arXiv:2303.01709v1 [cs.DS] 3 Mar 2023

专家学习的流式算法：确定性与鲁棒性

DavidP. Woodruff Fred Zhang* SamsonZhou†卡内基梅隆大学 加州大学伯克利分校 加州大学伯克利分校和莱斯大学
dwoodruf@cs.cmu.edu z0@berkeley.edu samsonzhou@gmail.com

摘要

在专家在线学习问题中，给定一组每天（或每个时刻）都会做出预测的 n 专家，算法必须在 T 天（或时刻）中的每一天，对某个结果做出预测。算法会收到每天结果的反馈，包括自身预测的成本以及专家预测的成本；其目标是做出成本最低的预测，具体而言，是与这组专家中的最佳专家相比。Srinivas、Woodruff、Xu 和 Zhou 最近的工作（STOC 2022）开始研究内存约束下的专家在线学习问题。

然而，专家或算法在某个时刻做出的预测往往会影响未来的结果，因此输入是自适应选择的。确定性算法能够抵御自适应输入，而现有算法则都关键性地依赖随机化来抽取少量专家。

本文研究专家问题的确定性算法和鲁棒算法。我们首先证明，对于任何在最佳专家犯下 M 次错误时实现遗憾 R 的确定性算法，其空间下界为 $\widetilde{\Omega}\left(\frac{nM}{RT}\right)$。我们的结果表明，自然的确定性算法——依次遍历各个专家池，直到池中的每位专家都犯过错——在相差多对数因子的范围内是最优的。另一方面，我们给出一种能够应对自适应输入的随机化算法，其空间开销为 $\widetilde{O}\left(\frac{n}{R\sqrt{T}}\right)$，适用于 $M = O\left(\frac{R^2T}{\log^2 n}\right)$，由此展示了平滑的空间-遗憾权衡。

*部分工作是在谷歌实习期间完成的。
†部分工作是在卡内基梅隆大学期间完成的。

1 引言

专家在线学习是一种序贯预测问题。在每个 T 天（或时刻），算法都必须根据一组 n 专家针对某个结果所作的预测，对该结果作出预测。随后，算法会收到关于其预测成本以及专家当天预测的反馈。在离散专家预测问题中，可能的预测被限制在一个有限集合内；如果预测正确，成本为 0，否则为 1。更一般地，可能的预测不必受到限制，但我们假设成本被限制在某个范围 $[0, \rho]$ 内，其中 $\rho > 0$是一个固定参数；成本越低，表示算法或专家的表现越好。这个过程持续 T 天（或时刻），之后将算法的表现与表现最佳的专家进行比较。更形式化地说，专家在线学习问题的目标通常用遗憾来衡量：遗憾是算法的总成本与表现最佳的专家的总成本之差，也就是总体成本最低的专家所产生的成本之差，并按总天数摊销。

一种广为人知、广泛流传的处理离散专家预测问题的算法是加权多数算法 [LW94]。加权多数算法的确定性变体只需将所有专家的“权重”初始化为 1，在某一天对任何预测错误的专家降低权重，并选择获得专家权重总和最高支持的预测。该算法解决离散专家预测问题所需的总错误数为 $O(M + \log n)$，其中 M 是最佳专家犯下的错误数，而大 O 符号隐藏的系数 M 约为 2.41，因此遗憾为 $O(M + \log n)$。更一般地，大量文献研究了对加权多数算法的优化，例如一种随机化变体：算法选择每种预测的概率，与支持该预测的专家权重之和成正比。随机加权多数算法的遗憾为$O\left(\sqrt{\log\ n/T}\right)$ [LW94],，且已证明该结果在信息论意义上是最优的，至多相差一个常数。此后，针对加权多数算法和随机加权多数算法又出现了许多后续研究，在达到相似遗憾界的同时改进了其他方面。例如，对于在线最短路径等各种结构化问题，跟随扰动领导者 [KV05]达到与随机加权多数算法相同的遗憾界，但每一天（或每个时间步）的运行时间更短。此外，乘法权重算法达到最优的 $\sqrt{\ln\ n/(2T)}$ 遗憾，且其首项系数是紧的 [GPS17]。然而，这些经典算法采用的框架需要维护每位专家的累计成本，因此算法在整个运行过程中需要存储 $\Omega(n)$ 比特的信息。

内存界。最近， [SWXZ22] 研究了内存对算法至关重要时的专家在线学习问题。在困难性方面，他们证明，任何达到目标遗憾 R 的算法都需要 $\Omega\left(\frac{n}{R^2T}\right)$ 空间，这意味着任何达到信息论 $O\left(\sqrt{\log\ n/T}\right)$ 遗憾的算法都必须使用近线性空间。另一方面，对于随机顺序数据流，算法可能收到最坏情况输入，但天的顺序是均匀随机的。针对这种情况， [SWXZ22] 提出了一种几乎匹配的随机化算法，使用 $\widetilde{O}\left(\frac{n}{R^2T}\right)$ 空间，并能达到 $R = \Omega\left(\sqrt{\frac{\log^2 n}{T}}\right)$，即几乎所有低至信息论极限的遗憾值。此外，当最佳专家犯下的错误数 M 较少时，也就是说，$M = O\left(R^2T\right)$， [SWXZ22] 提出了一种使用 $\widetilde{O}\left(\frac{n}{RT}\right)$ 空间、适用于任意顺序

数据流，从而表明，他们的下界所体现的困难源于最佳专家犯下大量错误的情形。

随后， [PZ23] 研究了算法使用的内存受限于次线性于 n的专家在线学习问题。他们提出了一个通用框架，使用 $o(T)$ 内存实现 $o(n)$ 遗憾，并通过一个权衡空间与遗憾的参数，实现了使用 $O_n\left(T^{4/5}\right)$ 遗憾和 $O\left(\sqrt{n}\right)$ 空间，以及使用 $O_n\left(T^{0.67}\right)$ 遗憾和 $O\left(n^{0.99}\right)$ 空间。

自适应输入与确定性。 到目前为止，讨论一直聚焦于非自适应设置：算法的输入可以是最坏情况，但其选择独立于算法及其输出。专家在线学习问题通常也在自适应设置下进行研究，此时允许算法的输入依赖于算法先前的输出。形式上，我们将自适应设置定义为算法$\mathcal{D}$ 与对手 $\mathcal{A}$ 之间的一场双人博弈，由对手自适应地为 $\mathcal{D}$生成输入流。随后，博弈按天进行，在第 t 天：

(1) 对手 $\mathcal{A}$ 根据所有先前的流更新和算法 $\mathcal{D}$ 先前的所有输出，选择第 t 天所有专家的输出以及第 t 天的结果。(2) 所有专家的输出（即预测）同时提供给算法 $\mathcal{D}$；该算法更新其数据结构，获取一批新的随机比特 R_t ，并输出对第 t 天结果的预测。(3) 第 t 天的结果会向 $\mathcal{D}$ 揭示，而由 $\mathcal{D}$ 对第 t 天作出的预测则会向对手 $\mathcal{A}$ 揭示。

目标是 $\mathcal{A}$ 诱使 $\mathcal{D}$ 在整个数据流期间尽可能多地作出错误预测。显然，专家在线学习问题的任何确定性算法在自适应模型中都将保持相同的保证。不幸的是， [SWXZ22] 和 [PZ23] 的算法都是随机化过程，它们依赖于反复采样专家“池”，而了解每个池中采样到的专家的自适应对手可能会利用这一点。有趣的是，随机加权多数算法 [LW94] 和乘法权重算法 [GPS17]已知对自适应输入具有鲁棒性。

1.1 我们的贡献

本文研究了在自适应输入下，针对专家问题的在线学习中，次线性空间算法的能力与局限。

确定性算法的紧界。首先，我们给出一种简单的确定性算法，其使用空间为 $\widetilde{O}\left(\frac{nM}{RT}\right)$。考虑一种算法，它迭代地选取下一组包含 $k=\widetilde{O}\left(\frac{nM}{RT}\right)$ 位专家的池，并在池中的专家上运行确定性多数算法，同时从池中移除所有预测错误的专家，直至池完全耗尽，此时再选取下一组包含 $\widetilde{O}\left(\frac{nM}{RT}\right)$ 位专家的池。其核心直觉是，每个池在完全耗尽前最多会产生 $O(\log\ n)$ 个错误，而最佳专家最多只会犯 M 个错误。当池已经轮换遍历了 nM 位专家，即每位 n 专家各轮换 M 次后，最佳专家便不再犯任何错误，并会留在池中。因此，确定性算法所犯错误的总数为 $\frac{nM}{k}\cdot O(\log n)$。因此，对于目标平均遗憾

R，算法所犯错误的总数必须至多为 $M + RT \geq RT$，因此只需将 $k = \widetilde{O}\left(\frac{nM}{RT}\right)$ 设为 R，即可达到遗憾 $k = \widetilde{O}\left(\frac{nM}{RT}\right)$。由于算法在一个包含 $\widetilde{O}\left(\frac{nM}{RT}\right)$ 位专家的池中运行确定性多数算法，因此该算法使用 M =空间。然而，当 RT为 Ω(n) 时，算法必须使用与专家数量 n 近线性的空间；当n很大时，这并不理想。（详细的形式化论证见 第4.1节）

因此，自然会问，是否存在一种比这种直接方法更节省空间的确定性算法。遗憾的是，我们首先证明，事实并非如此：

定理 1.1（确定性算法的内存下界；另见 定理 3.8）。对于$n = o(2^T)$，对于离散专家预测问题，任何实现 R 遗憾的确定性算法，都必须使用 $\Omega\left(\frac{nM}{RT}\right)$ 的空间，当最佳专家犯下 M 错误时。

结合上述确定性过程，这就解决了专家在线学习的确定性流式复杂度问题。

从概念层面来看，我们在定理 1.1中的下界表明，令人惊讶的是，最佳专家所犯错误的数量M是一个内在参数，决定了该模型中确定性算法的能力与局限。事实上，我们在 定理 3.8 中证明了一个更强的结果：任何以至少 $1 - \exp(-T)$ 的概率成功的随机化算法，在最佳专家犯下 $\left(\frac{nM}{RT}\right)$ 错误时，都必须使用 Ω M的空间。

