arXiv:2603.22795v1 [quant-ph] 24 Mar 2026

量子与经典单向额头数字通信的指数级分离

Guangxu Yang _Jiapeng Zhang *

2026年3月25日

摘要

额头数字（NOF）通信模型是通信复杂度中的一个核心模型。作为一种受限变体，单向NOF 模型尤其受到关注。建立强有力的单向NOF下界将意味着电路下界，解决加法组合学中的著名问题，并在密码学和分布式计算等领域带来广泛应用。然而，要在单向 NOF 通信中证明强下界仍然极具挑战；单向 NOF 通信中的许多基本问题依然悬而未决。其中一个由 Gavinsky 和 Pudlák 在 CCC 2008 提出的问题是：建立量子与经典单向 NOF 通信之间明确的指数分离。

本文通过建立单向 NOF 模型中量子与随机化通信复杂度之间的首个指数分离，解决了这一开放问题。具体而言，我们定义了 Bar-Yossef、Jayram 和 Kerenidis 在 STOC 2004 提出的隐藏匹配问题的一个提升变体，并证明该问题在单向NOF设置下存在一个成本为 $(O(\log n))$ 的量子协议。相比之下，我们证明，任何针对该问题的 k方单向随机化协议都需要 $\Omega(\frac{n^{1/3}}{2^{k/3}})$ 的通信量。值得注意的是，即使将结果推广到 k方单向通信，其中第一位玩家只发言一次，而其他所有 $k-1$ 位参与者均可自由通信，我们的分离结果仍然成立。

1 引言

量子优势研究中的一个根本目标，是展示不同模型之间的计算分离。通信复杂度领域在实现这一目标方面取得了长足进展：一系列研究 [BCW98、Raz99、BYJK04、GKK+07、RK11、Gav16、GRT22、Gav19、Gav20、GGJL24]现已在若干两方通信场景中确立了指数分离。在这些成果的基础上，Aaronson、Buhrman 和 Kretschmer 最近提出了量子信息至上性 [ABK24]这一范式，聚焦于这样一类任务：量子设备所需的资源（量子比特）比任何经典对应方案都少几个数量级。他们提出的任务植根于隐藏匹配问题中经典与量子之间的分离，最近在一项具有里程碑意义的囚禁离子实验中得以实现 [KGD+25]。

*本研究得到美国国家科学基金会CAREER奖2141536的支持。南加州大学托马斯·洛德计算机科学系。电子邮箱：{guangxuy}@usc.edu

尽管两方通信复杂度领域取得了这些成果，多方场景下的量子优势仍未得到充分理解。多方通信的主要模型是额头数字（NOF）模型，由 Chandra、Furst 和 Lipton 提出 [CFL83]。在该模型中，输入被划分为 k 份，玩家 i 可以看到除自己那份之外的所有部分（仿佛这些部分都“写在自己的额头上”）。当 $k = 2$ 时，该模型与标准两方模型一致；而当 $k \geq 3$时，NOF 协议能够模拟严格更广泛的一类计算模型，使其成为一个独特而强大的挑战性框架。最近，Göös、Gur、Jain 和 Li [GGJL24] 指出，NOF 模型中量子通信与随机化通信之间的分离是一项重要的开放问题。

在 NOF 模型中，要在量子协议与随机化协议之间证明强分离，主要障碍在于缺乏证明确定性和随机化 NOF 协议下界的技术；这一点已在 [GGJL24、YZ25b], 中指出。现有的大多数方法，例如差异度方法 [RY15], , 对量子、随机化和确定性通信同样适用，因此难以区分 NOF 场景下量子协议与经典协议的能力 [LS+09]。

因此，自然要在受限场景中考察 NOF 模型的量子优势。与两方通信复杂度的研究类似，研究重点通常从同时通信模型转向单向通信，再转向双向通信 [BCW98, Raz99, BYJK04, GKK+07, RK11, Gav16, GRT22, Gav19, Gav20, GGJL24]。该模型一种极为自然且研究充分的限制形式是单向 NOF 通信模型，其中每位参与者按照固定顺序恰好发言一次。关于同时 NOF 通信模型已有一些进展；它是比单向 NOF 模型更弱的变体。Gavinsky 和 Pudlák [GP08] 首次在同时 NOF 通信场景下证明了量子通信与经典通信之间的 $O(\log n)$ 与 $\Omega(n^{1/6k^2})$ 分离。最近，Yang 和 Zhang [YZ25b] 将这一结果改进为三方同时 NOF 中的 $O(\log n)$ 与 $\Omega(n^{1/16})$ 分离。在 [GP08] 和 [YZ25b], 中，他们进一步提出了以下开放问题：

指数级　　量子优势能否在单向额头数字通信中得以确立　　?

正如 [GP08], 所述，即使是单向额头数字通信的三参与者情形，也高度复杂且具有独立研究价值。

我们为何研究单向NOF通信。尽管单向 NOF 模型乍看之下可能只是一般 NOF 模型的一种受限变体，但它仍具有重要的理论动机和广泛的应用。

首先，该模型对于电路复杂性领域若干长期存在的开放问题具有至关重要的意义。例如，对于任意函数 f，若能证明其在 k方确定性单向 NOF 通信中、通信量为 $k = \log n$ 时具有 $\omega(\log n)$ 下界，则可推出 $f \notin \mathrm{ACC}^0$ [HG90, BT94, Cha07, VW07]。更为引人注目的是，在特定问题中仅针对三位参与者建立强确定性单向下界，将为布尔电路带来显著的规模—深度权衡 [Val77, PRS97]。除了电路复杂性之外，单向 NOF 下界还与加法组合学有着深刻联系。值得注意的是，在特定问题中建立强确定性单向 NOF 下界，可以为海尔斯-朱厄特定理、稠密的 Ruzsa-Szemerédi 图以及 k 项无算术级数集合提供定量下界 [LS+17, JLL+25]。

更广泛地说，单向 NOF 通信模型在理论计算机科学中有着广泛的应用，尤其对密码学具有深远影响。在密码学中，单向

NOF 通信与私有信息检索（PIR）协议密不可分 [CKGS98], 、基于位置的密码学下界、函数求逆下界 [BDFP17、CGK19], 以及抗泄漏密钥交换协议 [LMQW20]。除了这些密码学原语之外，它在分布式计算下界 [DKO14], 、空间有界伪随机生成器的构造 [BNS92、GR14],隐蔽分支程序的时间—空间权衡 [VW07], 以及流式算法下界 [KMPV19]。

尽管单向 NOF 通信模型意义深远、应用广泛，但其中若干基本问题仍未解决。尤其是，正如 [GP08] 和 [YZ25b], 最近指出的那样，如何明确证明随机化与量子单向 NOF 通信之间存在指数分离，仍是一项重大开放问题。在单向 NOF 通信中证明强下界仍极具挑战性。除了前述差异度方法之外，人们还开发了其他几种用于证明单向 NOF 下界的技术 [PRS97，BPSW05，VW07]。然而，这些方法都无法突破 $\Omega(n^{1/(k-1)})$ 下界壁垒。

