arXiv:2304.08745v1 [cs.DS] 18 Apr 2023

动态图问题的超对数下界

Kasper Green Larsen* Huacheng Yu†奥胡斯大学
普林斯顿大学

摘要

在这项工作中，我们证明了对于在 n 个节点的有向无环图中支持可达性查询、并支持边插入的动态数据结构，其查询时间与更新时间的最大值存在 $\tilde{\Omega}(\lg^{3/2} n)$ 的无条件下界。这是针对任何自然图问题的首个超对数下界。在证明该下界的过程中，我们还对最先进的数据结构下界技术作出了新的贡献，希望这些进展能推动下界证明取得进一步突破。

1 引言

图问题是算法和数据结构中研究最广泛的主题之一，每年都会涌现大量令人振奋的新成果。仅在最近一年，就出现了一个近线性时间的最大流算法 [3] ，以及一个求解带负权图中单源最短路径的算法 [2]。细粒度复杂性领域通过从若干精心挑选的猜想难题出发进行归约，给出了大量互补的条件下界。其中包括通过从全点对最短路径（全点对最短路径）归约 [1], ，得到的图直径和半径问题的下界；也包括动态图问题的下界，例如动态可达性，这些下界分别基于 3SUM猜想 [15], 、在线矩阵-向量猜想 [6] 和强指数时间假设 [7]。

然而，转向无条件下界时，情况就令人沮丧得多。对于任何自然图问题，已知最强的无条件下界是：在动态维护一个支持连通性查询的无向图时，更新时间和查询时间的最大值至少为 $\Omega(\lg n)$。这个下界由 P˘atra¸scu 和 Demaine [13] 提出，可追溯至 2004年。与此同时，人们已经开发出更强的技术来证明动态数据结构的下界，其中包括 Larsen [8] 提出的一种技术，可证明具有 $\Omega(\lg n)$ 比特输出的查询所对应的动态问题的 $\tilde{\Omega}(\lg^2 n)$ 下界；以及 Larsen、Weinstein 和 Yu [10]提出的一种技术，可证明动态判定问题（1 比特输出）的 $\tilde{\Omega}(\lg^{3/2} n)$ 下界。遗憾的是，迄今为止，这些技术都未能成功应用于自然图问题，而已知最强的无条件下界仍然是 P˘atra¸scu 和 Demaine 提出的 $\Omega(\lg n)$ 下界。本文的主要贡献是为图问题给出了首个这样的 $\omega(\lg n)$ 下界。具体而言，我们证明如下结果

定理 1. 对于 n 个节点的有向无环图，在边插入操作下实现动态可达性的任何数据结构，若最坏情况更新时间为 t_u、期望查询时间为 t_q，且内存单元为 w 位，并且 $w = \Omega(\lg n)$，则必须满足

$$t_q = \Omega\left(\frac{\lg^{3/2} n}{\lg^2(t_u w)}\right).$$

除了 P˘atra¸scu 和 Demaine 给出的 $\Omega(\lg n)$ 下界外，目前已知的 Dynamic Reachability 下界只有另外两个阈值下界。首先，P˘atra¸scu 和 Thorup [17] 证明，对于 Dynamic Reachability，即使在无向图的情形下，任何更新时间为 $t_u = o(\lg n)$ 的数据结构都必须

*larsen@cs.au.dk。由 DFF Sapere Aude 研究领袖资助（编号 9064-00068B）支持。
†yuhch123@gmail.com。由 Simons 初级教职奖（AWD1007164）支持。

具有查询时间 $t_q = n^{1-o(1)}$。作为互补结果，Clifford 等人 [4] 证明，任何查询时间为 $t_q = o(\lg n/\lg\lg n)$、空间为 $n \lg^{O(1)} n$（对于具有 $n \lg^{O(1)} n$ 条边的图）的数据结构，其更新时间必须为 $t_u = n^{1-o(1)}$。然而，这些下界在 t_u 和 t_q 的最大值上都不超过 $\Omega(\lg n)$。

除了为一个自然的图问题证明了第一个 $\omega(\lg n)$ 下界之外，我们还在技术层面做出了若干贡献，希望能为进一步证明动态数据结构问题的 $\omega(\lg n)$ 下界铺平道路。在下一节中，我们首先概述证明数据结构下界的已有技术。随后，我们将更具技术性地介绍我们的新方法，并说明我们如何克服阻碍以往研究在图问题上突破 $\lg n$ 瓶颈的一些障碍。

1.1 单元探测模型中的下界

姚 [19] 在单元探测模型中证明了数据结构操作时间的无条件下界。在该模型中，数据结构由随机访问存储器构成，并划分为大小为 w 位的单元。

对于静态数据结构，数据结构问题的输入会经过预处理，转化为内存表示。对于空间用量 S，数据结构使用地址为整数 $[S] = \{0, \ldots, S-1\}$ 的内存单元来表示输入。预处理不收费，测量的只有空间用量。

为了回答查询，数据结构最多可以读取或探测 t_q 个内存单元，并且必须根据被探测单元的内容给出查询答案。在此模型中，计算不计成本，待探测单元的地址可以由查询以及先前探测单元的内容任意决定。形式上，可以为每个查询建立一棵决策树来对此进行建模。树中的每个节点都标记有一个位于 $[S]$ 中的单元地址，并有 2^w 个子节点，分别对应该单元的每种可能内容。树的叶节点标记着查询的答案。

当 p 对于静态数据结构的探测下界，我们研究 S 与 t_q之间的权衡 .

对于动态数据结构，我们还需要支持对底层数据的更新。例如，这可能是图中的边插入或删除。对于动态数据结构，我们假设单元在 $[2^w] = \{0, \ldots, 2^w - 1\}$中具有整数地址。查询仍按照静态数据结构中的方式回答。处理更新时，数据结构最多可以探测 t_u 个内存单元。探测单元时，数据结构也可以更改单元的内容。与查询类似，在说明更新时间时，我们只计算单元探测次数，任何计算均不计成本。

静态下界的既有技术。 目前，证明静态数据结构下界的最先进技术是 Panigrahy 等人提出的单元采样 技术 [11]，后来在 [9] 中得到改进，并被 Siegel 在早期的哈希研究中采用 [18]。由于该技术在包括我们的方法在内的更先进的动态数据结构技术中发挥着核心作用，我们在此简要介绍它。为了一致地阐述不同技术，我们在讨论这些技术时使用同一个数据结构问题作为示例。这里的示例是二维范围求和。在该问题的静态版本中，输入是一组位于二维网格 $[n] \times [n]$ 上的 n 点，其坐标为整数。每个点都被赋予一个 b位权重。查询也由一个点 (x, y) 指定 $\in [n] \times [n]$，目标是返回满足 $x' \le x$ 和 $y' \le y$的输入点 (x', y') 所对应权重之和。

为了使用单元采样技术证明这个问题的下界，我们采用一种编码论证。其思路是考虑对固定的一组 n 个点进行权重的均匀随机赋值。假设存在一个高效的二维范围求和数据结构，我们现在给出一种编码和解码过程，用以重建大部分随机权重。直观地说，如果我们能从编码中重建 m 个权重，那么编码长度至少必须为 mb 比特。因此，我们的思路是给出一种编码，使其长度相对于 S 和 t_q较短。为此，单元采样技术首先在随机输入上构建一个数据结构。对于采样概率 $p = (n/(Sw))^{O(1)}$，我们以概率 p独立地随机抽样每个内存单元。编码由抽样单元的内容和地址构成，预期需要 $pS(w + \lg S) = O(pSw) = o(n)$ 比特。为了从该编码中重建许多权重，解码器现在可以模拟每个可能的查询（x， y） $\in [n] \times [n]$。模拟查询时，

解码器运行查询算法，并针对每个被探测的单元，检查它是否属于已编码的随机样本。如果是，模拟就可以继续；否则，解码器便丢弃该查询，并转向下一个查询点。注意，对于任意固定查询，它所探测的全部 t_q 个单元都在样本中的概率为 p^{t_q}。如果 $t_q = o(\lg\, n/\lg(Sw/n))$，那么该概率为 $n^{-o(1)}$。由于共有 n^2 个查询，解码器将成功恢复 $n^{2-o(1)}$ 个查询的答案。如果这些查询足够不同（将其视为点权重的线性组合时，其秩为 $\Omega(n)$），那么它们合起来就能揭示关于这些权重的 $\Omega(nb)$ 比特信息。这与编码大小为 $o(n)$相矛盾，因此可以得出 $t = \Omega(\lg\, n/\lg(Sw/n))$。我们指出，这种针对二维范围求和的秩论证最早由 P˘atra¸scu [14]在一篇基于通信复杂度的下界证明中使用 [14, 16]。

动态下界的计时图技术。 证明动态下界的大多数核心技术，其基本思路都是将静态下界提升一个对数因子。因此，这些技术仅适用于所谓的可分解问题。为了解释这一点，我们先介绍 Fredman 和 Saks 提出的开创性计时图技术 [5]。他们的技术的主要思路是考虑一系列 n 随机更新，并将其划分为大小按几何级数递减的时期 更新，其中$n_i = \beta^i$ 表示某个 $\beta \geq 2$。首先处理的是编号为 $\lg_\beta n - 1$ 的更新时期，接下来是时期 $\lg_\beta n - 2$，依此类推，直到时期 1。最后，在处理完这些更新时期后，提出一个随机查询。对于我们一直使用的二维范围求和示例，每个更新时期都会插入带有均匀随机权重的n_i 个点，而随机查询仍然是 $[n] \times [n]$中的一个点。查询的答案仍然是赋给点的所有权重之和（x'，y'），其中 $x' \leq x$ 且 $y' \leq y$。这个数据结构问题的关键性质在于它是可分解的。具体来说，如果我们知道时期 $j \neq i$ 中的所有更新以及某个查询的答案（x，y），那么即使只存在时期 i 的更新，我们也能得知该查询的答案。对于二维范围求和，只需减去时期 $j \neq i$对总和的贡献即可得出这一结论。根据这一观察，我们可以直观地利用动态数据结构，为任意时期 i构建一个高效的静态数据结构。

我们对此作更详细的解释。考虑一个动态数据结构，以及一系列划分为若干时期的 n 更新，并观察该数据结构处理完所有更新后的内存单元。随后，每个内存单元都与其最后一次被更新所在的时期相关联。令 C_i 表示与时期 i相关联的单元。现在有几个关键观察。首先，对于任意时期 i，如果各时期的更新彼此独立，那么 C_j 中属于 $j > i$ 的单元不可能包含关于时期i的任何信息。这是因为在时期 i 的更新到来之前，这些单元就已经是最后一次被写入的。其次，时期 $j < i$ 中的单元非常少。具体而言，当更新时间为 t_u时，我们有 $|C_j| \leq \beta^j t_u$，因此对于 $\beta = \omega(t_u w)$，有 $\sum_{j<i} |C_j| w = o(\beta^i)$。这意味着，在 i 之后各时期中发生变化的所有单元，平均而言，对于时期 i的每次 β^i 更新，仅包含 $o(1)$ 位信息。直观地说，如果随机查询的答案很大程度上取决于时期 i的更新，那么由于其他时期包含的信息太少，无法正确回答该查询，数据结构就必须从 C_i 中探查 $\Omega(1)$ 个单元。由于集合 C_i 两两不相交，我们可以将这一关于所有时期的下界相加，从而得到 $t_q = \Omega(\lg_\beta n) = \Omega(\lg\, n/\lg(t_u w))$。

具有预初始化内存和缓存的静态数据结构。 上述方法可以被视为隐式地证明了每个时期上的静态下界。在本文中，我们通过定义一种适用于该归约的特殊形式的静态数据结构，使这一联系更加明确。我们将带预初始化内存和缓存的静态单元探测数据结构定义为一种静态数据结构：在看到输入之前，它可以将所有内存单元（地址位于 $[2^w]$ 中）预初始化为任意内容（且与输入无关）。收到输入后，它会更新至多 S 个内存单元，最后创建一个至多包含 S_{cac} 个内存单元的缓存。进行查询时，该数据结构会探测内存单元，并且必须根据所探测单元的内容和缓存给出查询答案。每一步所探测的单元可以是缓存以及此前所有已探测单元的任意函数。与标准静态单元探测数据结构相比，它可以免费访问缓存（缓存不计入查询时间），并且还可以探测预初始化内存。带预初始化内存和缓存的数据结构的查询时间由两个参数构成。我们用 t_{tot} 表示回答查询时探测的单元总数，其中既计入对已更新内存单元的探测，也计入对看到输入时未发生改变的单元的探测。

我们用 t_q 表示对已更新单元的探测次数。

Fredman 和 Saks 的计时图技术现在可以看作是归约到一个带有预初始化内存和缓存的静态数据结构问题。为说明这一点，再次考虑二维范围求和问题。在时期 $\lg_\beta n-1$、……、1 中，由于集合 C_i 两两不相交，必定存在一个时期 i，使得对 C_i 中单元的预期探测次数为 $O(t_q/\lg^\beta n)$。我们聚焦于这样一个时期 i。现在，我们为在 $n_i=\beta^i$ 个点上进行二维范围求和这一静态问题构建一个带有预初始化内存和缓存的静态数据结构，具体如下：在看到输入的 n_i 个点之前，我们先利用动态数据结构，针对时期 $j>i$ 执行一段硬编码的更新序列，以预初始化内存。由于各时期的更新彼此独立，因此无需知道时期 i 的输入即可完成此操作。收到输入后，我们将其视为时期 i 的更新，并在动态数据结构上执行这些更新。这至多会更新 $S=t_un_i$ 个单元。最后，我们在动态数据结构上执行一段针对时期 $j<i$ 的硬编码更新序列，并将所有发生变化的单元放入缓存。因此，我们有 $S_{\text{cac}}\le\sum_{j<i}\beta^jt_u=o(n_i/w)$。要在静态数据结构上回答查询，我们运行动态数据结构的查询算法。每当它探测一个单元时，如果该单元在时期 $j<i$ 更新过，那么该单元的内容就在缓存中；否则，我们直接探测内存。动态数据结构的查询算法结束后，我们利用该问题是可分解搜索问题这一点，从查询答案中减去硬编码时期 $j\ne i$ 对答案的贡献。如果 t_q 是动态数据结构的查询时间，那么静态数据结构的查询时间为 $t_{\text{tot}}\le t_q$。此外，我们有 $t'_q=O(t_q/\lg^\beta n)$，其中 t'_q 表示静态数据结构对已更新单元进行的探测次数。

鉴于上述内容，计时图技术现在归结为：对于一种具有预初始化内存和缓存的静态数据结构，当该数据结构更新 $S=n_it_u$ 个单元且缓存大小为 $S_{\text{cac}}=o(n_i/w)$ 个单元时，证明其对更新单元的探测次数下界为 $t'_q=\Omega(1)$。