此外，当 $M = \Omega(T$时，我们给出一种另一种证明。该证明不同于定理 1.1的证明。相反，它利用了 [KPW21]最近提出的一种新集合不相交问题的通信复杂度。该结论在技术上弱于定理 1.1，并收录于附录中；参见附录A。

定理定理 1.1的证明概述。为证明该定理，我们考虑 ε-DiffDist的通信问题。该问题结合了 n 个来自 [BGM+16]的分布式检测问题实例，最早由 [SWXZ22] 此前提出，用于证明随机顺序数据流中专家学习的空间下界。

具体而言，给定固定的 T，带有 $\varepsilon = \frac{M}{T}$ 的 ε-DiffDist 问题由 T 位玩家组成，每位玩家持有 n 比特，索引从 1 到 n。这些玩家必须区分以下情形：

(1) 否定情形 $\mathcal{D}^{(n)}_{\text{否定}}$，其中每位玩家的每个比特均独立同分布地从公平硬币中抽取，并且

(2) YES 情形 $\mathcal{D}^{(n)}_{\text{YES}}$：任意选取一个索引 $L \in [n]$，每个玩家的第 L 位比特均独立同分布地从参数为 $\left(1 - \frac{M}{T}\right)$ 的伯努利分布中选取，而每个玩家的所有其他比特均独立同分布地由公平硬币决定。

从整体上看，证明分两步进行：

(1) 首先，我们证明，对于任何以概率 $1 - 2^{-\Theta(T)}$ 成功的协议（包括确定性协议），ε-DiffDist的通信复杂度存在下界。(2) 其次，我们说明，可以将 ε-DiffDist 问题归约为流式处理场景中的专家预测问题。

第二步很直接，这个想法由 [SWXZ22] 提出。在该归约中，ε-DiffDist 实例中的每个玩家都对应专家预测问题中的一天。每个玩家持有的 n 位

输入对应于每天的 n 专家预测。因此，在否定情形下，每位专家大约有一半天数预测正确。在 YES 情形下，存在一位专家$L \in [n]$，其大约在 $1/2+\delta$ 的天数里预测正确（对于 $\delta = 1/2 - M/T$），而所有其他专家每天都随机猜测。假设存在一个用于专家预测问题的流式算法，其平均遗憾为 $\delta/2$。那么粗略地说，在 YES 情形下，该算法大约在 $1/2+\delta/2$ 的天数里预测正确；而在每位专家都随机猜测的否定情形下，该算法预测正确的天数不到 $1/2+\delta/2$。这就区分了 YES 情形和否定情形，从而解决了 ε-DiffDist。

第二步，我们证明，以至少$1-2^{-\Theta(T)}$的概率解决 ε-DiffDist 问题需要 $\Omega(nM)$ 的总通信量。

注意，若将输入视为 $T \times n$ 矩阵，则 $\mathcal{D}^{(n)}_{\text{否定情形}}$ 是一个按列构成的乘积分布，可写为 ζ^n，其中 ζ 是单列上的分布，使得该列的所有元素均为参数为$1_{\ 2}$的独立同分布伯努利随机变量。我们将 $\mathcal{D}^{(n)}_{\text{否定情形}}$ 视为困难分布，并进行信息复杂度分析。根据直接和论证，只需证明单列问题（即区分 $\mathcal{D}^{(1)}_{\text{否定情形}}$ 与 $\mathcal{D}^{(1)}_{\text{肯定情形}}$，也就是 $n=1$）需要 $\Omega(M)$ 的总通信量。

设 $(C_1, C_2, \ldots, C_T)$ 是从困难分布中抽取的单列，即否定情形，其中每个玩家持有一个参数为 $1/2$ 的独立同分布伯努利随机变量。设 A 是一个成功概率至少为 $1-\exp(-\Theta(T))$的固定协议。对于所有 $i < T$，令 M_i表示从玩家P_i发送给玩家 P_{i+1}的消息，且 $M_{<i} = \{M_j : \ j < i\}$。令 $\Pi = \Pi(C_1, \cdots, C_T)$表示 A 在输入$(C_i)_{i=1}^T$下的通信记录。标准的信息复杂度论证 [BJKS04] 表明，总通信量至少为信息成本，其定义为 $I(C_1, \ldots, C_T;\ \Pi(C_1, \ldots, C_T))$，其中 $I(X, Y)$表示随机变量 X 与 Y之间的互信息。

因此，我们证明的关键步骤是将信息成本下界约束为 $\Omega(M)$。主要思路如下。对于任意 $i \in [T]$，若满足以下条件，我们称 $(M_i,\ M_{<i})$ 关于输入 C和通信记录 $\Pi = (M_1,\ M_2,\ \ldots,\ M_T)$ 对 i而言是信息丰富的：

$$\left|\Pr\left(C_i = 0 \mid M_i, M_{<i}\right) - \Pr\left(C_i = 1 \mid M_i, M_{<i}\right)\right| \geq c \tag{1.1}$$

对某个常数 $c > 0$成立。否则，我们称 M_i 是不具信息性的。直观而言，信息丰富的消息 M_i 会揭示关于 C_i 的足够多信息，使得互信息$I(M_i,\ C_i \mid M_{<i})$会很大。

现在，对所有 $i \in [T]$，令 p_i 表示 $(M_i,\ M_{<i})$ 具有信息丰富性的概率（对 i而言，关于C 和 Π），该概率取遍协议中所有可能的输入和随机性。很容易证明，

$$I(\Pi; C_1, C_2, \ldots, C_T) = \sum_{j=1}^{T} I\left(M_j; C_j \mid M_{<j}\right) \geq \Omega\left(\sum_{j=1}^{T} p_j\right).$$

具体而言，我们首先利用互信息链式法则将互信息分解为求和中的各个项，再利用条件熵进一步分解。随后，所需的界即可由二元熵函数的一个标准界直接得到。接下来，只需证明

$$\sum_{j=1}^{T} p_j > \gamma \cdot M,$$

对某个固定常数 $\gamma > 0$ 成立。

为此，我们注意到，如果 $\sum_{j=1}^{T} p_j = o(M)$，那么根据马尔可夫不等式，集合 S中非信息性指标的数量至少为 $T - o(M)$ 的概率至少为 9 10。我们证明，通过修改 C 在非信息性指标 S上的取值，可以找到一个输入 C'，使得 A 无法以至少 $1 - \exp(-\Theta(T))$ 的概率保证正确性。令 C' 为一个输入，它在信息性指标 $[T] \setminus S$上与 C一致，因此对于 $i \in [T] \setminus S$，有 $C'_i = C_i$；而在非信息性指标 S上的取值则任意选取。根据信息性指标的定义，协议 A 在输入 C' 上生成 Π 的概率至少是协议 A 在输入C上生成 Π的概率的 $(1-c)^T \geq e^{-cT}$倍。然而，由于 C可能在 S处与 C'不同，因此 C可能在 $|S| = T - o(M)$ 个指标上与 C'不同。由此可知，存在一种 C' 的取值，其中 0 的数量少于 $\frac{M}{2}$，使得 A 也会以至少 $\frac{e^{-cT}}{2}$ 的概率输出 Π。另一方面，由于 Π 对应于一条使 A 输出 NO 的通信记录，因此 A 在输入 C'上成功的概率不可能达到 $1 - \frac{e^{-cT}}{8}$。另一方面，YES 实例以 2^{-T}的概率生成 C'，这就产生了矛盾。因此可得 $\sum_{j=1}^{T} p_j = \Omega(M)$，证毕。

针对自适应输入的算法。 从积极的一面来看，我们证明，对于离散专家预测问题，存在一种能够抵御自适应输入的随机化算法：

定理 1.2 （针对自适应输入的鲁棒算法）。 设 $R > 64 \log_T{}^2 n$，且假设最佳专家至多犯 $M \leq \frac{R^2 T}{128 \log^2 n}$ 个错误。那么，对于离散专家预测问题，存在一种算法，使用 $\widetilde{O}\left(\frac{n}{R\sqrt{T}}\right)$ 空间，且遗憾至多为 R，其成功概率至少为 $1 - \frac{1}{\text{poly}(n,T)}$。

我们指出，定理 1.2 在空间和遗憾之间提供了平滑的权衡，几乎达到了针对一般最坏情况输入的信息论极限 $R = O_n\left(\sqrt{\frac{1}{T}}\right)$。然而，与无适应性输入下的最优算法相比，它的空间开销存在 $\widetilde{O}(\sqrt{T})$ 倍的乘法因子。因此，我们认为，自适应输入下离散专家预测问题的空间复杂度的完整刻画，是这项工作自然引出的一个开放问题。

我们针对定理 1.2 的算法使用差分隐私（差分隐私）来向自适应对手隐藏算法的内部随机性。该技术最早由近期工作 [HKM+20、ACSS23、BKM+22] 提出，用于在数据流算法中实现对抗鲁棒性。为利用该技术解决专家学习问题，我们运行 $\widetilde{O}\left(\sqrt{T}\right)$ 个无偏算法 [SWXZ22] 的副本，然后利用高级组合证明：在 $\widetilde{O}\left(\sqrt{T}\right)$ 个副本上分别运行私有中位数，经过 T次交互后可保证差分隐私。正确性随后由差分隐私的泛化推出。

1.2 相关工作

专家问题。 专家问题已得到广泛研究 [CBL06], 既包括离散决策设定 [LW94] 也包括由各种损失函数决定成本的设定 [HKW95、Vov90、Vov98、Vov99、Vov05]。因此，专家问题可应用于许多不同的领域，例如投资组合优化 [CO96、Cov91], 集成提升 [FS97],以及预测 [Her22]。在对专家作出某些假设的前提下，例如假设专家是

决策树 [HS97、TMV01], 阈值函数 [MW98], 或具有良好的线性结构 [KV05],此外，人们还通过进一步优化来缩短专家问题算法的运行时间。更一般地说，现有工作大多忽视了针对内存约束的优化，而着重关注时间复杂度或遗憾保证，因此往往需要使用 $\Omega(n)$ 内存来跟踪每位专家的表现。