通过提升技术实现量子优势 提升定理是一种通用方法，可将较弱计算模型中的下界转化为相对较强计算模型中的下界。提升定理的一个典型例子是查询到通信的提升定理 [RM97，Zha09，GPW18，PR17，GPW20，CFK+19，LMM+22，YZ24，MYZ25], 它们通过将适当的基函数与小工具函数复合，把查询复杂度下界转化为通信复杂度下界。

在双方面设置中，将提升应用于量子决策树相比随机化决策树具有指数级优势的问题（例如 Forrelation问题） [Aar10，AA15],，我们可以得到双向量子与经典通信复杂度之间的指数分离 [GRT22、GGJL24]。探究类似的提升技术能否扩展到更复杂的单向NOF设置，是一个自然且极具前景的方向。

最近，Yang 和 Zhang [YZ25a] 提出了一种新颖的提升框架，将双方面通信与额头数字（NOF）模型联系起来。具体而言，他们建立了一个确定性提升定理，将单向双方下界转化为单向NOF设置中的下界。然而，他们将随机化版本留作一个重要的开放问题，目前只获得了确定性下界。

受 [YZ25a], 中的技术启发，我们成功绕过了这一 $\Omega(n^{1/(k-1)})$ 下界障碍，并解决了上述开放问题。具体而言，我们利用提升技术，首次明确证明了随机化与量子单向NOF 通信之间存在指数分离。

1.1 我们的贡献

本文首次在单向 NOF 模型中证明了量子通信复杂度与随机化通信复杂度之间存在指数分离。

我们的构造基于 Bar-Yossef 等人提出的隐藏匹配（HM）问题的一个提升版本。 [BYJK04]。在标准的双方面隐藏匹配问题中：

1. Alice 得到一个字符串 $z \in \{0，1\}^n$。

2. Bob 获得一个包含 n 个节点的完美匹配 $M \in \mathrm{M}_n$。

目标是让 Bob 输出一个元组 i, j, b, 使得边 $(i, j) \in M$并且 $b = z_i \oplus z_j$.

文献 [BYJK04] 证明了，HM 存在一个 $O(\log n)$同时量子协议，而任何单向随机化协议都需要 $\Omega(\sqrt{n})$ 通信。

在我们的构造中，我们使用了一个完美匹配的结构化子集。固定 m，对于每个 $i \in [m]$，我们定义集合 $\{0, \ldots\ldots, m-1\}$ 与 $\{m, \ldots\ldots, 2m-1\}$ 之间的一个完美匹配 M_i，如下所示：

$$M_i := \{(\ell, m + ((i + \ell) \bmod m)) : \ell \in [m]\}.$$

令 $\mathrm{M} = \{M_1, \ldots\ldots, M_m\}$ 表示这个集合。提升隐藏匹配问题记作 $\mathrm{HM} * g$，定义如下：

定义 1.1。令 $g: \{0,1\}^{n(k-1)} \to \{0,1\}^{n_0}$ 为构件函数，其中 $n_0 = \binom{n}{2k}^{2/3}$。提升隐藏匹配问题记作 $HM * g$，涉及分配给参与者的 k 输入如下：令$m = n_0/2$,

- 第 i 位玩家收到（$x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k$），其中 $x_1 \in [m]$ 和 $x_i \in \{0,1\}^n$ 对于 $2 \le i \le k$。

目标是让最后一位玩家输出一个元组$\langle \ell, r, b \rangle$，使得 $(\ell, r) \in M_{x_1}$ 且 $b = g(x_2, \ldots, x_k)_\ell \oplus g(x_2, \ldots, x_k)_r$。

值得注意的是，对于量子通信而言，这个问题仍然很简单。与隐藏匹配问题类似，第一位玩家只需发送字符串$g(x_2, \ldots, x_k)$的均匀叠加态，通信成本为 $O(\log n)$ 个量子比特。随后，最后一位玩家可以对这个叠加态进行测量；测量取决于匹配 M_{x_1}，并输出 M_{x_1} 中的某一对的奇偶校验（更多详情见附录）。我们注意到，在此协议中，其他参与者无需发送任何消息。因此，我们论文的主要结果是随机化单向 NOF 通信下界。

定理 1.2。设 $n_0 = \binom{n}{2k}^{2/3}$，存在一个显式构件函数 $g: \{0,1\}^{n(k-1)} \to \{0,1\}^{n_0}$，使得 HM 的随机化单向NOF通信复杂度 $* g$ 为 $\Omega\left(\binom{n^{1/3}}{2k/3}\right)$。

2 预备知识

2.1 通信复杂度

我们首先回顾通信复杂度中的标准定义。在双参与方通信模型中，Alice 和 Bob 分别接收输入 $x \in X$ 和 $y \in Y$，他们的目标不是计算一个简单的布尔函数，而是求解一个搜索问题（或计算一个关系）$\mathrm{P} \subseteq X \times Y \times Z$。对于任意给定的输入 (x, y)，目标是输出一个有效答案 $z \in Z$，使得 $(x, y, z) \in \mathrm{P}$。

定义 2.1（随机单向通信复杂度）。在随机单向通信模型中，*Alice* 和 *Bob* 共享一个公共随机串 r。*Alice* 向 *Bob* 发送一条消息 $\Pi(x, r)$，*Bob* 则根据 y、收到的消息和共享随机性输出答案 $z \in Z$。如果对于每个输入 (x, y)，*Bob* 输出无效答案的概率（对共享随机性取概率）至多为 δ，则称该协议具有 δ 错误率。错误率为 δ 时，$\mathcal{P}$ 的随机单向通信复杂度是 *Alice* 的消息在所有输入和随机串中的最大长度。

根据 Yao 极小极大原理，要证明最坏情况下错误率为 δ的随机化协议的下界，只需证明分布复杂度的下界——也就是说，在选定的输入分布（在我们的情形下为均匀分布）下，任何错误概率至多为 δ的确定性协议的通信复杂度下界。

定义 2.2（搜索问题的单向 NOF 通信模型）。在 k方单向额头数字（*NOF*）模型中，k位参与者合作解决搜索问题 $\mathcal{P} \subseteq X_1 \times \cdots \times X_k \times Z$。输入的分配方式使得每位参与者 i都知道除自己输入以外的所有输入 x_i（即，参与者 i可以看到x_{-i}）。在随机单向设定中，参与者按照固定顺序通信，从第一位玩家到最后一位玩家。每位参与者 i根据自己可见的输入、此前发送的消息以及共享随机性 r，发送一条消息 Π_i（x_{-i}，r）。随后，最后一位玩家输出答案 $z \in Z$。

定义 2.3（柱交）。若存在一个指标 $i \in [k]$，使得集合 S 中的元素是否归属不取决于 x_i的取值，则称集合 $S \subseteq X_1 \times \cdots \times X_k$ 为柱集。若集合 S 可写为 $S = S_1 \cap \cdots \cap S_k$，且其中每个 S_i 都是柱集，则称其为柱交。

