mathcal{L}}(f, g) - \delta_{\mathcal{L}}(f, F) \geq \epsilon + \omega - \frac{\omega}{4} = \epsilon + \frac{3\omega}{4}.$$

由于 $\epsilon + \frac{3\omega}{4} > \epsilon + \frac{\omega}{4}$，Bob 可以通过估计 $\delta_{\mathcal{L}}(F, g)$（加性误差小于 $\omega/10$）轻松区分这两种情况。因此，该协议是正确的。

**通信成本**。协议仅在**步骤 1**和**步骤 4**中进行通信。现在我们分别分析这两个步骤。

- 在**步骤 1**中，Alice 和 Bob 比较各自的近似谱范数，以确定两个函数中哪个值更小。这项比较需要交换 $O(\log t)$ 比特。

- 在**步骤 4**中，Alice 传输她的函数的截断谱表示。根据引理 2.1，截断表示的支撑集 $\mathcal{S}$ 满足

$$|\mathcal{S}| = O\left(t^2 \cdot \log(1/\omega)\right),$$

且其张成空间的维数为

$$\ell = O\left(t^2 \cdot \log(1/\omega)\right).$$

张成该空间的初始 $\ell$ 个向量均可用 $O(\ell)$ 比特表示。之后的每个向量都属于 $\mathcal{S}$ 张成空间，并可通过其在该基下的坐标，用 $\ell$ 比特描述。因此，此步骤中的总通信量不超过

$$O\left(\ell + |\mathcal{S}| \cdot \ell\right) = O\left(t^4 \cdot \log^2(1/\omega)\right).$$

因此，该协议的总通信成本为

$$O\left(t^4 \cdot \log^2(1/\omega)\right).$$

证明至此完成。 □

**备注 2.3**。 定理 *1.2* 的证明还给出了一个确定性通信协议，用于判定 $\delta_{affine}(f、g) \le \epsilon$ 或 $\delta_{affine}(f、g) \ge \epsilon + \omega$，且通信成本相同。只需对算法 *1* 的步骤 *5* 进行简单修改即可看出这一点：*Bob* 检查 $g$ 是否满足 $F \circ (M、a)$，其中所有 $M \in \mathrm{GL}_n(\mathbb{F}_2)$ 和 $a \in \mathbb{F}_2^n$ 均采用相同的参数选择。

---

**算法 1：** 判定线性同构的确定性协议

---

**输入**。 Alice 获得 $f: \mathbb{F}_2^n \to \{\pm 1\}$，Bob 获得 $g: \mathbb{F}_2^n \to \{\pm 1\}$，并承诺 $\delta_{\mathcal{L}}(f, g) \le \epsilon$ 或 $\delta_{\mathcal{L}}(f, g) \ge \epsilon + \omega$。

**步骤 1：** Alice 和 Bob 交替交换比特，以确定 $\left\lceil \|\widehat{f}\|_{1、1/3} \right\rceil \le \left\lceil \|\widehat{g}\|_{1、1/3} \right\rceil$。不失一般性，假设 $\lceil \|f\|_{1、1/3} \rceil \le \lceil \|g\|_{1、1/3} \rceil$。

**步骤 2：** Alice 构造

$$F(x) := \mathrm{sign}\Big( \sum_{\alpha \in \mathcal{S}} a_\alpha \chi_\alpha(x) \Big),$$

其中 $|\mathcal{S}| = O(\|f\|_{1,1/3}^2 \log(1/\omega))$，且对所有 $\alpha \in \mathcal{S}$，都有 $a_\alpha \in \{\pm 1\}$，使得 $\delta(f, F) \le \omega/4$ （引理 2.1 保证其存在）。

**步骤 3：** 由于 $\dim(\mathrm{span}(\mathcal{S})) \le |\mathcal{S}|$，Alice 找到 $M \in \mathrm{GL}_n(\mathbb{F}_2)$，使得

$$F \circ M(x) = \mathrm{sign}\left( \sum_{i=1}^{\ell} a_{e_i} \chi_{e_i}(x) + \sum_{j=1}^{w} a_{W_j} \chi_{W_j}(x) \right),$$

其中 $\ell + w = |\mathcal{S}|$, $W_j \in$ 张成$\{e_1, \ldots, e_\ell\}$，且 $e_i$ 是标准基向量。

**步骤 4：** Alice 向 Bob 发送:

- The integer $\ell$ and coefficients $a_{e_1}, \ldots, a_{e_\ell}$ using $O(|\mathcal{S}|)$ bits, and
- If $\ell < |\mathcal{S}|$, each $W_j$ (as an $\ell$-bit string) along with $a_{W_j}$.