最近， [SWXZ22] 开始研究专家问题中的内存-遗憾权衡。对于 $n \gg T$, [SWXZ22] 证明，在随机顺序数据流中，该问题的空间复杂度为 $\tilde{\Theta}\left(\frac{n}{R^2T}\right)$；但他们也给出了一种随机化算法，当最佳专家所犯的错误数 M “较小”时，该算法可在任意顺序数据流中使用 $\widetilde{O}\left(\frac{n}{RT}\right)$ 空间。随后， [PZ23]针对 $T \gg n$考察了专家在线学习问题，并提出了一个通用的空间-遗憾权衡框架：使用 $o(n)$内存可实现 $o(T)$遗憾，其中包括使用$O(\sqrt{n})$空间实现 $O_n(T^{4/5})$遗憾，以及使用 $O\left(n^{0.99}\right)$ 空间实现 $O_n(T^{0.67})$遗憾。

自适应输入。受非独立输入和对抗性攻击的启发，近期研究开始在集中式模型 [CN20, KSS22, CN22, CSW+23]、流式模型 [AMYZ19, BJWY21, HKM+20, WZ21, BHM+21, CGS22, BEO22, ABJ+22, ACGS22, CLN+22, ACSS23, DSWZ23], 以及动态模型 [Waj20, BKM+22]中考虑自适应输入。特别是，对于那些可依赖于算法先前输出的输入（即黑盒攻击）具有鲁棒性的算法，对于未来输入可能依赖于先前输出的情形也具有鲁棒性。这一点与预测等应用尤其相关：在这些应用中，对第 i 天的预测可能引发一系列行动，进而影响第 $i+1$ 天及之后的结果和专家预测。

当目标仅仅是实现尽可能最佳的遗憾时，自适应对手在在线学习文献中受到了相当多的关注 [BE98, CBL06, MB04]。在多臂老虎机问题的一系列结果基础上 [ACFS02, AK04, Kle04], , [MOSW02] 的工作首次研究了针对内存受限的自适应对手的专家设定，并给出了一种遗憾为 $O\left(T^{2/3}\right)$ 的算法。 [dFM06] 的一篇早期论文针对自适应输入引入了一族算法，但其所提供的保证采用的概念与遗憾的标准定义并不完全相关。较新的工作探索了带有额外考量的在线学习，例如可优化的替代量 [DTA12], 、额外的切换成本 [CDS13, DDKP14, RSC21], , 以及反馈图 [AMM19]。与我们的设定最接近的工作是 [PZ23] 的近期结果：当输入由能够访问算法内部状态的对手，即白盒对手，选择时，使用相对于 n 次线性空间的任何算法都无法实现关于 T 的次线性遗憾。

同期且独立的工作。与我们的工作同期， [PR23] 研究了这样一个问题变体：算法在每个时刻选择一位专家，而不是做出预测。随后，他们提出了一种能够抵御自适应对手的算法，该对手会在每个时刻观察算法所选择的具体专家；此外，他们还给出了任何能够抵御此类对手的算法的下界。

确保对抗鲁棒性的一种方式是采用确定性算法。在这方面，我们为确定性算法证明了更强的下界，表明其必须依赖于最佳专家所犯错误的数量，即任何实现摊销遗憾 M 的确定性算法都必须使用 R $\widetilde{\Omega}\left(\frac{nM}{RT}\right)$ 空间。事实上，当最佳专家所犯错误的数量足够少，即 M $M = O\left(\frac{R^2T\log}{^2n}\right)$ 摊销遗憾为 R 时，我们给出了一个随机化上界，其所需空间比该下界更少。相比之下， [PR23]

表明，任何实现 R 摊销遗憾的算法都必须使用 $\widetilde{\Omega}\left(\sqrt{\frac{n}{R}}\right)$ 空间，不过他们的下界也适用于随机化算法。

由于设置不同，我们的算法技术与[PR23]的截然不同。我们采用了 [HKM+20、ACSS23和BKM+22]提出的近期思想来隐藏算法的内部随机性，使其不被对手发现；而 [PR23] 则在专家组之间轮换，以防止对手通过在某个专家被选中后立即使其表现变差来造成高遗憾。

2 预备知识

记号。对于任意 $t \leq n$ 和向量（X_1、X_2、$\cdots$、X_n），我们令 $X_{<t}$ 表示（X_1、$\cdots$、X_{t-1}）、$X_{\leq t}$ =（X_1、$\cdots$、X_t）以及 X_{-t} =（X_1、$\cdots$、X_{t-1}、X_{t+1}、$\cdots$、X_n）。此外，$X_{>t}$ 和 $X_{\geq t}$ 也作类似定义。令 e_i 表示第 i 个标准基向量；对于任意 S、e_S，表示在索引 $i \in S$ 处为 1、其他位置均为 0 的向量。对于随机变量 X，令 $H(X)$ 表示其熵。

2.1 信息论

对于任意 $p \in [0,1]$，我们稍微滥用记号，将 $H(p) = -p\log_2 p - (1-p)\log_2(1-p)$ 记为二元熵函数。下面给出 $H(p)$ 的一个标准上界和下界。

引理 2.1（二元熵函数的界；例如参见 [Wik22]）。对于 $p \in [0,1]$，二元熵函数满足

$$4p(1-p) \leq H(p) \leq 2\sqrt{p(1-p)}.$$

2.2 通信复杂度

定义 *2.2*（互信息）。设 X 和 Y 是一对联合分布为 $p(x,y)$ 的随机变量。则互信息定义为 $I(X;Y) := \sum_{x,y} p(x,y) \log \frac{p(x,y)}{p(x)p(y)}$，其中边缘分布为 $p(x)$ 和 $p(y)$。

在一个由 t 个参与者组成的多方通信问题中，每个参与者都会获得 $x_i \in \mathcal{X}_t$。他们根据固定协议进行通信，以计算函数 $f\colon \mathcal{X}_t \times \cdots \times \mathcal{X}_t \to \mathcal{Y}$。如果存在函数 Π_{out}，使得 $\Pr[\Pi_{\text{out}}(\Pi(x, y)) = f(x, y)] \geqslant 1-\delta$，则称协议 Π 为针对 f 的 δ-错误率协议。对于一个（多方）通信问题，我们将协议中所有通信的通信记录记为 $\Pi \in \{0,1\}^*$。因此，协议的通信成本就是通信记录的比特长度。令 $R_\delta(f)$ 表示针对 f 的最佳 δ-错误率协议的通信成本。

定义 2.3（信息成本）。设 Π 是一个随机化协议，它在从分布 μ 中抽取的输入 $X_1, \ldots, X_T$ 上生成随机变量 $\Pi(X_1, \ldots, X_T)$ 作为通信记录。那么，Π 关于 μ 的信息成本定义为 $I(X_1, \ldots, X_T; \Pi(X_1, \ldots, X_T))$。

定义 2.4（信息复杂度）。函数 f 关于分布 μ 和失败概率 δ 的信息复杂度，是关于 μ 的协议针对函数 f 的最小信息成本；该协议在每个输入上的失败概率至多为 δ，记作 $\mathrm{IC}_{\mu,\delta}(f)$。

引理 *2.5*（信息成本分解引理，[*BJKS*04] 中的引理 *5.1*）。设 μ 是乘积分布的混合，且 Π 是针对输入 $(X_1, \ldots, X_T) \sim \mu^n$ 的协议。那么 $I(X_1, \ldots, X_T; \Pi(X_1, \ldots, X_T)) \geq \sum_{i=1}^{n} I(X_{1,i}, \ldots, X_{T,i}; \Pi(X_1, \ldots, X_T))$，其中 $X_{i,j}$ 表示 X_i 的第 j 个分量。

引理 2.6（信息复杂度给出通信复杂度下界；命题 4.3[BJKS04]）。对于任意分布 μ 和错误率 δ，$R_\delta(f) \geq \mathrm{IC}_{\mu,\,\delta}(f)$。

2.3 差分隐私

我们的算法结果依赖于差分隐私中的以下工具。

定义 2.7（差分隐私，[DMNS06]）。给定一个隐私参数 $\varepsilon > 0$ 和一个失败参数 $\delta \in$（0，1），若随机化算法 $\mathcal{A}$：$\mathcal{X}^* \to \mathcal{Y}$满足以下条件，则称其为（$\varepsilon$，$\delta$）-差分隐私：对于每一对相邻数据流 S 和 S'，以及所有 $E \subseteq \mathcal{Y}$，

$$\mathbf{Pr}\left[\mathcal{A}(S) \in E\right] \leq e^{\varepsilon} \cdot \mathbf{Pr}\left[\mathcal{A}(S') \in E\right] + \delta.$$

定理 *2.8*（私有中位数，例如 [*HKM*+20]）。给定一个数据库 $\mathcal{D} \in X^*$、一个隐私参数$\varepsilon > 0$和一个失败参数 $\delta \in (0, 1)$，存在一个（ε, 0）-差分隐私算法PrivMed，输出一个元素 $x \in X$，使得以至少 $1-\delta$ 的概率，S 中至少有 $\frac{|S|}{2} - m$ 个元素不小于 x，并且 S 中的 S 至少有 $\frac{|S|}{2} - m$ 个元素不大于 x，其中 $m = O\left(\frac{1}{\varepsilon} \log \frac{|X|}{\delta}\right)$。

定理 2.9 (高级组合，例如 [DRV10]）。设 ε，$\delta' \in (0, 1]$ 并设 $\delta \in [0, 1]$。任何允许 k 与保持 (ε, δ)-差分隐私保证的机制进行自适应交互的机制，都能保证 $(\varepsilon'$，$k\delta + \delta')$-差分隐私，其中 $\varepsilon' = \sqrt{2k \ln \frac{1}{\delta'}} \cdot \varepsilon + 2k\varepsilon^2$。

定理 *2.10*（差分隐私的泛化，例如 [*DFH*+15、*BNS*+21]）。设 $\varepsilon \in (0, 1/3)$、$\delta \in (0, \varepsilon/4)$，且 $n \geq \frac{1}{\varepsilon^2} \log \frac{2\varepsilon}{\delta}$。假设 $\mathcal{A}: X^n \to 2^X$ 是一个（ε，δ）-差分隐私算法，它整理一个大小为 n 的数据库，并生成一个函数 $h: X \to \{0, 1\}$。设 $\mathcal{D}$ 是 X 上的一个分布，且S 是从 $\mathcal{D}$中独立同分布抽取的 n 个元素组成的集合。那么

$$\mathop{\mathbf{Pr}}_{S \sim \mathcal{D}, h \leftarrow \mathcal{A}(S)}\left[\left|\frac{1}{|S|}\sum_{x \in S} h(x) - \mathop{\mathbb{E}}_{x \sim \mathcal{D}}\left[h(x)\right]\right| \geq 10\varepsilon\right] < \frac{\delta}{\varepsilon}.$$