2.2 信息论基础

我们的证明方法涉及信息论中的若干标准定义和结果，现回顾如下。

定义 n 2.4（熵）。给定随机变量 $\boldsymbol{X}$，$\boldsymbol{X}$ 的香农熵定义为 *by*

$$\mathcal{H}(\boldsymbol{X}) := \sum_x \Pr(\boldsymbol{X} = x) \log\left(\frac{1}{\Pr(\boldsymbol{X} = x)}\right).$$

对于两个随机变量 $\boldsymbol{X}$、$\boldsymbol{Y}$，给定 $\boldsymbol{Y}$ 时 $\boldsymbol{X}$ 的条件熵定义为

$$\mathcal{H}(\boldsymbol{X} \mid \boldsymbol{Y}) := \mathbb{E}_{y \sim \boldsymbol{Y}}\left[\mathcal{H}(\boldsymbol{X} \mid \boldsymbol{Y} = y)\right].$$

对于 $p \in [0,1]$，二元熵函数定义为 $H_2(p) = -p\log_2 p - (1-p)\log_2(1-p)$。众所周知，$H_2(p)$ 是一个凹函数。

引理 2.5 (熵的次可加性**)**。对于一组随机变量 $\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots, \boldsymbol{X}_d$，有：

$$\mathcal{H}(\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots, \boldsymbol{X}_d) \leq \sum_{i=1}^{d} \mathcal{H}(\boldsymbol{X}_i).$$

定义 2.6 (互信息**)**。联合随机变量 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$之间的互信息定义为

$$\mathrm{I}(\boldsymbol{X}; \boldsymbol{Y}) = \mathcal{H}(\boldsymbol{X}) - \mathcal{H}(\boldsymbol{X}|\boldsymbol{Y}),$$

引理 2.7 (数据处理不等式**)**。考虑构成马尔可夫链$\boldsymbol{X} \to \boldsymbol{Y} \to \boldsymbol{Z}$的随机变量 $\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}$。那么，互信息满足：

$$\mathrm{I}(X; Y) \geq \mathrm{I}(X; Z).$$

定义 2.8（汉明距离）。令 $x = (x_1, \ldots, x_n)$ $y = (y_1, \ldots, y_n) \in \{0,1\}^n$ 为两个字符串。它们的汉明距离 $d_H(x, y)$ 定义为：

$$d_H(x, y) := |\{i : x_i \neq y_i\}|.$$

定义 2.9（总变差距离）。对于取值于有限样本空间 Ω 中的两个离散随机变量 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$，它们的概率分布之间的总变差距离定义为：

$$\Delta_{TV}(\boldsymbol{X},\boldsymbol{Y}) := \frac{1}{2}\sum_{\omega\in\Omega} |\Pr(\boldsymbol{X}=\omega) - \Pr(\boldsymbol{Y}=\omega)|.$$

在本文中，我们用 U_m 表示一个在布尔超立方体$\{0,1\}^m$上均匀分布的随机变量。例如，$\Delta_{TV}(\boldsymbol{Z}, U_{n_0})$ 表示随机变量 $\boldsymbol{Z}\in\{0,1\}^{n_0}$ 的分布与$\{0,1\}^{n_0}$上的均匀分布之间的统计距离。

3 量子单向 NOF 通信的优势

本章节证明量子与随机化单向 Numbers-on-Forehead（NOF）通信之间存在指数分离。我们首先回顾该定理的陈述。

定理 3.1 (定理 1.2 重述)。存在一个显式构件函数 $g:\{0,1\}^{n(k-1)}\to\{0,1\}^{n_0}$使得 *HM* 的随机化单向 *NOF* 通信复杂度 $*g$ 为 $\Omega\left(\frac{n^{1/3}}{2^{k/3}}\right)$。 —

3.1 步骤1：选择构件函数

定义 3.2。设 q是一个素数幂，且 k、$r>0$。我们定义函数 $\mathrm{GIP}^k_{q,r}$：$(\mathbb{F}_q^r)^k\to\mathbb{F}_q$如下：

$$\mathrm{GIP}^k_{q,r}(x_1,\ldots,x_k) = \sum_{j\in[r]}\prod_{i\in[k]} x_{i,j},$$

其中 $\mathbb{F}_q$ 是一个有限域，所有算术运算均在 $\mathbb{F}_q$上进行。当 q、r、k 可由上下文明确得知时，为简便起见，我们将 $\mathrm{GIP}(x_1,\ldots,x_k)$ 记作

注意，GIP 是一个柱交提取器：

引理 3.3。 *[YZ25a]*对于 $r\geq 2^{k+1}.$，设 $S\subseteq(\mathbb{F}_q^r)^k$是一个大小为 $|S|\geq q^{r\cdot k-1}$的任意柱交。那么对于每个 $v\in\mathbb{F}_q$，都有

$$\Pr_{(x_1,\ldots,x_k)\in S}[\mathrm{GIP}(x_1,\ldots,x_k)=v] \leq \frac{1}{q} + q\cdot(k/q)^4$$

我们通过设置域的大小 $q=2^{n/2^k}$ 和块数$r=2^{k+1}$来修改函数 $\mathrm{GIP}^{k-1}_{q\,r}$，。我们定义构件函数 g：$\{0,1\}^{n(k-1)}\to\{0,1\}^{n_0}$，使其输出由 $\mathrm{GIP}^{k-1}_{q\,r}$，的前 n_0 个比特表示。

引理 3.4。令 $S\subseteq\{0,1\}^{n(k-1)}$为大小为 $|S|\geq 2^{n(k-1)-n/2^k}$ 的任意柱交。那么对于任意$z\in\{0,1\}^{n_0}$,

$$\Pr_{(x_2,\ldots,x_k)\in S}[g(x_2,\ldots,x_k)=z] \leq 2^{-n_0}+2^{-2n_0}.$$

证明。令 $N=n/2^k$，因此域的大小为 $q=2^N$。我们将 $\mathbb{F}_q$与布尔超立方体 $\{0,1\}^N$ 等同。根据 GIP 函数在柱交 S上的差异界，

GIP 的完整输出分布与均匀分布极为接近。具体而言，对于任意 $y \in \{0,1\}^N$，其点概率满足以下界：

$$\Pr_{(x_2,\ldots,x_k)\in S}[\mathrm{GIP}(x_2,\ldots,x_k)=y] \le 2^{-N}+2^{-2N},$$