超对数下界。 基于计时图技术，Larsen [8] 后来提出了一种技术，能够证明动态数据结构的下界为 $t_q=\Omega((\lg n/\lg(t_uw))^2)$。鉴于前面所述归约到具有预初始化内存和缓存的静态数据结构，他的方法非常直观：只需利用单元采样技术（针对静态数据结构），证明具有预初始化内存和缓存的静态数据结构的下界为 $t_q=\Omega(\lg n/\lg(Sw/n))$。结合上述归约，对于查询时间为 t_q、更新时间为 t_u 的动态数据结构，现在可得到一个具有预初始化内存的静态数据结构；对于某个时期 $i\in\{\lg_\beta n-1,\ \ldots\ldots,\ (1/2)\lg_\beta n\}$，该结构更新 $S=n_it_u$ 个单元，且缓存大小为 $o(n_i)$ 位。此外，该静态数据结构会探测 $O(t_q/\lg^\beta n)$ 个更新单元。单元采样给出的下界现在意味着 $t_q/\lg^\beta n=\Omega(\lg n_i/\lg(Sw/n_i))$。由于 $n_i\ge\sqrt{n}$ 和 $\beta=(t_uw)^{O(1)}$，这便是 $t_q=\Omega((\lg n/\lg(t_uw))^2)$。

乍看之下，这似乎只是一个简单的扩展。然而，在尝试证明静态下界时，单元采样技术中的一个关键步骤会失效。回想一下，在单元采样中，每个内存单元都以概率 $p=(n/(Sw))^{O(1)}$ 独立采样。为了对二维范围求和得出矛盾，我们希望对已更新单元采样 $o(n/w)$，并论证：如果对已更新单元的探测次数过少，那么就能从样本和缓存（其大小也为 $o(n)$ 位）中恢复关于权重的 $\Omega(n)$ 个信息比特。如果对已更新单元的探测次数为 $o(\lg n/\lg(Sw/n))$，那么确实会有 $n^{2-o(1)}$ 个查询属于 $[n]\times[n]$，使得它们对已更新单元的所有探测都落在样本中。如果解码过程模拟任意此类查询的查询算法，就能恢复其答案，因为每当它探测到一个既不在缓存中也不在样本中的单元时，我们都知道该单元的内容与预初始化内存后的内容相同（且与输入无关）。现在，关键的观察是，我们无法判断哪些查询对已更新单元的所有探测都落在样本中。对于普通的静态数据结构，我们只需在查询探测到样本之外的单元时将其丢弃；但在存在预初始化内存的情况下，如果某个单元既不在缓存中也不在样本中，我们就无法判断它究竟是一个未被采样的已更新单元，还是一个普通的预初始化单元。因此，解码过程根本无法确定要模拟哪些查询。Larsen 通过要求分配给每个点的权重都具有 $b\ge3\lg n$ 位来绕过这个问题。这样一来，编码过程就能够明确写出一组模拟成功的查询。由于写出一个查询需要 $2\lg n$ 位，而它能恢复关于权重的 $b=3\lg n$ 个信息比特，因此仍然可以得出矛盾。

Larsen 的技术关键在于需要大量输出位，使得查询答案所揭示的信息比描述该查询所需的信息更多。对于动态判定问题，也就是输出为 1 位的问题，如何突破对数障碍一直悬而未决，又过了 5 年，直到 Larsen、Weinstein 和 Yu 的工作 [10] 才取得进展。在这项工作中（本文正是在此基础上进一步拓展），他们证明，带有预初始化内存和缓存的静态数据结构可用于构造一种针对自然通信博弈的单向协议。在这个博弈中，Alice 收到静态数据结构问题的随机输入，而 Bob 收到一个随机查询。Alice 随后向 Bob 发送一条 $o(n)$ 位的消息，Bob 必须以略高于随机猜测的概率正确回答该查询。Larsen 、 Weinstein 和 Yu 证明，探测总次数为 t_{tot} 、且对已更新内存单元的探测次数为 t_q 的数据结构，可以用于构造一种协议，使 Bob 输出正确答案的概率至少为

$$1/2 + \exp(-\tilde{O}(\sqrt{t_{\mathrm{tot}} t_q})).$$

他们将其技术应用于二维范围奇偶校验问题。该问题实际上是权重为 1 比特、且答案只需对 2 取模的二维范围求和问题。他们还证明，任何具有 $o(n)$ 个通信比特的协议，预测查询答案的概率最多为 $1/2 + n^{-\Omega(1)}$。利用归约中从动态到静态数据结构的 $t_q = O(t_{\mathrm{tot}}/\lg^{\beta} n)$，这最终意味着 $t_{\mathrm{tot}}/\sqrt{\lg_{\beta} n} = \tilde{\Omega}(\lg n)$，即原始动态问题的 $\lg^{3/2} n$ 下界。

1.2 克服的技术障碍

在介绍了之前的技术后，我们现在准备概述为证明动态可达性的下界而克服的技术障碍。显然，可达性是一个判定问题，因此最相关的先前技术是 Larsen、Weinstein 和 Yu 提出的用于证明 $\tilde{\Omega}(\lg^{3/2} n)$ 下界的技术 [10] 。然而，有几个障碍阻止了对其框架的直接应用。首先，上述所有用于动态下界的先前技术都要求问题是可分解的。如果我们考虑动态可达性，以及使用预初始化内存和缓存从动态到静态数据结构的归约，这将对应于每个时期向图 G_i中插入 n_i 条边。完成插入后，会提出一个可达性查询。对于二维范围求和，计数查询的答案是所有时期上的答案之和，因此是可分解的，因为我们可以减去来自时期$j \neq i$的贡献。但如果我们考虑可达性，当需要遍历众多图$G_{\lg_\beta n-1}, \ldots, G_1$时，一个节点 s 是否能够到达节点 t ，可达性查询的答案是各个时期之间的逻辑或，而不是求和。也就是说，如果 s 利用图 G_j中的边能够到达 t ，那么无论其他时期如何，查询答案都是**是** 。因此，该问题并不可分解。

为克服这一问题，我们考虑输入图上的分布 G_i ，使得查询节点对 $(s,\ t)$ 能通过 G_i 相互到达的概率很小。具体而言，该概率约为 $1/\lg\ n$。这意味着，如果我们聚焦于时期 i，那么大多数查询节点对 $(s,\ t)$ 都无法通过满足 $j \neq i$ 的图 G_j相互到达。从某种意义上说，其他时期不会影响查询的答案，因此我们又回到了一个可分解问题。

尝试上述方法会带来另一个问题。Larsen、Weinstein 和 Yu 的技术有一个关键要求：静态问题中查询的答案必须在 0 和 1 之间均匀随机。简言之，如果查询答案为 0 的概率为 $1 - 1/\lg\ n$，那么 Bob 就能轻而易举地以远高于 $1/2$ 的概率预测查询答案。因此，我们的第二项贡献是将他们的通信博弈扩展到“有偏差”的问题，即查询答案并非均匀随机。我们认为，这一扩展以及我们新得到的下界，对于证明不可分解问题未来的下界至关重要。

最后需要指出，即使在调整了 Larsen、Weinstein 和 Yu 的框架之后，要证明动态可达性的具体下界也绝非易事，需要许多巧妙思路和并不简单的问题专用归约。我们将在后续章节中介绍这些内容。

2 Data 具有预初始化内存和缓存的数据结构

本节将更详细地介绍具有预初始化内存和缓存的静态数据结构（如第 1.1 节所述）。这种数据结构包含地址位于 $[2^w]$ 中的内存单元，每个内存单元都预先初始化为固定内容，且该内容与输入数据无关。不同单元的初始化内容可以不同。收到输入数据 I后，预处理算法将更新至多 S 个内存单元，并向一个独立缓存 写入 S_{cac} 个单元。我们将这组 S 个内存单元称为更新单元。更新单元的集合可以取决于输入数据。

然后，数据结构必须能够通过查询算法高效地回答查询 Q 。查询算法可以访问内存和缓存。探测缓存中的单元无需付费。令$t_{\text{tot}}(Q,\ I)$表示在 $(Q,\ I)$ 上的查询时间，即查询算法在回答输入 I 上的查询 Q 时探测的内存单元总数。令 $t_q(Q,\ I)$ 表示在 $(Q,\ I)$ 上对更新单元的查询时间，即针对输入 I 上的查询 Q ，它探测的更新单元数。最后，我们令 $t_{\text{tot}} = \mathbb{E}[t_{\text{tot}}(Q,\ I)]$ 和$t_q = \mathbb{E}[t_q(Q,\ I)]$ 表示期望查询时间。

带权数据结构问题和单向通信问题。如第 1.2 节所述，我们需要扩展 Larsen、Weinstein 和 Yu [10] 的技术，以处理查询答案并非均匀随机的问题。为此，我们定义带权数据结构问题。

设 $\mathcal{P}$ 是一个数据结构问题，其输入数据来自 $\mathcal{I}$ ，查询来自 $\mathcal{Q}$。如果 $\mathcal{P}$ 将查询-数据对 $\mathcal{Q}\times\mathcal{I}$ 映射到实数 $[-1,1]$，那么 $\mathcal{P}$ 就是一个带权重的数据结构问题。对于 $\mathcal{P}$，数据结构只需计算 $\mathcal{P}(Q,I)$ 的符号，其中查询为 Q ，输入为 I。等价地，可以将 $\mathcal{P}$ 视为一个具有单比特输出的数据结构问题，而 $|\mathcal{P}(Q,I)|$ 则是实例 (Q,I) 的权重 。

给定 $\mathcal{P}$ 和 $\mathcal{Q}\times\mathcal{I}$ 上的一个（乘积）分布 $\mathcal{D}_Q\times\mathcal{D}_I$，使得对所有 Q，$\mathbb{E}_I[\mathcal{P}(Q,I)]=0$，我们将单向通信问题 $G_{\mathcal{P}}$ 定义如下：Alice 获得一个随机输入 $I\sim\mathcal{D}_I$，Bob 获得一个随机查询 $Q\sim\mathcal{D}_Q$，Alice 向 Bob 发送一条包含 C 比特的消息 M_A ，他们的目标是最大化加权优势

$$\mathop{\mathbb{E}}_{Q,M_A}\left[\left|\mathop{\mathbb{E}}_{I}[\mathcal{P}(Q,I)\mid M_A]\right|\right]. \tag{1}$$

优势的最大值记为 $\text{adv}(G_{\mathcal{P}},\mathcal{D}_Q,\mathcal{D}_I,C)$。

当 $\mathcal{P}(Q,\ I)$ 仅取值于 $\{-1,1\}$ 时，它就是一个输出为单比特的普通数据结构问题。在这种情况下，(1) 就是给定 M_A 时查询 Q 输出的偏差：$\text{adv}(G_{\mathcal{P}},\ \mathcal{D}_Q,\ \mathcal{D}_I,\ C)$ 衡量 Bob 在看到 Alice 发来的消息后，相较于随机猜测所具有的优势。一般而言，当实例可能具有不同权重时，我们会衡量这一偏差。注意，严格来说，在计算偏差时，我们也可以将其视为根据 $|\mathcal{P}(Q,\ I)|$ 对分布 $\mathcal{D}_Q\times\mathcal{D}_I$ 重新加权，但期望查询时间仍是相对于“未加权”分布 $\mathcal{D}_Q\times\mathcal{D}_I$ 定义的。

2.1 模拟

与 Larsen、Weinstein 和 Yu [10], 的工作类似，我们也证明，利用具有预初始化内存和缓存的高效数据结构，可以为上述单向通信博弈构造一个高效协议。我们的模拟定理如下

定理 2. 设 $\mathcal{P}$：$\mathcal{Q}\times\mathcal{I}\to[-1,1]$ 是一个带权重的数据结构问题，且 $\mathcal{D}_Q\times\mathcal{D}_I$ 是查询和输入上的一个分布，使得对于所有 $Q\in\mathcal{Q}$，$\mathbb{E}_I[\mathcal{P}(Q,I)]=0$；并且对于某个 $\beta>0$，$|\mathcal{P}(Q,I)|\geq\beta$。若存在一个数据结构 D，它具有预初始化内存以及用于 $\mathcal{P}$ 的缓存，并且 D 至多有 S 个更新单元、缓存中有 S_{cac} 个单元、期望查询时间为 t_{tot}，且对更新单元的期望查询时间为 t_q，那么对于任意$p\in(0,\ 1)$，存在一个针对 $G_{\mathcal{P}}$ 的单向通信协议，使得

$$\text{adv}(G_{\mathcal{P}},\mathcal{D}_Q,\mathcal{D}_I,(8pS+S_{\text{cac}})\cdot w)\geq 2^{-O(\sqrt{t_{\text{tot}}(t_q\lg 1/p+\lg 1/\beta)}\cdot\lg 1/p)}-2^{-\Omega(pS)}.$$

由于该证明深受先前工作的启发，我们将证明推迟到第 6 节。

3 数据结构问题

有了从具有预初始化内存和缓存的静态数据结构中构造单向协议所需的框架，我们现在可以着重讨论动态可达性这一具体问题。在证明中，我们考虑一种所谓蝴蝶图变体中的可达性查询。P˘atra¸scu [12] 也曾在其开创性工作中使用这种图，并由此为许多静态数据结构问题确立了下界。然而，在构造涉及多个蝴蝶图的动态问题时，我们发现定义一个称为“多个蝴蝶图中的 0-XOR”的中间数据结构问题更为方便。证明该问题的单向通信下界更为容易。随后，我们通过归约证明，可利用动态可达性的数据结构来解决多个蝴蝶图中的 0-XOR。下面定义这个新的数据结构问题。

蝴蝶图。 对于度为 B、深度为 d的蝴蝶图，其度为 B、深度为 d，包含 $d+1$层，每层有 B^d 个节点。第 0 层的节点是源点，第 $d+1$ 层的节点是汇点。除了汇点以外，所有节点的度均为 B。

为了描述这些边，我们用 $[B^d]$ 中的连续整数为每一层的节点编索引。对于第 i 层中满足 $0 \le i \le d$ 的节点，每个节点都有 B 条出边。从节点 v_j^i 出发的边通向第 $i+1$ 层中满足以下条件的 B 个节点 v_k^{i+1}： j 和 k 的以 B 为底的表示在除数字 $c \neq i$ 以外的所有位上都相同（它们在数字 i 位上可以相同，也可以不同）。最低有效位是第 0 位，依此类推。

注意，任意源汇点对（s，t）之间都存在唯一路径。求得这条路径的方法是将 s 和 t 写成以 B 为底的数。然后，对于每一层 $i = 0$，.....，d，从第 0 层的节点 s 出发，我们依次将 s 的第 i 位改为 t 的第 i 位。这意味着，如果我们位于第 i 层的某个节点 v_j^i，就转到节点 v_k^{i+1}；j 和 k 除了第 i 位可能不同以外，其余各位都相同，而 k 在该位上的数字与 t 相同。图 1 给出了一个度为 2、深度为 3 的蝴蝶网络示例。

