arXiv:2302.11476v1 [cs.CC] 22 Feb 2023

# 矩阵乘法与额头数字通信

Josh Alman* Jarosław Błasiok†

2023年2月23日

摘要

三方额头数字通信可以视为一种三方手中数字承诺模型：每位参与方都获得据称位于另外两位参与方额头上的输入，并得到保证，这些输入与其他参与方的输入相一致。在此承诺下所有允许输入的集合可以视为一个三阶张量。令人惊讶的是，我们发现这个张量恰好就是矩阵乘法张量，而矩阵乘法张量在快速矩阵乘法算法的设计中得到了广泛研究。

利用这一联系，我们证明了许多关于额头数字通信和矩阵乘法的结果；在每种情况下，我们都利用了关于另一者的已知结果或技术。例如，我们展示了激光法这一设计最佳矩阵乘法算法的关键技术，也可用于为各种问题设计通信协议。我们还展示了额头数字通信的已知下界如何用于界定矩阵乘法张量的性质，例如其消零子秩。最后，我们大幅推广了基于切片秩的已知通信研究方法，并展示了这些方法如何直接关联到矩阵乘法指数 $\omega$。

*哥伦比亚大学。josh@cs.columbia.edu
†哥伦比亚大学。jb4451@columbia.edu

# 1 引言

额头数字（NOF）通信复杂度由 Chandra、Furst 和 Lipton [CFL83] 提出，是 Yao 通信复杂度模型的一种变体。在这里，我们考虑 $k$ 名参与者，每人拥有 $k$个输入；但我们不直接向参与者提供各自的输入，而是假设他们的输入写在自己的额头上——具体而言，每位参与者都能看到除自己输入之外的所有输入。与标准通信复杂度类似，参与者希望尽可能少地进行通信，以共同计算其输入的某个函数。

事实证明，这一看似无关紧要的改动会带来深远的数学后果。例如，若能为具有 $k = \Theta(\log^c n)$ 个参与者的特定 NOF问题证明下界，就意味着可以得到显式的电路复杂度下界 [HG90, BT94]。

此外，即使只考虑三位参与者，NOF 通信复杂度理论也同时极其深奥，却又令人遗憾地缺乏成果。其深奥之处，部分源于 NOF 通信复杂度中的自然问题与 Ramsey 理论、极值组合学和加法组合学中一些研究充分的问题之间，存在诸多引人入胜且可能出人意料的联系。例如，在开创性论文 [CFL83], 中，作者已经为一个 NOF问题提供了一个效率出奇高的确定性协议：判断 $x+y+z=0$ in $\mathbb{Z}_N$，其中 $x$、$y$、$z \in \mathbb{Z}_N$ 是各参与者额头上的输入（我们从现在起将这个问题称为 $\textsc{Eval}_{\mathbb{Z}_N}$）。该协议只需 $\mathcal{O}(\sqrt{\log N})$ 通信，并利用了 Behrand~~构造~~：构造一个相对稠密、且不含三项等差数列的集合 [Beh46]。另一方面，他们在同一篇论文中利用 Hales–Jewett 定理（一条深刻的 Ramsey 理论定理），证明了该 $\textsc{Eval}_{\mathbb{Z}_N}$问题的一个 $\omega(1)$ 下界。此后，人们发现了与 Ruzsa–Szemer´edi 问题、无角集及极值组合学中其他对象的联系，这些联系往往带来了最先进的构造 [LPS19, AS20, AMS12, LS21, CFTZ22]。

与此同时，或许正是由于这些联系，许多看似简单的 NOF 通信复杂度问题仍未解决，尽管它们的手中数字变体非常容易回答。例如，要彻底确定 $\textsc{Eval}_{\mathbb{Z}_N}$ 的通信复杂度，就需要更深入地理解 Roth 定理中正确的定量依赖关系（即 $[N]$ 的高密度子集包含一个三项等差数列），而这似乎远超当前技术所能达到的范围。

同样，目前仍未解决如何找到一个明确的三方 NOF问题：该问题的 $\mathcal{O}$(假设使用共享随机性)$n$随机化通信复杂度可以通过 $\textsc{Equality}$ 解决，但却要求 $\Omega(\ )$ 的确定性通信；尽管对于08]两方通信而言，这是一个相对简单的性质，而且通过非构造性论证可以证明此类 NOF问题确实存在 $x+y+z=0$ DP $\mathbb{F}_3^n$。这类问题的一个自然候选是检查 $xyz=1$是否属于 $G^n$ （或者更一般地，检查 $G$ 是否属于某个固定群 $\textsc{Eval}_{G^n}$的高次幂，该群不一定是阿贝尔群——我们将这类问题称为），但要证明 NOF 通信复杂度

的下界迄今仍然难以实现。

像 $\textsc{Eval}_{G^n}$ 这样的问题，如果两个参与者的任意一对输入都恰好对应第三个参与者的一个输入，使得他们应当接受，则称为置换问题。这些问题的随机化通信复杂度总是 $\mathcal{O}(1)$，因此很自然会想到尝试证明其确定性通信下界为 $\Omega(n)$。事实上，近期有不少研究以此为目标探讨了置换问题 [BDPW10, CFTZ 22]。

构造 [CFL83] 的高效协议 $\textsc{Eval}_{\mathbb{Z}_N}$ 可以解释为这样一个结论：阿贝尔群 $G$ 中一个不含三项等差数列的大集合 $S \subset G$ 可用于为 $\textsc{Eval}_G$提供高效协议；反过来说，若能证明 $\textsc{Eval}_G$ 的通信复杂度下界，就能推出任何此类集合 $S$的大小上界。几十年来，关于群 $\mathbb{F}_3^n$ 的这一结论一直被称为帽集猜想；2016年，EG16、CLP17 和 Tao16] 著名地肯定解决了这一猜想——某些 $c < 3$下，最大的不含三项等差数列的集合 $S \subset \mathbb{F}_3^n$ 大小为 $\mathcal{O}(c^n)$。这引出了一个自然的问题：能否将证明帽子集定理所用的技术推广，以证明 $\textsc{Eval}_{\mathbb{F}_3^n}$的通信复杂度存在一个线性下界?

Christandl等人 [CFTZ22] 最近发现了直接应用此类技术的障碍——他们使用一种称为组合退化的方法，证明了与阿贝尔群 $G$ 上的通信问题 $\textsc{Eval}_{G^n}$ 相关的特定张量的子秩接近最大值；而对该子秩的上界将意味着通信复杂度所需的下界。

## 1.1 我们的贡献

本文从承诺数手问题的角度研究三方通信。对于一个字母表 $\Sigma$，承诺问题（$I$，$P$）由两个子集 $I \subset P \subset \Sigma \times \Sigma \times \Sigma$ 构成。在该问题中，三位参与者分别获得输入 $a$、$b$、$c \in \Sigma$，并承诺（$a$、$b$、$c$）$\in P$；他们的目标是确定（$a$、$b$、$c$）是否 $\in I$。例如，通常的手中数通信对应于这一模型，其中 $P = \Sigma \times \Sigma \times \Sigma$。

NOF问题也可以视为承诺数手问题。每个参与方获得一对输入 $(a_i, b_i) \in \Sigma^2$，对应于 $i \in \{1, 2, 3\}$，并且可以保证他们的输入满足 $a_2 = b_1$、$a_3 = b_2$ 和 $a_1 = b_3$。（例如，可以将 $a_2$ 和 $b_1$ 视为参与方 3 头部的输入，因此我们承诺参与方 1 和 2 在那里看到的值相同。）用 $P_{\text{NOF}} \subset \Sigma^2 \times \Sigma^2 \times \Sigma^2$ 表示满足该承诺的输入。

我们采用的一个关键思路是，不仅将 $I$ 和 $P$ 视为输入的子集，也将它们视为取值于 $\{0, 1\}$ 的三阶（三维）张量。例如，令 $N = |\Sigma|$，我们可以将 $P_{\text{NOF}}$ 表示为一个取值于 $\{0, 1\}$ 的张量 $P_{\text{NOF}} \in \mathbb{F}^{N^2 \times N^2 \times N^2}$；当对应的元组是合法输入时，张量中的相应元素取值为 1。

事实证明，$P_{\text{NOF}}$ 恰好就是矩阵乘法张量，也就是在快速矩阵乘法算法理论中得到广泛研究的那个张量。

我们利用这一极其出人意料、即便只是形式上的联系，将快速矩阵乘法研究中发展出的思想迁移过来，为 NOF 通信复杂度带来新的见解；反过来，也利用最初针对 NOF 通信复杂度证明的结果，为矩阵乘法张量的重要性质提供新的替代证明。

我们利用这一联系证明以下结果。

**激光法得到的通信协议** 我们采用激光法——Strassen 提出并用于设计已知最佳矩阵乘法算法的技术 [Str86, CW87], ——作为设计 NOF 通信协议的工具。对于任意三个 NOF 问题 $I, J, K$，令 $I \otimes J \otimes K$（“它们的乘积”）表示同时解决这三个问题的 NOF 问题；也就是说，给定每个问题的一个输入，判断它们是否都属于接受输入。利用激光法，我们证明：对于任意三个具有 $n$ 位输入的置换 NOF 问题$I, J, K$，其乘积 $I \otimes J \otimes K$（输入长度为 $3n$ 位）可以通过确定性通信协议，仅用 $n$ 位通信量求解。

例如，对于任意具有 $n$ 位输入的置换 NOF 问题 $I$，可以考虑这样一个问题：给定 $N$ 个同时输入至 $I$，判断它们是否都属于接受输入。我们的协议带来的一个推论是，该问题可以通过确定性通信协议以 $\frac{1}{3}nN + \mathcal{O}(n)$ 位通信量求解。这意味着，我们可以为任意阿贝尔群的幂 $G$ 构造规模出人意料地大的无角集。

相比之下，我们通过计数论证表明，一个随机的 NOF 置换问题 $I$ 在输入为 $n$ 位时，要求确定性通信复杂度为 $\geq n/3 - \mathcal{O}(1)$。此前尚不清楚这一界有多紧；我们的协议表明，至少对于本身是三个置换问题之积的任意置换问题，这一界是可以达到的。

我们的协议还应与 [CFTZ22], 中通过概率方法给出的证明作对比；该证明表明，每个输入为 $n$ 位的 NOF 置换问题都有一个通信复杂度为 $n/2 + \mathcal{O}(1)$ 的协议，进而改进了平凡的 $n$ 上界。

**矩阵乘法的消零子秩** 在矩阵乘法算法理论中经常出现的一个量是矩阵乘法的消零子秩，记作 $Q_{zo}(\langle n, n, n\rangle)$。它表示对用于计算两个 $n \times n$ 矩阵乘法的张量 $\langle n, n, n\rangle$ 进行置零后，能够得到的最大单位张量（单位矩阵的三维类比）的大小。Strassen [Str86] 曾著名地证明 $Q_{zo}(\langle n, n, n\rangle) \geq n^{2-o(1)}$，这个值大致已达到可能的最大值（因为 $\langle n, n, n\rangle$ 是一个 $n^2 \times n^2 \times n^2$ 张量），并将其作为激光法的一部分，用来设计更快的矩阵乘法算法[1]。近期的障碍结果也利用了这一界

[1]例如，参见 [Bl¨a13，第 8] 节。算法中使用的界有时被称为“单项式退化子秩”或“组合退化子秩”的界，但归根结底，这些界又是通过 [Bin05] 来限定消零子秩的。注意，关于.....的界