根据我们选择的 $r=2^{k+1}$ and $k \le \log_2{}^{n}$ 所对应的指数和界。 ___

我们的构件函数 $Z=g(x_2,\ldots\ldots,x_k)$ 恰好输出 GIP 的前 n_0 个比特。对于任意特定的前缀 $z\in\{0,1\}^{n_0}$，恰好有 2^{N-n_0} 个完整输出 $y\in\{0,1\}^N$ 与此前缀匹配。因此，在柱交 S 上得到 z 的概率，等于这些匹配扩展对应概率之和：

$$\begin{aligned}\Pr_{(x_2,\ldots,x_k)\in S}[g(x_2,\ldots,x_k)=z] &= \sum_{y\in\{0,1\}^N:\, y \text{ matches } z} \Pr_{(x_2,\ldots,x_k)\in S}[\mathrm{GIP}(x_2,\ldots,x_k)=y] \\ &\le 2^{N-n_0}\left(2^{-N}+2^{-2N}\right) \\ &= 2^{-n_0}+2^{-N-n_0} \le 2^{-n_0}+2^{-2n_0}.\end{aligned}$$

最后一个不等式由 $n_0=(n/2^k)^{2/3} \le n/2^k = N$ 这一事实得出。 □

3.2 步骤 2：简化单向 NOF 协议

要证明随机化通信下界，根据 Yao 极小极大原理，只需证明：对于均匀输入分布下能取得常数优势的任意协议，都有一个下界。

为简化分析，我们先对任意单向 NOF 协议应用以下简化过程。令 $m=n_0/2$ 表示可能的匹配数量。

定义 3.5（简化协议）。对于均匀分布下的任意 *HM* 协议 $\Pi * g$，我们将其简化版本 Π^* 定义如下：

- 第一位玩家发送 $\Pi_1^*(x_{-1}) = \Pi_1(x_{-1})$。
- F对于每个 $2 \le i \le k$，第 i 位玩家发送 $\Pi_i^*(x_{-i}) = (\Pi_i(j、x_2、\ldots、x_{i-1}、x_{i+1}、\ldots、x_k))_{j\in[m}$].

简化协议背后的直观理解是，每位玩家 i 在给定 $2 \le i \le k$的情况下，都会枚举 $x_1 \in [m]$ 所有可能取值对应的通信记录，并发送完整列表。我们注意到简化协议具有以下有用性质。

断言 3.6。设 Π 是均匀分布下用于 *HM* $* g$ 且错误率为 δ的确定性协议。那么，以下陈述成立：

1. 协议 Π^* 是均匀分布下用于 *HM* $* g$ 且错误率为 δ的确定性协议。

2. $|\Pi_1^*| = |\Pi_1|$与 $|\Pi_i^*| = m\cdot|\Pi_i|$针对 $2 \le i \le k$。Π^* 的通信复杂度为 $|\Pi_1|+m\cdot\sum_{i=2}^{k}|\Pi_i|$。

3. 在均匀分布下，协议 Π^* 仅依赖于$(x_2, \ldots, x_k)$。也就是说，它们分别独立于 x_1。

证明。 该结论可直接由 Π^* 的构造得出。对于第 1 项，最后一位玩家知道 x_1 的实际值（这是 NOF 模型的特点），因此只需从每位玩家发送的元组中提取第 x_1 个分量 $i \geq 2$。这便完美地模拟了原协议 Π，从而达到完全相同的 δ 错误率。第 2 项显然成立，因为每位玩家 $i \geq 2$ 恰好发送 m 条 Π_i 的模拟通信记录。第 3 项成立，是因为在 NOF 模型中，玩家 1 看不到 x_1；而对于 $i \geq 2$，枚举所有可能的虚拟值下的消息 $j \in [m]$，便完全消除了对实际输入的依赖 x_1。 □

我们强调，第 3 项至关重要，并显著简化了后续分析。通过确保 Π^* 的完整通信记录严格独立于 x_1，我们便可以评估该协议揭示了多少关于构造输出 $g(x_2,\ldots,x_k)$ 的信息，而无需针对具体匹配 M_{x_1} 进行条件化。

3.3 步骤 3：证明简化协议的通信下界

为了分析简化协议的通信复杂度，我们首先注意到一个关键事实：由于协议 Π^* 独立于 x_1，因此本质上不包含关于匹配 M_{x_1} 的信息。因此，要解决隐藏匹配问题，Π^* 必须包含关于 $g(x_2,\ldots,x_k)$ 的充分信息。我们的分析思路是根据玩家之间关于 g 的信息分布情况，考虑两种穷尽所有情况的情形：

- **情形 1：** 第一位玩家的消息 $\Pi_1^*(x_2,\ldots,x_k)$ 包含关于 $g(x_2,\ldots,x_k)$ 的充分信息，使得最后一位玩家能够计算 HM $*g$。在这种情况下，必有 $|\Pi_1^*| = \Omega(\sqrt{n_0})$，这是根据隐藏匹配问题已知的随机单向通信复杂度 隐藏匹配问题 [BYJK04] 得出的。

- **情况 2：** 其余的 $k-1$ 个参与者通过 NOF 通信，集体传递关于 $g(x_2,\ldots,x_k)$ 的足够信息。在这种情况下，总通信量必须满足 $\sum_{i=2}^{k} |\Pi_i^*| = \Omega(n/2^k)$。这由 g 的 柱交提取器性质得出：除非通信量达到 $\Omega(n/2^k)$，否则 $g(x_2,\ldots,x_k)$ 的分布在统计上仍接近均匀分布。

以下定理将这一直觉形式化：

定理 3.7。设 $g\colon \{0,1\}^{n(k-1)} \to \{0,1\}^{n_0}$ 为引理 3.4中描述的构件函数。对于在均匀分布下误差为 Π^*、用于隐藏匹配的简化协议 $*g$，有 1/16，我们有

$$|\Pi_1^*| = \Omega(\sqrt{n_0}) \quad or \quad \sum_{i=2}^{k} |\Pi_i^*| = \Omega(n/2^k).$$

我们注意到，主要结果（定理1.2）可直接由定理 3.7推出。取参数 $n_0 = \left(\frac{n}{2^k}\right)^{2/3}$ 和 $m = n_0/2$，根据定理 3.7 和断言 3.6，对于任意一个Π 隐藏匹配 $*g$ 协议，在均匀分布下的误差为 1/16：

$$|\Pi| = \Omega\left(|\Pi_1^*| + \frac{1}{m}\sum_{i=2}^{k} |\Pi_i^*|\right) = \Omega\left(\frac{n^{1/3}}{2^{k/3}}\right).$$

至此，定理 1.2的证明完成。

本章节余下的篇幅将用于证明定理 3.7。设 Π^* 是任意一个求解隐藏匹配 HM $*\, g$ 的简化协议，其总体期望错误率至多为 1/16。设 $\boldsymbol{\tau}$ 为表示协议 Π^*完整通信记录的随机变量。设输入 $(\boldsymbol{x_2}, \ldots, \boldsymbol{x_k})$ 是取值于 $\{0,1\}^{(k-1)n}$上的均匀分布随机变量，并设 $Z = g(\boldsymbol{x_2}, \ldots, \boldsymbol{x_k}) \in \{0,1\}^{n_0}$为诱导得到的隐藏目标随机变量。