3 任意顺序数据流的下界

本节给出专家问题在任意顺序数据流上的空间下界。作为预热，我们首先在 第 3.1 节证明，当最佳专家犯下“少量”错误时，随机化算法的一般空间下界。随后，我们在 第 3.2 节给出主要的下界结果，证明任何能实现遗憾 R 的确定性算法都必须使用 $\Omega\left(\binom{nM}{RT}\right)$ 空间，而最佳专家会犯下 M 个错误。

3.1 预热：准确最佳专家下界

本节将说明，任何能够实现遗憾 R 的随机化算法，即使最佳专家造成 $\left(\binom{n}{RT}\right)$错误，也必须使用 $\Omega\ \Theta(RT)$ 的空间。相比之下，[SWXZ22] 给出了 $\Omega\ \left(\binom{n}{R^2T}\right)$的空间下界：

定理 3.1（内存下界；[SWXZ22]的定理 1）。设 $R > 0, p < \frac{1}{2}$ 为固定常数，即与其他输入参数无关。任何以至少 R 的概率为专家问题实现遗憾 $1-p$ 的算法，都必须至少使用 $\Omega\left(\frac{n}{R^2T}\right)$ 的空间。

此外，即使代价是二元的，且专家预测和正确答案在各天之间均受限为独立同分布（尽管不同专家对应的分布不同），这个下界依然成立。

这个下界的证明利用了一种构造，其中最佳专家会犯 $\Theta(T)$ 个错误。因此，最佳专家犯较少错误时，该问题的空间复杂度如何变化并不明确。事实上，[SWXZ22] 还给出了一种算法，当最佳专家犯 $\widetilde{O}\left(\frac{n}{RT}\right)$ 空间的错误时，该算法使用 $O(RT)$ 空间，从而绕过了上述下界。

现在我们证明，在这种少量错误情形下，该算法是紧的。为此，我们首先定义 ε-DiffDist 问题，它可归约为专家问题。该问题由[SWXZ22] 提出，用于证明随机顺序流中专家问题的内存下界。

定义 3.2 (ε-DiffDist问题)。有 T 个参与者，每人持有 n 比特，索引从1 到 n。我们必须区分两种情况，分别称为"$V=0$"和"$V=1$"。设 μ_0 为参数1 2的伯努利分布，即公平硬币；设 μ_1 为参数为 $\frac{1}{2}+\varepsilon$的伯努利分布。

- *(否定情形，"$V=0$")* 每位玩家的每个索引都独立同分布地由公平硬币产生，即 μ_0。
- *(YES 情形，"$V=1$")* 任意选取一个索引 $L \in [n]$ ——每位玩家的第 L 位比特独立同分布地从 μ_1 中选取。每位玩家的所有其他比特均独立同分布地从 μ_0 中选取。

任何能够以大于 ε-DiffDist问题的常数概率成功求解该问题的协议，其概率必须大于 1 2 至少需要 $\Omega\left(\frac{n}{\varepsilon^2}\right)$ 通信；这一结果由 [SWXZ22]提出：

引理 3.3 (ε-DiffDist的通信复杂度；[SWXZ22]的引理 3)。求解 ε-DiffDist 问题的通信复杂度，对于任意 $1-p$ 概率$p \in [0, 0.5)$，均为 $\Omega\left(\frac{n}{\varepsilon^2}\right)$。

证明定理 3.1由 [SWXZ22] 使用 n 抛硬币，在每位 T 参与者之间生成 n 专家预测，覆盖每个 T 天。在否定情形下，每位专家大约会有 $\frac{T}{2}$ 天预测正确；而在 YES 情形下，有一位专家大约会有 $\frac{T}{2}+\varepsilon T$ 天预测正确，因此遗憾为 $R = O(\varepsilon)$ 的算法将能够区分这两种情形。证明中有一个细微之处：我们使用掩蔽论证，以避免那些碰巧在"幸运"输入上成功的"平凡"算法；不过，就本节的证明而言，并不需要掩蔽论证。由此可知，$\left(\frac{n}{R^2}\right)$ 位参与者之间的总通信量为 $\Omega\, T$，因此任何流式算法都必须使用至少 $\Omega\left(\frac{n}{R^2T}\right)$ 比特的空间。

假设我们改为考虑有 RT 个玩家的 ε-DiffDist 问题，用来表示专家问题中的 RT 天。此外，假设我们在 ε-DiffDist 问题中设置 $\varepsilon = \Theta(1)$，这样在否定情形下，每位专家大约有 $\frac{RT}{2}$ 天预测正确；而在 YES 情形下，某一位专家大约有 $\frac{RT}{2}+C\sqrt{RT}$ 天预测正确，其中 $C > 0$ 为某个常数。再假设我们额外添加 $T - RT$ 天，让所有专家在这些天都做出错误预测，因此总天数为 T，但专家预测正确的次数保持不变。那么，能够实现遗憾 $O(R)$ 的算法将能够区分这两种情形，因此总通信量为 $\Omega\left(\frac{n}{R}\right)$，这意味着任何流式算法都必须至少使用 $\Omega\left(\frac{n}{RT}\right)$ 比特的空间。

推论 3.4. 令 R、 $p < \frac{1}{2}$ 为固定常数，即与其他输入参数无关。对于专家问题，任何以至少 $1-p$ 的概率实现 R 遗憾的算法，即使最佳专家仅犯下 $\Theta(RT)$ 次错误，也必须至少使用 $\Omega\left(\binom{n}{RT}\right)$ 空间。即使代价为二元值，且专家预测和正确答案在各天之间均为独立同分布（尽管不同专家的分布各异），这个下界仍然成立。

证明。 将 $T = RT$ 和 $R = \Theta$代入 定理 3.1的证明中的 (1) 式即可得出该结论。 □

3.2 确定性算法的下界

现在我们证明确定性算法的主要空间下界（定理 1.1）。首先，我们介绍一些基本记号，并引入一个困难分布。

令 T为任意固定的正整数。令 $\mathcal{D}^{(n)}_{\text{NO}}$ 为定义在大小为 $T \times n$ 的矩阵 A 上的分布，其中矩阵的所有元素均为参数为 $1/2$ 的独立同分布伯努利变量，即 A 中的每个元素以概率 $1/2$ 取 0，以概率 $1/2$取 1。令 $\mathcal{D}^{(n)}_{\text{YES}}$ 为定义在大小为$T \times n$ 的矩阵 M 上的分布，其中随机选取一列 $L \in [n]$，该列由参数为$\left(1 - \frac{M}{T}\right)$ 的独立同分布伯努利变量构成，其余各列则由参数为 $1/2$ 的独立同分布伯努利变量构成。令 $\textsc{BiasDetect}_n$ 为判断 A 是从 $\mathcal{D}^{(n)}_{\text{YES}}$ 还是 $\mathcal{D}^{(n)}_{\text{NO}}$中抽取的问题。

设 Π 是一个用于 $\textsc{BiasDetect}_n$ 的通信协议，其正确概率至少为$1 - \exp(-\Theta(T))$。由于 $\mathcal{D}^{(n)}_{\text{NO}}$ 在各列之间服从乘积分布，因此可以将其写为ζ^n，其中 ζ 是单列上的分布，该列的所有条目均为参数为 $1/2$ 的独立同分布伯努利变量。令 $\textsc{BiasDetect}_1$ 表示在单列上区分 $\mathcal{D}^{(1)}_{\text{NO}}$ 和 $\mathcal{D}^{(1)}_{\text{YES}}$ 的问题，即 $n = 1$。将 $\mathcal{D}^{(n)}_{\text{NO}}$ 作为困难分布，我们得到以下直和定理。

引理 3.5 （ $\textsc{BiasDetect}$ 的直和）。 $\textsc{BiasDetect}_n$ 的信息复杂度满足

$$\mathsf{IC}_{\mathcal{D}^{(n)}_{\text{NO}},2^{-\Theta(T)}}(\textsc{BiasDetect}_n) \geq n \cdot \mathsf{IC}_{\mathcal{D}^{(1)}_{\text{NO}},2^{-\Theta(T)}}(\textsc{BiasDetect}_1).$$

证明。根据定义， $\mathcal{D}^{(n)}_{\text{NO}} = \zeta^n$ 是 n 列上的乘积分布。该引理由信息成本的标准直和引理（引理 2.5）得出。 □

利用上述针对 $\textsc{BiasDetect}_n$ 的直和定理，现在只需给出针对 $\textsc{BiasDetect}_1$ 的单坐标信息成本下界。证明推迟到第 3.3 节。

引理 3.6 （单坐标信息成本下界）。 令 $c \in (0,1)$ 和 Π 为任意一个针对 $\textsc{BiasDetect}_1$、错误率为 $\delta = 2^{-\Theta(T)}$ 的协议。我们有， Π 相对于 ζ的信息成本至少为

$$I(\Pi(C_1, C_2, \ldots, C_T); C_1, C_2, \ldots, C_T) \geq \Omega(M), \tag{3.1}$$

其中，比特 $C_i \sim \zeta$ 是独立同分布的单坐标。

结合 引理 3.6 和直和定理（引理 3.5），我们立即得到以下针对 $\textsc{BiasDetect}_n$的信息复杂度下界：

定理 3.7 （n-坐标信息复杂度下界）。设 $c \in (0,1)$。则

$$\mathsf{IC}_{\mathcal{D}^{(n)}_{\text{NO}},2^{-\Theta(T)}}(\textsc{BiasDetect}_n) = \Omega(nM).$$

证明。 这可通过将直和定理（引理 3.5）应用于单坐标界引理 3.6得出。

□

这意味着，任何遗憾为 R 且成功率至少为 $1-2^{-\Theta(T)}$ 的算法，都需要 $\Omega\left(\binom{nM}{RT}\right)$ 内存，其中 M 是最佳专家的错误界。