来排除设计更快矩阵乘法算法的某些方法 [AW21, Alm21, CVZ21]。

在界限 $Q_{zo}(\langle n,n,n\rangle) \geq n^{2-o(1)}$ 中，自然会问 $o(1)$ 所隐藏的内容。例如，最近已有研究表明，$\langle n,n,n\rangle$ 的“边界子秩”为 $\lceil \frac{3}{4}n^2 \rceil$ [KMZ20]；那么我们是否也可能有 $Q_{zo}(\langle n,n,n\rangle) \geq \Omega(n^2)$？这或许能够改进某些应用中的低阶项。

事实上，我们证明这是不可能的，并且 $Q_{zo}(\langle n,n,n\rangle) < n^2/\omega(1)$。为证明这一点，我们在 [LPS19]，的工作基础上展开研究；他们证明了一个 NOF 通信下界，即任何 NOF置换问题都需要 $\omega(1)$ 的确定性通信。利用我们关于 NOF 通信与矩阵乘法之间的联系，我们得以修改他们的证明，从而得到关于 $Q_{zo}(\langle n,n,n\rangle)$ 的上界。

有趣的是，先前的工作 [LPS19] 借助极值组合学中的 Ruzsa–Szemer´edi 问题与其通信下界之间的联系，证明了该下界。我们的新证明不仅揭示了 $Q_{zo}(\langle n,n,n\rangle)$ 与 Ruzsa–Szemer´edi 问题之间的联系，实际上还证明了二者等价！更确切地说，若不解决 Ruzsa–Szemer´edi 问题，就不可能确定 $Q_{zo}(\langle n,n,n\rangle)$的精确渐近行为。这一点很有趣，因为“边界子秩”已被精确确定 [KMZ20]。

最后，借助与 NOF 通信的联系，我们还给出了 Strassen 下界 $Q_{zo}(\langle n,n,n\rangle) \geq n^{2-o(1)}$的另一种证明，并将其推论为高效确定性 NOF 协议存在性的推论，该协议适用于$\textsc{Eval}_{\mathbb{Z}_N}$。

切片秩方法 自 [CFL83]，NOF问题 $I$被提出以来，它们就与相应的三元超图 $H$ 联系在一起，而该超图的色数恰好刻画了其确定性通信复杂度$I$。近年来，一种用于界定此类超图色数的有力方法是“切片秩”方法，该方法最初是为了解决帽集猜想而提出的 [CLP17, EG16]。粗略来说，如果能够证明 $H$ 的邻接张量的切片秩不太大，那么就意味着 $H$ 的色数不会太小，进而得到一个通信下界。

自那以后，已有一些有效技术被提出，用于界定许多不同张量的切片秩 [Tao16, BCC+17]。近期的工作 [CFTZ21]探讨了这些技术能否给出线性确定性 NOF 通信下界。然而，他们发现，遗憾的是，这些技术不可能用于证明任何 $\textsc{Eval}$ 群问题的通信下界。他们通过定义相应的邻接张量，并计算出其具有最大渐近子秩、因而切片秩很大，证明了这一点。我们将他们的结果推广，证明切片秩方法无法用于证明

诸如“边界子秩”或“子秩”这样的更一般概念，在这些算法中并不足够，因为子秩分解只应用于激光法中张量的“外部结构” [Str86]。

任何 NOF 置换问题（而不仅仅是 EVAL 群问题）的线性确定性通信下界。为此，我们注意到，对于任何 NOF 置换问题，相应的邻接张量实际上就是矩阵乘法张量 $P_{\text{NOF}}$的一个置换。由于已知矩阵乘法张量具有最大渐近子秩 [Str86]，因此邻接张量的切片秩永远不会小到足以满足要求。特别是，这意味着事后看来，先前工作 [CFTZ21] 中计算渐近子秩的张量恰好就是矩阵乘法张量。

相比之下，我们使用切片秩方法，为其他承诺问题证明线性下界。关键在于，只要承诺张量的切片秩较低，这种方法就适用。例如，考虑承诺问题 $\text{EQ}_{\mathbb{F}_3^N}$：参与者分别收到输入 $x$、$y$、$z \in \mathbb{F}_3^N$，并承诺 $x+y+z=0$，他们希望判定 $x=y$ 是否成立。我们证明，这个问题需要 $\Omega(N)$ 通信。这看起来似乎很容易证明（“第三位玩家的输入 $z=-(x+y)$ 怎么可能有助于前两位玩家检验相等性问题呢？”），但我们证明，这个问题实际上等价于帽集问题（这曾是一个长期悬而未决的猜想）。

一般秩方法与张量渐近谱切片秩是衡量张量“复杂度”的一种方法，但还有许多其他方法，包括其他张量秩概念；更广泛地说，还有一系列不同的度量，这些度量在代数复杂性和张量组合学中得到了充分研究，统称为“张量渐近谱”[Str86, WZ22]。令 $r$为这些度量中的任意一种（读者不妨重点考虑 $r$ 为张量秩的情形）。我们将切片秩方法加以推广，并证明，对于任意承诺问题（$I$，$P$），其确定性通信复杂度至少为 $\log_2(r(I)/r(P))$. 因此，找到一种度量 $r$，使得问题 $I$的值大于承诺 $P$ 的值，就能得到通信下界。（这就是为什么对于切片秩而言，承诺 $P_{\text{NOF}}$ 具有最大切片秩这一事实意味着无法用这种方法证明下界。）

当 $r$ 是张量秩 $R$ 时，这已经带来了引人入胜的结论。

对于手中数通信，我们知道承诺张量 $P_{NIH}$ 是全 1 张量，其秩为 $R(P_{NIH}) = 1$。因此，对于任意手中数问题 $I$，我们都能得到一个为 $\log_2(R(I))$ 的通信下界。这与两方确定性通信复杂度的标准上界类似，后者由通信矩阵的秩的对数给出。此外，任何 $n$ 位输入问题所对应的 $2^n \times 2^n \times 2^n$ 张量 $I$，只要在某种意义上不是“退化的”，其秩至少为 $2^n$。这也解释了为什么几乎所有手中数通信问题都需要线性通信量。

对于 $n$ 位输入的 NOF 通信，正如我们所讨论的，承诺张量 $P_{NOF}$ 是矩阵乘法张量。确定矩阵乘法的秩，是设计矩阵乘法算法时的核心问题；矩阵乘法指数 $\omega$ 的定义恰好使得 $P_{NOF}$ 的秩为 $R(P_{NOF}) = (2^n)^{\omega+o(1)}$。因此，对于任何满足 $I$ 的問題

秩为 $R(I) \geq (2^n)^c$的问题，我们得到的通信下界为 $(c-\omega-o(1)) \cdot n$。这个通信下界中 $\omega$ 以负号出现，这一点很有意思：这意味着，设计更快的矩阵乘法算法，从而降低已知的 $\omega$上界，会为此类问题 $I$带来更强的通信下界。

作为通信问题的矩阵乘法 最后，我们考虑如何利用其他承诺问题，进一步理解 NOF 通信下界。令 $I$ 为任意一个 $n$ 位 NOF 问题，令 $N = 2^n$，并令 $T_{(\mathbb{Z}/N\mathbb{Z})^2}$ 表示群 $(\mathbb{Z}/N\mathbb{Z})^2$，的结构张量，即张量

$$T_{(\mathbb{Z}/N\mathbb{Z})^2} = \sum_{a,b,c,d \in [N]} x_{(a,b)} y_{(c,d)} z_{(a+c \pmod N, b+d \pmod N)}.$$

我们注意到 $P_{NOF} \subset T_{(\mathbb{Z}/N\mathbb{Z})^2}$ （在适当置换变量之后），因此考虑基于这三个张量的三个不同承诺问题是有明确定义的：$(I, P_{NOF})$、$(P_{NOF}, T_{(\mathbb{Z}/N\mathbb{Z})^2})$ 和 $(I, T_{(\mathbb{Z}/N\mathbb{Z})^2})$。此外，一个简单的三角不等式式论证表明，它们的通信复杂度满足以下关系：

$$\mathcal{CC}(I, P_{NOF}) \geq \mathcal{CC}(I, T_{(\mathbb{Z}/N\mathbb{Z})^2}) - \mathcal{CC}(P_{NOF}, T_{(\mathbb{Z}/N\mathbb{Z})^2}).$$

左边恰好是问题 $I$ 的确定性 NOF 复杂度，而我们希望证明该问题的下界。右边的 $(I, T_{(\mathbb{Z}/N\mathbb{Z})^2})$ 与原始的 NOF问题 $I$ 类似，但其承诺更弱，因此证明它的通信下界应该更容易。那么 $\mathcal{CC}(P_{NOF}, T_{(\mathbb{Z}/N\mathbb{Z})^2})$ 呢？（请回忆，在这个问题中，输入是张量 $T_{(\mathbb{Z}/N\mathbb{Z})^2}$ 中的一个项，我们的目标是判断它是否为来自 $P_{NOF}$ 的有效 NOF 输入。）

对于这个问题，我们给出了一个通信量为 $\leq n$ 的协议（平凡的界为 $2n$）。此外，我们证明了通信下界为 $\geq (\omega - 2)n$（这可由上文讨论的基于秩的方法推出）。因此，若要进一步改进通信协议，实际上就需要快速矩阵乘法（因为这将通过该不等式推出 $\omega$ 的一个上界）。如果 $\omega = 2$（这是广为流传的猜想），那么这个问题确实可能具有亚线性通信复杂度。在这种情况下，要证明 NOF 问题（$I$，$P_{NOF}$）的线性下界，只需证明看似更难的问题（$I$，$T_{(\mathbb{Z}/N\mathbb{Z})^2}$）的线性下界。总之，如果我们能够设计出一种更快的矩阵乘法算法，实现 $\omega = 2$，那么这或许是证明 NOF 通信下界的一条有希望的途径。

## 2 张量预备知识

本文将探讨通信问题与相关张量及其性质之间的联系。我们将重点关注三阶张量（也称为三维

张量）。对于域 $\mathbb{F}$ 以及三个正整数 $A$、$B$、$C$，我们将 $\mathbb{F}^{A\times B\times C}$定义为由张量组成的集合

$$T = \sum_{a\in A}\sum_{b\in B}\sum_{c\in C} T_{a,b,c}x_a y_b z_c$$

对于系数 $T_{a,b,c} \in \mathbb{F}$（其中 $x_a$、$y_b$、$z_c$ 是形式变量）。当具体集合并不重要时，我们通常用 $\mathbb{F}^{|A|\times|B|\times|C|}$ 代替 $\mathbb{F}^{A\times B\times C}$。

若对于所有 $a$、$b$、$c$，都有 $T_{a,b,c} \in \{0,1\}$，则称 $T$ 是取值于 $\{0,1\}$ 的张量。此类张量与 $A\times B\times C$ 的子集构成双射。除非另有说明，本文中讨论的所有张量都假定为取值于 $\{0,1\}$。

我们所使用的域 $\mathbb{F}$ 对以下定义至关重要。若（不一定取值于 $\{0,1\}$ 的）张量 $T$ 可以写成如下形式，则称其秩为 1：

$$T = \left(\sum_{a\in A}\alpha_a x_a\right)\left(\sum_{b\in B}\beta_b y_b\right)\left(\sum_{c\in C}\gamma_c z_c\right)$$

对于系数 $\alpha_a$、$\beta_b$、$\gamma_c \in \mathbb{F}$。更一般地，（不一定取值于 $\{0,1\}$ 的）张量 $T$ 的秩记为 $R(T)$，是指若干个秩为 1 的张量之和等于 $T$ 时所需张量的最少个数。