定理 3.7 的证明。我们假设参与者 2 至 k的通信成本不超过 $c_0 = \sum_{i=2}^{k} |\Pi_i^*| = o(n/2^k)$。设 $c_1 = |\Pi_1^*|$ 表示第一位玩家的通信成本。我们要证明 $c_1 = \Omega(\sqrt{n_0})$。

证明分为两个主要部分。第一部分中，我们利用条件 $c_0 = o(n/2^k)$以及柱交提取器的性质，建立信息上界 $\mathrm{I}(Z; \boldsymbol{\tau}) \le c_1 + 2$，并将其形式化为引理 3.8。第二部分中，我们利用单向隐藏匹配问题和简化协议的结构性质，证明相应的下界 $\mathrm{I}(Z; \boldsymbol{\tau}) = \Omega(\sqrt{n_0})$，并将其形式化为引理 3.9。

结合引理 3.8 和引理 3.9，我们立即得出：

$$c_1 + 2 \ge \mathrm{I}(Z; \boldsymbol{\tau}) \ge \Omega(\sqrt{n_0}),$$

这直接推出 $|\Pi_1^*| = c_1 = \Omega(\sqrt{n_0})$。至此，定理 3.7的证明完成。 □

我们先证明信息上界。

引理 3.8。 假设参与者 *2* 到 k在 Π^* 中的通信成本为 $c_0 = o(n/2^k)$，则$\mathrm{I}(Z; \boldsymbol{\tau}) \le c_1 + 2$，其中 $c_1 = |\Pi_1^*|$。

引理 3.8 的证明。令 $\mathrm{X} = X_2 \times \cdots \times X_k$ 为第一位玩家可见的输入空间。根据断言 3.6，整个协议 Π^* 与 x_1 无关。因此，转录随机变量 $\boldsymbol{\tau} = (\boldsymbol{\tau_1}, \boldsymbol{\tau_{>1}})$ 完全由从 X 中均匀抽取的输入决定。对于任意特定的转录实现，第一位玩家的消息 τ_1 将输入限制在 X 的一个子集 $S_{\tau_1} \subseteq$ 中，此类子集至多有 2^{c_1} 个。给定τ_1后，后续消息 $\tau_{>1}$ 将 X 划分为至多 2^{c_0} 个柱交。因此，任意特定的通信记录 $\tau = (\tau_1, \tau_{>1})$ 都对应一个柱交 C_τ。生成 τ 的有效输入的实际集合恰好是 $S_{\tau_1} \cap C_\tau$。

令 $p_\tau = \Pr[\boldsymbol{\tau} = \tau] = \frac{|S_{\tau_1} \cap C_\tau|}{|\quad|} X$ 为生成 τ 的真实概率，并令 $q_\tau = \frac{|C_\tau|}{|\quad|} X$ 为其对应柱交的体积。由于 $S_{\tau_1} \cap C_\tau \subseteq C_\tau$，显然有 $p_\tau \le q_\tau$。注意，对于任意固定的 τ_1，柱集 $\{C_\tau\}_{\tau_{>1}}$ 将 X 划分为若干部分，即 $\sum_{\tau_{>1}} q_\tau = 1$。因此，对所有可能的转录实现求和，可得紧确的上界：

$$\sum_{\tau} q_\tau = \sum_{\tau_1} \sum_{\tau_{>1}} q_\tau \le 2^{c_1} \times 1 = 2^{c_1}.$$

若通信记录 τ 的柱集很小，即满足 $q_\tau \le 2^{-n/2^k}$，我们就将其归类为“坏”。对于任意固定的 τ_1，柱集至多有 2^{c_0} 个，因此给定 τ_1 时，坏柱集的总测度至多为$2^{c_0} \cdot 2^{-n/2^k} = 2^{c_0 - n/2^k}$。协议生成坏通信记录的总概率，可通过对所有坏 τ的 q_τ 求和来界定：

$$\Pr[\boldsymbol{\tau} \in \mathrm{Bad}] = \sum_{\tau \in \mathrm{Bad}} p_\tau \le \sum_{\tau \in \mathrm{Bad}} q_\tau \le \sum_{\tau_1} 2^{c_0 - n/2^k} \le 2^{c_1 + c_0 - n/2^k}.$$

我们可以不失一般性地假设 $c_1 \le \frac{1}{2}\Omega(n/2^k)$（否则，所需的界 $c_1 = \Omega(\sqrt{n_0})$ 显然成立）。给定 $c_0 = o(n/2^k)$，我们有 $c_1 + c_0 - n/2^k \le -\Omega(n/2^k)$。因此，$\Pr[\boldsymbol{\tau} \in \text{坏}] \le 2^{-\Omega(n/2^k)}$。以极高的概率 $1 - 2^{-\Omega(n/2^k)}$，通信记录 τ是“好”的。

对于任意有效的良好通信记录 τ（其中 $p_\tau > 0$ 且 $q_\tau > 2^{-n/2^k}$），C_τ是一个大型柱交。根据引理 3.4，目标随机变量 $Z = g(x_2, \ldots\ldots, x_k)$ 在 C_τ上极其均匀，其上界为 $\Pr[Z = z \mid C_\tau] \le 2^{-n_0} + 2^{-2n_0} \le 2^{-n_0+1}$。在给定已实现的通信记录 $\boldsymbol{\tau} = \tau$的条件下，Z的概率按密度成比例变化。令 $x = (x_2, \ldots\ldots, x_k) \in \mathcal{X}$，则有：

$$\begin{aligned}
\Pr[Z = z \mid \boldsymbol{\tau} = \tau] &= \frac{|\{x \in S_{\tau_1} \cap C_\tau : g(x) = z\}|}{|S_{\tau_1} \cap C_\tau|} \\
&\le \frac{|\{x \in C_\tau : g(x) = z\}|}{|S_{\tau_1} \cap C_\tau|} \\
&= \frac{\Pr[Z = z \mid C_\tau] \cdot |C_\tau|}{|S_{\tau_1} \cap C_\tau|} \\
&= \frac{\Pr[Z = z \mid C_\tau] \cdot q_\tau}{p_\tau} \le \frac{q_\tau}{p_\tau} 2^{-n_0+1}.
\end{aligned}$$

取对数可得，给定特定良好通信记录时的条件熵下界为：

$$\mathcal{H}(Z \mid \boldsymbol{\tau} = \tau) \ge n_0 - 1 - \log \frac{q_\tau}{p_\tau}.$$

现在，我们计算关于随机变量 $\boldsymbol{\tau}$ 的期望条件熵。由于熵非负，我们可以直接忽略坏通信记录的贡献：

$$\mathcal{H}(Z \mid \boldsymbol{\tau}) = \sum_\tau p_\tau \mathcal{H}(Z \mid \boldsymbol{\tau} = \tau) \ge \sum_{\tau \in \text{Good}} p_\tau \left(n_0 - 1 - \log \frac{q_\tau}{p_\tau} \right).$$