**步骤 5：** Bob 构造函数 $F$。

- 如果 $\delta_{\mathcal{L}}(F, g) \le \epsilon + \omega/4$ 则协议接受，并且
- 如果 $\delta_{\mathcal{L}}(F, g) \ge \epsilon + 3\omega/4$ 则协议拒绝。

---

## 2.2 确定性协议的下界

本节通过将通信复杂度中的字符串相等问题 EQU 归约到布尔函数的线性同构问题 LinIso，证明定理 1.2 的下界部分。为描述该归约，我们首先形式化定义 EQU 和 LinIso 问题的非容错变体。

**定义 2.4** ($\mathsf{EQU}_n$)。 *Alice* 和 *Bob* 分别获得输入 $x \in \{0,1\}^n$ 和 $y \in \{0,1\}^n$，他们的目标是计算 $\mathsf{EQU}_n(x,y)$，其定义如下：

$$\mathsf{EQU}_n(x,y) = \begin{cases} 1 & if\ x = y \\ 0 & otherwise \end{cases}$$

也就是说，判断他们的输入是否相等。

**定义 2.5** ($\mathsf{LinIso}_\ell$)。 *Alice* 和 *Bob* 分别获得输入 $f: \mathbb{F}_2^\ell \to \{-1,1\}$ 和 $g: \mathbb{F}_2^\ell \to \{-1,1\}$。他们的目标是计算 $\widetilde{\mathsf{LinIso}}_\ell(f,g)$，其定义如下：

$$\widetilde{\mathsf{LinIso}}_\ell(f,g) = \begin{cases} 1 & if\ \delta_{\mathcal{L}}(f,g) = 0 \\ 0 & if\ \delta_{\mathcal{L}}(f,g) > \omega \end{cases}$$

注意到，$\mathsf{LinIso}_\ell$ 可通过取 $\epsilon = 0$ 从 $\mathsf{LinIso}_\ell$ 得到。

现在我们证明一种特殊映射的存在，称为 $\Phi$。这种映射的主要作用在于消除输入字符串之间的线性关系。在详细介绍 $\Phi$ 之前，我们需要引入一些记号，以简化表述。设 $T$ 为一个长度为 $2^p$ 的字符串。这个字符串可以看作某个布尔函数的真值表，我们将其记作 $f_T: \mathbb{F}_2^p \to \mathbb{F}_2$。

**引理 2.6** ($\Phi$–映射)。 设 $n > 0$ 和 $\omega \in (0, 1/2)$。设 $m = 2^\ell$ 满足：当常数 $c$足够大时，$2cn/\omega \geq m \geq cn/\omega$。将每个 $y \in \mathbb{F}_2^m$视为函数 $f_y: \mathbb{F}_2^\ell \to \mathbb{F}_2$的真值表。则存在一个映射 $\Phi: \mathbb{F}_2^n \to \mathbb{F}_2^m$，使得对所有 $x, y \in \mathbb{F}_2^n$

1. $f_{\Phi(x)} = f_{\Phi(y)}$ 若 $x = y$，且 2. $\delta_{\mathcal{L}}(f_{\Phi(x)}, f_{\Phi(y)}) \geq \omega$ 若 $x \neq y$。

首先，利用引理 2.6 完成定理 1.2 下界部分的证明；随后，我们将在本节后文证明引理 2.6。

### 2.2.1 定理 1.2 (b) 的证明

我们的证明依赖于一类由相等性函数 $\mathsf{EQU}_n$归约得到的函数。回顾一下，对于 $\mathsf{EQU}_n$，任何确定性通信协议在最坏情况下都必须在 Alice 和 Bob 之间交换 $\Omega(n)$ 比特。

考虑算法 2。首先，注意若 $a = b$，则相应的函数 $f$ 和 $g$线性同构，因为相同的函数显然线性同构。若 $a \neq b$，则根据引理 2.6，我们有

$$\delta_{\mathcal{L}}(f_{\Phi(a)}, f_{\Phi(b)}) \geq \omega.$$

此外，回顾一下，$f_{\Phi(a)}$ 和 $f_{\Phi(b)}$ 均定义在定义域 $\mathbb{F}_2^\ell$上，且它们的近似谱范数均有界于 $O(2^{\ell/2})$（由柯西–施瓦茨不等式得出）。