0-单个蝴蝶图上的异或。这是一个静态数据结构问题，输入是一个度为 B、深度为 d 的蝴蝶网络，并为蝴蝶网络的每条边赋值一个 b 位比特串。查询由一个源汇点对 (*s*，*t*) 指定；如果从 s 到 t 的路径上的比特串异或结果是全零位串，则查询答案为 1，否则为 0。图 1 展示了一个示例。

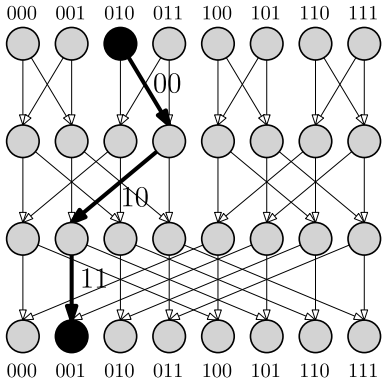


图 1：度为 2、深度为 3 的蝴蝶网络，其边上标有用于 $b = 2$ 的 b 位比特串。给定查询 (2，1)，我们将 2 解释为源点索引，将 1 解释为汇点索引。因此，查询 (2，1) 询问从索引为 $2 = 010$ 的源点到索引为 $1 = 001$ 的汇点的路径上的比特串异或结果是否为全零位串。在此例中，异或结果为 $00 \oplus 10 \oplus 11 = 01$，即并非全零位串。因此，查询答案为 0。为清晰起见，我们仅展示了查询路径上各边的比特串。

0-多个蝴蝶图中的异或。这是一个动态数据结构问题。对于深度为 d、度为 B的情况，我们必须维护多个蝴蝶图 G_d，...，G_1，它们的度均为 B，且 G_i 的深度为 i。

此问题中的更新按时期进行。第一个时期的编号为 d，接着是时期 $d-1$，依此类推，直到时期 1。时期 i 的更新会为蝴蝶图 G_i的每条边赋予一个 b 位比特串。

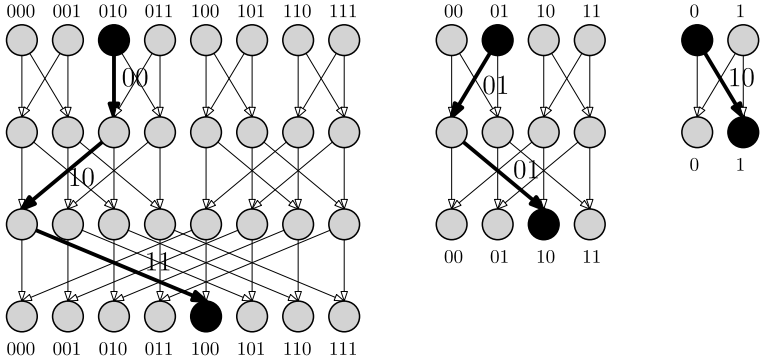


图 2：考虑度为 2、深度分别为 3、2 和 1 的三个蝴蝶图中的 0-XOR，其中 $b=2$ 对应 b 位串。给定查询 (2、4)，我们将 $\lfloor 2/2^0 \rfloor = 2 = 010$ 解释为第一个图中源点的索引，$\lfloor 2/2^1 \rfloor = 1 = 01$ 解释为第二个图中的源点索引，$\lfloor 2/2^2 \rfloor = 0$ 解释为第三个、也是最小的图中源点的索引。在第一个图中，汇点为 $\lfloor 4/2^0 \rfloor = 4 = 100$；在第二个图中，汇点为 $\lfloor 4/2^1 \rfloor = 2 = 10$；在第三个图中，汇点为 $\lfloor 4/2^2 \rfloor = 1$。因此，查询 (2、4) 询问：沿至少一条加粗路径上的比特串异或后是否为全零位串。第二个图中确实如此，其中 $01 \oplus 01 = 00$，因此该查询的答案为 1。

处理完更新后，我们必须回答查询。查询由两个整数 $(s,\ t) \in [B^d] \times [B^d]$ 指定。在每个蝴蝶网络中，数对 $(s,\ t)$ 指定源汇点对 $(s_i,\ t_i)$，其中 s_i是 G_i 中索引为 $\lfloor s/B^{d-i} \rfloor$ 的源，t_i 是 G_i中索引为 $\lfloor t/B^{d-i} \rfloor$ 的汇点。对于查询 $(s,\ t)$，如果至少存在一个 G_i，使得对于单个 Butterfly 中的 0-XOR，查询 $(s_i,\ t_i)$ 的答案为 1，则该查询的答案为 1。否则，答案为 0。图 2 给出了示意图。

多个蝴蝶图中的 0-XOR 到动态可达性

本节将介绍从多个蝴蝶图中的 0-XOR 到动态可达性（在有向图中）的归约。为便于说明，我们分两步执行该归约。

单个蝴蝶图的归约。首先考虑单个蝴蝶图中的 0-XOR（静态）问题。回顾一下，在这个问题中，给定一个度为 B、深度为 d 的蝴蝶图 G，并为每条边分配一个 b 位比特串。对于查询 $(s,\ t)$，我们必须返回沿唯一的 s-t 路径上各比特串的异或是否为全零位串 0。

根据 G，我们构造一个用于可达性查询的新图 G'。其目的是使得 G 中的每个 0-XOR 查询都能通过 G'中的一次可达性查询来回答。对于 G中的每个节点 u，我们在 G'中构造 2^b 个节点。我们将这些节点视为分别代表 b 位比特串的 2^b 种可能取值。因此，节点 $u \in G$ 会被替换为 G'中的节点 $\{u^\sigma\}_{\sigma \in \{0,1\}^b}$。对于 G 中一条从节点 u 指向节点 v、比特串为 $\sigma \in \{0,1\}^b$的边，我们在 G'中插入 2^b 条边。每个节点 u^τ都有一条这样的出边。离开 u^τ 的边进入 $v^{\tau \oplus \sigma}$，其中$\oplus$ 表示按位异或。关键观察是，对于 G中从源点 s 到汇点 t 的任意路径，如果我们从 G' 中的 $s^{\bar{0}}$ 出发，沿着同一条路径向下遍历，并始终沿当前节点u^τ 到路径上节点 $v^{\tau \oplus \sigma}$ 的唯一出边前进，那么恰好有一个汇点 t^σ可达。此外，σ 等于 G中沿 s-t 路径各边所分配比特串的异或。因此，G 中的 0-XOR 查询 (s,t) 的答案为 1，当且仅当源点 $s^{\bar{0}}$ 能够到达汇点 $t^{\bar{0}}$（在 G'中）。示意见图3。

完整归约。现在，我们使用上述针对单个蝴蝶图的归约，将多个蝴蝶图中的 0-XOR 归约为动态可达性问题。在我们的动态可达性问题中，图有 $n = \sum_{i=1}^{d} 2^b(i+1)B^i +$

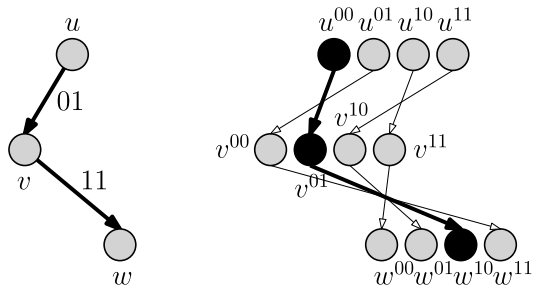


图3：左侧是蝴蝶网络中的三个节点 G，边上带有 b 位比特串，用于表示 $b = 2$。为了将其转换为可达性实例 G'，每个节点由 $2^b = 4$ 个节点表示，每个节点对应一个 b 位比特串。对于从 u 到 v、比特串为 01 的边，我们为每个 $\sigma \in \{0,1\}^2$添加一条从 u^σ 到 $v^{\sigma\oplus 01}$ 的边。节点 $u^{\bar{0}} = u^{00}$ 恰好可以到达对应于异或 $01 \oplus 11 = 10$的节点 w^{10}。

$2\sum_{i=0}^{d} B^i$ 个节点。其中有 $2^b(i+1)B^i$ 个节点对应蝴蝶图 G_i。这些节点对应于将度为 B 、深度为 i 的单个 Butterfly 中的 0-XOR 归约到可达性时所构造的 G'_i 中的节点。其余 $2\sum_{i=0}^{d} B^i$ 个节点对应两棵完美的 B叉树 $\mathcal{S}$和 $\mathcal{T}$，每棵树有 B^d个叶节点。初始时，图中没有边。

回想一下，在多个蝴蝶图中的 0-XOR 问题中，更新按时期到达；时期i 的更新为 G_i的边分配比特串，其中 G_i 的度为 B，深度为 i。

在时期 d （第一个要处理的时期），我们首先插入边，构建两棵完美的 B 叉树 $\mathcal{S}$ 和 $\mathcal{T}$，每棵树有 B^d 个叶节点。我们将 $\mathcal{S}$ 的叶节点视为表示 G_d中的源点。紧邻其上的节点表示 G_{d-1} 中的源点，依此类推。类似地，对于 $\mathcal{T}$，叶节点表示G_d 的汇点，依此类推。树 $\mathcal{S}$ 的边从子节点指向父节点，而树 $\mathcal{T}$的边从父节点指向子节点。对于 $\mathcal{S}$中深度为 i 的节点（叶节点的深度为 d），我们添加一条边，从 G_i 中表示源点 s 的节点指向 G'_i中对应的源点 $s^{\bar{0}}$。对于 $\mathcal{T}$中深度为 i 的节点 t，我们改为添加一条边，从 G'_i 中的汇点 $t^{\bar{0}}$ 指向 t。

为处理时期 i 的更新，我们只需插入 $2^b iB^i$ 边到 G'_i，这对应于上文展示的从单个 Butterfly 中的 0-XOR 到可达性的归约。最后，在处理完所有更新时期后，要回答查询 $(s,\ t) \in [B^d] \times [B^d]$，我们只需询问 s 在 $\mathcal{S}$ 中对应的叶节点是否能够到达 t 在 $\mathcal{T}$中对应的叶节点。要说明这种做法能够正确回答查询，注意到，与 s 对应的叶节点只能通过 s的某个祖先节点离开 $\mathcal{S}$。如果它从深度为 i的祖先节点离开，就会进入索引为 $\lfloor s/B^{d-i} \rfloor$ 的源点 $s^{\bar{0}}$，该源点位于 G'_i中。要离开 G'_i，它必须到达某个汇点 $t^{\bar{0}}$。如果它到达的汇点的索引不是 $\lfloor t/B^{d-i} \rfloor$，那么通向 $\mathcal{T}$的边会进入节点 u，此时 t 不在以 u 为根的子树中，因此无法到达 t。另一方面，如果它到达索引为 $\lfloor t/B^{d-i} \rfloor$的汇点 $t^{\bar{0}}$，那么离开该汇点的边会进入 $\mathcal{T}$中的节点 u，其中 t 位于该子树中，因此能够到达 t。由此可知，s 能够到达 t，当且仅当至少存在一个 G'_i，使得源点 $\lfloor s/B^{d-i} \rfloor$ 能够到达汇点 $\lfloor t/B^{d-i} \rfloor$。至此，归约完成。图4对此作了说明。因此，我们有

定理 3。 如果存在一个针对 n 个节点图中的动态可达性的数据结构，其最坏情况更新时间为 t_u，期望查询时间为 t_q，那么对于任意满足 $n \geq \sum_{i=1}^{d} 2^b(i+1)B^i + 2\sum_{i=0}^{d} B^i$ 的 d、B 和 b，都存在一个针对度为 B、深度至多为 d 且使用 b 比特串的0-*XOR*（多个蝴蝶图中的 *0-XOR*）数据结构；该数据结构在处理时期 i 的更新时会探测 $O(t_u n/B^{d-i-1})$ 个单元，并能在期望 t_q 次探测内回答查询。

鉴于此，我们为多个蝴蝶图中的 0-XOR 证明一个下界：

定理 4。 考虑度为 B、深度至多为 d 且比特串长度为0-*XOR* 的多个蝴蝶图，其中 $(\lg_2 d + 6)$，对于 d，其值至少为一个足够大的常数。若 $B = (dt_u w)^{12},$，那么任何更新

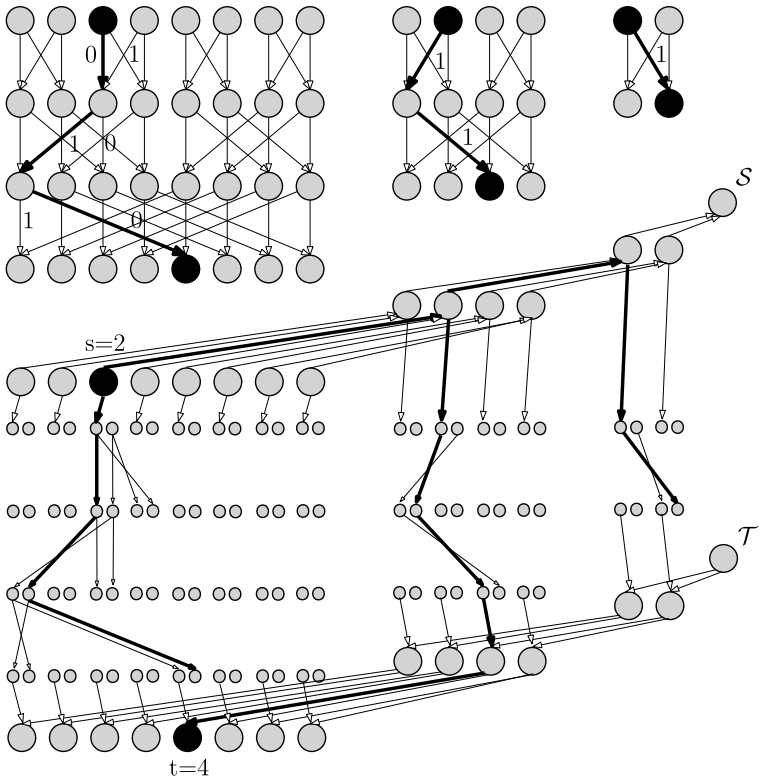


图4：完整归约。在三个度为 2、深度分别为 3、2、1 的蝴蝶网络上进行查询（$s,\ t$）$=(2,\ 4)$，其 $b=1$ 为 b 位串。为清楚起见，可达性实例中的大多数边均已隐藏。在此例中，查询的答案为 1。$\mathcal{S}$ 中对应于 s 的叶节点，可以通过深度为 2 的蝴蝶网络到达 $\mathcal{T}$ 中对应于 t 的叶节点；该网络中从源点 $\lfloor s/2 \rfloor$ 到汇点 $\lfloor t/2 \rfloor$ 的路径上的异或结果为全零位串。