秩对于定义矩阵乘法指数 $\omega$ 至关重要。对于 $n,m,p\in\mathbb{N}$，我们将 $\langle n,m,p\rangle \in \mathbb{F}^{n^2\times n^2\times n^2}$ 记作矩阵乘法张量

$$\langle n,m,p\rangle = \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{p} x_{i,j}y_{j,k}z_{k,i}.$$

指数 $\omega$ 定义为

$$\omega := \inf\{t \mid R(\langle n,n,n\rangle) \le n^t \text{ for some } n\in\mathbb{N}\}.$$

事实上，已知对于任意 $\varepsilon > 0$，$n\times n$ 矩阵的矩阵乘法都可以通过规模为 $\mathcal{O}(n^{\omega+\varepsilon})$ 的算术电路完成；反过来，任何用于矩阵乘法的算术电路都可以转化为一个张量秩上界，并由此得到相同的运算次数 [Str73]。

我们称 $T$ 为单位张量，若对于所有 $a\in A$，至多存在一对 $(b,c)\in B\times C$ 使得 $T_{a,b,c}\neq 0$；对于所有 $b\in B$ 和所有 $c\in C$，情况也类似。通常，当 $A=B=C$ 时，人们会特别将大小为 $k$ 的单位张量视为一个张量 $\sum_{a\in S} x_a y_a z_a$，其中某些子集 $S\subset A$ 的大小为 $|S|=k$。为明确指出这是充分条件而非必要条件（因为一般情况下可以置换指标），我们将称之为恒等张量的置换。

如果 $T$、$T'\in\mathbb{F}^{A\times B\times C}$，那么当存在子集 $A'\subset A$ $B'\subset B$ $C'\subset C$ $T'_{a,b,c}$ $T_{a,b,c}$ $a\in A'$ $b\in$、，使得无论何时，，，$T'_{a,b,c}=0$ 否则，我们称 $T'$ 是 $T$ 的置零。换句话说，我们将 $A'$、$B'$、$C'$ 之外的系数设为零。我们有时会写作 $T'=T|_{A',B',C'}$。

$T$的消零子秩记作 $Q_{zo}(T)$，是满足以下条件的最大 $k$：$T$ 可以通过归零操作得到一个大小为 $k$的单位张量的置换。这个关于“子秩”概念的组合式变体（子秩使用的是“限制”，而非归零操作）将会多次派上用场。

# 3 承诺问题与带颜色张量

定义 1. 字母表 $\Sigma$ 上的承诺问题是两个子集 $I \subset P \subset \Sigma \times \Sigma \times \Sigma$构成的一对，其中 $P$是允许输入的集合（即承诺），而 $I$是接受输入的子集（即问题）。

为了研究这些对象，我们将引入带颜色张量的概念。带颜色张量是一个二元组 $(I, T_P)$，其中 $T_P \in \mathbb{F}^{\Sigma\times\Sigma\times\Sigma}$是一个张量，而 $I \subset \mathrm{supp}(T_P)$ 是其非零项的一个子集。（我们可以把这些项想象成具有一种特殊颜色，接下来称它们为绿色项。）因此，字母表为 $\Sigma$ 的三方承诺数值持有问题，与定义在 $\mathbb{F}^{\Sigma\times\Sigma\times\Sigma}$上、取值于 $\{0,1\}$的带颜色张量一一对应；张量 $T$ 的非零项对应于允许输入的集合，而绿色项的子集 $I$ 对应于接受输入。

定义 2. 对于任意域 $\mathbb{F}$ ，我们可以将承诺问题 $(I, P)$ 的通信张量定义为带颜色张量 $(I, T_P)$，其中 $T_P \in \mathbb{F}^{\Sigma\times\Sigma\times\Sigma}$定义为

$$T_P := \sum_{(i,j,k)\in P} x_i y_j z_k.$$

我们称 $T_P$为问题 $(I, P)$ 的承诺张量。

有时我们会滥用记号，在上下文足够明确时，用同一个符号表示一个 $\{0,1\}$ 值张量 $P \in \mathbb{F}^{A\times B\times C}$及其支撑集 $\mathrm{supp}(P) \subset A \times B \times C$。本文讨论的所有张量都是 $\{0,1\}$ 值的；在绝大多数讨论中，底层的域并不重要。

通信复杂度模型 我们用 $CC(I, P)$ 表示承诺问题 $(I, P)$ 的确定性通信复杂度。具体来说，我们考虑共享黑板模型：一个协议由三个函数组成，每个参与方各有一个函数，用于根据黑板的当前状态及其私有输入，确定该参与方在每一轮通信中应向黑板追加什么内容。参与者按循环顺序在黑板上写下通信内容；在每个阶段，每位参与者都可以向黑板追加内容、接受当前实例或拒绝当前实例。只有当所有参与者都接受某个具体实例时（依据各自的输入和黑板的最终状态），该实例才算被接受。如果一个协议接受来自 $I$ 的所有输入，并拒绝其他所有来自 $P \setminus I$ 的输入，那么该协议就解决了承诺问题 $(I, P)$。（由于 $P$ 是承诺，该协议对 $P$ 之外的输入无需有任何特定行为。）

渐近通信复杂度 对于承诺问题 $(I, P)$，我们用 $(I, P)^{\otimes n}$ 表示这样一个承诺问题：各方获得原承诺问题 $(I, P)$ 的 $n$ 个有效实例，并希望判断这些实例是否同时全部为接受实例。

更形式化地说，$(I,P)^{\otimes n}$是满足承诺 $P^{\otimes n} \subset(\Sigma^n) \times(\Sigma^n) \times(\Sigma^n)$ 的承诺问题，也就是说，对于 $A,B,C \in \Sigma^n$，当且仅当对所有 $i \in [n]$ 都有 $(A_i,B_i,C_i) \in P$ 时，序列三元组 $(A,B,C)$ 属于 $P^{\otimes n}$。接受实例集合 $I^{\otimes n}$ 的定义类似。此操作对应于相关通信张量的克罗内克积。

定义 3. 对于张量 $I^{(1)} \subset T^{(1)} \subset \mathbb{F}^{A_1\times B_1\times C_1}$ 和 $I^{(2)} \subset T^{(2)} \subset \mathbb{F}^{A_2\times B_2\times C_2}$，我们将着色张量 $(I^{(1)},T^{(1)}) \otimes(I^{(2)},T_{(2)})$ 的克罗内克积定义为 $\mathbb{F}^{A_1A_2\times B_1B_2\times C_1C_1}$ 中的着色张量 $(I,T)$，其中 $T = T_1 \otimes T_2$ 满足

$$T_{(a_1,a_2),(b_1,b_2),(c_1,c_2)} = T^{(1)}_{a_1,b_1,c_1} \cdot T^{(2)}_{a_2,b_2,c_2},$$

以及 $I = \{(a_1,a_2)、(b_1,b_2)、(c_1,c_2) : (a_i,b_i,c_i) \in I_i$，对于 $i \in \{1,2\}\}$。

我们指出，本文讨论的所有张量都是三阶张量（也称为三维张量），并且我们将专门用符号 $\otimes$ 表示张量的克罗内克积（而非张量积）。

我们将问题 $P$的渐近通信复杂度定义为

$$\underline{\mathcal{CC}}(I,P) := \lim_{n\to\infty} \frac{\mathcal{CC}((I,P)^{\otimes n})}{n}.$$

置换问题 我们特别关注一类特定的通信问题，称之为单射问题——正如我们稍后将看到的，单射问题的确定性通信复杂度具有非常简单的组合解释，而且它们在公开随机性下都具有通信量为常数的协议。

定义 4（单射问题）。令 $\pi_1$、$\pi_2$、$\pi_3$：$\Sigma^3 \to \Sigma$ 分别为投影到第一、第二和第三个坐标的投影。

如果张量 $T_I := \sum_{(i,\ j,\ k)\in I} x_i y_j z_k$ 限制在 $I$ 中出现的坐标上（即 $(T_I)|_{\pi_1(I)\ \pi_2(I)\ \pi_3(I)}$）是单位张量的一个置换，那么我们称 $(I,P)$（其中 $I \subset P \subset \Sigma^3$）为一个单射问题。

也就是说：对于第一位参与方的 $i \in \Sigma$ 的每个有效输入，至多存在一对 $j$、$k$，使得 $(i,j,k) \in I$；对于第二位和第三位参与方，情况也类似。

定义 5（置换问题）。如果 $(I,P)$ 是一个置换问题，即 $(I,P)$ 是一个单射问题，且还满足 $|I| = \Sigma$，我们就称之为置换问题。

注意，如果 $(I,P)$ 是一个单射问题（分别为置换问题），那么 $(I,P)^{\otimes n}$ 也同样是一个单射问题（置换问题）。

## 3.1 将额头上的数字问题视为承诺数在手问题

我们可以将 NOF问题 $I \subset \Sigma\times\Sigma\times\Sigma$ 视为字母表 $\Gamma := \Sigma\times\Sigma$上的承诺问题，其中承诺 $P_{\text{NOF}} \subset \Gamma^3$ 由以下内容给出

承诺张量

$$P_{\text{NOF}} := \sum_{i,j,k \in \Sigma} x_{i,j} y_{j,k} z_{k,i}.$$

本文将探讨的一个关键观察是， $P_{\text{NOF}}$ 恰好是矩阵乘法张量 $P = \langle N、\ N、\ N \rangle$，其中 $N = |\Sigma|$。

接受实例集合 $I \subset \Gamma \times \Gamma \times \Gamma$ 可以通过双射

˜ ˜映射 $I \subset \langle N$到承诺张量非零项的一个子集 $N、\ N \rangle$，映射为 $I := \{((x,y),(y,z),(z,x)) : (x,y,z) \in I\}$。

将前额数问题解释为带有承诺 $\langle N、\ N、\ N \rangle$的手中数字问题后，我们注意到，我们对置换问题的更一般定义与[LPS19] 中针对NOF问题的置换问题定义一致——而后者又等价于大小为 $N \times N$的拉丁方。

NOF置换问题的一个重要示例族是 EVAL由阿贝尔群诱导的问题 $G$。具体而言，对于任意阿贝尔群 $G$，令 $\text{EVAL}_G$ 为如下定义的问题。参与者的额头上分别有 $x、\ y、\ z \in G$，他们希望判断 $x + y + z = 0$是否成立。我们可以用其接受实例集合 $I \subset G^3$ 来表示该问题，该集合定义为 $I = \{(x,y,z) : x + y + z = 0\}$。

所有 NOF 置换问题都存在高效随机化协议这一观察，可以推广到不论承诺如何的单射问题：对于双参与方 EQUALITY问题，可以使用常数通信量的随机化协议。

事实 6. 不论承诺如何，每个单射问题都存在一个使用共享随机性的 $O(1)$ 随机化协议。

证明. 第一位参与者收到自己的输入 $x$ 后，可以找到唯一的 $y_1、\ z_1$，使得 $(x, y_1, z_1) \in I$。随后，他可以使用针对 EQUALITY 的双参与方随机化协议，检查 $y_1 = y$ 和 $z_1 = z$ 是否成立，其中 $y、\ z$ 分别是第二位和第三位参与者的输入。 □

我们对承诺单射问题的确定性通信复杂度能说些什么？结果表明，我们可以将其等价地表述为一个关于通信张量 $(I, P)$ 的最小合法着色的问题。

定义 7. 考虑一个着色张量 $T = (I, P)$。我们称其绿色项的子集 $S \subset I$ 为独立集，若 $S$ 是一个单位张量的置换，且限制 $T|_{\pi_1(S)\ \pi_2(S)\ \pi_3(S)}$ 等于 $S$。我们用 $\alpha(T)$ 表示着色张量 $T$ 中最大独立集的大小。