By 对良好通信记录上的对数项应用詹森不等式：

$$\sum_{\tau \in \text{Good}} p_\tau \log \frac{q_\tau}{p_\tau} \le \log \left(\sum_{\tau \in \text{Good}} p_\tau \frac{q_\tau}{p_\tau} \right) \le \log \left(\sum_\tau q_\tau \right) \le \log(2^{c_1}) = c_1.$$

因此，条件熵的期望值有明确的上界：

$$\mathcal{H}(Z \mid \boldsymbol{\tau}) \ge \Pr[\boldsymbol{\tau} \in \text{Good}](n_0 - 1) - c_1 \ge \left(1 - 2^{-\Omega(n/2^k)}\right)(n_0 - 1) - c_1 \ge n_0 - c_1 - 1 - o(1).$$

由于 Z在整个空间 X 上均匀分布，其无条件熵为 $\mathrm{H}(Z) \ge n_0$。因此，协议揭示的互信息为：

$$\mathrm{I}(Z; \boldsymbol{\tau}) = \mathcal{H}(Z) - \mathcal{H}(Z \mid \boldsymbol{\tau}) \le n_0 - (n_0 - c_1 - 1 - o(1)) = c_1 + 2.$$

证明至此完成。 □

现在我们关注证明的第二部分。回顾一下，最后一位玩家 k（充当裁判）知道 x_1 和完整的通信记录 $\boldsymbol{\tau}$。由于 Π^* 求解隐藏匹配问题 $*\, g$ 的期望错误率至多为 1/16，因此通信记录必须包含足够的信息来求解隐藏匹配问题。下面的引理给出了所需的信息下界。

引理 3.9。 设 Π^* 是任意一个求解隐藏匹配问题 $*g$ 的简化协议，其总期望错误率至多为1/16。那么，$\mathrm{I}(Z;\boldsymbol{\tau}) = \Omega(\sqrt{n_0})$。

引理 3.9 的证明。令 $\mathbf{M} = \{M_1, \ldots, M_m\}$ 为由 $m = n_0/2$ 个边不相交完美匹配构成的集合。回顾一下，通信记录 $\boldsymbol{\tau}$ 与第一位玩家的输入 x_1 独立（该输入均匀决定匹配 $\boldsymbol{M} \in \mathbf{M}$）。因此，对于任意固定的通信记录 τ 和特定选定的匹配 $M \in \mathbf{M}$，协议的输出是一个常量三元组 (i_M, j_M, b_M)，其中 $(i_M, j_M) \in M$ 是预测边，而 $b_M \in \{0,1\}$ 是预测奇偶校验值。由于输出边保证属于 M，对于固定的 M，当且仅当 $b_M \neq Z_{i_M} \oplus Z_{j_M}$ 时才会出错。

令 ε_τ 表示仅以通信记录 $\boldsymbol{\tau} = \tau$ 为条件时协议的总体错误概率。由于总体期望错误为 $\mathbb{E}_{\boldsymbol{\tau}}[\varepsilon_{\boldsymbol{\tau}}] \leq 1/16$，马尔可夫不等式推出 $\Pr[\boldsymbol{\tau} \in \mathrm{T}_{\mathrm{good}}] \geq 1/2$，其中 $\mathrm{T}^{\mathrm{good}}$ 定义为满足 $\varepsilon_\tau \leq 1/8$ 的通信记录集合。

固定任意一个良好通信记录 $\tau \in \mathrm{T}^{\mathrm{good}}$。令

$$\varepsilon_{\tau,M} = \Pr[b_M \neq Z_{i_M} \oplus Z_{j_M} \mid \boldsymbol{\tau} = \tau, \boldsymbol{M} = M]$$

表示在给定通信记录 τ 和特定匹配 M 的条件下的错误率。

由于在均匀随机选择的匹配上的期望错误率为 $\mathbb{E}_{M \in \mathcal{M}}[\varepsilon_{\tau,M}] = \varepsilon_\tau \leq 1/8$，再次应用马尔可夫不等式可得一个匹配子集 $\mathbf{M}'_\tau := \{M \in \mathbf{M} : \varepsilon_{\tau,M} \leq 1/4\}$，其大小为 $|\mathbf{M}'_\tau| \geq m/2 = n_0/4$。我们构造一个简单二分图 $G'_\tau = (L, R, E'_\tau)$，其边恰好对应于每个 $M \in \mathbf{M}'_\tau$ 下作出的常数预测（i_M, j_M）。由于原始匹配两两边不相交，G'_τ 恰好包含 $|E'_\tau| = |\mathbf{M}'_\tau| \geq n_0/4$ 条边。

根据图兰定理，一个包含秩为 r 的生成森林的简单二分图至多有 $2r$ 个顶点，因此至多有 r^2 条边。因此，G'_τ 的秩至少为 $\sqrt{|E'_\tau|} \geq \sqrt{n_0}/4$。令 $A_\tau \subseteq E'_\tau$ 为这样的生成森林，它提供了 $|A_\tau| = \Omega(\sqrt{n_0})$ 条线性无关边。

令 u_Z、$v \in \{0,1\}^{|A_\tau|}$ 分别表示 A_τ 上的真实奇偶校验值和预测奇偶校验值。根据构造，每条边 $e \in A_\tau$ 都唯一对应于 $\mathbf{M}'_\tau$ 中的一个匹配；令 M_e 表示该匹配。由于 $\mathbf{M}'_\tau$ 中的每个匹配在给定条件下的错误率至多为 1/4，因此对边 e 的奇偶校验值预测错误的概率恰为 $\varepsilon_{\tau,M_e} \leq 1/4$。根据期望的线性性，$A_\tau$ 上真实奇偶校验值与预测奇偶校验值之间的预期汉明距离至多为：

$$\mathbb{E}_Z[d_H(u_Z, v) \mid \boldsymbol{\tau} = \tau] = \sum_{e \in A_\tau} \varepsilon_{\tau,M_e} \leq \frac{1}{4}|A_\tau|.$$

接下来，我们应用以下引理。该引理是 Bar-Yossef、Jayram 和 Kerenidis 对 Fano不等式的推广 [BYJK04]，，用于给 u_Z 的熵设定上界。

引理*3.10*（[*BYJK*04]）。令 $\boldsymbol{W}$ 为一个取值于 $\{0,1\}^k$ 的随机变量，并假设存在一个固定向量 $v \in \{0,1\}^k$，使得 $\mathbb{E}[d_H(\boldsymbol{W}, v)] \leq \epsilon \cdot k$，其中某个 $0 \leq \epsilon \leq 1/2$。则 $\boldsymbol{W}$ 的熵有如下上界：

$$\mathcal{H}(\boldsymbol{W}) \leq k \cdot H_2(\epsilon),$$

其中，$H_2(\cdot)$ 是二元熵函数。

应用广义Fano不等式（引理 3.10），在 $k = |A_\tau|$ 且错误界为 1/4 的条件下，我们有 $\mathcal{H}(u_Z \mid \boldsymbol{\tau} = \tau) \leq |A_\tau| H_2(1/4)$。此外，由于森林 A_τ 是无环的，其奇偶校验