回到我们的归约，Alice 和 Bob 现在对输入 $f_{\Phi(a)}$ 和 $f_{\Phi(b)}$ 调用一个用于函数 $\mathsf{LinIso}_\ell$ 的高效确定性协议。为证矛盾，假设存在一个用于 $\mathsf{LinIso}_\ell$ 的确定性协议，其通信复杂度为

$$o\left(\min\left\{\left\lceil \|\widehat{f}\|_{1,1/3} \right\rceil, \left\lceil \|\widehat{g}\|_{1,1/3} \right\rceil\right\}^2\right),$$

其中 $f$ 和 $g$ 是上文描述的函数（见定义 2.5）。那么，可以利用该协议以仅 $o(n)$ 个通信比特解决 EQU$_n$ 。这与已知下界矛盾：任何用于 EQU$_n$ 的确定性协议，在最坏情况下都必须交换至少 $\Omega(n)$ 个比特。证明至此完成。

---

**算法 2：** 从 EQU$_n$ 问题到 LinIso$_\ell$**输入。** Alice 获得 $a \in \mathbb{F}_2^n$，Bob 获得 $b \in \mathbb{F}_2^n$。

**输出。** 若 $a = b$ 则输出 YES，否则输出 NO**步骤 1：** Alice 计算 $x = \Phi(a)$ 和函数 $f_{\Phi(a)}$：$2^\ell \to \{-1, 1\}$**步骤 2：** 同样，Bob 计算 $y = \Phi(b)$ 和函数 $f_{\Phi(b)}$：$2^\ell \to \{-1, 1\}$**步骤 3：** Alice 和 Bob 针对 $f_{\Phi(a)}$ 和 $f_{\Phi(b)}$调用高效线性同构协议**步骤 5：** 若 $f$ 与 $g$同构，则输出 YES，否则输出 NO。

---

### 2.2.2 引理 2.6 的证明

我们使用算法 3 设计了一个迭代过程，用于构造映射 $\Phi$: $\mathbb{F}_2^n \to \mathbb{F}_2^m$。回顾一下，我们假设 $m$ 具有 $2^\ell$ 的形式，因此任何 $y \in \mathbb{F}_2^m$都可以视为某个布尔函数 $f_y : \mathbb{F}_2^\ell \to \mathbb{F}_2$的真值表。为便于迭代过程，我们维护两个集合：

$\mathcal{S}$：$x \in \mathbb{F}_2^n$ 的（部分）集合，映射已针对该集合完成。该集合应初始化为空集，而在过程结束时，它必须为 $\mathbb{F}_2^n$。

$\mathcal{R}$：$x \in \mathcal{S}$ 及其所有线性同构组成的 $\Phi(x)$ 集合，当被解释为 $\ell$ 个变量上的布尔函数的真值表时。

我们还维护以下映射：

$\mathcal{T}$：$\{0,1\}^m \to \mathbf{B}_\ell$。长度为 $m = 2^\ell$ 的二进制字符串与 $\ell$ 个变量上的布尔函数集合之间的双射映射，记为 $\mathbf{B}_\ell$。

为了证明算法 3 的正确性，我们需要以下技术引理。

**引理 2.7.** 设 $f$：$\{0,1\}^r \to \{0,1\}$，且令 $L(f, \omega)$ 为所有与 $f_{\Phi(x)}$ 的线性距离至多为 $\omega$ 的 $\ell$ 位布尔函数的真值表集合。则 $|L(f, \omega)| = O(2^{r^2} \times 2^{H(\omega)2^r})$。

证明。维数为 $r \times r$ 的非奇异线性变换数量上界为 $2^{r^2}$。因此，在 $r$ 个变量上，至多有 $2^{r^2}$ 个布尔函数与给定的布尔函数 $f$ 线性同构。此外，对于这些函数中的每一个，其真值表与该函数至多有 $\omega$ 比例的条目不同的布尔函数数量上界为 $2^{H(\omega)2^r}$，参见 [Wik24]。

这是因为，给定定义在 $r$ 个变量上的一个固定布尔函数，计算与它至多有 $\omega$ 比例的条目不同的邻近函数数量，等价于估计特征为 2 的域中长度为 $2^r$、熵为 $H(\omega)$ 的汉明球的体积。结合这些观察，我们得到了所声称的界。