如果 $T$ 是一个普通张量，我们用 $\alpha(T)$ 表示着色张量（$\text{supp}(T)$ $T$）中最大独立集的大小（即将其所有项视为绿色）。这与张量的通常零化子秩概念一致。

注意，如果 $T = (I, P)$ 是一个单射问题，那么 $S \subset I$ 是独立集，当且仅当限制 $T|_{\pi_1(S)\ \pi_2(S)\ \pi_3(S)}$ 中的所有非零项都属于 $I$ ——

也就是说，如果我们记 $S_i := \pi_i(S)$，那么集合 $S$ 是独立集，当且仅当

$$\mathrm{supp}(T) \cap (\pi_1(S_1)^{-1} \times \pi_2(S_2)^{-1} \times \pi_3(S_3)^{-1}) = S.$$

定义了独立集之后，我们可以自然地定义着色张量的合法着色和色数。

定义 8. 对于着色张量 $T:=(I,P)$，如果对所有颜色 $c \in [k]$，集合 $\tau^{-1}(c)$ 都是独立集，则称 $\tau\colon I \to [k]$ 为合法着色。

我们用 $\chi(T)$ 表示张量 $T$ 的色数，即满足存在合法着色 $\tau : I \to [k]$ 的最小 $k$。同样，如果 $T$ 是普通张量，我们使用简写 $\chi(T) := \chi(\mathrm{supp}(T)\ T)$。

以下刻画的证明与 [CFL83], 中的原始证明完全相同，只是将表述稍微推广为承诺问题的语言，而不是专门针对额头数字问题。

定理 9. 任意承诺单射问题 $(I,P)$ 的确定性通信复杂度等于 $\lceil \log\ \chi(I,P) \rceil$。

证明。给定一个着色 $\tau\colon I \to [k]$，我们将描述一个复杂度为 $\lceil \log k \rceil$ 的通信协议。第一位参与方的输入为 $x$，他查看唯一的 $y^{(1)}, z^{(1)}$，使得 $(x, y^{(1)}, z^{(1)}) \in I$，并记下颜色 $\tau(x, y^{(1)}, z^{(1)})$。类似地，第二位参与方的输入为 $y$，他将记下的颜色与 $(x^{(2)}, y, z^{(2)}) \in I$ 的颜色进行比较，第三位参与方也以同样的方式操作。显然，如果 $(x,y,z)$ 是一个接受实例，那么所考虑的三个三元组都相同，即 $(x^{(2)} = x^{(3)} = x, y^{(1)} = y^{(3)} = y, z^{(1)} = z^{(2)} = z)$，因此所比较的颜色也会一致——该协议将正确接受这样的实例。

另一方面，如果所有 $(x, y^{(1)}, z^{(1)})$、$(x^{(2)}, y, z^{(2)})$、$(x^{(3)}, y^{(3)}, z)$ 都具有相同的颜色 $c$，取独立集 $S := \tau^{-1}(c) \subset I$，则 $x \in \pi_1(S)\ y \in \pi_2(S)\ z \in \pi_3(S)$；又由于 $(x,y,z) \in P$ 且 $S$ 是一个独立集，我们必有 $(x,y,z) \in I$——也就是说，该实例是接受的。这就证明了着色 $\tau : I \to [k]$ 蕴含存在一个高效协议。

反向证明类似：给定一个针对问题 $(I,P)$ 的协议，其通信量至多为 $k$，我们可以将每个输入 $(x,y,z) \in I$ 上的通信记录用作该项的颜色。这就得到一个映射 $\tau\colon I \to [2^k]$，我们只需验证它是一个合法着色。确实，任取一种颜色 $c$，并取一个集合 $S = \tau^{-1}(c)$。如果存在 $(x,y,z) \in P - I$，使得 $(x,y,z) \in \pi_1(S) \times \pi_2(S) \times \pi_3(S)$，那么在（允许的）输入 $(x,y,z)$ 上的通信记录就会与接受输入 $(x, y^{(1)}, z^{(1)})$、$(x^{(2)}, y, z^{(2)})$、$(x^{(3)}, y^{(3)}, z)$ 上的通信记录相同，因此每个参与方都会接受它——这与协议的正确性矛盾，因为 $(x,y,z) \notin I$。 □

## 3.2 与 NOF 通信复杂度的标准界比较

我们目前讨论的是一种略有不同的视角，用来刻画标准的 NOF 通信复杂度（这一方法已见于 [CFL83]）。

传统上，对于 NOF置换问题 $I \subset \Gamma \times \Gamma \times \Gamma$，人们会关联一个有向3-超图 $H$，而该超图色数的对数等于相关问题的确定性通信复杂度。

我们将证明，事实上，前述超图 $H$ 的邻接张量只是承诺张量 $P_{\text{NOF}}$ （即矩阵乘法张量）的一个置换，而且该置换由问题 $I$ 唯一确定——它对应于以一种使 $I$恰好位于张量对角线上的方式置换变量 $y_i$ 和 $z_i$ 。

这为关于利用切片秩或任何其他邻接张量子秩界来证明 $H$通信复杂度下界的障碍，提供了一种推广和另一种视角。

具体而言，请注意，任意独立集 $S \subset V$（$H$）都会将超图 $H$ 的邻接张量归零，从而得到一个较大的恒等子张量（通过限制到 $S \times S \times S$ 中的索引得到——请注意，在构造超图 $H$及其邻接张量时，我们为每个 $t \in V$（$H$）都包含了自环（$t$、$t$、$t$））。因此，可以尝试通过给出该超图 $H$ 的色数下界来限制最大独立集的大小，而独立集的大小又可以通过邻接子张量的子秩来界定。最后，已知任意张量的子秩总是有切片秩作为上界，而且人们已经发展出一些成功的方法来控制若干值得关注的特定张量的切片秩 [Tao16、BCC$^+$17]。

遗憾的是，这条看似有望证明特定 NOF置换问题下界的路径必然行不通。在 [CFTZ22] 中，研究者证明了：可以采用 Strassen 为证明矩阵乘法张量的渐近子秩下界而使用的类似技术，来证明任意 $\textsc{Eval}$群问题的邻接张量的渐近子秩下界——其大小达到了最大值。我们注意到，这并非巧合：事实上，以这种方式构造的所有邻接张量都只是矩阵乘法张量的置换，因此矩阵乘法张量的渐近子秩下界可以直接适用——不仅适用于源自 $\textsc{Eval}_G$的问题，也更一般地适用于所有额头上的数置换问题。

定义 10（通信超图 [CFL83]）。对于置换 NOF问题 $I \subset \Gamma \times \Gamma \times \Gamma$，我们将其通信超图定义为 $H(I)$，这是一个 3 阶超图，其顶点为 $V(H(I)) = I$ ——所有接受实例的集合；超边按如下方式构造：对于所有 $(x, y, z) \in \Gamma \times \Gamma \times \Gamma$，令 $T_1 := (x, y, z') \in I$为 $I$中与 $(x, y, z)$ 的前两个坐标一致的唯一三元组，并类似地令 $T_2 := (x', y, z) \in I$、$T_3 := (x, y', z) \in I$。

那么 $E(H(I)) = \{(T_1, T_2, T_3) : (x, y, z) \in \Gamma^3\}$。

事实 11. 超图 $H(I)$ 的邻接张量是矩阵乘法张量 $\langle |\Gamma|, |\Gamma|, |\Gamma| \rangle$ 的一个置换。

此外，如果我们考虑一组绿色顶点 $(x, y)$、$(y, z)$、$(z, \tilde{x})$ 给出：在问题 $I$的着色通信张量中，该集合在上述置换下对应

于邻接张量中恰好由 $\{(t,t,t):\ t\in I\}$ 给出的集合，其中$H(I)$。

证明。考虑映射 $\pi_{12}:\ I\to\Gamma\times\Gamma$，其定义为 $\pi_{12}(x,y,z)=(x,y)$，类似地还有 $\pi_{23},\pi_{13}$。注意，这三个双射是 $I$ 与 $\Gamma\times\Gamma$ 之间的双射。将这些双射分别作用于超图 $H(I)$ 的邻接张量 $A$ 的三个轴，我们看到，任意超边 $(T_1,T_2,T_3)$ 在定义 10 中的像为 $(\pi_{12}(T_1)\ \pi_{23}(T_2)\ \pi_{13}(T_3))=((x,y),(y,z),(x,z))$ ——矩阵乘法张量 $\langle|\Gamma|,|\Gamma|,|\Gamma|\rangle$ 的一个非零项。矩阵乘法张量的所有非零项都可以通过这种方式得到：因为根据通信超图的构造，任意项 $((x,y),(y,z),(x,z))$ 都可以提升为一条超边 $(T_1,T_2,T_3)\in H(I)$。

最后，关于对角线像的陈述直接由置换 $\pi_{12}$、$\pi_{23}$ 和 $\pi_{13}$ 的定义以及超图 $H$ 的构造得到。

□

推论12。对于任意 NOF置换问题，其通信超图的邻接张量具有最大渐近子秩。

## 3.3 随机 NOF置换问题的通信复杂度下界

本节将证明，在字母表 $[N]\times[N]\times[N]$ 上的随机 NOF置换问题需要 $\geq n/3-\mathcal{O}(1)$ 的确定性通信，其中 $N=2^n$。这是一个简单的计数论证，其思想与 [DP08] 中所使用的论证类似。由于在 $[N]\times[N]\times[N]$ 上的 NOF置换问题与大小为 $N\times N$ 的拉丁方一一对应，因此可以在证明中使用拉丁方数量的已知上界和下界。

以下结论源于这样一个事实：任何拉丁方都可以通过在正则二分图中反复选取完美匹配来构造，并使用 $k$-正则二分图中完美匹配数量的标准界。

定理 13（[VLW01]）。满足条件的 NOF置换问题总数 $\#P$ of NOF置换问题 over $[N]\times[N]\times[N]$

$$N^{N^2}e^{-N^2}\leq\#P\leq N^{N^2}.$$

有了这一点，我们可以证明

定理14。对于字母表$[N]$上的大多数 NOF置换问题（$I$，$P$），其中 $N=2^n$，我们有 $\mathcal{CC}$（$I$，$P$）$\geq\frac{n}{3}-\mathcal{O}$（1）。

证明。设 $(I,P)$ 是定义在 $[N]\times[N]\times[N]$ 上、通信复杂度为 $d$ 的 NOF置换问题。根据定理 9，通信复杂度等价于存在合法着色 $\kappa:\ I\to\{0,1\}^d$。由于 $I$ 是一个置换问题，对于任意 $x\in[N]\times[N]$，存在唯一的 $\pi_1^{-1}(x)\in I\subset([N]\times[N])^3$（其中 $\pi_1:\ ([N]\times[N])^3\to[N]\times[N]$ 是到第一坐标的投影）。

我们可以将 $\kappa_1$ 定义为：$[N]\times[N]\to\{0,1\}^d$，即 $\kappa_1(x):=\kappa(\pi_1^{-1}(x))$。类似地，我们定义 $\kappa_2$ 和 $\kappa_3$。

我们注意到，函数三元组（$\kappa_1$，$\kappa_2$，$\kappa_3$）唯一确定了 $I$。事实上，对于（$a$，$b$，$c$）$\in P$，要检查（$a$，$b$，$c$）$\in I \iff \kappa_1(a)=\kappa_2(b)=\kappa_3(c)$。因此，描述一个通信复杂度为 $d$ 的问题所需的比特数（即此类问题的数量的对数）至多为 $3dN^2$——要描述一个函数 $\kappa$：$[N]\times[N]\to\{0,1\}^d$，我们需要 $dN^2$ 比特。