$O(t_u d B^{i+1})$ 个单元的数据结构在时期 i 的期望查询时间 t_q 必须满足

$$t_q = \Omega\left(\frac{\lg^{3/2} n}{\lg^2(t_u w)}\right)$$

其中 $n = \sum_{i=1}^{d} dB^i$ 是所有蝴蝶网络中的节点总数。

结合定理 3 和定理 4，即可得到动态可达性的下界。

对于任意充分大的 n，假设我们有一个数据结构，用于处理 n 个节点的图上的动态可达性问题，其最坏情况更新时间为 t_u，期望查询时间为 t_q。令 d 为满足以下条件的最大整数：对于$B=(dt_u w)^{12}$,，有 $\sum_{i=1}^{d} 2^6 d(i+1)B^i + 2\sum_{i=0}^{d} B^i \le n$。注意，当 $w=\Omega(\lg n)=\Omega(d)$ 时，d 增加 1 会使总和增加 $(t_u w)^{O(1)}$ 倍。因此，对于选定的 d，我们得到$\sum_{i=1}^{d} 2^6 d(i+1)B^i + 2\sum_{i=0}^{d} B^i \ge n/(t_u w)^{O(1)}$，这意味着 $B^d \ge n/(t_u w)^{O(1)}$。

由定理 3 及 $b=(\lg_2 d+6)$，我们现在得到一种用于多个蝴蝶图中的 0-XOR 的数据结构，其度为 $B=(dt_u w)^{12}$，深度最高达 d，探测次数为

$$O(t_u n/B^{d-i-1}) = t_u B^d (t_u w)^{O(1)}/B^{d-i-1} = B^{i+1}(t_u w)^{O(1)}$$

处理时期 i 的更新时的单元。定理 4，结合 $t'_u=(t_u w)^{O(1)}$，最终可推出

$$t_q = \Omega\left(\frac{\lg^{3/2} n}{\lg^2(t_u w)}\right).$$

这证明了我们的主要结果，即定理 1。

5 多个蝴蝶图中的0-异或下界

本节将证明定理 4 中所述的多个蝴蝶图中的 0-XOR 下界。

证明的第一步是将单个蝴蝶图中的 0-XOR 归约为多个蝴蝶图中的 0-XOR。具体而言，我们证明，对于多个蝴蝶图中的 0-XOR，如果存在一个高效的（动态）数据结构，那么就能为带有预初始化内存和缓存的单个蝴蝶图中的 0-XOR 构造一个（甚至更加）高效的（静态）数据结构。准确表述如下

引理 5。 如果存在一个用于度为 B 、深度至多为 d、具有 b 位比特串的 $b \geq \lg_2 d+6$ 的多个蝴蝶图中的 0-异或动态数据结构，其最坏情况更新时间为 t_u，并且能在期望 t_q 次探测内回答查询，那么就存在一个 $i \in \{d/2+1, \ldots, d\}$、一个查询集合 $\mathcal{Q} \subseteq [B^i] \times [B^i]$ （满足 $|Q| \geq B^{2i}/4$）以及一个用于度为 B 、深度为 i 的单个蝴蝶图中的 0-异或确定性静态数据结构；该数据结构具有预初始化内存，可更新 $S = O(t_u dB^{i+1})$ 个单元，并使用包含 $S_{\text{cac}} = O(t_u dB^i)$ 个单元的缓存，使得对于将 b 位比特串均匀随机赋值给输入蝴蝶图的边这一情况，有

- 对于所有查询 $q \in Q$，该数据结构都能 q 正确作答；对更新内存单元的探测次数（对 b位比特串的随机选择取期望）为 $O(t_q/d)$，总探测次数的期望 $t_{\text{总计}}$ 至多为 $O(t_q)$。

最后一步是证明针对具有预初始化内存和缓存的静态数据结构，在单个蝴蝶图中解决 0-XOR 问题的下界。这里我们证明如下结果

引理 6。 考虑度为 B、深度为 d 、使用 b位比特串的单个蝴蝶图中的0-*XOR* 问题，其中 $B \geq d^7$ 和d 至少为一个充分大的常数。假设存在一个查询子集 $\mathcal{Q} \subseteq [B^d] \times [B^d] = [n] \times [n]$，满足$|\mathcal{Q}| \geq n^2/4$，并且有一个带预初始化内存的确定性数据结构，最多更新 S 个单元，缓存大小为 S_{cac}，对于任意查询 $(s,t) \in \mathcal{Q}$，其期望总探测次数为 t_{tot}；对于任意查询 $(s,t) \in \mathcal{Q}$，其对已更新单元的探测次数期望至多为 t_q。这里两个期望均针对均匀随机输入取值。若 $S_{\text{cac}} = o(nB^{1/6}/w)$，则必有

$$t_{\text{tot}}(t_q \lg(Sw/n) + b) = \Omega((\lg n/\lg(Sw/n))^2).$$

我们将两个引理结合起来证明定理 4。考虑度为B、深度不超过 d，且比特串长度为 $b = \lg_2 d + 6$ 的多个蝴蝶图中的 0-XOR。假设存在一种数据结构，其最坏情况更新时间为 t_u，并且能够以期望 t_q 次探测回答查询。对于 $B = (dt_u w)^{12},$，我们调用引理 5，得到一个用于单个蝴蝶图中 0-XOR 的确定性静态数据结构 G_i，其度为 B、深度为 $i \geq d/2+1$，并带有预初始化内存；该结构更新 $S = O(t_u dB^{i+1})$ 个单元，并使用包含 $S_{\text{cac}} = O(t_u dB^i)$ 个单元的缓存。此外，对于 $n = B^i$，存在一个集合 $\mathcal{Q} \subseteq [n] \times [n]$，满足 $|\mathcal{Q}| \geq n^2/4$；静态数据结构对 $\mathcal{Q}$ 中的每个查询，回答时所需的期望总探测次数为 $O(t_q)$，对已更新单元的期望探测次数为 $O(t_q/d)$。这里的期望是针对将 b 位比特串均匀随机赋值给蝴蝶网络 G_i 的边而言的。

对于 $B = (dt_u w)^{12},$，我们看到 $S_{\text{cac}} = O(t_u dB^i) = O(t_u dn) = o(nB^{1/6}/w)$。因此，由引理 6 可得

$$t_q((t_q/d)\lg(Sw/n) + \lg d) = \Omega((\lg n/\lg(Sw/n))^2).$$

由于 $\lg n = d\lg B$，我们有 $\lg d \leq \lg\lg n$。因此，下界变为

$$t_q = \Omega\left(\min\left\{\frac{\sqrt{d}\lg n}{\lg^{3/2}(Sw/n)}, \frac{\lg^2 n}{\lg^2(Sw/n)\lg\lg n}\right\}\right).$$

我们还有 $Sw/n = O(t_u dB) = (t_u w)^{O(1)}$，并且 $d = \lg_B n$，因此下界变为

$$t_q = \Omega\left(\min\left\{\frac{\lg^{3/2} n}{\lg^2(t_u w)}, \frac{\lg^2 n}{\lg^2(t_u w)\lg\lg n}\right\}\right) = \Omega\left(\frac{\lg^{3/2} n}{\lg^2(t_u w)}\right).$$

由于 $n = B^i \geq B^{d/2}$和 $B > d$，我们有 $\lg n = \Omega(\lg N)$，其中 N是所有蝴蝶图中的节点总数。这就完成了定理 4 的证明。

5.1 单个蝴蝶图中的 0-XOR 到多个蝴蝶图中的 0-XOR

接下来，我们将证明，针对多个蝴蝶图中的 0-XOR 的高效动态数据结构，可以得到针对单个蝴蝶图中的 0-XOR 的高效静态数据结构。具体而言，我们将证明上述引理 5。

引理 *5* 的证明。回顾一下，在多个蝴蝶图中的 0-XOR 问题中，有 d 个深度分别为 d、……、G_1 $d-1$、、……、1 的蝴蝶图 G_d。更新分时期到达，从时期 d开始，然后依次到达 $d-1$，直至时期 1。在时期 i，我们将 G_i 边上的比特串独立地设置为均匀随机的 b比特串。令 $\mathbf{U}_i$表示给出时期 i更新的随机变量。

在时期 1 之后，我们提出一个均匀随机选择的二元组（$\mathbf{s}$，$\mathbf{t}$）$\in [B^d]\times[B^d]$作为查询。令 $\mathcal{D}$ 表示随机更新 $\mathbf{U}=\mathbf{U}_d$、……、$\mathbf{U}_1$ 与查询（$\mathbf{s}$，$\mathbf{t}$）的联合分布。

图 G_i 有 $n_i=(i+1)B^i$ 个节点和 $m_i=iB^{i+1}$ 条边，因此时期 i中有 m_i 次更新。给定一个用于多个蝴蝶图中的 0-XOR 的动态数据结构，其最坏情况更新时间为 t_u，并且在分布 $\mathcal{D}$下回答查询（$\mathbf{s}$，$\mathbf{t}$）的期望查询时间为 t_q，我们首先固定其随机性，从而得到一个确定性数据结构，使其在 $\mathcal{D}$下的期望查询时间不超过 t_q。

接下来，我们聚焦于一个时期 i，并为单个 Butterfly 中的 0-XOR 推导出一种静态数据结构。该数据结构将包含与时期 $j>i$ 中发生变化的内存单元相对应的预初始化内存，以及与时期 $j<i$中发生变化的单元相对应的缓存。更形式化地，对于支撑集 $\mathcal{D}$中的更新序列 $U=U_d,\ldots,U_1$，考虑使用确定性数据结构处理这些更新。将内存中的每个单元分配给它最后一次被更新时所属的时期。我们用 $C_i(U)$ 表示分配给时期i的单元。对于查询 (s,t)，我们用 $T(U,(s,t))$ 表示在更新 U之后回答查询 (s,t) 时探测到的单元集合。由于集合 $C_i(U)$ 两两不相交，我们有 $t_q=\mathbb{E}[\sum_{i=1}^{d}|T(\mathbf{U},(\mathbf{s},\mathbf{t}))\cap C_i(\mathbf{U})|]$。根据期望的线性性，必定存在一个时期 $i\in\{d/2+1,\ldots,d\}$，使得 $\mathbb{E}[|T(\mathbf{U},(\mathbf{s},\mathbf{t}))\cap C_i(\mathbf{U})|]\le 2t_q/d$。固定这样一个时期 i。

接下来，我们希望将这些更新 $\mathbf{U}_{\neq i}=\mathbf{U}_d,\ldots,\mathbf{U}_{i+1},\mathbf{U}_{i-1},\ldots,\mathbf{U}_1$ 固定在不同于 i 的时期中。直观地说，这将为与 G_i 对应的单个蝴蝶图中的 0-XOR 提供一种数据结构，其随机边字符串由 $\mathbf{U}_i$ 给出。

为方便记号，对于查询 (s,t)，将 $\phi_j(s,t)$ 在 G_j 上从 (s,t) 到 G_j 的查询答案定义为：若 G_j 中从 $s_j=\lfloor s/B^{d-j}\rfloor$ 到 $t_j=\lfloor t/B^{d-j}\rfloor$ 的路径上的异或结果为全 0 比特串，则答案为 1；否则令 $\phi_j(s,t)$ 为 0。因此，查询 (s,t) 的答案为 $\phi(s,t)=1-\prod_{j=1}^{d}(1-\phi_j(s,t))$。我们的目标是固定 $\mathbf{U}_{\neq i}$，使得对于大多数点对 (s,t)，我们可以根据 $\phi(s,t)$ 计算 $\phi_i(s,t)$。主要问题在于，如果任何时期 $j\neq i$ 满足 $\phi_j(s,t)=1$，那么无论 $\phi_i(s,t)$ 如何，$\phi(s,t)=1$。在这种情况下，我们称时期 j 阻塞了答案。我们将固定 $\mathbf{U}_{\neq i}$，以避免阻塞大多数查询。

对于一个查询 (s,t)，如果对于某个固定的 $U_{\neq i}$ 满足以下条件，则称其为有效查询：

1. (s,t) 未被某个时期 $j\neq i$ 阻塞。
2. $\mathbb{E}[|T(\mathbf{U},(s,t))\cap C_i(\mathbf{U})|\,|\,\mathbf{U}_{\neq i}=U_{\neq i}]\le 72t_q/d$。
3. $\mathbb{E}[|T(\mathbf{U},(s,t))|\,|\,\mathbf{U}_{\neq i}=U_{\neq i}]\le 36t_q$。

对于时期 i，有 $n=B^i$ 个源点和 n 个汇点。我们断言，存在一个固定的 $U_{\neq i}$，使得至少有 $n^2/4$ 个对 $(s_j,t_j)\in[n]\times[n]$ 满足：存在一个有效查询 (s,t)，其中 $s_j=\lfloor s/B^{d-i}\rfloor$ 且 $t_j=\lfloor t/B^{d-i}\rfloor$。为证明这一点，注意对于均匀随机的 $\mathbf{U}_{\neq i}$，任意查询 (s,t) 以 2^{-b} 的概率被时期 j 阻塞。因此，查询 (s,t) 至多以 $d2^{-b}$ 的概率被某个时期 $j\neq i$ 阻塞。于是，被阻塞查询的期望数量至多为 $d2^{-b}(B^d)^2$。马尔可夫不等式和并集界意味着，存在一个固定的 $U_{\neq i}$，使得至多有 $3d2^{-b}(B^d)^2$ 个查询被时期 $j\neq i$ 阻塞；同时，对于均匀的 $(\mathbf{s},\mathbf{t})$，我们有 $\mathbb{E}[|T(\mathbf{U},(\mathbf{s},\mathbf{t}))\cap C_i(\mathbf{U})|\,|\,\mathbf{U}_{\neq i}=U_{\neq i}]\le 6t_q/d$ 且 $\mathbb{E}[|T(\mathbf{U},(\mathbf{s},\mathbf{t}))|\,|\,\mathbf{U}_{\neq i}=U_{\neq i}]\le 3t_q$。我们断言，这样的固定 $U_{\neq i}$ 满足我们的要求。

为说明这一点，我们首先将 $\mathcal{Q}(s_j,t_j)$ 定义为满足 $s_j=\lfloor s/B^{d-i}\rfloor$和 $t_j=\lfloor t/B^{d-i}\rfloor$的所有查询 $(s,t)\in[B^d]\times[B^d]$ 的集合。现在，为了导出矛盾，假设满足存在有效查询 $(s,t)\in\mathcal{Q}(s_j,t_j)$ 这一条件的数对 $(s_j,t_j)\in[n]\times[n]$少于 $n^2/4$ 个。在此假设下，至少有 $(3/4)n^2$ 个数对 (s_j,t_j) 不存在有效查询 $(s,t)\in\mathcal{Q}(s_j,t_j)$。令 (s_j,t_j) 为任意一个这样的数对。以下三种情况必有一种成立：1）至少有 $|\mathcal{Q}(s_j,t_j)|/3$ 个查询 $(s,t)\in\mathcal{Q}(s_j,t_j)$ 被阻断；或者 2）至少有 $|\mathcal{Q}(s_j,t_j)|/3$ 个查询 $(s,t)\in\mathcal{Q}(s_j,t_j)$ 满足 $\mathbb{E}[|T(\mathbf{U},(s,t))\cap C_i(\mathbf{U})|\,|\,\mathbf{U}_{\neq i}=U_{\neq i}]>72t_q/d$；或者 3）至少有 $|\mathcal{Q}(s_j,t_j)|/3$ 个查询