□

**算法 3：** 构造 Φ映射

**初始化：** $\mathcal{S}=\emptyset, \mathcal{R}=\mathbb{F}_2^m$**当** $\mathcal{S}\neq\mathbb{F}_2^n$ **时执行**1. 选取某个 $x\in\mathbb{F}_2^n\setminus\mathcal{S}$ 并令 $\mathcal{S}=\mathcal{S}\cup\{x\}$2. 从集合 $\mathcal{R}$ 中选取某个 $y$，并令 $\Phi(x)=y$(a) 如果不存在这样的 $y$，则返回 Fail。3. 令 $L(f_{\Phi(x)},\omega)\subseteq\mathbb{F}_2^m$ 为所有与 $f_{\Phi(x)}$ 的线性距离至多为 $\omega$ 的 $\ell$ 位布尔函数的真值表集合。4. $\mathcal{R}=\mathcal{R}\setminus L(f_{\Phi(x)},\omega)$**结束**

返回成功。

现在，对于算法 3 中每次**while** 循环迭代，根据引理 2.7，我们可以得到步骤 3 中集合 $L(f_{\Phi(x)},\omega)$ 基数的上界 $2^{\ell^2}2^{H(\omega)2^\ell}$。由于**while**循环的迭代次数至多为 $2^n$，若选择 $m$ 使得满足以下关系

$$2^m\geq 2^n\cdot 2^{\ell^2}2^{H(\omega)\cdot m} \tag{1}$$

那么，该算法在**步骤 2 (a)**中不会返回 Fails，并会在过程结束时成功构造 $\Phi$。

剩下要证明的是，若 $2cn/\omega\geq m\geq cn/\omega$，且常数 $c$ 足够大，则方程 (1) 成立。注意到

$$\begin{aligned}
2^m\geq 2^n\cdot 2^{\ell^2}\cdot 2^{m\cdot\mathbf{H}(\omega)} &\iff m\geq n+\ell^2+m\cdot\mathbf{H}(\omega)\\
&\iff m-\log m^2-m\cdot\mathbf{H}(\omega)\geq n\\
&\iff m(1-\frac{\log m^2}{m}-\mathbf{H}(\omega))\geq n\\
&\iff m(1-\mathbf{H}(\omega)-o(1))\geq n
\end{aligned}$$

由于对于 $\omega\in(0,1/2)$，$(1-\mathbf{H}(\omega))\geq\omega$，因此适当选取常数 $c$ 后，我们有 $m\geq cn/\omega$。请记住，对于每个正整数 $d$，总存在一个整数 $e$，使得 $d\leq 2^e\leq 2d$。我们取区间 $[cn/\omega,2cn/\omega]$ 内最小的 2 的幂作为 $m$。

# 3 随机化设置

在随机通信复杂度中，两种标准模型在随机性的获取方式上有所不同：公开硬币模型和私币设置。在公开硬币模型中，Alice 和 Bob 可以访问一个共享随机比特串，双方都能在整个协议过程中使用该比特串，从而无需额外通信即可协调随机性。相比之下，私有随机币模型限制每一方只能使用自己独立生成的随机比特，这些比特对另一方不可见。

首先，我们注意到，在公币设置下，线性同构问题可以用常数通信成本解决（详情参见第 1.1 节）。因此，

本节中，我们聚焦于私币设置。**通过应用上一节用于证明确定性下界的归约，并利用私有随机币模型下相等性问题的通信复杂度为$\Omega(\log n)$这一事实，可以得到一个$\Omega(\log t)$的通信下界**。 接下来，我们将证明，在私币设置下存在一种高效的随机通信协议，其通信成本关于输入函数的近似谱范数呈多项式关系。与确定性情形相比，这使得通信复杂度关于谱范数实现了二次级的改进。

我们证明了一个支撑本协议的关键引理。引理 2.1 给出了一个具有有界傅里叶支撑、可近似原函数的函数；我们进一步强化了这一结果，证明当近似谱范数有界时，存在一个能够紧密近似原函数的侏儒函数。该引理将在我们私有随机币模型下的通信协议中发挥核心作用。除了这一应用之外，它在学习、性质测试和复杂性理论等领域也可能具有独立的研究价值。

**引理 3.1**（线性距离下的侏儒函数近似）。令 $h\colon\ \mathbb{F}_2^n \to \{\pm 1\}$ 为一个布尔函数$\widehat{\ }$，其近似谱范数满足 $\|h\|_{1,\ 1/3} \le t$，且 $\omega \in$（0，1）。那么，存在一个布尔函数 $j\colon\ \mathbb{F}_2^n \to \{-1, 1\}$，它依赖于 $O\left(t^2/\omega^2\right)$ 个坐标（即一个侏儒函数），且其线性距离满足 $\delta_{\mathcal{L}}(h,\ j) < \omega/8$。