定理 3.8 (专家学习的内存下界)。 设 R、M 为固定值，且与其他输入参数无关。任何以至少 $1-2^{-\Theta(T)}$ 的概率，在专家问题上实现 R 遗憾的流式算法，都必须使用至少 $\Omega(\binom{nM}{RT})$ 空间，其中 $n=o\left(2^T\right)$，且最佳专家会犯 M 个错误。

证明。 现在我们考虑矩阵规模为 $RT\times n$ 的问题 $\textsc{BiasDetect}_n$。注意，在否定情形下，对于任意固定的列 $i\in[n]$，其中 0 的实例数超过 $\frac{3RT}{5}-\frac{M}{2}$ 的概率（ $M\leq\frac{RT}{8}$）至多为 $2\exp(-c_1RT)$，其中 $c_1\in$ 是一个足够小的常数（0，1）。因此，根据并集界，存在某个索引 $i\in[n]$，其 0 的实例数超过 $\frac{3RT}{4}-\frac{M}{2}$ 的概率至多为 $2n\exp(-c_1RT)$。

同样，在 YES 情形下，对于固定的 $i\in[n]$ 和 $M\leq\frac{RT}{8}$，出现少于 $\frac{4RT}{5}-\frac{M}{2}$ 个 0 的实例的概率至多为 $2\exp(-c_2RT)$，其中 $c_2\in$ 是一个充分小的常数（0,1）。因此，根据并集界，存在一个索引 $i\in[n]$，其 0 的实例数少于 $\frac{3RT}{4}-\frac{M}{2}$ 的概率至多为 $2n\exp(-c_2RT)$。因此，对于 $n=o(2^T)$，存在常数 $c\in$（0,1），使得任何以至少 $1-\exp(-cT)$ 的概率实现总遗憾至多为 $\frac{RT}{5}$ 的算法，都能以 $1-\exp(-\Theta(T))$ 的概率区分 YES 情形和否定情形。

根据 引理 2.6 和 定理 3.7， RT 位参与者之间的总通信量至少为 $\Omega(nM)$。因此，任何以至少 $1-2^{-\Theta(T)}$ 的概率，在专家问题上实现平均 R 遗憾的流式算法，都至少需要 $\Omega(\binom{nM}{RT})$ 空间。

□

3.3 单坐标信息成本下界的证明

现在我们证明引理 3.6中的单坐标下界。

证明引理 3.6。考虑一个正确概率为 $1-2^{-\Theta(T)}$ 的协议，并令 $(C_1,C_2,\ldots,C_T)\sim\zeta^T$表示从否定情形中抽取的一列，其中每个坐标均为参数 $1/2$ 的独立同分布伯努利随机变量。为方便记号，令 $\Pi=\Pi(C_1,\cdots,C_T)$ 表示输入为 $(C_1,C_2,\cdots,C_T)$ 时的通信记录。我们考虑单向消息传递模型，其中每个玩家 P_i 持有输入 C_i。对于所有 $i<T$，令 M_i 表示从玩家 P_i 发送给玩家 P_{i+1}的消息。

根据互信息链式法则，我们需要界定的通信记录的信息成本，即公式 3.1左侧，可以写为

$$I(\Pi;C_1,C_2,\ldots,C_T)=\sum_{j=1}^{T}I\left(M_j;C_1,C_2,\ldots,C_T\mid M_{<j}\right). \tag{3.2}$$

根据单向通信的独立性，我们有

$$I\left(M_j;C_1,C_2,\ldots,C_T\mid M_{<j}\right)=I\left(M_j;C_j\mid M_{<j}\right). \tag{3.3}$$

结合上述两个等式，信息成本等于

$$I(\Pi; C_1, C_2, \ldots, C_T) = \sum_{j=1}^{T} I\left(M_j; C_j \mid M_{<j}\right). \tag{3.4}$$

现在我们给出右侧的下界。首先，作如下定义。对于任意 $i \in [T]$，如果存在常数 $i \in [T]$，使得针对输入 C和通信记录 $\Pi = (M_1, \ldots, M_T)$，$(M_i, M_{<i})$ 对 i 而言是**信息丰富的**，则称其为信息丰富的；

$$\left|\Pr(C_i = 0 \mid M_i, M_{<i}) - \Pr(C_i = 1 \mid M_i, M_{<i})\right| \geq c \tag{3.5}$$

否则称其为信息贫乏的。直观而言，相对于 $(M_i, M_{<i})$，索引 i 是信息丰富的，意味着在给定过往消息 $M_{<i}$ 的条件下，消息 M_i 揭示了关于 C_i 的大量信息。因此，在这种情况下，$I(M_i, C_i \mid M_{<i})$ 会很大。现在，对于所有 $i \in [T]$，令 p_i 表示 $(M_i, M_{<i})$ 对 i 而言是信息丰富的概率（相对于 C 和 Π）。

从概念上说，我们需要证明 $\sum_i p_i$ 很大，因为这样一来，信息丰富的消息就足够多，因此 公式 3.4 左侧的信息成本就很高。我们在下面的引理中将这一想法形式化。

引理 3.9。 *在上述设定中，$c > 0$ 为常数时，信息成本可以下界为*

$$I(\Pi; C_1, C_2, \ldots, C_T) = \sum_{j=1}^{T} I\left(M_j; C_j \mid M_{<j}\right) \geq \Omega\left(\sum_{j=1}^{T} p_j\right) \tag{3.6}$$

证明。 我们先展开互信息各项的定义。对于每个 $j \in T$，有

$$I\left(M_j; C_j \mid M_{<j}\right) = H\left(C_j \mid M_{<j}\right) - H\left(C_j \mid M_j, M_{<j}\right) \tag{3.7}$$

对于第一项，注意到 C_j 和 $M_{<j}$ 在单向通信中相互独立。此外，根据定义，C_j 服从参数为 $1/2$ 的伯努利分布。因此，

$$H(C_j \mid M_{<j}) = H(C_j) = H(1/2) = 1.$$

对于第二项，

- 要么 $(M_j, M_{<j})$ 是信息丰富的，这种情况以概率 p_j 发生；此时，条件熵上界为 $H\left(C_j \mid M_j, M_{<j}\right) \leq H(1/2 + c/2)$;
- 要么 $(M_j, M_{<j})$ 是非信息丰富的；此时，我们可以平凡地将条件熵上界为 $H\left(C_j \mid M_j, M_{<j}\right) \leq 1$;

综合这些观测结果并利用公式 3.7，可得

$$\begin{aligned}
I\left(M_j; C_j \mid M_{<j}\right) &= H\left(C_j \mid M_{<j}\right) - H\left(C_j \mid M_j, M_{<j}\right) \\
&\geq 1 - \left(p_j \cdot H(1/2 + c/2) + (1 - p_j) \cdot 1\right) \\
&= p_j - p_j \cdot H(1/2 + c/2) \\
&\geq p_j \left(1 - \sqrt{1 - c^2}\right) \\
&\geq c^2 \cdot \Omega(p_j),
\end{aligned}$$

其中，倒数第二步使用了引理 2.1 的上界，最后一步是因为$1-\sqrt{1-x^2} \geq x^2/5$对于 $x \in [0,1]$成立。对 $j = 1$、2、……、T在方程 3.6 中求和即可完成证明。

□

为证明所声称的信息成本不等式 公式 3.1，我们证明 $\sum_i p_i = \Omega(M)$。

引理 3.10。 存在一个常数 $\gamma > 0$，使得

$$\sum_{j=1}^{T} p_j > \gamma \cdot M.$$

证明。 反设 $\sum_{j=1}^{T} p_j = o(M)$。令 A 为一个协议，该协议在随机输入 $C \in \{0,1\}^T \sim \zeta^T$上发送（可能是随机的）消息 M_1、……、M_T，其中 $C \in \{0,1\}^T \sim \zeta^T$从 NO 分布中均匀抽取，即 $C := C_1$、……、C_T的每个坐标以1_2 的概率取 0，以1_2的概率取 1。此外，假设 A 是一个能够以至少 $1 - \frac{e^{-cT}2^{-T}}{8}$的概率区分 YES 实例和 NO 实例的协议，其中 $c > 0$为某个常数。

由于 p_i 是 M_i 具有信息性的概率，根据假设，消息 M_1、……、M_T中的信息性指标 i的期望数量为 $f(M)$，其中 $f(M) = o(M)$。因此，根据马尔可夫不等式，信息性指标数量至多为 $10f(M) = o(M)$ 的概率至少为9_{10}。令 S为非信息性指标的集合，使得 $|S| = T - 10f(M) = T - o(M)$。令 C'为一个输入：它在信息性指标 $[T] \setminus S$上与 C一致，并在非信息性指标 S上任意选取，从而对于 $i \in [T] \setminus S$，$C'_i = C_i$。

根据定义，每个无信息索引只会将输出的分布改变一个 $(1 \pm c)$ 因子。特别地，对于 $c \in (0, 1/2)$，协议 A 在输入 C' 上生成 Π 的概率至少是协议 A在输入 C上生成 Π的概率的 $(1-c)^T \geq e^{-2cT}$ 倍。然而，由于 C在 S上可能不同于 C'，因此 C在 $(|S| = T - 10f)$ 个（M）$= T - o$（M）索引上可能不同于 C'。

现在，由于 C 的每个坐标以 1_2 的概率取 0、以 1_2的概率取 1，因此当 T足够大时，C 包含超过 $T - M$ 个零的概率至少为 $1 - T^M \cdot \frac{1}{2^T} \geq 1 - 2^{T/2}$。但这样一来，就存在一个包含少于 $\frac{M}{2}$ 个零的 C' 的取值，使得 A 也以至少 $\frac{e^{-cT}}{2}$ 的概率输出 Π。由于 C' 包含少于 $\frac{M}{2}$ 个零，因此 C' 更有可能由 YES 实例生成；事实上，YES 实例将以 2^{-T}的概率生成 C。另一方面，由于 Π 对应于一个使 A 输出 NO 的通信记录，因此 A 在 C' 上的错误概率至少为 $\frac{e^{-cT}}{4}$，这与 A 以 $1 - \frac{e^{-cT}2^{-T}}{8}$的概率成功这一断言相矛盾。因此可得 $\sum_{j=1}^{T} p_j = \Omega(M)$，正如所需。

□

现在我们结合引理 3.9和引理 3.10。这意味着信息成本的下界为

$$I(\Pi; C_1, C_2, \ldots, C_T) \geq \Omega\left(\sum_{j=1}^{T} p_j\right) \geq \gamma M, \tag{3.8}$$

其中 $\gamma > 0$ 为常数。证明至此完成。 □

4 对抗自适应对手的算法

在本节中，我们证明存在能够应对自适应输出的离散专家预测问题算法。

4.1 一种近乎最优的确定性算法

我们首先介绍一种 适用于无适应性输入的任意顺序数据流的简单确定性算法 s.