$(s,\ t) \in \mathcal{Q}(s_t,\ t_j)$ 满足 $\mathbb{E}[|T(\mathbf{U},\ (s,\ t)) \cap C_i(\mathbf{U})| \mid \mathbf{U}_{\neq i} = U_{\neq i}] > 36t_q$。将第一种情况称为类型 1 失败，第二种情况称为类型 2 失败，最后一种情况称为类型 3 失败。

由此可知，以下情况至少有一种成立：1）至少有 $(1/4)n^2$ 个点对 (s_j, t_j) 出现类型 1 失败；2）至少有 $(1/4)n^2$ 个点对 (s_j, t_j) 出现类型 2 失败；或 3）至少有 $(1/4)n^2$ 个点对出现类型 3 失败。由于$|\mathcal{Q}(s_j, t_j)| = (B^{d-i})^2$,，第一种情况会产生至少 $(1/3)(1/4)(B^i)^2(B^{d-i})^2 = (1/12)(B^d)^2$ 个被阻塞的点对 (s,t)。如果令 $b \geq \lg_2 d + 6$，这与至多有 $3d2^{-b}(B^d)^2$ 个点对被阻塞相矛盾。对于第二种情况，由于 (s, t) 是均匀随机的，我们有 $\mathbb{E}[|T(\mathbf{U}, (s, t)) \cap C_i(\mathbf{U})| \mid \mathbf{U}_{\neq i} = U_{\neq i}] > (1/4)(1/3)(72t_q/d) = 6t_q/d$。这与 $\mathbb{E}[|T(\mathbf{U}, (s, t)) \cap C_i(\mathbf{U})| \mid \mathbf{U}_{\neq i} = U_{\neq i}] \leq 6t_q/d$ 相矛盾。对于第三种情况，我们有$\mathbb{E}[|T(\mathbf{U}, (s, t)) \cap C_i(\mathbf{U})| \mid \mathbf{U}_{\neq i} = U_{\neq i}] > (1/4)(1/3)(36t_q) = 3t_q$，这同样导出矛盾。

现在我们有了静态数据结构。对于固定的 $U_{\neq i}$，我们通过执行时期 $j > i$中的所有更新来预初始化内存。对于度为 B、深度为 i的单个蝴蝶图中 0-XOR 的均匀随机输入，我们注意到边字符串的分布与$\mathbf{U}_i$相同。因此，我们将单个蝴蝶图中 0-XOR 的输入视为多个蝴蝶图中 0-XOR 的时期 i 的更新。于是，我们执行$\mathbf{U}_i$中的更新，以更新部分预初始化内存单元。最后，我们执行对应于时期 $j < i$ 的固定更新 $U_{\neq i}$，并将它们修改的所有单元放入缓存。令 $\mathcal{Q}$ 为所有源汇点对 (s_j, t_j) 的集合，其中在 $\mathcal{Q}(s_j, t_j)$ 中至少存在一个有效查询 (s, t)（此集合不依赖于具体输入$\mathbf{U}_i$）。

要回答单个蝴蝶图中 0-XOR 的查询 $(s_j, t_j) \in \mathcal{Q}$，我们令 (s, t) 为 $\mathcal{Q}(s_j, t_j)$ 中字典序最小的有效查询，并直接在查询 (s, t) 上执行确定性动态数据结构的查询算法。当它请求一个单元时，我们首先检查该单元是否在缓存中（是否在时期$j < i$期间更新过）。如果是，则可以免费访问。否则，我们直接探测该单元。由于 (s, t) 有效，我们知道它未被阻塞，而且 $\mathbb{E}[|T(\mathbf{U}, (s, t)) \cap C_i(\mathbf{U})| \mid \mathbf{U}_{\neq i} = U_{\neq i}] \leq 72t_q/d$，并且 $\mathbb{E}[|T(\mathbf{U}, (s, t))| \mid \mathbf{U}_{\neq i} = U_{\neq i}] \leq 36t_q$。因此，$\mathcal{Q}$ 满足定理中的结论。由于最坏情况更新时间为 t_u，时期 i 的更新至多更新 $S = t_u m_i = t_u i B^{i+1} = O(t_u d B^{i+1})$ 个单元。根据同样的论证，缓存中至多包含 $O(\sum_{j<i} t_u d B^{j+1}) = O(t_u d B^i)$ 个单元。 □

5.2 单个蝴蝶图中的0-XOR 下界

现在，我们转而证明静态数据结构问题“单个蝴蝶图中的 0-XOR”的下界，其中数据结构具有预初始化内存和缓存。为了与上一节给出的归约相兼容，即使只能正确回答常数比例的查询，这个下界也必须成立。本节的目标是证明引理 6。

为了证明引理 6，我们希望运用模拟定理，为这样一个通信博弈构造单向协议：Alice 收到单个蝴蝶图中 0-XOR 的均匀随机输入，而 Bob 收到一个具有良好优势的均匀随机查询（$\mathbf{s}$，$\mathbf{t}$），其优势取决于 S，S_{cac}，t_{tot} 和 t_q。这样，只要证明不存在具有较大优势的此类单向协议，就能推出该引理。

然而，直接在查询集合 $\mathcal{Q} \subseteq [B^d] \times [B^d]$ 上这样做，并不能得到所需的下界。这是因为存在一种通信量低、优势高的协议。为方便记号，令$n = B^d$。为了得到我们想要的下界，基本上需要证明，没有通信量为 $n/\lg^{\Theta(1)} n$ 的协议能够达到超过 $n^{-\Omega(1)}$ 的优势。但存在一种优势高得多的简单协议（至少当 $\mathcal{Q}$ 是所有查询的集合时如此）。我们在此为感兴趣的读者概述该协议：

- Alice 选取前 $n/\lg^{\Theta(1)} n$ 个源点和汇点。由于这些路径之间存在大量重叠（各层中所访问节点的所有前导数字都以 0 开头），这些源点与汇点之间路径上的边总数为 $n/\lg^{\Theta(1)} n$。她将所有这些边上的比特串发送给 Bob。对于一个均匀随机查询（$\mathbf{s}$,$\mathbf{t}$），查询中的 $\mathbf{s}$ 和$\mathbf{t}$ 同时属于前 $n/\lg^{\Theta(1)} n$ 个源点和汇点的概率为 $1/\lg^{\Theta(1)} n$。在这种情况下，Bob 知道该查询的答案。否则，Bob 只能进行猜测。因此，优势为 $1/\lg^{\Theta(1)} n$，即远高于 $n^{-\Omega(1)}$。

我们在上述协议中利用的是，有一大类查询合在一起很容易处理，即所有满足 s 和 t 都位于前 $n/\lg^{\Theta(1)} n$ 个索引中的 $(s,\ t)$。为了解决这一问题，我们沿用以往工作的做法，引入元查询这一概念。一个元查询由一组查询指定

$T \subseteq \mathcal{Q}$，其答案是 T 中所有查询答案的异或。显然，如果一个数据结构能在期望 t_{tot} 次总探测和 t_q 次对更新单元的探测内回答每个单独的查询 $(s,\ t) \in T$，那么它也能在期望 kt_{tot} 次总探测和 kt_q 次对更新单元的探测内回答该元查询。因此，我们将定义足够分散的元查询，即计算异或所依据的路径之间不共享任何节点或边。我们在下文中将其形式化。

元查询。设 $\mathcal{Q} \subseteq [n]\times[n]$ 是查询的一个子集。根据 Q，我们构造一组元查询 $M(\mathcal{Q})$。设 $k = n/\lg_2 n$。对于每个由 k 个源汇点对 $T = \{(s_1,t_t)\ldots,(s_k,t_k)\}$组成的集合 T，只要其中各源汇点对 (s_i,t_i) 之间的唯一路径互不共享节点，我们就在 $M(\mathcal{Q})$ 中添加一个查询。查询 $T = \{(s_1,t_t)\ldots,(s_k,t_k)\}$ 的答案按如下方式得出：若 I 是单个蝴蝶图中 0-XOR 的输入，那么对于查询 $(s,t) \in \mathcal{Q}$，若沿着从 s 到 t 的路径、边权重由 I 给定时，路径上各边的比特串异或结果全为零，则令 $\psi_I(s,t)$ 为 1；否则，令 $\psi_I(s,t) = 0$。最后，令查询 T 的答案为 $\bigoplus_{(s,t)\in T}\psi_I(s,t)$。因此，该元查询的答案就是各个单独查询答案的异或。

我们首先证明，如果 $\mathcal{Q}$ 很大，那么 $M(\mathcal{Q})$ 也很大

引理 7。 对于任意满足 $|\mathcal{Q}| \geq n^2/4$ 的 $\mathcal{Q} \subseteq [n]\times[n]$，如果 n 和 B 至少是某些足够大的常数，那么我们有 $|M(\mathcal{Q})| \geq n^k/9$。

证明。 我们给出一个概率论证。考虑一个固定的元查询 $T \in M(\mathcal{Q})$，满足 $T = \{(s_i,t_i)\}_{i=1}^{k}$。现在令 $T' = (s'_1,t'_1)\ldots,(s'_{10k},t'_{10k})$ 为一个有序列表，其中包含 $10k$ 个均匀且相互独立的源汇点对。我们证明两件事。首先，我们论证，(s_i,t_i) 中的所有源汇对都属于 T' 中的查询的概率极小。其次，我们论证，T' 很可能包含一个由 k 个查询构成的子集 T''，使得 $T'' \in M(\mathcal{Q})$。只有当 $M(\mathcal{Q})$ 很大时，这两件事才可能同时成立。

对于第一部分，注意，对于固定的 T，满足 $T \subseteq T'$ 的 T' 至多有 $\binom{10k}{k}k!(n^2)^{9k}$ 种选择。$\binom{10k}{k}$ 项对应列表 T' 中出现 T 的位置，$k!$ 表示这些位置的所有排列，而 $(n^2)^{9k}$ 则对应 T' 中选定的 k 个位置之外的查询。对于均匀随机的 T'，共有 $(n^{2\ 10k} \quad T' \quad T \subseteq T' \quad \binom{10k}{k}k\ n^{-2k} =)$ $n^{-2k}\ 10k\ /\ 9k\ \leq n^{-2k}\ 10k\ ^k = 10k/n^{2\ k} = 10/\ n\ _2 n\ ^k \quad n \geq 2^{10} \quad n^{-k}$ 种选择，因此该概率的上界为 ! ( )! ( )! ( ) ( ) ((lg)) 。对于，这至多为 。

对于第二部分，对 T' 中的每一对 (s'_i,t'_i)，定义一个指示变量 X_i。若 $(s'_i,t'_i) \in \mathcal{Q}$，且从 s'_i 到 t'_i 的蝴蝶网络唯一路径与任意其他一对 (s'_j,t'_j)（其中 (s'_j,t'_j) 属于 T'）之间的路径不共享任何节点，则该指示变量取值为 1。我们首先说明 $\mathbb{E}[X_i]$ 很大。为此，先注意到 $\Pr[(s'_i,t'_i) \in \mathcal{Q}] \geq 1/4$。接下来，考虑一对满足 $i \neq j$ 的 (s'_j,t'_j)。对于蝴蝶网络的任意一层 ℓ，两条路径所经过节点的分布均为均匀随机，且二者相互独立。因此，它们在 $d+1$ 层中的任意一层经过同一节点的概率至多为 $(d+1)/B^d = (d+1)/n = (\lg_B n)/n$。对 $10k-1$ 种 j' 选择应用并集界可知，从 s'_i 到 t'_i 的路径与其他任意一条路径相交的概率至多为 $10k(\lg_B n)/n = 10/\lg_2 B$。当 B 大于某个常数时，这个概率至多为 $1/100$。由此可得 $\Pr[X_i = 1] \geq 1/4 - 1/100 = 24/100$。因此，$\mathbb{E}[\sum_i X_i] \geq 10k(24/100) = (24/10)k > 2k$。现在考虑随机变量 $Y = 10k - \sum_i X_i$。这是一个非负随机变量，其期望至多为 $8k$。因此，根据马尔可夫不等式，我们有 $\Pr[Y > 9k] < 8/9$。也就是说，$\Pr[\sum_i X_i < k] < 8/9$。但是，任取一组 k 对 (s'_i,t'_i)，其中每一对都满足 $X_i = 1$，便可得到一个集合 $T'' \in M(\mathcal{Q})$。因此，以至少 $1/9$ 的概率存在一个 T''。

现在我们结合上述两点，给 $|M(\mathcal{Q})|$ 导出一个下界。为此，注意到随机的 T' 包含一个 $T'' \in M(\mathcal{Q})$，但又不包含任何 $T \in M(\mathcal{Q})$ 的概率包含在 T' 中时，该概率为 0（这两者相互矛盾）。然而，并集界意味着该事件的概率至少为 $1/9 - |M(\mathcal{Q})|n^{-k}$。因此必有 $|M(\mathcal{Q})| \geq n^k/9$。 □

元查询通信博弈。 定义了元查询之后，我们就可以将问题归约为一个单向通信博弈。假设我们有一个满足引理 6 要求的单个 Butterfly 中的 0-XOR 数据结构。设 $\mathcal{Q} \subseteq [n]\times[n]$ 为至少包含 $n^2/4$ 个查询的承诺集合，且 M（$\mathcal{Q}$）为相应的元查询。设 $\mathcal{I}$ 为将 b 位比特串赋值给度为 B 、深度为 d 的蝴蝶网络的所有可能赋值集合。

现在，我们定义一个权重为 $M(\mathcal{Q}) \times \mathcal{I} \to [-1,1]$ 的数据结构问题 $\mathcal{P}$。对于查询 $(s,\ t) \in M(\mathcal{Q})$，定义 $\phi_I(s,\ t)$ 为 $-(1-2^{-b})$，当且仅当 $\psi_I(s,\ t) = 1$；否则，将其定义为 2^{-b}。现在定义

$$\mathcal{P}(T, I) := \prod_{(s,t)\in T} \phi_I(s,t)$$

关于 $\mathcal{P}$，我们可以作出几点观察。首先，始终有 $|\mathcal{P}(T,I)| \geq 2^{-kb}$。其次请注意，如果一个数据结构能够计算出对元查询 Ton $M(\mathcal{Q})$ 的答案 $\bigoplus_{(s,t)\in T} \psi_T(s,t)$，那么它也能计算出 $\mathcal{P}(T,I)$ 的符号。这是因为，$\mathcal{P}(T,I)$ 的符号等于 $(-1)^{\sum_{(s,t)\in T} \psi_I(s,t)}$，而这可以由 $\sum_{(s,t)\in T} \psi_I(s,t)$ 的奇偶性确定；后者等于 $\bigoplus_{(s,t)\in T} \psi_I(s,t)$。