另一方面，利用定理 13 的下界，我们需要 $N^2\log N-\mathcal{O}(N^2)$ 比特来写出任意的 NOF置换问题。因此，如果$d\le(\log N)/3-\mathcal{O}(1)$，大多数问题都没有通信复杂度为 $d$ 的协议。

□

## 3.4 矩阵乘法张量的独立数与着色背景

下面的结论指出，矩阵乘法张量具有几乎最大的零化子秩，这是矩阵乘法研究中的一项重要见解。该结论最初由 Strassen 在 [Str87]，中证明，并被用作设计某些快速矩阵乘法算法的技术步骤。这里我们将把它用作证明定理 20 的工具。另一方面，在第 3.6 节中，我们将讨论如何利用额头上的数字协议与矩阵乘法张量结构性质之间的联系，从 NOF 通信复杂度中关于某些置换问题的高效协议的已知结果，轻松推导出下面的结论。

定理 15（[Str87]）。存在 $I\subset\operatorname{supp}\langle N,N,N\rangle$，使得 $|I|\ge N^{2-o_{(1)}}$，且限制 $\langle N,N,N\rangle|_{\pi_1(I)\ \pi_2(I)\ \pi_3(I)}$ 是单位张量的一个置换，即 $Q_{zo}(\langle N,N,N\rangle)\ge N^{2-o_{(1)}}$。

等价地，使用本文中引入的记号，

$$\alpha(\langle N,N,N\rangle)\ge N^{2-o(1)}.$$

下面介绍一种标准技术，将对称组合对象中的大独立集提升为较小的着色。为完整起见，我们给出证明。

定义 16（自同构群）。对于着色张量 $T=(I,P)$，我们将 Aut($T$) 定义为满足 $\sigma(I)=I$ 的所有置换三元组 $(\sigma_1,\sigma_2,\sigma_3)$ 的集合；此外，对于所有 $(x,y,z)$，有 $T_{x,\ y,\ z}=T_{\sigma_1(x)\ \sigma_2(y)\ \sigma_3(z)}$。

引理17。对于着色张量 $T=(I,P)$，若任意两个绿色元素 $a,b\in I$ 都存在一个 $\sigma\in$ Aut($T$)，使得 $\sigma(a)=b$，则

$$\chi(T)\le\frac{|I|}{\alpha(T)}\log|I|.$$

证明。设 $S \subset I$ 是一个独立集， $\sigma \sim \mathrm{Aut}(T)$ 是从自同构群中均匀随机选取的一个元素。显然， $\sigma(S)$ 也是一个独立集。我们断言，对于任意 $x \in I$，都有 $\Pr(x \in \sigma(S)) = \frac{|S|}{|I|}$。事实上，设 $S = \{s_1, s_2, \ldots s_m\}$。置换 $\sigma$ 的子集 $T \subset \mathrm{Aut}(T)$ 中，满足 $\sigma(s_1) = x$ 的置换恰好构成 $\mathrm{Aut}(T)$ 中子群 $H$ 的一个陪集，其中 $H$ 是固定 $x$ 的置换集合，即 $H = \{\sigma\colon \sigma \in \mathrm{Aut}(T)\ \sigma(x) = x\}$。此类陪集的数量恰好为 $|I|$，因为我们假设 $x$ 可通过 $\mathrm{Aut}(T)$ 中的某个置换映射到任意其他 $s \in I$ （根据自同构群的性质，不可能映射到其他元素：每个 $\sigma \in \mathrm{Aut}(T)$ 都保持绿色顶不变： $\sigma(I) = I$）。由于同一子群的所有陪集彼此不相交且大小相同，因此有 $\Pr(\sigma(s_1) = x) = 1/|I|$）。因此

$$\Pr(x \in \sigma(S)) = \sum_{i \le |S|} \Pr(x = \sigma(s_i)) = |S|/|I|.$$

最后，考虑 $K = C(|I| \log |S|)/|S|$ 个相互独立的随机置换 $\sigma_1, \sigma_2, \ldots, \sigma_m \in \mathrm{Aut}(T)$。我们希望说明，以正概率，对每个元素 $x \in I$，至少有一个集合 $\sigma_i(S)$ 覆盖它。事实上，从期望来看，每个元素会被 $C \log |S|$ 个这样的集合覆盖；应用标准的 Chernoff 界和并集界论证，即可得出结论。

有了由 $K$ 个独立集构成的 $I$ 覆盖后，我们便可轻松找到一种着色 $\tau$ ：将元素 $x \in I$ 映射 $I \to [K]$ 到满足 $x \in \sigma_i(S)$ 的最小 $i \in [K]$ 。 □

推论 18. 矩阵乘法张量的色数满足

$$\chi(\langle N, N, N\rangle) \le N^{1+o(1)}.$$

我们还需要以下关于矩阵乘法张量的 Kronecker 积的标准事实。

事实 19（参见例如 [Bl¨a13，第 24] 页）。矩阵乘法张量的 Kronecker 积满足

$$\langle N_1, M_1, P_1\rangle \otimes \langle N_2, M_2, P_2\rangle = \langle N_1 N_2, M_1 M_2, P_1 P_1\rangle$$

## 3.5 激光法为所有 NOF 置换问题提供了一个非平凡的渐近协议

本节将使用著名的激光法，该方法最初由 Str86、CW87], 提出，用于设计快速矩阵乘法算法 [，以证明任意置换问题中第三位玩家的渐近 NOF 通信复杂度满足以下令人惊讶的上界。

定理 20. 对于每组三元 NOF置换问题 $I$，每个问题均定义在 $\{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n$ 上，我们有

$$\mathcal{CC}(I \otimes J \otimes K) \le (1 + o(1))n.$$

（注意，平凡界为 $\mathcal{CC}(I \otimes J \otimes K) \leq 3n$。）

特别地，对于任意 NOF置换问题 $P$，定义在 $\{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n$ 上，我们有

$$\underline{\mathcal{CC}}(P) \leq (1+o(1))\frac{n}{3}.$$

我们将分块着色张量定义为：在 $A \times B \times C$ 上的着色张量（$I$，$T$），以及划分集合 $A = A_1 \cup \ldots A_p$、$B = B_1 \cup \ldots \cup B_q$ 和 $C = C_1 \cup \ldots C_q$。

分块张量 $T$ 的外部结构是一个在 $[p] \times [q] \times$ 上的张量 Out($T$)，其中 $[r]$ Out($T$)$_{i,\ j,\ k} = 1$ 当且仅当限制 $T|_{A_i,\ B_j,\ C_k} \neq 0$ （否则为 Out($T$)$_{i,\ j,\ k} = 0$ ）。分块张量 $T$ 的内部结构 $\mathcal{I}(T)$ 是由（着色）张量 $T|_{A_i,\ B_j,\ C_k}$ 构成的集合。外部结构和内部结构的概念在激光法中占有重要地位；例如参见 [Bl¨a13 的第 8] 节。

引理 21. 对于一个分块着色张量 $T$，我们有

$$\chi(T) \leq \chi(\mathrm{Out}(T)) \cdot \max_{T' \in \mathcal{I}(T)} \chi(T').$$

证明。显然——为了为块张量 $T$ 的绿色项$I$集合找到一种合法着色，我们可以将元素 $x \in I$映射到 ($c_1, c_2$)，其中 $c_1$ 是对 Out($T$) 的着色中包含 $x$ 的块所分配的颜色，而 $c_2$ 是对块自身进行着色时分配给 $x$ 的颜色。

我们需要证明每个颜色类都是一个独立集。对于 $A, B, C$ 的一个诱导划分，这等价于注意到：对于任意块张量，如果 Out($T$) 是单位张量的一个置换，并且$\mathcal{I}(T)$中的所有张量也满足这一点，那么整个张量同样是单位张量的一个置换。□

事实 22. 设 $T^1, T^2$ 是一对分块着色张量。那么 $T := T^1 \otimes T^2$ 是一个分块着色张量，其外部结构为 Out($T$) $=$ Out($T^1$)$\otimes$Out($T^2$)，内部结构为 $\mathcal{I}(T) \subset \mathcal{I}(T^1) \otimes \mathcal{I}(T^2)$（这里，对于两个张量集合$\mathcal{A}$ 和 $\mathcal{B}$，我们使用 $\mathcal{A} \otimes \mathcal{B} := \{a \otimes b \colon a \in \mathcal{A}, b \in \mathcal{B}\}$。）

证明。由定义可直接得出。□

事实 23. 对任意一对带颜色张量 $T_1, T_2$，我们有 $\chi(T_1 \otimes T_2) \leq \chi(T_1)\chi(T_2)$。

证明。给定两个着色 $\kappa_1 \colon I_1 \to [k_1]$ 和 $\kappa_2 \colon I_2 \to [k_2]$，我们可以用成对的 $[k_1] \times [k_2]$ 为克罗内克积 $T_1 \otimes T_2$ 构造一种着色，方法是将一项 (($i_1, i_2$), ($j_1, j_2$), ($k_1, k_2$)) $\in I_1 \otimes I_2$ 映射为一对 ($\kappa_1(i_1, j_1, k_1)$ $\kappa_2(i_2, j_2, k_2)$)。它是合法着色这一事实，直接源于两个单位张量的克罗内克积仍是单位张量这一事实。□

引理 24. 存在三个划分 $\mathcal{A}, \mathcal{B}, \mathcal{C}$，使得对于任意 NOF置换问题 ($I, P_{\mathrm{NOF}}$)，由这些划分诱导的分块着色张量 $T := (I, P_{\mathrm{NOF}}, \mathcal{A}, \mathcal{B}, \mathcal{C})$ 满足以下条件

- 外部结构 Out($T$) $= \langle N,\ 1,\ 1 \rangle$。

• 内部结构 $(Y, T')\ \in\ \mathcal{I}(T)$ 中的每个着色张量都有 $T'$ =⟨1、 $N$、 $N\rangle$ 和 $\chi$ $(Y, T')\ = 1$。

证明。考虑划分 $\mathcal{A}:=(A_1, \ldots, A_n)$，其中 $A_t := \{(i,t) :\ i \in [N]\}$；类似地， $\mathcal{B}:=(B_1,$ $\ldots B_N)$，其中 $B_t = \{(t,i) :\ i \in [N]\}$；最后， $\mathcal{C}:=(C) :=([N] \times [N])$ 是只有一个部分的平凡划分。

首先注意，对于矩阵乘法张量 $P$ 的这一划分，块 $A_{t_1} \times B_{t_2} \times C$ 非空当且仅当 $t_1 = t_2$,

$$\mathrm{Out}(T) = \sum_t x_{1,t} y_{t,1} z_{1,1},$$

是矩阵乘法张量 $\langle N,\ 1, 1\rangle$。

此外，考虑任意非空块 $A_t \times B_t \times C$。限制在该块上的张量 $T$ 为

$$T|_{A_t \times B_t \times C} = \sum_{j,k} x_{j,t} y_{t,k} z_{k,j},$$

这恰好是一个 $\langle 1, N, N\rangle$ 矩阵乘法张量。

现在注意，投影 $\pi_3 :\ A_t \times B_t \times C \to C$ 在 $C$与 $Y$:=supp$(T|_{A_t \times B_t \times C})$ 之间诱导了一个双射。如果考察 $S := I \cap Y$，我们希望论证 $S$ 是 $T|_{A_t \times B_t \times C}$中的一个独立集。事实上，记 $S_i := \pi_i(S)$，由于 $(I, P_{\mathrm{NOF}})$ 是一个置换问题，我们只需论证

$$\pi_1^{-1}(S_1) \times \pi_2^{-1}(S_2) \times \pi_3^{-1}(S_3) \cap Y = S.$$

但由于 $\pi_3$ 是双射，我们已经有 $(A_t \times B_t \times \pi_3^{-1}(S_3))\ \cap Y = S$。 □

现在我们已经准备好证明定理 20。

定理 20 的证明。对于置换 NOF 问题 $I$、 $J$、 $K$，根据引理 24，我们可以选择一个块着色张量结构 $T_I$、 $T_J$、 $T_K$，使得 Out$(T_I)$ =⟨$N$、 1、 1⟩，Out$(T_J)$ = ⟨1、 $N$、 1⟩，以及 Out$(T_K)$ = ⟨1、 1、 $N$⟩。