算法 1 用于专家问题的确定性算法

输入： 一个长度为 T、包含 n 个专家的数据流，最佳专家所犯错误数的上界为 M，
目标遗憾为 R

输出： 一系列预测及其遗憾 R

$k \leftarrow O\left(\frac{nM}{RT}\log\ n\right)$
$S \leftarrow \emptyset$
当 数据流持续时**执行**
  如果 S 为空 **那么** ▷我们已经将所有 n 专家都循环遍历了一遍
    $S \leftarrow [n]$
  令 P 为 S的前 k 个索引
  $S \leftarrow S \setminus P$
  当 $P \neq \emptyset$ **时执行**
    对于之后的每一天，选择 P 中多数专家输出的结果
    删除当天判断错误的专家

现在，我们证明算法 1的正确性和空间复杂度。

定理 4.1。 在长度为 T 的数据流中，设有 n 位专家，且最佳专家犯下 M 个错误。则存在一种使用 $\widetilde{O}\left(\frac{nM}{RT}\right)$ 空间并实现 R 遗憾的确定性算法。

证明。 首先注意，对于每个大小为 k 的专家池，该算法在其生命周期内至多犯下 $\log k \leq \log n$ 个错误：$= \frac{2nM}{RT}\log n$，因为每当算法犯下一个错误时，池中至少有一半的专家必定判断错误并被删除，因此每次错误都会使池的大小至少减少一半。

由于每个池 P 的大小为 k，且共有 n 个专家，因此在整个集合 S（初始化为 n）耗尽之前，最多有 $\frac{2n}{k}$ 个池。因此，遍历整个专家集合最多需要经过 $\frac{2n}{k}$ 个池。此外，算法每次遍历完整个专家集合时，每位专家都至少犯过一次错误。这是因为只有当专家犯错时，才会将其从池 P 中删除；而既然所有专家都已从P中删除，那么所有专家都至少犯过一次错误。

由于最佳专家至多犯 M 次错误，因此最佳专家最多会从池 P 中被删除 M 次。换句话说，算法最多可以遍历整个 n个专家的集合 M 次。

因此，算法犯错的总次数至多为

$$\frac{2n}{k} \cdot \log n \cdot M \leq \frac{2nRT}{2nM \log n} \cdot \log n \cdot M = RT,$$

因此，算法实现的遗憾至多为 R。由于算法选择的专家子集大小为 $k = \frac{2nM}{RT}\log n$，空间复杂度由此可得。 □

鉴于定理 3.8，显然定理 4.1 对于确定性算法而言几乎是最优的，误差仅在多对数因子范围内；而确定性算法天然具有对抗鲁棒性。另一方面，似乎并非所有对抗鲁棒算法都必须是确定性的。事实上，下面我们给出一种随机化对抗鲁棒算法，它具有更好的空间保证。

4.2 随机鲁棒流式算法

我们先回顾一种适用于无适应性输入（即非自适应输入）的任意顺序数据流的随机化算法：

引理 4.2（无适应性输入算法；[SWXZ22]）。令 $R > \frac{16}{\log_T^2 n}$，并假设最佳专家至多犯 $M \le \frac{\delta T}{128 \log^2 n}$ 个错误。那么，对于离散专家预测问题，存在一个算法 DiscPred，使用 $\widetilde{O}\left(\frac{n}{RT}\right)$ 空间，且遗憾至多为 R，其发生概率至少为 $1 - \frac{1}{\mathrm{poly}(n,\ T)}$。

引理 4.2 中的算法通过对 $k = \widetilde{O}\left(\frac{n}{RT}\right)$ 名专家池进行采样并在池中进行多数投票，同时不断删除表现不佳的专家，直到池中不再有专家；此时随机采样一个新的 k 名专家池。其主要直觉是：要么专家池表现良好并实现较低的遗憾，要么专家池会不断被重新采样，直到最佳专家被多次采样；此后，该专家便不会再从池中被删除。遗憾的是，这种算法是否能抵御自适应输入并不明显，因为对手可能获知每个采样专家池中的专家，并迫使这些专家只在算法对其进行采样的天里犯错。

相反，我们利用差分隐私来隐藏算法的内部随机性，尤其是每个池所抽取专家的身份。我们首先运行 $\widetilde{O}(\sqrt{T}$ 个算法副本，然后输出 $\widetilde{O}(\sqrt{T}$ 个副本的私有中位数，从而保证大约 $\left(\frac{1}{\widetilde{O}(\sqrt{T})}, 0\right)$-差分隐私，因为我们使用了 $\widetilde{O}(\sqrt{T}$ 个算法副本。高级组合，即 定理 2.9，进而保证 $\left(O(1), \frac{1}{\mathrm{poly}(n)}\right)$-差分隐私，因此正确性可由差分隐私的泛化性质推出，即 定理 2.10。我们的完整算法见算法 2。

算法 2 用于专家问题的随机化鲁棒流式算法**输入：** 长度为 T 的数据流，其中有 n 位专家，目标遗憾为 R**输出：** 一系列遗憾为 R 的预测1: 运行 $m = O\left(\sqrt{T}\log(nT)\right)$ 个 DiscPred 的独立实例，遗憾为 $\frac{R}{4}$ 2: 在这 m 个实例上运行 PrivMed，隐私参数为 $\varepsilon = O\left(\frac{1}{\sqrt{T}\log(nT)}\right)$，失败概率为 $\delta = \frac{1}{\mathrm{poly}(n,T)}$3: 在每个时刻 $t \in [T]$，选择 PrivMed 的输出

现在我们证明，我们的算法在自适应输入上的正确性。

定理 4.3 (自适应输入算法**)**。令 $R > \frac{64}{\log_T^2 n}$，并假设最佳专家至多犯 $M \le \frac{R^2 T}{128 \log^2 n}$ 个错误。那么，对于离散专家预测问题，存在一种算法，使用 $\widetilde{O}\left(\frac{n}{R\sqrt{T}}\right)$ 空间，且以至少 $1 - \frac{1}{\mathrm{poly}(n,T)}$ 的概率实现至多为 R 的遗憾。

证明。假设我们运行 $m = O\left(\sqrt{T}\log(nT)\right)$ 个 DiscPred 的独立实例，其遗憾为 $\frac{R}{4}$。注意，对于 $R > \frac{64}{\log_T^2 n}$，有 $\frac{R}{4} > \frac{16}{\log_T^2 n}$，这是 DiscPred 在 引理 4.2中的有效输入。

根据 引理 4.2，每个实例在任意顺序数据流上成功的概率至少为$1 - \frac{1}{\mathrm{poly}(n,T)}$。通过对 m 个实例应用并集界，所有实例均成功的概率至少为$1 - \frac{1}{\mathrm{poly}(n,T)}$。特别地，每个实例的遗憾至多为 $\frac{R}{4}$，因此每个实例的错误总数至多为 $M + \frac{RT}{4}$。由此，所有实例的错误总数至多为 $m\left(M + \frac{RT}{4}\right)$。

考虑自适应数据流时，注意到 PrivMed 在隐私参数为$O\left(\frac{1}{\sqrt{T\log(nT)}}\right)$、失败概率为$\frac{1}{\mathrm{poly}(n,T)}$的情况下被调用。根据定理 2.9，该机制允许进行 T次自适应交互，并以失败概率$\frac{1}{\mathrm{poly}(n,T)}$保证隐私 $O(1)$。根据定理 2.10，以高概率可知，如果算法的输出不正确，那么至少有 $\frac{m}{3}$ 个实例 DiscPred 也不正确。由于所有实例的错误总数至多为$m\left(M + \frac{RT}{4}\right)$，因此算法的错误总数至多为 $3\left(M + \frac{RT}{4}\right) \le M + RT$，因为 $M \le \frac{R^2 T}{128\log^2 n}$。因此，该算法以高概率实现 R 遗憾。

根据 引理 4.2， DiscPred 的每个实例使用 $\widetilde{O}\left(\frac{n}{RT}\right)$ 空间。由于我们使用了 $m = O\left(\sqrt{T}\log(nT)\right)$个相互独立的 DiscPred实例，因此总空间为 $\widetilde{O}\left(\frac{n}{R\sqrt{T}}\right)$。□

致谢

感谢 Binghui Peng 提供了有益的讨论。David P. Woodruff 和 Samson Zhou 获得了 Simons Investigator Award 的资助，以及美国国家科学基金会 CCF-1815840 号拨款的资助。Fred Zhang 获得了美国海军研究办公室 N00014-18-1-2562 号拨款的资助。

参考文献

[ABJ+22] Mikl´os Ajtai、Vladimir Braverman、T.S. Jayram、Sandeep Silwal、Alec Sun、David P. Woodruff 和 Samson Zhou。白盒对抗数据流模型。载于第 41 届 ACM SIGMOD-SIGACT-SIGAI 数据库系统原理研讨会论文集（PODS），2022。1.2[ACFS02] Peter Auer、Nicol`o Cesa-Bianchi、Yoav Freund 和 Robert E. Schapire。非随机多臂老虎机问题。《SIAM 计算杂志》，32(1):48–77，2002。1.2[ACGS22] Sepehr Assadi、Amit Chakrabarti、Prantar Ghosh 和 Manuel Stoeckl。通过确定性算法和对抗鲁棒算法实现图流着色。CoRR，abs/2212.10641，2022。1.2[ACSS23] Idan Attias、Edith Cohen、Moshe Shechner 和 Uri Stemmer。通过差分隐私和差分估计器实现对抗流式处理的框架。载于第 14 届理论计算机科学创新会议（ITCS），第 8:1–8:19 页，2023。1.1，1.2，1.2[AK04] Baruch Awerbuch 和 Robert D. Kleinberg。具有端到端反馈的自适应路由：分布式学习与几何方法。载于第 36 届 ACM 年度计算理论研讨会论文集（STOC），2004。1.2