令 $\mathcal{D}_{M(\mathcal{Q})} \times \mathcal{D}_{\mathcal{I}}$ 为定义在 $M(\mathcal{Q}) \times \mathcal{I}$ 上的乘积分布，它生成均匀随机的$\mathbf{T} \in M(\mathcal{Q})$，以及在 $\mathcal{I}$ 中均匀随机的$\mathbf{I}$。注意，对于每个 $T \in M(\mathcal{Q})$，都有 $\mathbb{E}_{\mathbf{I}}[\mathcal{P}(T,\mathbf{I})] = 0$。这是因为 T 中的 $^-$ 条路径互不相交，因此每条路径异或后恰好得到全零位串 0 的概率为 2^{-b}，且这些事件彼此独立。因此我们有

$$\begin{aligned}
\mathop{\mathbb{E}}_{\mathbf{I}}[\mathcal{P}(T,\mathbf{I})] &= \mathop{\mathbb{E}}_{\mathbf{I}}\left[\prod_{(s,t)\in T} \left(1_{\psi_{\mathbf{I}}(s,t)=1} \cdot (-(1-2^{-b})) + 1_{\psi_{\mathbf{I}}(s,t)=0} \cdot 2^{-b}\right)\right] \\
&= \prod_{(s,t)\in T} \mathop{\mathbb{E}}_{\mathbf{I}}\left[1_{\psi_{\mathbf{I}}(s,t)=1} \cdot (-(1-2^{-b})) + 1_{\psi_{\mathbf{I}}(s,t)=0} \cdot 2^{-b}\right] \\
&= \prod_{(s,t)\in T} \left(2^{-b} \cdot (-(1-2^{-b})) + (1-2^{-b}) \cdot 2^{-b}\right) \\
&= 0.
\end{aligned}$$

现在注意，满足引理 6 中假设的数据结构可以回答任意元查询 $T \in M(\mathcal{Q})$，其探测次数的期望总数为 kt_{tot}，对更新单元的探测次数期望为 kt_q，其中期望是对随机 $\mathbf{I} \sim \mathcal{D}_{\mathcal{I}}$ 取的。这是因为 T 中的每个单独查询都可以用期望为 t_{tot} 的总探测次数和对更新单元期望为 t_q 的探测次数来回答。

现在我们希望调用定理 2，为 $G_{\mathcal{P}}$ 得到一个单向协议。我们看到可以选择$\beta = 2^{-kb}$。对于任意 $p \in (0,1)$，定理 2 现在给出一个针对 $G_{\mathcal{P}}$ 的单向协议，该协议在乘积分布$\mathcal{D}_{M(\mathcal{Q})} \times \mathcal{D}_{\mathcal{I}}$ 下满足

$$\begin{aligned}
\mathrm{adv}(G_{\mathcal{P}}, \mathcal{D}_{M(\mathcal{Q})}, \mathcal{D}_{\mathcal{I}}, (8pS + S_{\mathrm{cac}}) \cdot w) &\geq 2^{-O(\sqrt{kt_{\mathrm{tot}}(kt_q \lg 1/p + kb)} \cdot \lg 1/p)} - 2^{-\Omega(pS)} \\
&= 2^{-O(k\sqrt{t_{\mathrm{tot}}(t_q \lg 1/p + b)} \cdot \lg 1/p)} - 2^{-\Omega(pS)}.
\end{aligned}$$

剩下要证明的是，没有协议能够拥有很大的优势。以下引理给出了这一点。

引理 8. 存在一个绝对常数 $c > 0$，使得对于 $B \geq d^7$，且当 d 至少为一个充分大的常数时，针对 $G_{\mathcal{P}}$ 的任意协议要么至少发送 $cnB^{1/6}$ 位，要么在 $\mathcal{D}_{M(\mathcal{Q})} \times \mathcal{D}_{\mathcal{I}}$ 下的优势至多为 $\exp(-ck \lg n)$。

在证明引理 8 之前，我们先用它完成引理 6 的证明。取 $p = c'n/(Sw)$，其中 $c' > 0$ 是一个足够大的常数。在这种情况下，$8pSw$ 通信小于 $cn/2$，因此我们得出，要么 $S_{\mathrm{cac}} = \Omega(nB^{1/6}/w)$，要么

$$k\sqrt{t_{\mathrm{tot}}(t_q \lg(Sw/n) + b)} \cdot \lg(Sw/n) = \Omega(k \lg n + n/w) = \Omega(k \lg n).$$

由此得到下界

$$t_{\mathrm{tot}}(t_q \lg(Sw/n) + b) = \Omega((\lg n / \lg(Sw/n))^2).$$

正如引理 6 所述。

因此，剩下要做的就是证明通信下界。

引理 8 的证明。设 $\mathcal{Q} \subseteq [n] \times [n]$ 具有 $|\mathcal{Q}| \geq n^2/4$，令 $M(\mathcal{Q})$ 为相应的元查询，并令 $\mathcal{P}$： $M(\mathcal{Q}) \times \mathcal{I} \to [-1,1]$ 为带权重的数据结构问题，其中 $\mathcal{I}$ 是将 b 位比特串赋值给一个度为 B、深度为 d 且具有 $n = B^d$ 的蝴蝶网络的所有赋值集合。令 $\mathcal{D}_{M(\mathcal{Q})} \times \mathcal{D}_{\mathcal{I}}$ 为以下乘积分布：在 $M(\mathcal{Q})$ 中均匀随机选取 $\mathbf{T}$，并在 $\in \mathcal{I}$ 中均匀随机选取 $\mathbf{I}$。

假设存在一个单向协议 $\pi : \mathcal{I} \to \{0,1\}^m$，用于通信博弈 $G_{\mathcal{P}}$，其优势为 ε，且通信量为 m 个通信比特。对于 Alice 可能发送的任意消息 A，令 $\chi_A \in \{-1,1\}^{|M(\mathcal{Q})|}$ 为一个向量，每个 $T \in M$ 对应一个分量（$\mathcal{Q}$）。分量 χ_A（T）的取值为 $\mathrm{sign}(\mathbb{E}_{\mathbf{I}}[\mathcal{P}(T, \mathbf{I}) \mid \pi(\mathbf{I}) = A])$。类似地，定义向量 $P_I \in [-1,1]^{|M(\mathcal{Q})|}$，其中与一个 $T \in M$（$\mathcal{Q}$）对应的分量取值为 $\mathcal{P}(T, I)$。

根据优势的定义，我们有

$$\varepsilon = |M(\mathcal{Q})|^{-1} \mathop{\mathbb{E}}_{\mathbf{I}}[\langle P_{\mathbf{I}}, \chi_{\pi(\mathbf{I})} \rangle].$$

我们先将注意力限制在一个具体消息 A 及其对应的向量 χ_A 上。我们声称，必定存在一条消息 A，使得以下两项同时成立

- $\mathbb{E}_{\mathbf{I}}[\langle P_{\mathbf{I}}, \chi_{\pi(\mathbf{I})} \rangle \mid \pi(\mathbf{I}) = A] \geq (\varepsilon/2)|M(\mathcal{Q})|$.
- $\Pr_{\mathbf{I}}[\pi(\mathbf{I}) = A] \geq (\varepsilon/2)2^{-m}$.

为说明这一点，反设不存在这样的消息。于是我们有

$$\begin{aligned}
|M(\mathcal{Q})|\varepsilon &= \mathop{\mathbb{E}}_{\mathbf{I}}[\langle P_{\mathbf{I}}, \chi_{\pi(\mathbf{I})} \rangle] \\
&= \sum_{A \in \{0,1\}^m} \Pr_{\mathbf{I}}[\pi(\mathbf{I}) = A] \mathop{\mathbb{E}}_{\mathbf{I}}[\langle P_{\mathbf{I}}, \chi_{\pi(\mathbf{I})} \rangle \mid \pi(\mathbf{I}) = A] \\
&= \sum_{A \in \{0,1\}^m : \Pr_{\mathbf{I}}[\pi(\mathbf{I}) = A] < (\varepsilon/2)2^{-m}} \Pr_{\mathbf{I}}[\pi(\mathbf{I}) = A] \mathop{\mathbb{E}}_{\mathbf{I}}[\langle P_{\mathbf{I}}, \chi_{\pi(\mathbf{I})} \rangle \mid \pi(\mathbf{I}) = A] \\
&+ \sum_{A \in \{0,1\}^m : \Pr_{\mathbf{I}}[\pi(\mathbf{I}) = A] \geq (\varepsilon/2)2^{-m}} \Pr_{\mathbf{I}}[\pi(\mathbf{I}) = A] \mathop{\mathbb{E}}_{\mathbf{I}}[\langle P_{\mathbf{I}}, \chi_{\pi(\mathbf{I})} \rangle \mid \pi(\mathbf{I}) = A] \\
&< \sum_{A \in \{0,1\}^m : \Pr_{\mathbf{I}}[\pi(\mathbf{I}) = A] < (\varepsilon/2)2^{-m}} (\varepsilon/2)2^{-m} \mathop{\mathbb{E}}_{\mathbf{I}}[\|P_{\mathbf{I}}\|_1 \mid \pi(\mathbf{I}) = A] \\
&+ \sum_{A \in \{0,1\}^m : \Pr_{\mathbf{I}}[\pi(\mathbf{I}) = A] \geq (\varepsilon/2)2^{-m}} \Pr_{\mathbf{I}}[\pi(\mathbf{I}) = A](\varepsilon/2)|M(\mathcal{Q})| \\
&\leq 2^m(\varepsilon/2)2^{-m}|M(\mathcal{Q})| + (\varepsilon/2)|M(\mathcal{Q})|,
\end{aligned}$$

也就是说，这就产生了矛盾。因此，固定这样一条消息 A，并令 $\mathcal{I}' \subseteq \mathcal{I}$ 为满足 $\pi(I) = A$ 的输入 I 的子集。那么 $|\mathcal{I}'| \geq (\varepsilon/2)\, 2^{-m}|\mathcal{I}|$，对于均匀随机的 $\mathbf{I}' \in \mathcal{I}'$，我们有 $\mathbb{E}_{\mathbf{I}'}[\langle P_{\mathbf{I}'}, \chi_A \rangle] \geq (\varepsilon/2)\,|M(\mathcal{Q})|$。

我们证明，对于任意 $\chi \in \{-1,1\}^{|M(\mathcal{Q})|}$，

$$\mathop{\mathbb{E}}_{\mathbf{I}'}[\langle P_{\mathbf{I}'}, \chi \rangle]$$

当 $\mathcal{I}'$ 较大时，它必须较小。为此，考虑以下 r 阶矩，其中 $r \geq 2$ 是一个待确定的偶整数。这里的期望是对 $\mathcal{I}$ 中均匀 $\mathbf{I}$ 取值的：

$$\begin{aligned}
\mathop{\mathbb{E}}_{\mathbf{I}}[\langle P_{\mathbf{I}}, \chi \rangle^r] &= \\
\sum_{T_1, \ldots, T_r} \prod_{i=1}^{t} \chi(T_i) \cdot \mathop{\mathbb{E}}_{\mathbf{I}} \left[\prod_{i=1}^{r} P_{\mathbf{I}}(T_i) \right] &\leq \\
\sum_{T_1, \ldots, T_r} \left| \mathop{\mathbb{E}}_{\mathbf{I}} \left[\prod_{i=1}^{r} P_{\mathbf{I}}(T_i) \right] \right| &= \\
\sum_{T_1, \ldots, T_r} \left| \mathop{\mathbb{E}}_{\mathbf{I}} \left[\prod_{i=1}^{r} \prod_{(s,t) \in T_i} \phi_{\mathbf{I}}(s,t) \right] \right|. &
\end{aligned}$$

现在考虑一个对应于某些 $T_1, \ldots, T_r$ 的项。每个查询 $(s,t) \in T_1 \cup \cdots \cup T_r$ 都指定了一条源汇路径。假设存在一条边 e，它恰好出现在这些路径中的一条上，并令 $(s^\star, t^\star)$ 为对应的查询。那么，$\phi_{\mathbf{I}}(s^\star, t^\star)$ 与所有其他 $\phi_{\mathbf{I}}(s,t)$ 独立，因为即使在给定分配给除 e 以外所有边的比特串的条件下，沿着 s-t 路径的异或仍然是均匀随机的。因此，对于这样的 $T_1, \ldots, T_r$，我们有

$$\mathop{\mathbb{E}}_{\mathbf{I}}\left[\prod_{i=1}^{r}\prod_{(s,t)\in T_i}\phi_{\mathbf{I}}(s,t)\right] =$$

$$\mathop{\mathbb{E}}_{\mathbf{I}}[\phi_{\mathbf{I}}(s^\star,t^\star)]\mathop{\mathbb{E}}_{\mathbf{I}}\left[\prod_{i=1}^{r}\prod_{(s,t)\in T_i\setminus\{(s^\star,t^\star)\}}\phi_{\mathbf{I}}(s,t)\right] = 0.$$

另一方面，如果每条出现在一条 s-t 路径中的边都至少出现两次，那么

$$\left|\mathop{\mathbb{E}}_{\mathbf{I}}\left[\prod_{i=1}^{r}\prod_{(s,t)\in T_i}\phi_{\mathbf{I}}(s,t)\right]\right| \le 1.$$

因此，如果 Γ 表示满足以下条件的列表 $T_1, \ldots, T_r \in M(\mathcal{Q})^r$ 的数量：对于所有元查询 $T_1, \ldots, T_r$中的所有查询，每条 e 中的边 G_i 在任意 s-t 查询路径中出现零次或至少两次，那么

$$\mathop{\mathbb{E}}_{\mathbf{I}}[\langle P_{\mathbf{I}}, \chi\rangle^r] \le \Gamma.$$

利用 $\Pr_{\mathbf{I}}[\mathbf{I} \in \mathcal{I}'] = |\mathcal{I}'|/|\mathcal{I}|$ 以及 $\langle P_I, \chi\rangle^r$ 的非负性，我们进一步得到，对于 $\mathcal{I}'$ 中均匀的 $\mathbf{I}'$，

$$\mathop{\mathbb{E}}_{\mathbf{I}'}[\langle P_{\mathbf{I}}, \chi\rangle^r] = \mathop{\mathbb{E}}_{\mathbf{I}}[\langle P_{\mathbf{I}}, \chi\rangle^r \mid \mathbf{I} \in \mathcal{I}'] \le \Gamma|\mathcal{I}|/|\mathcal{I}'|.$$