证明。设 $h^*$ ： $\mathbb{F}_2^n \to \mathbb{R}$ 个逐点（1/3）逼近 $h$ 且满足条件的实值函数 es

$$\|\widehat{h^*}\|_1 := \sum_{\alpha \in \mathbb{F}_2^n} |\widehat{h^*}(\alpha)| = t.$$

注意

$$\mathop{\mathbb{E}}_{x \in \mathbb{F}_2^n}\left[h^*(x)^2\right] \le \left(1 + \frac{1}{3}\right)^2 = \frac{16}{9}. \tag{2}$$

定义截断傅里叶近似：

$$\widetilde{h^*}(x) := \sum_{\substack{\alpha \in \mathbb{F}_2^n \\ |\widehat{h^*}(\alpha)| \ge \frac{\omega}{18t}}} \widehat{h^*}(\alpha)\chi_\alpha(x).$$

Let

$$T := \left\{\alpha \in \mathbb{F}_2^n : |\widehat{h^*}(\alpha)| < \frac{\omega}{18t}\right\}.$$

利用帕塞瓦尔恒等式（参见 [dW08，第2节.2]）以及傅里叶变换的线性性，我们得到

$$\begin{aligned}
\mathop{\mathbb{E}}_{x \in \mathbb{F}_2^n}\left[(h^*(x) - \widetilde{h^*}(x))^2\right] &= \sum_{\alpha \in \mathbb{F}_2^n} \widehat{g}(\alpha)^2 && \text{where } g := h^* - \widetilde{h^*} \\
&= \sum_{\alpha \in \mathbb{F}_2^n} \left(\widehat{h^*}(x) - \widehat{\widetilde{h^*}}(x)\right)^2 && \text{linearity of Fourier transformation} \\
&= \sum_{\alpha \in T} \widehat{h^*}(\alpha)^2 \\
&< \left(\frac{\omega}{18t}\right) \cdot \sum_{\alpha \in \mathbb{F}_2^n} |\widehat{h^*}(\alpha)| && \text{from the definition of the set } T \\
&= \left(\frac{\omega}{18t}\right) \cdot t \\
&= \frac{\omega}{18}
\end{aligned}$$

现在注意，如果 $\mathrm{sign}(h^*(x)) \neq \mathrm{sign}\left(\widetilde{h^*}(x)\right)$，那么 $\left|h^*(x) - \widetilde{h^*}(x)\right| \geq 2/3$。结合这一事实与马尔可夫不等式可得

$$\begin{aligned}
\Pr_{x\in\mathbb{F}_2^n}\left[\mathrm{sign}(h^*(x)) \neq \mathrm{sign}(\widetilde{h^*}(x))\right] &\leq \Pr_{x\in\mathbb{F}_2^n}\left[\left|h^*(x) - \widetilde{h^*}(x)\right| \geq 2/3\right] \\
&= \Pr_{x\in\mathbb{F}_2^n}\left[\left|h^*(x) - \widetilde{h^*}(x)\right|^2 \geq 4/9\right] \\
&\leq \left(\frac{3}{2}\right)^2 \cdot \mathop{\mathbb{E}}_{x\in\mathbb{F}_2^n}\left[(h^*(x) - \widetilde{h^*}(x))^2\right] \quad \text{from Markov's inequality} \\
&< \frac{9}{4}\cdot\frac{\omega}{18} \\
&= \frac{\omega}{8}.
\end{aligned}$$

定义显著傅里叶系数集合为

$$S := \left\{\alpha \in \mathbb{F}_2^n : |\widehat{h^*}(\alpha)| \geq \frac{\omega}{18t}\right\},$$

并令 $k := |S|$。根据帕塞瓦尔恒等式（参见 [dW08，第 2 节.2]）和公式 (2)，我们有

$$\sum_{\alpha\in\mathbb{F}_2^n} \widehat{h^*}(\alpha)^2 = \mathbb{E}_x[h^*(x)^2] \leq \frac{16}{9}.$$

由于对所有 $\alpha \in S$，每个 $\widehat{h^*}(\alpha)^2 \geq \left(\frac{\omega}{18t}\right)^2$，因此可得

$$k \cdot \left(\frac{\omega}{18t}\right)^2 \leq \frac{16}{9} \quad \Rightarrow \quad k \leq \frac{16}{9}\cdot\left(\frac{18t}{\omega}\right)^2 = \frac{5184}{9}\cdot\frac{t^2}{\omega^2} = \frac{576t^2}{\omega^2}.$$