在 Z 上施加 $|A_\tau|$ 个独立线性约束，对于任意固定的 u_Z，恰好留下 $n_0 - |A_\tau|$ 比特的不确定性。根据链式法则，

$$\mathcal{H}(Z \mid \boldsymbol{\tau} = \tau) \le \mathcal{H}(u_Z \mid \boldsymbol{\tau} = \tau) + \mathcal{H}(Z \mid u_Z, \boldsymbol{\tau} = \tau) \le |A_\tau| H_2(1/4) + n_0 - |A_\tau| = n_0 - \Omega(\sqrt{n_0}).$$

对 $\boldsymbol{\tau}$取期望，并对错误的通信记录使用平凡界 $\mathrm{H}(Z \mid \boldsymbol{\tau} = \tau) \le n_0$，则总体条件熵有如下界：

$$\mathcal{H}(Z \mid \boldsymbol{\tau}) \le \frac{1}{2}(n_0) + \frac{1}{2}\left(n_0 - \Omega(\sqrt{n_0})\right) = n_0 - \Omega(\sqrt{n_0}).$$

最后，由于目标的无条件熵为 $\mathrm{H}(Z) \ge n_0$，该协议揭示的互信息有如下精确下界：

$$\mathrm{I}(Z; \boldsymbol{\tau}) = \mathcal{H}(Z) - \mathcal{H}(Z \mid \boldsymbol{\tau}) \ge \Omega(\sqrt{n_0}).$$

证明至此完成。 □

参考文献

[AA15] Scott Aaronson 和 Andris Ambainis。《Forrelation：一个能以最优方式区分量子计算与经典计算的问题》。载于第四十七届 ACM 计算理论研讨会论文集，第 307–316 页，2015 年。3[Aar10] Scott Aaronson。《BQP 与多项式层级》。载于第四十二届 ACM 计算理论研讨会论文集，第 141–150 页，2010 年。3[ABK24] Scott Aaronson、Harry Buhrman 和 William Kretschmer。《一个量子比特、一枚硬币和一串建议步入一个关系问题》。载于 Venkatesan Guruswami 编，理论计算机科学创新会议第 15 届会议论文集，第 287 卷 LIPIcs，第 1:1–1:24 页。Schloss Dagstuhl - Leibniz-Zentrum für Informatik，2024 年。1[BCW98] Harry Buhrman、Richard Cleve 和 Avi Wigderson。《量子与经典通信和计算》。载于第三十届 ACM 计算理论研讨会论文集，第 63–68 页，1998 年。1，2[BDFP17] Joshua Brody、Stefan Dziembowski、Sebastian Faust 和 Krzysztof Pietrzak。《基于位置的密码学与多方通信复杂度》。载于密码学理论会议论文集，第 56–81 页。Springer，2017 年。3[BNS92] László Babai、Noam Nisant 和 Mário Szegedy。《多方协议、对数空间伪随机生成器与时间—空间权衡》。《计算机与系统科学杂志》，45(2)：204–232，1992 年。3[BPSW05] Paul Beame、Toniann Pitassi、Nathan Segerlind 和 Avi Wigderson。《关于腐化的直和定理以及集合不相交性的多方 NOF 通信复杂度》。载于第 20 届 IEEE 计算复杂性年会（CCC'05），第 52–66 页。IEEE，2005 年。3[BT94] Richard Beigel 和 Jun Tarui。《关于 ACC》。《计算复杂性》，4(4)：350–366，1994 年。2

[BYJK04] Ziv Bar-Yossef、Thathachar S Jayram 和 Iordanis Kerenidis。《量子与经典单向通信复杂度的指数分离》。载于第三十六届 ACM 计算理论研讨会论文集，第 128–137 页，2004 年。1，2，3，4，8，11，16[CFK+19] Arkadev Chattopadhyay、Yuval Filmus、Sajin Koroth、Or Meir 和 Toniann Pitassi。《使用低差异度构件实现查询到通信提升》。arXiv 预印本 arXiv:1904.13056，2019 年。3[CFL83] Ashok K Chandra、Merrick L Furst 和 Richard J Lipton。《多方协议》。载于第十五届 ACM 计算理论研讨会论文集，第 94–99 页，1983 年。2[CGK19] Henry Corrigan-Gibbs 和 Dmitry Kogan。《函数求逆问题：障碍与机遇》。载于密码学理论会议论文集，第 393–421 页。Springer，2019 年。3[Cha07] Amit Chakrabarti。《多玩家指针跳转的下界》。载于第二十二届 IEEE 计算复杂性年会（CCC'07），第 33–45 页。IEEE，2007 年。2[CKGS98] Benny Chor、Eyal Kushilevitz、Oded Goldreich 和 Madhu Sudan。《私人信息检索》。《ACM学报》（JACM），45(6)：965–981，1998 年。3[DKO14] Andrew Drucker、Fabian Kuhn 和 Rotem Oshman。《拥塞团模型的能力》。载于 2014 年 ACM 分布式计算原理研讨会论文集，第 367–376 页，2014 年。3[Gav16] Dmitry Gavinsky。《通信复杂度中的纠缠同步性与经典交互性》。载于第四十八届 ACM 计算理论研讨会论文集，第 877–884 页，2016 年。1，2[Gav19] Dmitry Gavinsky。《通信复杂度中的量子同步性与经典同步性》。《IEEE信息论汇刊》，65(10)：6466–6483，2019 年。1，2[Gav20] Dmitry Gavinsky。《通信复杂度中的裸量子同步性与经典交互性》。载于第 52 届 ACM SIGACT计算理论研讨会论文集，第 401–411 页，2020 年。1，2[GGJL24] Mika Göös、Tom Gur、Siddhartha Jain 和 Jiawei Li。《TFNP 中的量子通信优势》。arXiv 预印本 arXiv:2411.03296，2024 年。1，2，3[GKK+07] Dmitry Gavinsky、Julia Kempe、Iordanis Kerenidis、Ran Raz 和 Ronald De Wolf。《单向量子通信复杂度的指数分离及其在密码学中的应用》。载于第三十九届 ACM 计算理论研讨会论文集，第 516–525 页，2007 年。1，2[GP08] Dmitry Gavinsky 和 Pavel Pudlák。《量子与经典非交互式多方通信复杂度的指数分离》。载于 2008 年第 23 届 IEEE 计算复杂性年会，第 332–339 页，2008 年。2，3