根据事实 22 和事实 19，块着色张量 $T = T_I \otimes T_J \otimes T_K$ 满足 Out$(T)$ = ⟨$N$、 $N$、 $N\rangle$；根据事实 23，每个着色张量 $Z \in \mathcal{I}(T)$ 都有 $\chi(Z)$ =1（因为它是三个色数为 1 的着色张量的乘积）。

根据推论 18， $\chi(\langle N$、 $N$、 $N\rangle) \le N^{1+o_{(1)}}$，最后利用引理 21,

$$\chi(T) \le \chi(\mathrm{Out}(T)) \max_{T' \in \mathcal{I}(T)} \chi(T') \le N^{1+o(1)}.$$

通信复杂度界现在可由定理 9 中的刻画得出。

□

## 3.6 矩阵乘法张量的消零子秩

我们将利用额头数字通信复杂度与矩阵乘法张量结构性质之间的联系，来求得一个

矩阵乘法张量零化子秩的非平凡上界——也就是说，矩阵乘法张量经过零化后所能得到的最大对角子张量的大小上界。

这项工作 [LPS19] 的作者观察到了 NOF 通信复杂度与 Ruzsa–Szemerédi 问题之间的联系。具体而言，他们将 Ruzsa–Szemerédi 定理（该定理又是通过三角形移除引理证明的）作为推论，证明了任意置换问题的 NOF 通信复杂度具有超常数下界。

在这里，我们观察到，借助 NOF 通信与矩阵乘法张量之间的联系，可以运用他们的证明得到一个略强的结论——矩阵乘法的零化子秩上界。

定理25. 矩阵乘法的零化子秩满足

$$Q_{zo}(\langle N, N, N\rangle)) \leq N^2/2^{c\log^* N}.$$

注意，该定理（结合命题 27）事实上蕴含了 [LPS19],中所有 NOF 置换问题的 $\Omega(\log^* N)$ 下界，且证明几乎完全相同。

继续之前，我们先陈述 Ruzsa–Szemerédi 定理一个方便且广为人知的等价表述。Ruzsa 和 Szemerédi 在1978 [RS78], 中借助著名的三角形移除引理，证明了下述量的次二次上界（事实上，他们考虑的是一个略有不同的表述，即(6, 3)问题，但很容易看出它与以下结论等价 [CEMS91]）。在他们的证明中用 Fox [Fox11] 给出的三角形移除引理定量版本替代原有版本，可得以下定量界。

定理26（[RS78、CEMS91、Fox11]）。对于任意图 $G(V, E)$，设 $\mathcal{C}$ 是图 $G$中所有三角形的集合。如果所有这些三角形都是边不相交的，那么 $|\mathcal{C}| \leq N^2/2^{c\log^* N}$，其中 $N = |V|$。

有了这个定理，我们很容易证明矩阵乘法张量中最大独立集的一个次二次上界。事实上，关于矩阵乘法张量中最大独立集密度的定量问题，等价于 Ruzsa–Szemer´edi 问题。

˜定理25的证明。考虑一个独立集 $S \subset \langle N、\ N、\ N\rangle$——我们可以将其视为子集 $S \subset [N] \times [N] \times [N]$。现在考虑定义在 $[N] \times [3]$上的如下三部图：对于每个（$a$，$b$，$c$）$\in S$，我们在顶点（$a$，0）、（$b$，1）和（$c$，2）上放置一个三角形。该构造得到一个 $G$，它有 $3N$个顶点，并带有一个由其 $|S|$ 个三角形组成的集合 $\mathcal{C}$。为了应用定理26，我们需要证明集合 $\mathcal{C}$ 中的三角形是边不相交的，并且它们构成图 $G$中的全部三角形。

首先，它们是边不相交的——如果 $\mathcal{C}$ 中有一对不同的三角形共用一条边，就会对应两个元素（$a$、$b$、$c_1$）$\in S$和

（$a$、 $b$、 $c_2$） $\in S$——这与 $S$ 是矩阵乘法张量中的一个独立集这一假设矛盾。

同样，由于图 $G$ 是三部的，唯一可能的三角形形式为 $(a, 0)$、$(b, 1)$、$(c, 2)$，其中 $a$、$b$、$c$ 取某些值。我们希望证明，若 $S$ 是一个独立集，则这只能在 $(a', b', c') \in S$ 的情况下成立。

事实上，如果边 $(a, 0)$、$(b, 1)$ 被包含在图中，那么必定存在一个元组 $(a, b, c') \in S$；同理，也存在 $(a, b', c) \in S$ 和 $(a', b, c) \in S$，其中 $a'$、$b'$、$c'$ 取某些值。由于 $S$ 是一个独立集，这立即意味着 $a' = a, b' = b, c' = c$，而且事实上 $(a, b, c) \in S$。□

### 3.6.1 基于 NOF 协议的矩阵乘法子秩下界

在研究矩阵乘法张量时，零化子秩的下界比上界重要得多。Strassen 证明了$\alpha(\langle N, N, N\rangle) \geq N^{2-o(1)}$，这个结果几乎达到最大值（因为张量 $\langle N, N, N\rangle$的大小为 $N^2 \times N^2 \times N^2$，而理论上有望在其中找到的最大对角张量大小为 $N^2$）。他将这一结果与激光法结合，设计出了一种快速矩阵乘法算法，即 [Str86], ，此后所有创造纪录的矩阵乘法算法也都采用了这一方法。与此同时，近期的障碍结果 [AW21, Alm21, CVZ21] 利用矩阵乘法子秩的下界，证明某些旨在证明矩阵乘法常数 $\omega = 2$ 的方法存在障碍。（粗略地说，用本文的记号表示，他们表明，由于 $\alpha(\langle N, N, N\rangle)$ 非常大，要设计足够快的算法，就需要使用一个 $\alpha(T)$ 也很大的中间张量 $T$。）

利用激光法证明$\alpha(\langle N, N, N\rangle) \geq N^{2-o(1)}$的一个关键要素，是利用这样一个子集 $S \subset [N]$的存在：它不含三项等差数列，且密度相对较高。利用 Behrend 的 [Beh46] 构造得到密度为 $2^{-\mathcal{O}(\sqrt{\log N})}$的此类集合，可推出 $\alpha(\langle N, N, N\rangle) \geq N^2/2^{\mathcal{O}(\sqrt{\log N})}$。

利用 Behrend 集合的同一构造， [CFL83] 证明，NOF问题 $\textsc{Eval}(\mathbb{Z}_N)$存在一个确定性协议，其通信复杂度为 $\mathcal{O}(\sqrt{\log N})$，显著优于朴素的 $\mathcal{O}(\log N)$。我们注意到，他们构造高效 NOF 协议所用的技术要素，不仅与构造矩阵乘法张量中大独立集所用的技术要素相同，而且二者的关系实际上更为密切——通信复杂度领域的已知结果结合我们揭示的联系，直接推出了 Strassen 关于矩阵乘法张量子秩的结果。

命题 27. 如果存在任何置换问题 $I \subset [N] \times [N] \times [N]$ 具有 NOF 通信复杂度 $CC(\tilde{I}, P_{\text{NOF}}) \leq k$，那么 $\alpha(\langle N, N, N\rangle) \geq N^2 2^{-k}$。

˜证明。根据定理 9，如果承诺问题（$I, P_{\text{NOF}}$）的 NOF 通信复杂度为 $k$，那么 $\chi(I, P_{\text{NOF}}) \leq 2^k$，特别地，取最大颜色可得 $\alpha(I, P_{\text{NOF}}) \geq n^2 2^{-k}$。由于数字在额头通信问题的承诺张量 $P_{\text{NOF}}$ 恰好是矩阵乘法张量

$\langle n,n,n\rangle$，我们可以不考虑哪些项是绿色的，并推得 $\alpha(\langle n,n,n\rangle) \geq \alpha(I, P_{\text{NOF}})$ $\geq n^2 2^{-k}$。 □

## 3.7 其他承诺问题

正如我们现在所理解的，基于切片秩的方法未能为 NOF 置换问题的渐近通信复杂度证明下界，这是因为该技术仅依赖于承诺张量，而不受具体问题的影响——并且与额头数字问题相对应的承诺张量是一个矩阵乘法张量，具有最大子秩。

鉴于此，值得研究具有其他承诺张量的承诺问题；希望对于这些张量，我们已知其渐近子秩不是最大的——仅此论断就意味着，具有此类承诺的每个置换问题都应具有正的渐近通信复杂度。

事实28. 如果承诺张量 $P$在 $\Sigma \times \Sigma \times \Sigma$ 上的渐近子秩不是最大的

$$\underline{\alpha}(P) := \limsup \alpha(P^{\otimes N})^{1/N} < |\Sigma|,$$

那么对于每个置换问题 $I \subset P$ 我们都有

$$\mathcal{CC}((I,P)^{\otimes N}) \geq \Omega(N).$$

利用我们目前为止讨论的内容，该事实的证明是直接的。我们稍后将给出一个严格更强定理（定理 33）的完整证明，因此将这一特殊情形的直接证明留给读者。

帽集问题 [CLP17、EG16、Tao16] 及其后续推广 [BCC+17] 的解可以解释为：对于任意阿贝尔群 $G$，其结构张量

$$T_G := \sum_{g,h \in G} x_g y_h z_{-g-h},$$

具有 $\underline{\alpha}(T_G) < |G|$。特别地，所有承诺张量为此类群的结构张量的置换问题，其渐近通信复杂度均为正。例如，以下结论成立

推论29。考虑承诺问题 $\text{EQ}_{\mathbb{F}_3^N}$，双方分别收到输入 $x$、$y$、$z \in \mathbb{F}_3^N$，且承诺条件为 $x+y+z=0$；他们希望判断 $x=y$是否成立。该问题需要 $\Omega(N)$ 通信。

如果没有前面的讨论，我们不会立刻明白是否应该预期这一结论成立——问题的关键部分涉及 Alice 和 Bob，他们只想判断各自输入是否满足相等谓词；而使用普通的确定性双方协议完成这项任务需要 $\Omega(N)$ 通信。但我们是否应该指望知道 $x+y$ 的 Charlie 能在解决这项任务时提供多少帮助?