因此，

$$k = O\left(t^2/\omega^2\right).$$

令 $\{\alpha_1, \ldots, \alpha_r\} \subseteq S$ 为 $S$ 的一个线性无关子集，其中 $r := \dim(\mathrm{span}(S))$。定义一个非奇异线性映射 $A : \mathbb{F}_2^n \to \mathbb{F}_2^n$，使得对所有 $i = 1, \ldots, r$，都有 $A(\alpha_i) = e_i$，其中 $\{e_i\}$ 表示 $\mathbb{F}_2^r$ 的标准基。最后，定义布尔函数

$$j(x) := \mathrm{sign}\left(\widetilde{h^*}(Ax)\right).$$

注意　仅依赖于 $r = O(t^2/\omega^2)$ 个坐标的 $j$，并满足 $\delta_{\mathcal{C}}(h, j) < \omega/8$。 □

现在我们给出定理 1.3 (a) 的证明。

*定理 1.3 (a) 的证明。*该定理的证明基于对算法 4 的分析。

**完备性**。假设 $f$ 和 $g$ 是线性同构的布尔函数。那么，它们的傅里叶 $\widehat{\ }$ 变换 $f$ 和 $\widehat{g}$ 也线性同构：存在一个线性变换 $L \in \mathrm{GL}_n(\mathbb{F}_2)$，使得对每个 $\alpha \in \mathbb{F}_2^n$，

$$\widehat{g}(L\alpha) = \widehat{f}(\alpha).$$

由此可知，$f$ 和 $g$的显著傅里叶系数集合（分别记为 $S_f$ 和 $S_g$）满足$\sim S_g = L(S_f)$。因此，仅保留显著$\widetilde{\ }$系数得到的截断近似 $f$ 和 $\widetilde{g}$也通过 $L$线性同构。于是，函数 $p = \mathrm{sign}(f)$和$q = \mathrm{sign}(\widetilde{g})$线性同构，且它们的典范形式满足 $p^* = q^*$。

**算法 4：** 用于判定线性同构的随机私有硬币协议

**输入。** Alice 获得 $f\colon\ \mathbb{F}_2^n \to \{-1,1\}$，Bob 获得 $g\colon\ \mathbb{F}_2^n \to \{-1,1\}$，并承诺 $\delta_{\mathcal{L}}(f,\ g) = 0$ 或 $\delta_{\mathcal{L}}(f,\ g) \geq \omega$。

**步骤 1：** Alice 和 Bob 交替交换比特，以确定是否

$$\left\lceil \|\widehat{f}\|_{1,1/3} \right\rceil = \left\lceil \|\widehat{g}\|_{1,1/3} \right\rceil .$$

如果不是，则拒绝。

**步骤 2：** Alice 计算 $f^*\colon\ \mathbb{F}_2^n \to \mathbb{R}$，该函数逐点 $1/3$-近似于 $f$，并满足 $\|f^*\|_1 = t$。随后她定义截断傅里叶近似：

$$\widetilde{f^*}(x) := \sum_{\substack{\alpha \in \mathbb{F}_2^n \\ |\widehat{f^*}(\alpha)| \geq \omega/(18t)}} \widehat{f^*}(\alpha)\chi_\alpha(x).$$

Let

$$S := \left\{ \alpha \in \mathbb{F}_2^n : |\widehat{f^*}(\alpha)| \geq \frac{\omega}{18t} \right\},$$

并令 $\{\alpha_1, \ldots, \alpha_r\} \subseteq S$ 为一个线性无关子集，其中 $r\colon\ = \dim(\mathrm{span}(S))$。定义一个非奇异线性映射 $A\colon\ \mathbb{F}_2^n \to \mathbb{F}_2^n$，使得

$$A(\alpha_i) = e_i \quad \text{for all } i = 1, \ldots, r,$$

其中 $\{e_i\}$ 表示 $\mathbb{F}_2^r$ 的标准基。然后定义布尔函数

$$j(x) := \mathrm{sign}(\widetilde{f^*}(Ax)).$$

接下来，定义线性映射 $T\colon\ \mathbb{F}_2^n \to \mathbb{F}_2^r$ 使得

$$T(e_i) = \begin{cases} e_i & \text{for } 1 \leq i \leq r, \\ 0 & \text{for } r < i \leq n, \end{cases}$$