[GPW18] Mika Göös、Toniann Pitassi 和 Thomas Watson。确定性通信与划分数。SIAM计算杂志，47(6):2435–2450，2018年。3[GPW20] Mika Göös、Toniann Pitassi 和 Thomas Watson。针对有界错误概率多项式时间的查询到通信提升。SIAM计算杂志，49(4):FOCS17–441，2020年。3[GR14] Anat Ganor 和 Ran Raz。通过通信复杂度下界构造空间伪随机生成器。载于《近似、随机化与组合优化：算法与技术》（APPROX/RANDOM 2014），第692–703页。Schloss Dagstuhl–Leibniz-Zentrum für Informatik，2014年。3[GRT22] Uma Girish、Ran Raz 和 Avishay Tal。量子与随机化通信复杂度之比较：参与者高效的情形。《计算复杂性》，31(2):17，2022年。1, 2, 3[HG90] J. Hastad 和 M. Goldmann。论小深度阈值电路的能力。载于*[1990] 31*届计算机科学基础年会论文集，第610–618页，第2卷，1990年。2[JLL+25] Michael Jaber、Yang P. Liu、Shachar Lovett、Anthony Ostuni 和 Mehtaab Sawhney。角点定理的准多项式界，2025年。2[KGD+25] William Kretschmer、Sabee Grewal、Matthew DeCross、Justin A. Gerber、Kevin Gilmore、Dan Gresh、Nicholas Hunter-Jones、Karl Mayer、Brian Neyenhuis、David Hayes 和 Scott Aaronson。证明量子与经典信息资源之间存在无条件分离，2025年。1[KMPV19] John Kallaugher、Andrew McGregor、Eric Price 和 Sofya Vorotnikova。邻接表流模型中的环计数复杂度。载于第38届ACM SIGMOD-SIGACT-SIGAI数据库系统原理研讨会论文集，第119–133页，2019年。3[LMM+22] Shachar Lovett、Raghu Meka、Ian Mertz、Toniann Pitassi 和 Jiapeng Zhang。利用向日葵进行提升。《莱布尼茨国际信息学会议录》，215，2022年。3[LMQW20] Xin Li、Fermi Ma、Willy Quach 和 Daniel Wichs。抗泄漏密钥交换与双种子提取器。载于《国际密码学年会》，第401–429页。Springer，2020年。3[LS+09] Troy Lee、Adi Shraibman 等。通信复杂度下界。《理论计算机科学前沿与趋势》，3(4):263–399，2009年。2[LS+17] Nati Linial、Adi Shraibman 等。论高维置换的通信复杂度。arXiv预印本 arXiv:1706.02207，2017年。2[MYZ25] Xinyu Mao、Guangxu Yang 和 Jiapeng Zhang。无构造提升胜过轮次消除：指针追逐的改进下界。载于第16届理论计算机科学创新大会（ITCS 2025），第75–1页。Schloss Dagstuhl–Leibniz-Zentrum für Informatik，2025年。3

[PR17] Toniann Pitassi 和 Robert Robere。单调计算的强指数下界。载于第49届ACM SIGACT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1246–1255页。ACM，2017年。3[PRS97] Pavel Pudlák、Vojtech Rödl 和 Jirí Sgall。布尔电路、张量秩与通信复杂度。SIAM计算杂志，26(3):605–633，1997年。2, 3[Raz99] Ran Raz。量子与经典通信复杂度的指数分离。载于第31届ACM计算理论年会论文集，第358–367页，1999年。1, 2[RK11] Oded Regev 和 Bo'az Klartag。量子单向通信的能力可比经典通信强一个指数级。载于第43届ACM计算理论年会论文集，第31–40页，2011年。1, 2[RM97] Ran Raz 和 Pierre McKenzie。单调NC层次的分离。载于第38届计算机科学基础年会论文集，第234–243页。IEEE，1997年。3[RY15] Anup Rao 和 Amir Yehudayoff。简化的不相交性多方通信复杂度下界。载于第30届计算复杂性会议（CCC 2015），第88–101页。Schloss Dagstuhl–Leibniz-Zentrum für Informatik，2015年。2[Val77] Leslie G Valiant。低层复杂度中的图论论证。载于计算机科学数学基础国际研讨会，第162–176页。Springer，1977年。2[VW07] E. Viola 和 A. Wigderson。指针跳跃的单向多方通信下界及其应用。载于2007年第48届IEEE计算机科学基础研讨会论文集，第427–437页，美国加利福尼亚州洛斯阿拉米托斯，2007年10月。IEEE计算机学会。2, 3[YZ24] Guangxu Yang 和 Jiapeng Zhang。通过密度增量论证求解碰撞问题的通信下界。载于第56届ACM计算理论年会论文集，第630–639页，2024年。3[YZ25a] Guangxu Yang 和 Jiapeng Zhang。单向额头编号通信的确定性提升定理。arXiv预印本 arXiv:2506.12420，2025年。3, 6[YZ25b] Guangxu Yang 和 Jiapeng Zhang。同时额头编号通信中的量子与经典分离。CoRR，abs/2506.16804，2025年。2, 3[Zha09] Shengyu Zhang。论Buhrman-Cleve-Wigderson模拟的紧确性。载于算法与计算国际研讨会，第434–440页。Springer，2009年。3

附录

用于隐藏匹配的量子协议 $*g$ **[BYJK04]:** 我们提出了一个用于提升隐藏匹配问题的量子协议，其通信复杂度为 $O(\log n)$ 量子比特。并且 $x_2, \ldots\ldots, x_k \in \{0,1\}^n$ 是第一位玩家的输入，而 $x_1, \ldots\ldots, x_{k-1} \in \{0,1\}^n$ 是最后一位玩家的输入。

令 $z = (z_1, \ldots, z_{n_0}) = g(x_2, \ldots, x_k)$。

1. 第一位玩家发送状态 $|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n_0} (-1)^{z_i} |i\rangle$。

2. 最后一位玩家在标准正交基下对状态 $|\psi\rangle$ 进行测量

$$B = \left\{ \frac{1}{\sqrt{2}} (|k\rangle \pm |\ell\rangle) \mid (k,\ell) \in M_{x_1)} \right\}.$$

测量结果为基态 $\frac{1}{\sqrt{2}}(|k\rangle + |\ell\rangle)$ 的概率为

$$|\langle\psi| \frac{1}{\sqrt{2}} (|k\rangle + |\ell\rangle)\rangle|^2 = \frac{1}{2n} \left((-1)^{z_k} + (-1)^{z_\ell}\right)^2.$$

当 $z_k \oplus z_\ell = 0$ 时，这等于 $2/n$；否则为 0。类似地，对于状态 $\frac{1}{\sqrt{2}}(|k\rangle - |\ell\rangle)$，我们有

$$|\langle\psi| \frac{1}{\sqrt{2}} (|k\rangle - |\ell\rangle)\rangle|^2 = 0 \quad \text{if } z_k \oplus z_\ell = 0, \text{ and } \frac{2}{n} \text{ if } z_k \oplus z_\ell = 1.$$

因此，若测量结果为状态 $\frac{1}{\sqrt{2}}(|k\rangle + |\ell\rangle)$，那么最后一位玩家可以确定 $z_k \oplus z_\ell = 0$，并输出 $k, \ell, 0$。若结果为状态 $\frac{1}{\sqrt{2}}(|k\rangle - |\ell\rangle)$，那么最后一位玩家可以确定 $z_k \oplus z_\ell = 1$，因此输出 $k, \ell, 1$。注意，该测量仅取决于最后一位玩家的输入，而且该算法是零错误的。