[AMM19] Raman Arora、Teodor Vanislavov Marinov 和 Mehryar Mohri。带有反馈图和切换成本的多臂老虎机。载于神经信息处理系统进展（NeurIPS），2019。1.2[AMYZ19] Dmitrii Avdiukhin、Slobodan Mitrovic、Grigory Yaroslavtsev 和 Samson Zhou。在背包约束下进行对抗鲁棒的子模最大化。载于第 25 届 ACM SIGKDD知识发现与数据挖掘国际会议论文集，KDD，第 148–156 页，2019。1.2[BE98] Allan Borodin 和 Ran El-Yaniv。在线计算与竞争分析。剑桥大学出版社，1998年。1.2[BEO22] Omri Ben-Eliezer、Talya Eden 和 Krzysztof Onak。通过稠密-稀疏权衡实现对抗鲁棒的流式处理。载于第 5 届算法简洁性研讨会（SOSA@SODA），2022。1.2[BGM+16] Mark Braverman、Ankit Garg、Tengyu Ma、Huy L Nguyen 和 David P Woodruff。通过分布式数据处理不等式研究统计估计问题的通信下界。载于第四十八届 ACM 计算理论研讨会论文集（STOC），2016。1.1[BHM+21] Vladimir Braverman、Avinatan Hassidim、Yossi Matias、Mariano Schain、Sandeep Silwal 和 Samson Zhou。通过重要性抽样实现流式算法的对抗鲁棒性。载于神经信息处理系统进展（NeurIPS），2021年。1.2[BJKS04] Ziv Bar-Yossef、T. S. Jayram、Ravi Kumar 和 D. Sivakumar。数据流与通信复杂度的信息统计方法。《计算机与系统科学杂志》，68(4):702–732，2004。1.1，2.5，2.6[BJWY21] Omri Ben-Eliezer、Rajesh Jayaram、David P. Woodruff 和 Eylon Yogev。对抗鲁棒流式算法的框架。《SIGMOD Rec.》，50(1):6–13，2021年。1.2[BKM+22] Amos Beimel、Haim Kaplan、Yishay Mansour、Kobbi Nissim、Thatchaphol Saranurak 和 Uri Stemmer。针对自适应对手的动态算法：通用构造与下界。载于第 54 届 ACM SIGACT 计算理论研讨会（STOC），2022。1.1，1.2，1.2[BNS+21] Raef Bassily、Kobbi Nissim、Adam D. Smith、Thomas Steinke、Uri Stemmer 和 Jonathan R. Ullman。自适应数据分析的算法稳定性。《SIAM 计算杂志》，50(3)，2021年。2.10[CBL06] Nicol`o Cesa-Bianchi 和 G´abor Lugosi。预测、学习与博弈。剑桥大学出版社，2006年。1.2，1.2[CDS13] Nicol`o Cesa-Bianchi、Ofer Dekel 和 Ohad Shamir。具有切换成本及其他自适应对手的在线学习。载于神经信息处理系统进展（NIPS），2013。1.2[CGS22] Amit Chakrabarti、Prantar Ghosh 和 Manuel Stoeckl。图流的对抗鲁棒着色。载于第 13 届理论计算机科学创新会议（ITCS），2022。1.2

[CLN+22] Edith Cohen、Xin Lyu、Jelani Nelson、Tam´as Sarl´os、Moshe Shechner 和 Uri Stemmer。关于 CountSketch 对自适应输入的鲁棒性。在国际机器学习会议（ICML）上，第4112–4140页，2022年。1.2[CN20] Yeshwanth Cherapanamjeri 和 Jelani Nelson。关于自适应距离估计。在神经信息处理系统进展33：神经信息处理系统年度会议（NeurIPS）上，2020年。1.2[CN22] Yeshwanth Cherapanamjeri 和 Jelani Nelson。随机哈达玛变换的一致近似及其应用。在 STOC '22：第54届 ACM SIGACT 计算理论研讨会上，第659–671页，2022年。1.2[CO96] Thomas M. Cover 和 Erik Ordentlich。带侧信息的通用投资组合。《IEEE信息论汇刊》42(2):348–363，1996年。1.2[Cov91] Thomas M Cover。通用投资组合。《数学金融》1(1):1–29，1991年。1.2[CSW+23] Yeshwanth Cherapanamjeri、Sandeep Silwal、David P. Woodruff、Fred Zhang、Qiuyi Zhang 和 Samson Zhou。来自有界对手的自适应输入上的鲁棒算法。在第11届国际学习表征会议（ICLR）会议论文集，2023年。1.2[DDKP14] Ofer Dekel、Jian Ding、Tomer Koren 和 Yuval Peres。带切换成本的多臂老虎机：T 2/3 遗憾。在 ACM 计算理论年度研讨会（STOC）上，2014年。1.2[DFH+15] Cynthia Dwork、Vitaly Feldman、Moritz Hardt、Toniann Pitassi、Omer Reingold 和 Aaron Leon Roth。在自适应数据分析中保持统计有效性。在第47届 ACM 计算理论研讨会（STOC）论文集，2015年。2.10[dFM06] Daniela Pucci de Farias 和 Nimrod Megiddo。在反应式环境中结合专家建议。《J. ACM》53(5):762–799，2006年。1.2[DMNS06] Cynthia Dwork、Frank McSherry、Kobbi Nissim 和 Adam D. Smith。在隐私数据分析中根据敏感度校准噪声。在第三届密码学理论会议（TCC）上，2006年。2.7[DRV10] Cynthia Dwork、Guy N. Rothblum 和 Salil P. Vadhan。提升与差分隐私。在第51届 IEEE计算机科学基础研讨会（FOCS）上，2010年。2.9[DSWZ23] Itai Dinur、Uri Stemmer、David P. Woodruff 和 Samson Zhou。关于有界空间下的差分隐私与自适应数据分析。CoRR，abs/2302.05707，2023年。1.2[DTA12] Ofer Dekel、Ambuj Tewari 和 Raman Arora。对抗自适应对手的在线多臂赌博机学习：从遗憾到策略遗憾。在第29届国际机器学习会议（ICML）论文集，2012年。1.2[FS97] Yoav Freund 和 Robert E Schapire。在线学习的决策理论推广及其在提升中的应用。《计算机与系统科学杂志》55(1):119–139，1997年。1.2

[GPS17] Nick Gravin、Yuval Peres 和 Balasubramanian Sivan。乘法权重算法族的紧下界。在第44届国际自动机、语言与编程研讨会（ICALP）上，2017年。1, 1[Her22] Daniel A Herrmann。将专家建议预测应用于专家建议预测问题。《Synthese》200(4):1–24，2022年。1.2[HKM+20] Avinatan Hassidim、Haim Kaplan、Yishay Mansour、Yossi Matias 和 Uri Stemmer。通过差分隐私实现对抗鲁棒流式算法。在神经信息处理系统进展（NeurIPS）上，2020年。1.1, 1.2, 1.2, 2.8[HKW95] David Haussler、Jyrki Kivinen 和 Manfred K Warmuth。专家建议预测的紧最坏情况损失界。在欧洲计算学习理论会议（EuroCOLT）上，1995年。1.2[HS97] David P Helmbold 和 Robert E Schapire。预测效果几乎与决策树的最佳剪枝相当。《机器学习》27(1):51–68，1997年。1.2[Kle04] Robert D. Kleinberg。连续臂赌博机问题的近乎紧界。在神经信息处理进展（NIPS）上，2004年。1.2[KPW21] Akshay Kamath、Eric Price 和 David P Woodruff。带应用的新集合不相交性问题的简单证明。在第36届计算复杂性会议（CCC）上，2021年。1.1, A.4, A.5[KSS22] Aryeh Kontorovich、Menachem Sadigurschi 和 Uri Stemmer。带相关观测的自适应数据分析。在国际机器学习会议（ICML）上，第11483–11498页，2022年。1.2[KV05] Adam Tauman Kalai 和 Santosh S. Vempala。在线决策问题的高效算法。《计算机与系统科学杂志》71(3):291–307，2005年。1, 1.2[LW94] Nick Littlestone 和 Manfred K. Warmuth。加权多数算法。《信息与计算》108(2):212–261，1994年。1, 1, 1.2[MB04] H. Brendan McMahan 和 Avrim Blum。自适应对手下赌博机设定中的在线几何优化。在第17届学习理论年度会议（COLT）上，2004年。1.2[MOSW02] Neri Merhav、Erik Ordentlich、Gadiel Seroussi 和 Marcelo J. Weinberger。关于带记忆损失函数的序贯策略。《IEEE信息论汇刊》48(7):1947–1958，2002年。1.2[MW98] Wolfgang Maass 和 Manfred K Warmuth。利用虚拟阈值门进行高效学习。《信息与计算》141(1):66–83，1998年。1.2[PR23] Binghui Peng 和 Aviad Rubinstein。在线学习中近乎最优的记忆-遗憾权衡，2023年。1.2[PZ23] Binghui Peng 和 Fred Zhang。次线性空间中的在线预测。在 ACM-SIAM离散算法研讨会（SODA）上，2023年。1, 1, 1.2, 1.2