因此必然有

$$\mathop{\mathbb{E}}_{\mathbf{I}'}[\langle P_{\mathbf{I}'}, \chi\rangle] \le \Gamma^{1/r}(|\mathcal{I}|/|\mathcal{I}'|)^{1/r}.$$

但我们已经证明，存在一个 χ_A，使得 $\mathbb{E}_{\mathbf{I}'}[\langle P_{\mathbf{I}'}, \chi_A\rangle] \ge (\varepsilon/2)|M(\mathcal{Q})|$，而 $|\mathcal{I}'| \ge (\varepsilon/2)2^{-m}|\mathcal{I}|$。因此我们得出

$$(\varepsilon/2)|M(\mathcal{Q})| \le \Gamma^{1/r}(\varepsilon^{-1}2^{m+1})^{1/r}.$$

对于 $r \ge 8$，这意味着

$$(\varepsilon/2)^{1+1/r} \le |M(\mathcal{Q})|^{-1}\Gamma^{1/r}2^{m/r} \Rightarrow \varepsilon \le 2|M(\mathcal{Q})|^{-8/9}\Gamma^{1/r}2^{m/r}.$$

根据引理 7，我们有 $|M(\mathcal{Q})| \ge n^k/9$，因此

$$\varepsilon \le 18n^{-8k/9}\Gamma^{1/r}2^{m/r}.$$

因此，剩下的就是选取 r 并对 Γ给出上界。为此，注意到任意一个 $T_1, \ldots, T_r$，其中每条边在查询路径中出现的次数要么为零，要么至少为两次，都可以唯一地描述如下：首先，指定一个边集 E，使得所有查询路径只使用 E中的边。由于有 rk 条长度为 d的查询路径，且每条边出现的次数要么为零，要么至少为两次，因此存在一个这样的集合 E，其基数仅为 $rkd/2$。指定这样的边集后，每个 T_i 都可以通过将其 kd 条边指定为 E的子集来唯一确定。这是因为同一个元查询中的所有查询路径都不共享节点或边。因此，知道路径中出现的边集，就能唯一确定 T_i中的整个查询集合。这正是我们利用元查询分布良好的地方。回想 $k = n/\lg_2 n$ 和 $n = B^d$，由此我们得到

$$\Gamma \le \binom{dB^{d+1}}{rkd/2}\binom{rkd/2}{kd}^r \le \left(\frac{2eB^{d+1}}{rk}\right)^{rkd/2}\left(\frac{er}{2}\right)^{rkd} = \left(\frac{e^3rB^{d+1}}{2k}\right)^{rkd/2} = \left(\frac{e^3rB\lg_2 n}{2}\right)^{rkd/2}$$

现在固定 $r = B^{1/6}$，并假设 $B \geq d^7$ 和 d 至少是一个充分大的常数。对于这样的 B 和 d，有 $(e^3 \lg_2 n)$ $= (e^3 d \lg_2 B) \leq B^{1/3}$。于是我们得到

$$\Gamma \leq (B^{3/2})^{rkd/2} = B^{(3/4)rk \lg_B n} = 2^{(3/4)rk \lg_2 n} = n^{(3/4)rk}.$$

代入上式后，我们得出

$$\varepsilon \leq 18n^{-8k/9} n^{(3/4)k} 2^{m/r} \leq 18n^{-k/9} 2^{m/r} \leq 18n^{-k/9} 2^{m/B^{1/6}}.$$

由于 $k = n/\lg_2 n$，我们得出存在一个常数 $c > 0$，使得 $m \geq cnB^{1/6}$ 或者 $\varepsilon \leq \exp(-ck \lg n)$。

□

6 延后的模拟定理证明

本节给出定理 2 的延后证明。在证明中，我们将用到 Larsen、Weinstein 和 Yu 提出的峰均引理:

引理 9 (峰均引理 [10])**.** 设 $f\colon \Sigma^k \to \mathbb{R}$ 是定义在字母表Σ上的所有长度为k 的字符串上的任意实值函数，满足:

1. $\sum_{z \in \Sigma^k} |f(z)| \leq 1$; 以
及 *2.* 最大值$_{z \in \Sigma^k} |f(z)$
$| \geq \varepsilon$

因此 些 $\varepsilon \in (0, 1]$。于是存在一个索引子集 Y，使得 $|Y| \leq O(\sqrt{k \cdot \lg(1/\varepsilon)}$，满足 t

$$\sum_{y \in \Sigma^Y} \left| \sum_{z|_Y = y} f(z) \right| \geq \exp(-\sqrt{k \cdot \lg(1/\varepsilon)}).$$

注意， [10] 中所述的引理要求满足 $\varepsilon \geq 2^{-O(k)}$。不过，当$\varepsilon \leq 2^k$时，该命题显然成立，因为我们只需令 $Y = [k]$，便有

$$\sum_{y \in \Sigma^Y} \left| \sum_{z|_Y = y} f(z) \right| = \sum_z |f(z)| \geq \varepsilon.$$

下面给出定理 2 的证明

定理 *2* 的证明。 由马尔可夫不等式和并集界可知，对于随机 $Q \in \mathcal{D}_Q$，以概率 $1/2$，我们有

$$\mathop{\mathbb{E}}_I [t_{\text{tot}}(Q, I)] \leq 4t_{\text{tot}} \qquad \text{and} \qquad \mathop{\mathbb{E}}_I [t_q(Q, I)] \leq 4t_q.$$

将这组查询记为 $\mathcal{Q}'$。由于 (1) 是非负项的期望，只需证明 $Q \in \mathcal{Q}'$ 的下界。因此，不失一般性，我们可以假设对每个 Q， t_{tot} 和 t_q 都是随机输入下期望时间的上界，而这只会损失常数因子。

为了构造具有较大优势的协议，我们采用与 [10]模拟数据结构D 相似的策略。首先，让 Alice 在 I 上模拟 D 的预处理算法。然后，Alice 以 p 的概率对每个已更新单元进行抽样，并将抽样得到的单元发送给 Bob，记为 C_0。接着，Alice 使用公共随机性以 p 的概率对每个单元进行抽样，并将抽样得到的单元中哪些已更新及其内容告知 Bob。将这组抽样单元记为 C_1。最后，Alice 将缓存中的所有单元发送给 Bob，记为 C_2。三元组 (C_0, C_1, C_2) 构成该消息。协议的正式描述见图5。

用于 $G_{\mathcal{P}}$ 的单向协议 π

"发送一个单元"是指发送该单元的地址和内容。我们用 $C \leftarrow z$ 表示内存单元 C 的内容为 z。

1. Alice 通过在 I 上模拟该数据结构，生成 D 的内存状态和缓存。
2. Alice 以概率 p 独立地对每个已更新单元进行采样。令 C_0 为采样得到的集合单元。如果 $|C_0| \geq 2pS$，Alice 发送比特 0 并中止。否则，她发送比特 1，随后发送所有 C_0 中的单元。
3. Alice 使用公共随机性 以概率 p独立抽取每个单元 。令 C_1 为抽样单元格的集合。如果 C_1 中至少有 $2pS$ 个已更新 单元，Alice 发送比特 0 并中止。否则，她发送比特 1，随后发送 C_1 中所有已更新 单元。
4. Alice 将缓存中的所有单元发送给 Bob。将这组单元记为 C_2。

（仅用于分析：）

5. Bob 生成 D 的预初始化内存 M_0 。Bob 更新 M_0 中 C_0 的内容，并更新缓存 C_2，获得内存状态 M'，然后模拟 D 的查询算法，对使用内存状态 M' 查询 Q 。令 C_{sim} 为 D 在在此模拟中。
6. 应用引理 9，其中 $\Sigma := [2^w]$, $k := |C_{\mathrm{sim}}|$， $\varepsilon := \beta \cdot p^{4t_q}/4$，以及

$$f(z) := \Pr_I[C_{\mathrm{sim}} \leftarrow z \mid C_0, C_2] \cdot \mathop{\mathbb{E}}_I[\mathcal{P}(Q, I) \mid C_{\mathrm{sim}} \leftarrow z, C_0, C_2]\,.$$

如果满足引理前提且 $k \leq 4t_{\mathrm{tot}}$，令 $Y \subset C_{\mathrm{sim}}$ 为一个大小为 κ 的单元子集：$=|Y| \leq O\left(\sqrt{t_{\mathrm{tot}}(t_q \lg 1/p + \lg 1/\beta)}\right)$，根据引理，该子集必定存在。

图5：数据结构 D 的单向弱模拟协议。

通信成本。 根据算法的描述，Alice 仅在 C_0 包含的单元少于 $2pS$ 个时才发送它，并且仅在 C_1 包含的已更新 单元少于 $2pS$ 个时才发送它。因此，发送 C_0 和 C_1 最多需要 $(4pS-2)\cdot 2w$ 位（因为发送地址或内容需要 w 位）。另一方面，发送 C_2 最多需要 $S_{\mathrm{cac}}\cdot w$ 位。因此，总通信量最多为

$$(4pS-2)\cdot 2w+2+S_{\mathrm{cac}}\cdot w\le(8pS+S_{\mathrm{cac}})\cdot w$$

位，如所述。

我们还注意到，根据切尔诺夫界，$|C_0|\ge 2pS$ 发生的概率至多为 $2^{-\Omega(pS)}$，而 C_1 至少有 $2pS$ 个更新单元的概率也至多为 $2^{-\Omega(pS)}$。由于 $|\mathcal{P}(Q,\ I)|\le 1$，这两个事件最多只会使优势降低 $2^{-\Omega(pS)}$。接下来，我们假设 Alice 总是发送 C_0 以及 C_1 中的更新单元，不论它们的大小如何，并证明该协议的优势至少为

$$2^{-O(\sqrt{t_{\mathrm{tot}}(t_q\lg 1/p+\lg 1/\beta)}\cdot\lg 1/p)},$$

这将推出该定理。

优势分析。 考虑抽样单元格 C_0。对于每个查询 Q，令 $\mathcal{W}_Q$ 表示 C_0 包含所有满足以下条件的更新单元： Q 探测。于是我们知道

$$\Pr_{C_0,I}[\mathcal{W}_Q]\ge p^{4t_q}\cdot\Pr_I[t_q(Q,I)\le 4t_q]\ge p^{4t_q}/4.$$

如果 Bob 知道 $\mathcal{W}_Q$ 是否发生（也就是说，如果 $\mathcal{W}_Q$ 是 Q 和 Alice 的消息 $C_0,\ C_2$ 的函数），那么问题就解决了：当 $\mathcal{W}_Q$ 发生时，Bob 掌握了足够的信息，可以在查询 Q 上模拟查询算法，因此 Bob 知道查询输出，也就是 $\mathcal{P}$ 的符号 $(Q,\ I)$。也就是说，在给定 $(C_0,\ C_2)$ 以及使 $\mathcal{W}_Q$ 发生的 Q 的条件下， $\mathcal{P}(Q,\ I)$ 的符号是固定的，并且我们有

$$\left|\mathop{\mathbb{E}}_I[\mathcal{P}(Q,I)\mid C_0,C_2]\right|=\mathop{\mathbb{E}}_I[|\mathcal{P}(Q,I)|\mid C_0,C_2]\ge\beta.$$

在这种情况下，我们有

$$\mathop{\mathbb{E}}_{Q,C_0,C_2}\left[\left|\mathop{\mathbb{E}}_I[\mathcal{P}(Q,I)\mid C_0,C_2]\right|\right]\ge\Pr[\mathcal{W}_Q]\cdot\mathop{\mathbb{E}}_{Q,C_0,C_2|\mathcal{W}_Q}\left[\left|\mathop{\mathbb{E}}_I[\mathcal{P}(Q,I)\mid C_0,C_2]\right|\right]\ge\Omega(\beta\cdot p^{4t_q}),$$

其中，第一个不等式利用了这一假设： $\mathcal{W}_Q$ 由 Q 和 C_0、C_2确定。这一优势远大于我们所声称的优势。

然而，Bob没有足够的信息来确定 Q 探测到的所有更新单元是否都在 C_0中被采样。这是因为，对于不在 C_0 （或 C_2）中的单元，Bob无法判断它们是已更新但未被采样，还是未更新且仍保留着预初始化内容。Bob可以做的是生成预初始化内存，并更新 C_0 和 C_2中的所有单元，然后在此内存状态下模拟 Q 上的查询算法（见图5中的第5步）。这种模拟可能出错，因为Bob可能没有必要单元的正确内容。模拟甚至可能探测错误的单元，因为查询算法可能是自适应的。

不过，令 C_{sim} 为此次模拟中探测到的单元集合。现在固定 $\mathsf{addr}(C_{\mathrm{sim}})$，即 C_{sim}的地址，并考虑 Bob 视图中真实 内容的后验分布，即 $\mathsf{cont}(C_{\mathrm{sim}})\mid C_0,\ C_2$.[1] 由于 $\mathcal{W}_Q$ 确实以非平凡概率发生，因此此次模拟实际上正确的概率也非平凡。令 z^* 为 Bob 用于模拟的 C_{sim} 的内容。这意味着平均而言，在此后验分布中， z^* 比大多数其他内容稍微更有可能。此外，当 C_{sim} 的真实内容为 z^*时，在给定 $C_{\mathrm{sim}}\leftarrow z^*$ 的条件下， $\mathcal{P}(Q,\ I)$的期望绝对值至少为 β（此时 $\mathcal{P}(Q,\ I)$的符号已确定）。我们定义函数 f，它将 C_{sim} 的可能内容映射到 $\mathbb{R}$，其值为在给定

[1]我们用 $\mathsf{addr}(C)$ 表示单元 C的地址，用 $\mathsf{cont}(C)$ 表示单元 C的内容。

该内容的条件下，对 (,)（即优势）按后验分布中的概率加权所得的期望（步骤 6）。于是， f 在 z^*处取得高于平均水平的（绝对）值。峰均引理（引理 9）保证存在一个较小的子集$Y \subseteq C_{\mathrm{sim}}$ ，使得知道 Y 的内容能够带来非平凡优势。我们进一步让 Alice 发送另一个随机集合 C_1 （步骤 3）。优势的最终下界来自事件 Y 包含于 C_1。在这种情况下，Bob 可以识别该事件，因为他能够计算 Y。此外，由于 Y 很小，该事件以非平凡概率发生；而一旦发生，根据引理 9，优势便是非平凡的。形式化论证如下。

固定 Q ，并考虑一个随机的 I。关于 Q 查询时间的假设（因为我们只考虑$Q \in \mathcal{Q}'$）保证了

$$\mathop{\mathbb{E}}_{I}[t_{\mathrm{tot}}(Q,I)] \le t_{\mathrm{tot}} \qquad \text{and} \qquad \mathop{\mathbb{E}}_{I}[t_q(Q,I)] \le t_q.$$