另一方面，人们可能会认为，上述陈述——如果为真——应该可以相对直接地证明，其证明类似于

确定性两方相等问题的通信下界。我们注意到，事实上该陈述很容易等价于帽子集定理，因此，直接证明它将成为一个有趣的新证明，证明这一命题曾经作为帽集猜想存在了近四十年。

事实 30：对于任意阿贝尔群 $G$，如果存在一个大小为 $|G|^{1-\delta}$ 且不含三项等差数列的 $S \subset G$，那么 $\mathcal{CC}(\mathrm{EQ}_G) \leq \delta \log |G| + \mathcal{O}(\log \log |G|)$

证明。一个问题 $\mathrm{EQ}_G$ 所对应的通信张量为 $(I, T_G)$，其中 $T_G$ 是群 $G$ 的结构张量，而 $I = \{(x, x, -2x) \colon x \in G\} \subset T_G$。

我们首先证明 $\alpha(I, T_G) \geq |S|$。我们希望证明：如果 $S$ 不含三项等差数列，那么 $S' := \{(x, x, -2x) \colon x \in S\} \subset I$ 是一个独立集。事实上，为了导出矛盾，假设对于某个 $x \neq y$，$(x, y, -x-y)$ 具有 $x \in \pi_1(S')$ $y \in \pi_2(S')$ $-x-y \in \pi_3(S')$。这意味着 $x$、$y \in S$，并且对于某个 $z \in S$ 有 $-x-y = -2z$——也就是说，$x$、$z$、$y$ 构成一个三项等差数列。

要将大独立集提升为小规模着色，我们将引用引理17——只需证明存在一个 $(I, T_G)$ 的自同构，能将任意的 $(x, x, -2x)$ 映射到 $(y, y, -2y)$。这可由三个置换$\sigma_1 = \sigma_2 \colon w \mapsto w - x + y$，以及 $\sigma_3 \colon w \mapsto w + 2y - 2x$ 给出。最后，根据定理 9，将张量 $(I, T_G)$ 着色为 $|G|^{\delta} \log |G|$ 种颜色，可得到一个复杂度为 $\delta \log |G| + \log \log |G|$ 的协议。 □

## 3.8 基于张量渐近谱的下界

本节的结果涉及不一定是置换问题的承诺问题。我们首先需要对这类问题的通信复杂度作一个简单的组合描述。

对于协议 $\pi$ 的任意一条通信记录，产生该通信记录的输入集合 $S_\pi \subset \Sigma \times \Sigma \times \Sigma$ 是一个组合立方体 $A_\pi \times B_\pi \times C_\pi$，其中 $A_\pi$、$B_\pi$、$C_\pi \subset \Sigma$ 满足某些条件。若协议正确，则在每个这样的立方体中，来自 $P$ 的所有项要么都包含在 $I$ 中，要么都不包含在 $I$ 中。因此，复杂度为 $k$ 的正确协议会将张量 $P$ 划分为 $2^k$ 个单色组合立方体（其中，立方体是否为单色按上述含义判定）。

特别地，对于任意承诺问题（$I, P$），$I$中的所有项都可以由 $2^{\mathcal{CC}(I,P)}$ 个组合立方体覆盖，其中每个组合立方体都不包含$P - I$中的任何项。

定理 31。设 $r \colon \mathbb{F}^{\Sigma \times \Sigma \times \Sigma} \to \mathbb{R}_{\geq 0}$ 是任意满足以下条件的函数：

- 次可加，也就是说，若 $A, B \in \mathbb{F}^{\Sigma \times \Sigma \times \Sigma}$，则 $r(A + B) \leq r(A) + r(B)$，并且
- 在置零操作下单调，也就是说，如果 $A$、$B \in \mathbb{F}^{\Sigma \times \Sigma \times \Sigma}$ 和 $B$ 是对 $A$ 的一次置零操作，那么 $r(B) \leq r(A)$。

假设 $P$ 是 $\Sigma \times \Sigma \times \Sigma$ 上的任意承诺张量，且 $I \subset P$ 是任意问题（不一定是置换问题）。那么，

$$\mathcal{CC}(I, P) \geq \log_2 \left( \frac{r(I)}{r(P)} \right).$$

证明。设 $k = 2^{\mathcal{CC}(I,P)}$。根据前面的讨论，存在 $k$ 个张量 $T_1$，.....，$T_k \in \mathbb{F}^{\Sigma \times \Sigma \times \Sigma}$，它们都是 $P$ 的置零结果，且满足 $T_1 + \cdots + T_k = I$。因此我们有

$$r(I) \leq \sum_{i=1}^{k} r(T_i) \leq k \cdot r(P),$$

这正是所需结论。 □

尽管定理 31 相对简单，但它的威力相当大，因为代数复杂性和张量组合学中有许多经过深入研究的函数 $r$，它们是次可加的，且在置零操作下单调。张量秩（$R$）是最突出的例子，但还有其他经过深入研究的秩变体，例如“Tao [的切片秩”和“KMZ [的几何秩”（16] 20]）。（注意，子秩（$Q$）是超可加的，而非次可加的。）

手中数模型 作为一个例子，考虑全 1 张量 $P_{NIH} \in \mathbb{F}^{\Sigma \times \Sigma \times \Sigma}$，它是手中数模型的承诺张量。这个非常简单的张量的秩为 $R(P_{NIH}) = 1$。因此，根据定理 31，任何满足 $R(I) \geq |\Sigma|^{\Omega(1)}$ 的张量 $I$，其手中数通信复杂度都基本达到最大值 Ω(log |Σ|)。注意，所有张量 $I \in \mathbb{F}^{\Sigma \times \Sigma \times \Sigma}$ 都有 $R(I) \geq |\Sigma|$，但有些“退化”的张量除外；例如，所有“精简”张量都具有这一性质 [CGL$^+$21]。

定理 31 的这一具体实例中，承诺是全 1 张量，且 $r$ 是问题张量 $I$的秩，这类似于双方确定性通信复杂度中的标准下界，即通信矩阵的对数秩。著名的对数秩猜想指出，在标准设定下，这一结论可以弱反向推出；事实上，任何双方通信问题（承诺平凡）都有一个复杂度为 $(\log \operatorname{rank}(I))^c$ 的协议，其中 $c$是某个常数。

额头上的数字 再看一个例子，考虑张量 $P_{NOF} \in \mathbb{F}^{\Sigma^2 \times \Sigma^2 \times \Sigma^2}$，它是额头数模型的承诺张量。正如我们所见，$P_{NOF} = \langle |\Sigma|, |\Sigma|, |\Sigma| \rangle$，因此我们知道 $R(P_{NOF}) = |\Sigma|^{\omega + o(1)}$。由此可知，如果 $I \subset P_{NOF}$ 是一个问题，且对某个常数$c > \omega$有 $R(I) \geq |\Sigma|^c$，那么 $I$的额头上的数字通信复杂度为 $\geq (c - \omega + o(1)) \log |\Sigma|$。

这将代数复杂性领域中寻找高秩张量这一经典开放问题，与证明确定性 NOF 下界的任务联系起来。此外，通信下界中减去 $\omega$（即矩阵乘法指数）这一点颇为耐人寻味。这意味着，设计更快的

矩阵乘法算法，从而降低目前已知的 $\omega$ 上界，实际上会让我们更容易通过这种方法证明 NOF 下界。

### 3.8.1 推广到渐近谱

最后，在本节中我们指出，虽然子秩不是次可加的，但我们一直在研究的置零变体（$Q_{ZO}$）对于直和是可加的（因而也是次可加的），所以定理 31 的类似版本对它仍然成立。此外，这对'张量的渐近谱' [Str86、WZ22], 中的任意 $r$ 都成立。这是一个经过深入研究的类，大致刻画了将矩阵的'秩'概念推广到张量的不同方式。

定义 32。张量 $B$ 是张量 $A$ 的一种识别，如果可以先进行一次置零操作，再将某些变量设为彼此相等，从而由 $A$ 得到 $B$。例如， $B = x_0y_0z_0 + x_0y_1z_1$ 是通过将 $z_2$ 置零并令 $x_1 \leftarrow x_0$而得到的 $A = x_0y_0z_0 + x_1y_1z_1 + x_0y_1z_2$ 的识别。识别推广了归零操作，但属于张量限制的特殊情形。

定理 33。设 $r : \mathbb{F}^{\Sigma\times\Sigma\times\Sigma} \to \mathbb{R}_{\geq 0}$ 是任意一个满足以下条件的函数：

- 对直和次可加，也就是说，若 $A \in \mathbb{F}^{\Sigma\times\Sigma\times\Sigma}$ 和 $B \in \mathbb{F}^{\Sigma'\times\Sigma'\times\Sigma'}$ 是定义在互不相交的集合 $\Sigma$、$\Sigma'$ 上的张量，则 $r(A + B) \geq r(A) + r(B)$，其中 $A + B$ 是定义在 $\mathbb{F}^{\Sigma\cup\Sigma'\times\Sigma\cup\Sigma'\times\Sigma\cup\Sigma'}$ 上的张量，并且
- 在识别下单调，也就是说，若 $A$、$B \in \mathbb{F}^{\Sigma\times\Sigma\times\Sigma}$，且 $B$ 是 $A$ 的一个识别，则 $r(B) \leq r(A)$。

设 $P$ 是定义在 $\Sigma \times \Sigma \times \Sigma$ 上的任意承诺张量，而 $I \subset P$ 是任意问题（不一定是置换问题）。那么，

$$\mathcal{CC}(I, P) \geq \log_2 \left( \frac{r(I)}{r(P)} \right).$$

证明。设 $k = 2^{\mathcal{CC}(I,P)}$。根据定义，存在 $k$ 个张量 $T_1$、.....、$T_k \in \mathbb{F}^{\Sigma\times\Sigma\times\Sigma}$，它们都是由 $P$ 进行归零操作得到的，并且满足 $T_1 + \cdots + T_k = I$。特别地， $k$ 个 $P$ 的直和可以通过置零得到所有 $T_i$ 个张量的直和，而后者又可以识别为 $I$。因此我们有

$$r(I) \leq \sum_{i=1}^{k} r(T_i) \leq k \cdot r(P),$$

如我们所愿。 □

事实 34. 消零子秩 $r = Q_{ZO}$ 满足定理 33 的前提。

证明。 $Q_{ZO}$ 对直和是次可加的，因为将直和置零为对角张量时，必须分别将每个部分置零为对角张量。它在识别下单调，因为通过识别将张量$A$ 变换为对角张量时，我们可以假设先进行置零，再令变量彼此相等；但令变量彼此相等不会增加对角张量的大小。

□

## 3.9 中间群承诺问题

假设 $T_1 \subset T_2 \subset T_3$ 是 $\{0,1\}$ 值张量。根据选择哪个作为承诺、哪个作为问题，可以得到三个承诺问题：$(T_1, T_2)$、$(T_1, T_3)$ 和 $(T_2, T_3)$。我们注意到，它们的通信复杂度之间存在一种简单的三角不等式式关系：

事实 35. $\mathcal{CC}(T_1, T_3) \leq \mathcal{CC}(T_1, T_2) + \mathcal{CC}(T_2, T_3)$

证明。为了求解 $(T_1, T_3)$，首先使用一个针对 $(T_2, T_3)$ 的协议，判断输入是否属于 $T_2$，然后使用一个针对 $(T_1, T_2)$ 的协议，判断输入是否属于 $T_1$。

□

现在我们将考虑事实 35 的一个特定实例化，它为证明确定性 NOF 下界提供了一种潜在途径。 $T_1$、$T_2$、$T_3$ 将是来自 $\mathbb{F}^{\Sigma^2 \times \Sigma^2 \times \Sigma^2}$ 的张量，其中 $\mathbb{F}^{\Sigma^2 \times \Sigma^2 \times \Sigma^2}$ 对应某个有限集 $\Sigma$。令 $n := |\Sigma|$。