定义布尔函数 $p\colon\ \mathbb{F}_2^r \to \{\pm 1\}$ 为

$$p(x) := \mathrm{sign}(j(Tx)).$$

类似地，Bob 对其函数 $g$ 使用相同的过程构造布尔函数 $q\colon\ \mathbb{F}_2^s \to \{\pm 1\}$。

**步骤 3：** Alice 和 Bob 交替交换比特，以确定 $r = s$。如果不是，则拒绝。

**步骤 4：** Alice 考虑对 $p$ 应用线性同构后得到的所有函数，并选取真值表按字典序最小的函数。将这个典范代表记为 $p^*$。类似地，Bob 计算与 $q$ 对应的字典序最小代表 $q^*$。

**步骤 5：** Alice 使用她的私有随机性，均匀随机地采样一个输入 $x \in \mathbb{F}_2^r$，并将该索引 $x$ 和 $p^*(x)$ 发送给 Bob。Bob 返回值 $q^*(x)$。如果 $p^*(x) = q^*(x)$，则接受；否则拒绝。

**可靠性**。 假设 $f$ 和 $g$ 与线性同构相差至少 $\omega$，即 ，

$$\min_{L\in \mathrm{GL}_n(\mathbb{F}_2)} \Pr_{x\in\mathbb{F}_2^n}[f(x)\neq g(Lx)]\geq \omega.$$

~ ~令 $f$ 和 $\tilde{g}$ 为它们的截断傅里叶近似，并定义 $p=\mathrm{sign}(f)$， $q=\mathrm{sign}(\tilde{g})$。假设 $\Pr_{x\in\mathbb{F}_2^n}[f(x)\neq p(x)]\leq \omega/8$，类似地，$\Pr_{x\in\mathbb{F}_2^n}[g(x)\neq q(x)]\leq \omega/8$。那么，对于所有线性映射 $L$，我们有

$$\Pr_{x\in\mathbb{F}_2^n}[p(x)\neq q(Lx)]\geq \omega-\frac{\omega}{8}-\frac{\omega}{8}=\frac{3\omega}{4}.$$

因此，典范形式 $p^*$ 和 $q^*$ 至少在 $3\omega/4$ 比例的输入上不同。

**通信成本**。 要以常数概率检测到这种差异，只需在 $O(1/\omega)$ 个随机输入上比较$p^*$ 和 $q^*$ 。在私币设置中，Alice 选择一个随机 $x\in\mathbb{F}_2^r$，其中 $r=O(t^2/\omega^2)$，并将 $(x,p^*(x))$ 发送给 Bob。发送 $x$ 和 $p^*(x)$ 的成本为 $O(r)$ 比特。重复进行 $O(1/\omega)$ 次试验后，总通信量为 $O\left(t^2/\omega^3\right)$ 比特。 □

# 4 讨论

我们研究了线性同构问题的通信复杂度，重点考察确定性协议和私有随机币随机化协议。我们的主要贡献是设计了高效协议，其通信成本关于输入函数的近似谱范数呈多项式依赖。我们还证明了下界，表明在这两种设置下，低通信协议都要求近似谱范数较小。在推导这些结果的过程中，我们还确立了近似谱范数较小的布尔函数的一些结构性质，这些性质本身也可能具有研究价值。

仍有若干问题悬而未决。首先，只有近似谱范数较小的函数类能够采用高效通信协议来判定线性同构吗？其次，能否缩小我们在私有随机币随机化设置下上下界之间的差距？最后，目前尚无已知的非平凡随机化协议可用于该问题的容错版本；即使在这一方向上取得部分进展，也将很有价值。

# 致谢

Arijit Ghosh 感谢科学与工程研究委员会（SERB）通过 MATRICS 项目资助 MTR/2023/001527 提供的部分支持，以及印度政府科学技术部（DST）通过项目 TPN-104427 提供的资助。

# 参考文献

[ASSY23] Emmanuel Abbe、Ori Sberlo、Amir Shpilka 和 Min Ye。《Reed-Muller 码》。《基础与趋势》® 通信与信息论，20(1-2):1–156，2023。[ASY21] Emmanuel Abbe、Amir Shpilka 和 Min Ye。《Reed-Muller 码：理论与算法》。《*IEEE*信息论汇刊》，67(6):3251–3277，2021。[AT00] Manindra Agrawal 和 Thomas Thierauf。《公式同构问题》。*SIAM* 计算杂志，30(3):990–1009，2000。