[RSC21] Chlo´e Rouyer、Yevgeny Seldin 和 Nicol`o Cesa-Bianchi。《一种适用于具有切换成本的随机与对抗多臂老虎机的算法》。载于第38届国际机器学习会议（ICML）论文集，2021年。1.2[SWXZ22] Vaidehi Srinivas、David P. Woodruff、Ziyu Xu 和 Samson Zhou。《专家问题的内存界》。载于第54届 ACM SIGACT 计算理论研讨会（STOC）论文集，2022年。1、1、1.1、1.1、1.1、1.2、3.1、3.1、3.1、3.3、3.1、4.2[TMV01] Eiji Takimoto、Akira Maruoka 和 Vladimir Vovk。《通过动态规划方案，预测效果几乎与决策树的最佳剪枝相当》。《理论计算机科学》，261(1):179–209，2001年。1.2[Vov90] Vladimir Vovk。《策略聚合》。载于第三届计算学习理论年度研讨会（COLT）论文集，1990年。1.2[Vov98] Vladimir Vovk。《专家建议预测博弈》。《计算机与系统科学杂志》，56(2):153–173，1998年。1.2[Vov99] Vladimir Vovk。《随机预测策略去随机化》。《机器学习》，35(3):247–282，1999年。1.2[Vov05] Vladimir Vovk。《基于专家建议的防御性预测》。载于第16届算法学习理论国际会议（ALT），2005年。1.2[Waj20] David Wajc。《针对自适应对手对动态匹配进行舍入》。载于第52届 ACM SIGACT 计算理论研讨会（STOC）论文集，2020年。1.2[Wik22] 维基百科贡献者。《二元熵函数——维基百科，自由的百科全书》。https://en.wikipedia.org/w/index.php?title=Binary_entropy_function& oldid=1071507954，2022年。 [在线；访问日期：3-August-2022]。2.1[WZ21] David P. Woodruff 和 Samson Zhou。《通过差分估计器获得对抗鲁棒数据流和滑动窗口的紧确界》。载于第62届 IEEE计算机科学基础年会（FOCS），2021年。1.2

A 大量错误情形下的另一种证明

当 $M = \Omega(T)$ 时，我们给出信息成本的另一种分析，其中 M 是最佳专家犯下的错误数。

引理 A.1 (单坐标信息成本下界)。 设 $c \in (0,1)$，且 Π 是任意一个关于 $\textsc{BiasDetect}_1$、错误率为 $\delta = 2^{-T}$ 的协议。假设对于某个常数 c'，最佳专家犯了 $M = c'T$ 个错误。则 Π 关于 ζ 的信息成本至少为

$$I(\Pi(C_1, \cdots, C_T); C_1, \cdots, C_T) \geq \Omega\left((1-c)^2 T\right), \tag{A.1}$$

其中 $C_i \sim \zeta$ 是独立同分布的单坐标。

应用直和定理（引理 3.5），可得以下关于 $\textsc{BiasDetect}_n$ 的信息复杂度下界：

定理 A.2 （n-坐标信息复杂度下界）。 设 $c \in (0,1)$ 并假设$M = c'T$，其中常数为 c'。则

$$\mathsf{IC}_{\mathcal{D}^{(1)}, 2^{-\Theta(T)}}(\textsc{BiasDetect}_n) = \Omega\left((1-c)^2 nT\right).$$

通过类似于 定理 3.8 的论证，可得：

定理 A.3 (专家学习的内存下界)。 设 $M = c'T$ 为某个常数。任何以至少$1 - 2^{-\Theta(T)}$ 的概率在专家问题中达到常数遗憾的流式算法，都必须使用至少$\Omega(n)$ 空间，其中最佳专家犯 M 个错误。

为了证明引理 A.1，我们需要一些技术性引理。

引理 A.4 ([KPW21]的引理 3.5)。 考虑任意通信协议 Π，其中每位参与者接收一位，并且条件是输入固定为 $b \in \{0,1\}^T$。每位参与者 i 都可以这样实现：如果其他参与者收到输入 b_{-i}，参与者 i 仅以$d_{TV}(\Pi_b, \Pi_{b \oplus e_i})$的概率观察到自己的输入。

引理 A.5 ([KPW21]的引理 3.6)。 设 $c \in (0, 1)$、 $p \in (0, \frac{1-c}{2})$ 以及 $\gamma_c = c^{\frac{1}{\log(c/e)}}$。对于一组二元随机变量 $Y_1, Y_2, \cdots, Y_k$，满足 $\mathbb{E}\left[\sum_i Y_i\right] = pk$，存在一个大小为 ck的集合 $S \subset [n]$，使得$\Pr(Y_j = 0, \forall j \in S) > e^{-k/\gamma_c - 1}$。

证明引理 A.1。令$C_1, C_2, \cdots, C_n) \sim \zeta^n$ 为从否定情形中抽取的单个列，其中每个坐标均为参数为 $1/2$的独立同分布伯努利随机变量。令 $M = c'T$，其中 c'为某个常数。我们考虑单向消息传递模型，其中对所有 $i < T$， M_i 表示从玩家 P_i 发送给玩家 P_{i+1}的消息。只需给出下界

$$I(\Pi; C_1, \cdots, C_T) = \sum_{j=1}^{T} I(\Pi; C_j | C_{<j}).$$

根据互信息链式法则。我们声称，对于任意 j

$$I(\Pi; C_j | C_{<j}) = I(\Pi; C_j | C_{-j}).$$

首先，根据数据处理以及该协议的单向性质

$$I(\Pi; C_j | C_{<j}) = I(M_{\le j}; C_j | C_{<j}).$$

对于任意 j。现在我们只需证明

$$I(M_{\le j}; C_j | C_{<j}) = I(\Pi; C_j | C_{-j}).$$

根据互信息链式法则，我们可以将右侧写为

$$\begin{aligned} I(\Pi; C_j | C_{-j}) &= I(M_{\le j}; C_j | C_{-j}) + I(M_{>j}; C_j | M_{\le j}, C_{-j}) \\ &= I(M_{\le j}; C_j | C_{-j}) + I(M_{>j}; C_j | M_{\le j}, C_{>j}) \end{aligned}$$

注意，在给定 $M_{\le j}$ 和 $C_{>j}$ 的条件下， $M_{>j}$ 和 C_j 相互独立。因此，

$$I(M_{>j}; C_j | M_{\le j}, C_{>j}) = 0$$

这就证明了该结论。

令 Π_b 表示输入固定为 $b \in \{0,1\}^n$ 时协议转录的分布，并令 $\oplus$ 表示二进制异或。现在我们可以界定

$$\begin{aligned} I(\Pi; C_1, \cdots, C_T) &= \sum_{j=1}^{T} I(\Pi; C_j | C_{<j}) \\ &= \sum_{j=1}^{T} I(\Pi; C_j | C_{-j}) \\ &\ge \frac{1}{8}\frac{1}{2^T} \sum_{b \in \{0,1\}^T} \sum_{j=1}^{T} d_{\mathrm{TV}}^2(\Pi_{b \oplus e_j}, \Pi_b) \\ &\ge \frac{1}{8}\frac{1}{2^T} \sum_{b \in \{0,1\}^T} \sum_{j: b_j = 0} d_{\mathrm{TV}}^2(\Pi_{b \oplus e_j}, \Pi_b). \end{aligned} \tag{A.2}$$

在给定输入 $b \in \{0,1\}^T$ 的条件下，令 $k = |\{i : \ b_i = 0\}|$，并反设

$$\sum_{i: b_i = 0} d_{\mathrm{TV}}(\Pi_{b \oplus e_i}, \Pi_b) = kp, \tag{A.3}$$

其中 $p < \frac{1-c}{2}$。令 $p_i = d_{\mathrm{TV}}(\Pi_{b \oplus e_i}, \Pi_b)$，对每个玩家 $i \in [T]$ 均成立。引理 A.4 意味着，该协议可以等价地实现为：如果其他玩家收到 b_{-i}，玩家 i 仅以概率 p_i查看其输入。若玩家 i 不查看自己的比特，则其消息M_i 与自己的输入比特相互独立。令 Y_i 表示玩家 i 在这一等价协议中查看其输入这一事件的指示随机变量。

由我们的假设（A.3）可知，如果输入为 b，那么 $\mathbb{E}\left[\sum_{i: \ b_i = 0} Y_i\right] = \sum_i p_i = kp$。根据 Y_i 的定义，如果对于任意集合 S， $Y_i = 0$ 对所有 $i \in S$ 都成立，那么 S 中的所有参与者都不会查看自己的输入比特。令 E_S 表示事件：对于所有 $i \in S$，存在某个 $S \subseteq \{i$ ，使得 $Y_i = 0 : \ b_i = 0\}$。由于 S 中的参与者不会查看自己的输入比特，

$$d_{\mathrm{TV}}(\Pi_{b \oplus e_S} | E_S, \Pi_b | E_S) = 0.$$

特别地，利用这一点和全概率公式，我们得到

$$d_{\mathrm{TV}}(\Pi_{b\oplus e_S},\Pi_b) = \Pr(E_S)\cdot d_{\mathrm{TV}}(\Pi_{b\oplus e_S}|E_S,\Pi_b|E_S) + \Pr(\overline{E_S})\cdot d_{\mathrm{TV}}(\Pi_{b\oplus e_S}|\overline{E}_S,\Pi_b|\overline{E}_S)$$
$$\leq \Pr(\overline{E_S}). \tag{A.4}$$

根据我们的假设，$\mathbb{E}\left[\sum_{i:b_i=0} Y_i\right] = kp$ 对于 $p < \frac{1-c}{2}$。应用引理 A.5，我们得到存在一个集合 $S \subseteq \{i:\ b_i = 0\}$，满足 $|S| = ck$，使得 $\Pr(\overline{E_S}) \geq e^{-k/\gamma_c - 1}$。对于任意 $k < (T-2)\gamma_c < T-2$，我们有 $\Pr(E_S) > e\delta$，因此 $\Pr(E_S) < 1 - e\delta$。由等式 (A.4)，$d_{\mathrm{TV}}(\Pi_{b\oplus e_S},\Pi_b) < 1 - e\delta$。注意，$b \oplus e_S$ 比 b 多出 $|S| = ck$ 个 1；而它们在其他所有坐标上的取值都相同。回想一下，在典型的单坐标 YES 实例中，1 的数量为 $T - M$，比典型的 NO 实例多 $T/2 - M$。现在假设这个差距为 $T/2 - M < ck$；那么求解 $\textsc{BiasDetect}_1$ 的难度至多与区分 b 和 $b \oplus e_S$ 一样。因此，如果我们选择 c' 使得 $M = c'T > T/2 - ck$，那么协议 Π 的失败概率将大于 δ。这就产生了矛盾。

因此，对于任意满足 $ck = c\cdot|\{i \text{ 的 } b:\ b_i = 0\}| > T/2 - M$，

$$\sum_{i:b_i=0} d_{\mathrm{TV}}(\Pi_{b\oplus e_i},\Pi_b) \geq \Omega\left(\frac{(1-c)T}{2}\right).$$

由（A.2）和詹森不等式，

$$I(\Pi; C_1, \cdots, C_T) \geq \Omega\left((1-c)^2 T\right).$$

证明至此完成。 □