根据马尔可夫不等式和并集界，我们以至少 $1/2$ 的概率（对 I 的随机性而言）有 $t_{\mathrm{tot}}(Q,\ I) \le 4t_{\mathrm{tot}}$ ，以及 $t_q(Q,\ I) \le 4t_q$ 。在这种情况下， $\mathcal{W}_Q$ (C_0 包含Q 探测到的所有更新单元)的概率为

$$\Pr_{C_0,I}[\mathcal{W}_Q \mid t_{\mathrm{tot}}(Q,I) \le 4t_{\mathrm{tot}}, t_q(Q,I) \le 4t_q] \ge p^{4t_q}.$$

因此，我们有

$$\Pr_{C_0,I}[\mathcal{W}_Q \wedge t_{\mathrm{tot}}(Q,I) \le 4t_{\mathrm{tot}}] \ge \Pr_{C_0,I}[\mathcal{W}_Q \wedge t_{\mathrm{tot}}(Q,I) \le 4t_{\mathrm{tot}} \wedge t_q(Q,I) \le 4t_q] \ge p^{4t_q}/2. \tag{2}$$

现在，对于查询 Q，如果模拟给出 $|C_{\mathrm{sim}}| \le 4t_{\mathrm{tot}}$，且事件$\mathcal{W}_Q$ 在给定该对的条件下发生的概率为“并非太小”：$\Pr_I[\mathcal{W}_Q \mid C_0, C_2] \ge p^{4t_q}/4$，则称一对 ($C_0$，$C_2$) 对查询 Q 是良好的 。根据（2）、马尔可夫不等式以及 C_2 由 I决定这一事实，我们有

$$\Pr_{C_0,C_2}\left[\Pr_{I}[\mathcal{W}_Q \wedge t_{\mathrm{tot}}(Q,I) \le 4t_{\mathrm{tot}} \mid C_0, C_2] \ge p^{4t_q}/4\right] \ge p^{4t_q}/4.$$

这意味着 (C_0，C_2) 以至少 $p^{4t_q}/4$ 的概率对 Q 是良好的，因为 $\mathcal{W}_Q$ 意味着模拟是正确的，并且我们必须有 $|C_{\mathrm{sim}}| = t_{\mathrm{tot}}(Q,\ I)$。

下面我们只关注良好(C_0，C_2)对。考虑在给定良好对(C_0，C_2)的条件下， C_{sim} 的内容上的后验分布。设 z 是 C_{sim}的一个可能内容。定义 $f(z)$为 z的概率乘以在该分布中给定 z 时 $\mathcal{P}(Q,\ I)$的期望值（步骤 6），

$$f(z) := \Pr_I[C_{\mathrm{sim}} \leftarrow z \mid C_0, C_2] \cdot \mathop{\mathbb{E}}_{I}[\mathcal{P}(Q,I) \mid C_{\mathrm{sim}} \leftarrow z, C_0, C_2].$$

直观地说，当 $C_{\mathrm{sim}} \leftarrow z$时， $f(z)$是对 $\mathbb{E}[\mathcal{P}(Q,\ I) \mid C_0,\ C_2]$ 的贡献。关于良好对，我们有以下断言。

断言 10。 当(C_0, C_2) 是 Q的良好对时，引理前提成立，并且在步骤 6 中 $k \le 4t_{\mathrm{tot}}$ 。

要看出这一点，根据良好对的定义，我们有 $|C_{\mathrm{sim}}| \le 4t_{\mathrm{tot}}$，即 $k \le 4t_{\mathrm{tot}}$。对于引理 9 的前提，显然，f 是一个将 Σ^k 映射到 $\mathbb{R}$的函数。关于 f 的第一个条件总是成立的：由于$|\mathcal{P}(Q,\ I)| \le 1$，我们有

$$\begin{aligned}
\sum_{z\in\Sigma^k} |f(z)| &= \left|\sum_{z\in\Sigma^k} \Pr[C_{\mathrm{sim}} \leftarrow z \mid C_0, C_2] \cdot \mathop{\mathbb{E}}_{I}[\mathcal{P}(Q,I) \mid C_{\mathrm{sim}} \leftarrow z, C_0, C_2]\right| \\
&\le \sum_{z\in\Sigma^k} \Pr[C_{\mathrm{sim}} \leftarrow z \mid C_0, C_2] \cdot \mathop{\mathbb{E}}_{I}[|\mathcal{P}(Q,I)| \mid C_{\mathrm{sim}} \leftarrow z, C_0, C_2] \\
&\le \sum_{z\in\Sigma^k} \Pr[C_{\mathrm{sim}} \leftarrow z \mid C_0, C_2] \\
&= 1.
\end{aligned}$$

对于 f的第二个条件，由于 $(C_0,\ C_2)$ 是良好对，$\Pr_I[\mathcal{W}_Q \mid C_0, C_2] \geq p^{4t_q}/4 = \varepsilon/\beta$。当 $\mathcal{W}_Q$ 发生时，Bob 将使用 C_{sim} 的正确内容进行模拟。令 z^* 为 Bob 在第5步中使用的内容。因此，良好对意味着 $\Pr_I[C_{\text{sim}} \leftarrow z^* \mid C_0, C_2] \geq \varepsilon/\beta$。此外，在给定 $C_{\text{sim}} \leftarrow z^*$ 和 $(C_0,\ C_2)$ 的条件下，Q 的查询输出是确定的（因为查询算法得到了正确模拟）。也就是说，$\mathcal{P}(Q,\ I)$ 的符号 是确定的。因此，我们有

$$\begin{aligned}
|f(z^*)| &= \Pr_I[C_{\text{sim}} \leftarrow z^* \mid C_0, C_2] \cdot \left| \mathop{\mathbb{E}}_I [\mathcal{P}(Q, I) \mid C_{\text{sim}} \leftarrow z^*, C_0, C_2] \right| \\
&= \Pr_I[C_{\text{sim}} \leftarrow z^* \mid C_0, C_2] \cdot \mathop{\mathbb{E}}_I [|\mathcal{P}(Q, I)| \mid C_{\text{sim}} \leftarrow z^*, C_0, C_2] \\
&\geq \varepsilon,
\end{aligned}$$

where the last i不等 lit式使用 the fact that $|\mathcal{P}(Q, I)| \geq \beta$ and $\Pr_I[C_{\text{sim}} \leftarrow z^* \mid C_0, C_2] \geq \varepsilon/\beta$。因此，引理 9 保证存在一个大小为 $Y \subseteq C_{\text{sim}}$ 的集合

$$\kappa \leq O(\sqrt{k \cdot \lg 1/\varepsilon}) \leq O(\sqrt{t_{\text{tot}}(t_q \lg 1/p + \lg 1/\beta)}),$$

使得

$$\sum_{y \in \Sigma^Y} \left| \sum_{z|_Y = y} f(z) \right| \geq 2^{-O(\sqrt{t_{\text{tot}}(t_q \lg 1/p + \lg 1/\beta)})}. \tag{3}$$

注意，Bob 知道集合 Y，因为它由对 (C_0, C_2)（以及 Q）决定。注意，不等式左侧是仅在 Y 条件下的期望优势，即，

$$\begin{aligned}
\sum_{y \in \Sigma^Y} \left| \sum_{z|_Y = y} f(z) \right| &= \sum_{y \in \Sigma^Y} \left| \sum_{z|_Y = y} \Pr[C_{\text{sim}} \leftarrow z \mid C_0, C_2] \cdot \mathop{\mathbb{E}}_I [\mathcal{P}(Q, I) \mid C_{\text{sim}} \leftarrow z, C_0, C_2] \right| \\
&= \sum_{y \in \Sigma^Y} \left| \Pr[Y \leftarrow y \mid C_0, C_2] \cdot \sum_{z|_Y = y} \Pr[C_{\text{sim}} \leftarrow z \mid Y \leftarrow y, C_0, C_2] \cdot \mathop{\mathbb{E}}_I [\mathcal{P}(Q, I) \mid C_{\text{sim}} \leftarrow z, C_0, C_2] \right| . \\
&= \sum_{y \in \Sigma^Y} \left| \Pr[Y \leftarrow y \mid C_0, C_2] \cdot \mathop{\mathbb{E}}_I [\mathcal{P}(Q, I) \mid Y \leftarrow y, C_0, C_2] \right| . \qquad (4)
\end{aligned}$$

最后，Alice 使用公共随机性以概率 p 进一步对每个单元进行采样，得到 C_1，并将所有更新单元发送给 Bob（步骤 3）。于是，以概率 p^κ，有 $C_1 \supseteq Y$。注意，Bob 可以知道 C_1 中所有 单元的内容：如果某个单元未被更新，则其内容为预初始化内容。此外，对于良好对 (C_0, C_2) 以及满足 $C_1 \supseteq Y$ 的 $\text{addr}(C_1)$，期望优势为

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\text{cont}(C_1)|C_0,C_2} \left[\left| \mathop{\mathbb{E}}_I [\mathcal{P}(Q, I) \mid C_0, C_1, C_2] \right| \right] \\
\geq &\mathop{\mathbb{E}}_{\text{cont}(Y)|C_0,C_2} \left[\left| \mathop{\mathbb{E}}_I [\mathcal{P}(Q, I) \mid C_0, \text{cont}(Y), C_2] \right| \right] \\
= &\sum_{y \in \Sigma^Y} \Pr[Y \leftarrow y \mid C_0, C_2] \cdot \left| \mathop{\mathbb{E}}_I [\mathcal{P}(Q, I) \mid C_0, C_2, Y \leftarrow y] \right| \\
\geq &\ 2^{-O(\sqrt{t_{\text{tot}}(t_q \lg 1/p + \lg 1/\beta)})},
\end{aligned}$$

其中，最后一个不等式由方程 (3) 和 (4) 得出。

为了证明 π 具有所声称的优势，对于每个 $Q \in \mathcal{Q}'$，我们有：

$$\begin{aligned}
&\mathop{\mathbb{E}}_{M_A}\left[\left|\mathop{\mathbb{E}}_{I}[\mathcal{P}(Q,I) \mid M_A]\right|\right] \\
&\geq \Pr\left[(C_0,C_2) \text{ is good} \wedge C_1 \supseteq Y\right] \cdot \mathop{\mathbb{E}}_{M_A}\left[\left|\mathop{\mathbb{E}}_{I}[\mathcal{P}(Q,I) \mid M_A]\right| \mid (C_0,C_2) \text{ is good} \wedge C_1 \supseteq Y\right] \\
&\geq \Omega(p^{4t_q} \cdot p^{\kappa}) \cdot \mathop{\mathbb{E}}_{C_0,C_2,\mathrm{addr}(C_1)}\left[\mathop{\mathbb{E}}_{\mathrm{cont}(C_1)|C_0,C_2}\left[\left|\mathop{\mathbb{E}}_{I}[\mathcal{P}(Q,I) \mid C_0,C_1,C_2]\right|\right] \mid (C_0,C_2) \text{ is good} \wedge C_1 \supseteq Y\right] \\
&\geq \Omega(p^{4t_q} \cdot p^{\kappa}) \cdot 2^{-O(\sqrt{t_{\mathrm{tot}}(t_q \lg 1/p + \lg 1/\beta)})} \\
&= 2^{-O(\sqrt{t_{\mathrm{tot}}(t_q \lg 1/p + \lg 1/\beta)} \cdot \lg 1/p)}.
\end{aligned}$$

这证明了该定理。 □

参考文献

[1] A. Abboud、F. Grandoni 和 V. Vassilevska Williams。图中心性问题、全点对最短路径和直径之间的次三次等价关系。*ACM* 算法汇刊，19(1)，2023年3月。[2] A. Bernstein、D. Nanongkai 和 C. Wulff-Nilsen。近线性时间内求解负权单源最短路径。载于*FOCS*，第600–611页。IEEE，2022年。[3] L. Chen、R. Kyng、Y. P. Liu、R. Peng、M. P. Gutenberg 和 S. Sachdeva。近线性时间内求解最大流和最小费用流。载于*FOCS*，第612–623页。IEEE，2022年。[4] R. Clifford、A. Grønlund 和 K. G. Larsen。动态问题和在线问题的全新无条件困难性结果。载于第*56*届*IEEE*计算机科学基础研讨会论文集，2015年。[5] M. L. Fredman 和 M. E. Saks。动态数据结构的单元探测复杂度。载于第*21*届*ACM*计算理论研讨会年会论文集，第345–354页，1989年。[6] M. Henzinger、S. Krinninger、D. Nanongkai 和 T. Saranurak。通过在线矩阵向量乘法猜想，统一并强化动态问题的困难性。载于*ACM* 计算理论研讨会，第21–30页。ACM，2015年。[7] R. Impagliazzo、R. Paturi 和 F. Zane。哪些问题具有强指数复杂度？计算机系统科学杂志，63(4):512–530，2001年12月。[8] K. G. Larsen。动态范围计数的单元探测复杂度。载于第*44*届计算理论研讨会（*STOC 2012*）论文集，第85–94页，2012年。[9] K. G. Larsen。求值多项式的更高单元探测下界。载于第*53*届*IEEE*计算机科学基础研讨会论文集，第293–301页，2012年。[10] K. G. Larsen、O. Weinstein 和 H. Yu。突破动态布尔数据结构下界的对数障碍。*SIAM* 计算杂志，49(5)，2020年。[11] R. Panigrahy、K. Talwar 和 U. Wieder。通过度量扩张得到近邻搜索的下界。载于第*51*届*IEEE*计算机科学基础研讨会（*FOCS 2010*），第805–814页，2010年。[12] M. P˘atra¸scu。统一单元探测下界的全貌。*SIAM* 计算杂志，40(3):827–847，2011年。

[13] M. P˘atra¸scu 和 E. D. Demaine。部分和问题的紧确界。载于第十五届*ACM-SIAM*离散算法研讨会年会论文集（*SODA 2004*年），第20–29页，2004年。[14] M. P˘atra¸scu。二维范围计数的下界。载于第*39*届*ACM*计算理论研讨会论文集，第40–46页，2007年。[15] M. P˘atra¸scu。迈向动态问题的多项式下界。载于第*42*届*ACM*计算理论研讨会（*STOC 2010*）论文集，剑桥，马萨诸塞州，美国，*2010*年*6*月*5*日至*8*日，第603–610页。ACM，2010年。[16] M. P˘atra¸scu 和 M. Thorup。近邻搜索及其他复杂问题的更高下界。载于第*47*届*IEEE*计算机科学基础研讨会（*FOCS 2006*），第646–654页，2006年。[17] M. P˘atra¸scu 和 M. Thorup。并集莫急于求成：花些时间寻找根。载于第*43*届*ACM*计算理论研讨会（*STOC 2011*）论文集，第559–568页，2011年。[18] A. Siegel。关于极度随机的常数时间哈希函数通用类。*SIAM* 计算杂志，33(3):505–543，2004年。[19] A. C. Yao。表应该排序吗？*ACM* 杂志，28(3):615–628，1981年。