[Bem04] Alberto Bemporad。将混合逻辑动态系统高效转换为等价的分段仿射形式。《IEEE 自动控制汇刊》，49(5):832 – 838，2004。[BS92] Jehoshua Bruck 和 Roman Smolensky。多项式阈值函数、 $AC^0$ 函数和谱范数。《SIAM 计算杂志》，21(1):33–42，1992。[BS21] Nikhil Bansal 和 Makrand Sinha。 $k$-Forrelation 对量子与经典查询复杂性实现最优区分。载于第 53 届 ACM SIGACT 计算理论研讨会（STOC）论文集，第 1303–1316 页，2021。[BT22] Mark Bun 和 Justin Thaler。经典与量子计算中的近似次数。《计算理论中的基础与趋势》，15(3-4):229–423，2022。[CC07] Lingguo Cui 和 Yuanda Cao。一种名为仿射-幂-仿射的新型 S 盒结构。《创新计算、信息与控制国际期刊》，3(3):751–759，2007。[Cir03] Valentina Ciriani。利用仿射空间综合 SPP 三级逻辑网络。《IEEE 集成电路与系统计算机辅助设计汇刊》，22(10):1310– 1323，2003。[DKS12] Orr Dunkelman、Nathan Keller 和 Adi Shamir。密码学中的极简主义：重新审视 Even-Mansour 方案。载于第 31 届密码技术理论与应用国际会议（EUROCRYPT）论文集，第 336–354 页，2012。[DN06] Stanisa Dautovic 和 Ladislav A. Novak。关于“通过固定极性 Reed-Muller 形式对布尔函数进行分类”的评论。《IEEE 计算机汇刊》，55(8):1067 – 1069，2006。[DRT01] Iwan M. Duursma、Carlos Renter´ıa-M´arquez 和 Horacio Tapia-Recillas。完全交上的 Reed-Muller 码。《工程、通信与计算中的应用代数》，11(6):455–462，2001。[dW08] Ronald de Wolf。布尔立方体上傅里叶分析简介。《计算理论》，第 1–20 页，2008。[FP06] Jean-Charles Faug`ere 和 Ludovic Perret。多项式等价问题：算法与理论方面。载于第 24 届密码技术理论与应用国际会议（EUROCRYPT）论文集，第 30–47 页，2006。[GTW21] Uma Girish、Avishay Tal 和 Kewen Wu。奇偶决策树的傅里叶增长。载于第 36 届计算复杂性会议（CCC）论文集，第 200 卷，第 39:1–39:36 页，2021。[Hou94] Xiang-Dong Hou。Reed-Muller 码 $R(m-3,m)$的陪集分类。《离散数学》，128(1):203 – 224，1994。[HR16] Ishay Haviv 和 Oded Regev。傅里叶稀疏布尔函数的列表译码规模。《ACM 计算理论汇刊》，8(3):10:1–10:14，2016。本文的初步版本曾以扩展摘要形式发表于 CCC 2015 论文集。

[KM93] Eyal Kushilevitz 和 Yishay Mansour。使用傅里叶谱学习决策树。*SIAM* 计算杂志，22(6)，1993。[KN97] Eyal Kushilevitz 和 Noam Nisan。《通信复杂度》。剑桥大学出版社，1997。[Luk99] Eugene M. Luks。布尔函数的超图同构与结构等价。载于第*31*届 *ACM*计算理论研讨会论文集（*STOC*），第652–658页，1999。[STlV17] Amir Shpilka、Avishay Tal 和 Ben lee Volk。小谱范数布尔函数的结构。计算复杂性，26(1)，2017。[TWXZ13] Hing Yin Tsang、Chung Hoi Wong、Ning Xie 和 Shengyu Zhang。傅里叶稀疏性、谱范数与对数秩猜想。载于第*54*届 *IEEE*计算机科学基础研讨会论文集（*FOCS*），第658–667页，2013。[Wik24] 维基百科。汉明界——维基百科，自由的百科全书。http://en.wikipedia. org/w/index.php?title=Hamming%20bound&oldid=1192335152，2024。[在线；访问日期：7月12日，2024]。[WY13] Karl Wimmer 和 Yuichi Yoshida。线性不变函数同构测试。载于第*40*届自动机、语言与程序设计国际学术讨论会论文集（*ICALP*），第840–850页，2013。[Yao79] Andrew Chi-Chih Yao。与分布式计算相关的一些复杂性问题（初步报告）。载于第*11*届 *ACM*计算理论研讨会论文集（*STOC*），第209–213页，1979。[YTC+12] Boyan Yordanov、Jana Tumova、Ivana Cerna、Jiˇr´ı Barnat 和 Calin Belta。离散时间分段仿射系统的时序逻辑控制。*IEEE* 自动控制汇刊，57(6)：1491–1504，2012。