我们将选取 $T_3$ 作为群 $(\mathbb{Z}/n\mathbb{Z})^2$的结构张量。这个张量通常写作

$$T_3 = \sum_{a,b,c,d \in [n]} x_{(a,b)} y_{(c,d)} z_{(a+c,b+d)},$$

其中，下标中的加法（本小节此处及后文均如此）均模 $n$进行。不过，为了简化下一步，我们可以置换变量名（对所有 $a, b \in [n]$，将 $x_{(a,b)}$ 替换为 $x_{(a+b,b)}$；对所有 $c, d \in [n]$，将 $y_{(c,d)}$替换为 $y_{(c,c+d)}$；对所有$a, b, c, d \in [n]$，将 $z_{(a+c,b+d)}$ 替换为 $z_{(b+d,a+c)}$），从而等价地将其写成

$$T_3 = \sum_{a,b,c,d \in [n]} x_{(a+b,b)} y_{(c,d+c)} z_{(b+d,a+c)}.$$

接下来，我们将选取 $T_2 = P_{\text{NOF}} \in \mathbb{F}^{n^2 \times n^2 \times n^2}$ 作为额头上的数字承诺张量，即 $\langle n, n, n \rangle$ 矩阵乘法张量，

$$T_2 = \sum_{i,j,k \in [n]} x_{(i,j)} y_{(j,k)} z_{(k,i)}.$$

事实 36。 $T_2 \subset T_3$。

证明。对于每个 $i$、$j$、$k \in [n]$，我们需要证明存在一种对 $a$、$b$、$c$、$d \in [n]$ 的选择，使得 $x_{(i,j)} y_{(j,k)} z_{(k,i)} = x_{(a+b,b)} y_{(c,d+c)} z_{(b+d,a+c)}$。满足这一条件的选择是 $b = c = j$、$a = i - j$（模 $n$），以及 $d = k - j$（模 $n$）。

□

最后，我们可以任选一个 $T_1$ 作为额头数字问题 $T_1 \subset T_2$。事实 35 现在将问题 $T_1$ 的额头上的数字复杂度与两个具有承诺 $T_3$ 的不同承诺问题联系起来：

$$\mathcal{CC}(T_1, P_{NOF}) \geq \mathcal{CC}(T_1, T_3) - \mathcal{CC}(P_{NOF}, T_3).$$

利用迄今为止开发的工具，我们可以给出通信复杂度 $\mathcal{CC}(P_{NOF}, T_3)$ 的界。注意，这些是定义在 $\mathbb{F}^{n^2 \times n^2 \times n^2}$ 上的张量，因此平凡的通信上界为 $2 \log n$。

引理 37。

$$(\omega - 2) \log n \leq \mathcal{CC}(P_{NOF}, T_3) \leq \log(n).$$

证明。由于 $P_{NOF}$ 是 $\langle n, n, n \rangle$ 矩阵乘法张量，其秩为$R(P_{NOF}) = n^{\omega + o(1)}$。另一方面，由于 $T_3$ 是阿贝尔群的结构张量，其秩为 $R(T_3) = n^2$（例如，参见 [CU03，定理 2.3 和定理 4.1]）。因此，定理 31 给出了下界 $(\omega - 2) \log n \leq \mathcal{CC}(P_{NOF}, T_3)$。

对于上界，我们直接给出一个通信协议。在这个问题中，参与方 $A$ 获得 $(a + b, b)$，参与方 $B$ 获得 $(c, d + c)$，参与方 $C$ 获得 $(b + d, a + c)$，其中 $a, b, c, d \in \mathbb{Z}_n$ 是一些值；他们的目标是判断以下三个等式是否都成立：$b = c$、$d + c = b + d$ 和$a + c = a + b$。注意，这等价于检验 $b = c$，因为另外两个等式可由此推出。他们可以让参与方 $A$ 发送$b$来完成此事，这需要 $\log n$ 位；然后由参与方 $B$ 确认它是否等于$c$。 □

有趣的是，根据引理 37 中的下界，我们知道，要改进上界 $\mathcal{CC}(P_{NOF}, T_3) \leq \log(n)$，就必须使用快速矩阵乘法。事实上，任何形如 $\mathcal{CC}(P_{NOF}, T_3) \leq (1 - \delta) \log(n)$ 的界都将意味着 $\omega < 3 - \delta$。更具体地说，可以观察到，以这种方式得到的 $\omega$ 上界将属于矩阵乘法的“群论方法” [CU03], ，其中使用的群为 $(\mathbb{Z}/n\mathbb{Z})^2$。对于任何固定的 $n$ [BCC+17]，已知这种方法存在障碍；不过，已知的最佳障碍结果与这种方法通过使用越来越大的 $n$ 来证明 $\omega = 2$ 并不矛盾。（另一方面，最近关于群论方法的大多数研究转而聚焦于非阿贝尔群 [BCG+22]。）

结合引理 37 和事实 35 可得

事实 38。

$$\mathcal{CC}(T_1, P_{NOF}) \geq \mathcal{CC}(T_1, T_3) - \log(n).$$

对于任意 $T_1$，问题（$T_1$，$T_3$）的直接算法具有 $2 \log(n)$ 的通信复杂度。事实 38 表明，任何 $T_1$，其 $\mathcal{CC}$（$T_1$，$T_3$）$\geq (1 + \delta) \log(n)$，对于任意固定的 $\delta > 0$，都将给出一个线性额头数字问题下界 $\mathcal{CC}$（$T_1$，$P_{NOF}$）$\geq \Omega(\log n)$。

鉴于此，改进引理 37 的上界可能会非常有力。具体而言，如果 $\omega = 2$，并且可以据此得到一个算法，实现 $\mathcal{CC}(P_{NOF}, T_3) \leq o(\log(n))$，那么任何满足 $\mathcal{CC}(T_1, T_3) \geq \Omega(\log(n))$ 的 $T_1$

（对首项常数没有任何限制）也将给出线性额头上的数字问题下界 $\mathcal{CC}(T_1, P_{NOF}) \geq \Omega(\log\ n)$。

致谢 作者感谢 Madhu Sudan 和 Toniann Pitassi 提供的宝贵讨论。

## 参考文献

[Alm21] Josh Alman. 矩阵乘法通用方法的局限性。《计算理论》，17(1):1–30，2021年。[AMS12] Noga Alon、Ankur Moitra 和 Benny Sudakov。可分解为大型诱导匹配的近乎完全图及其应用。载于《第四十四届 ACM 计算理论研讨会年会论文集》，STOC '12，第 1079–1090 页，美国纽约州纽约市，2012年。计算机协会。[AS20] Noga Alon 和 Adi Shraibman。可生成稠密 Ruzsa-Szemerédi 图与超图的额头编号协议算法，2020年。[AW21] Josh Alman 和 Virginia Vassilevska Williams。所有已知（以及一些未知）矩阵乘法方法的局限性。SIAM计算杂志，(0):FOCS18–285，2021年。[BCC+17] Jonah Blasiak、Thomas Church、Henry Cohn、Joshua A Grochow、Eric Naslund、William F Sawin 和 Chris Umans。关于帽集及矩阵乘法的群论方法。《离散分析》，3，2017年。[BCG+22] Jonah Blasiak、Henry Cohn、Joshua A Grochow、Kevin Pratt 和 Chris Umans。通过矩阵群进行矩阵乘法。arXiv 预印本 arXiv:2204.03826，2022年。[BDPW10] Paul Beame、Matei David、Toniann Pitassi 和 Philipp Woelfel。确定性与随机多方通信复杂度的分离。《计算理论》，6(1):201–225，2010年。[Beh46] Felix A Behrend。关于不包含三项等差数列的整数集。《美国国家科学院院刊》，32(12):331–332，1946年。[Bin05] Dario Bini。ap× q× 2 张量的边界秩及一对双线性形式的最优近似。载于《自动机、语言与编程：第七届学术讨论会，荷兰诺德韦克豪特，1980年7月14日至18日》，第98–108页。施普林格，2005年。[Bl¨a13] Markus Bl¨aser。快速矩阵乘法。《计算理论》，第1–60页，2013年。

[BT94] Richard Beigel 和 Jun Tarui。关于 ACC。计算复杂性，4:350–366，1994年。[CEMS91] Lane H Clark、Roger C Entringer、Joseph E McCanna 和 L´aszl´o A Sz´ekely。图局部性质的极值问题。《澳大拉西亚组合学杂志》，4:25–32，1991年。[CFL83] Ashok K Chandra、Merrick L Furst 和 Richard J Lipton。多方协议。载于《第十五届 ACM 计算理论研讨会年会论文集》，第94–99页，1983年。[CFTZ21] Matthias Christandl、Omar Fawzi、Hoang Ta 和 Jeroen Zuiddam。张量的对称子秩及其应用，2021年。[CFTZ22] Matthias Christandl、Omar Fawzi、Hoang Ta 和 Jeroen Zuiddam。通过组合退化构造更大的无角集。Schloss Dagstuhl - 莱布尼茨信息学中心，2022年。¨CGL[Austin Conner、Fulvio Gesmundo、Joseph M Landsberg、Emanuele Ventura 和 Yao Wang。迈向 Strassen 渐近秩猜想的几何方法。《数学汇刊》，72:63–86，2021年。+21] CLP[Ernie Croot、Vsevolod F Lev 和 P´eter P´al Pach。中的无等差数列集呈指数级小。《数学年刊》，第331–337页，2017年。[CU03] Henry Cohn 和 Christopher Umans。一种快速矩阵乘法的群论方法。载于《第44届 IEEE 计算机科学基础年会论文集》，第438–449页。IEEE，2003年。[CVZ21] Matthias Christandl、P´eter Vrana 和 Jeroen Zuiddam。不可逆性带来的快速矩阵乘法障碍。《计算理论》，17(2):1–32，2021年。[CW87] Don Coppersmith 和 Shmuel Winograd。通过等差数列进行矩阵乘法。载于《第十九届 ACM 计算理论研讨会年会论文集》，第1–6页，1987年。[DP08] Matei David 和 Toniann Pitassi。分离 NOF 通信复杂度类 RP 与 NP，2008年。[EG16] Jordan S. Ellenberg 和 Dion Gijswijt。关于不含三项等差数列的 $f_q^n$大子集，2016年。[Fox11] Jacob Fox。图移除引理的新证明。《数学年刊》，第561–579页，2011年。

[HG90] J. Hastad 和 M. Goldmann。《小深度阈值电路的能力》。载于《第 *[1990] 31*届计算机科学基础年会论文集》，第 610–618 页，第 2 卷，1990 年。[KMZ20] Swastik Kopparty、Guy Moshkovitz 和 Jeroen Zuiddam。《张量的几何秩与矩阵乘法的子秩》。arXiv 预印本 arXiv:2002.09472，2020 年。[LPS19] Nati Linial、Toniann Pitassi 和 Adi Shraibman。《高维置换的通信复杂度》，2019 年。[LS21] Nati Linial 和 Adi Shraibman。《由更优的 NOF 精确$n$ 协议构造更大的无角集》，2021 年。[RS78] Imre Z Ruzsa 和 Endre Szemer´edi。《不含六个点构成三个三角形的三元系统》。《组合学》（凯斯特海伊，1976），Bolyai János 数学学会论文集，第 18 卷（939–945 页）：第 2 页，1978年。[Str73] Volker Strassen。《避免除法》。《纯粹与应用数学杂志》，264：184–202，1973 年。[Str86] Volker Strassen。《张量渐近谱与矩阵乘法指数》。载于《第 27 届计算机科学基础年会》（SFCS 1986），第 49–54 页。IEEE，1986 年。[Str87] V Strassen。《相对双线性复杂度与矩阵乘法》。《纯粹与应用数学杂志》，375：406–443，1987 年。[Tao16] Terence Tao。《Croot–Lev–Pach–Ellenberg–Gijswijt capset 界的对称表述》。博客文章，2016年。[VLW01] Jacobus Hendricus Van Lint 和 Richard Michael Wilson。《组合学教程》。剑桥大学出版社，2001 年。[WZ22] Avi Wigderson 和 Jeroen Zuiddam。《渐近谱：理论、应用与扩展》，2022 年。