Monte C arlo 到拉斯维加斯参加递归复合函数会议 S

Bandar Al-Dhalaan滑铁卢大学
bandar.al-dhalaan@uwaterloo.ca

Shalev Ben-David量子计算研究所 滑铁卢大学
shalev.b@uwaterloo.ca

arXiv:2601.08073v1 [cs.CC] 12 Jan 2026

摘要

对于一个（可能是部分的）布尔函数 $f\colon \{0,1\}^n \to \{0,1\}$ 以及一个将布尔函数映射到实数的查询复杂度测度 \mathrm{M}，定义 \mathrm{M} 在 f 上的复合极限为 \mathrm{M}^*(f) = \mathrm{l}\mathrm{i}\mathrm{m}_{k\to\infty} \mathrm{M}(f^k)^{1/k}。

我们研究查询复杂度中一般测度的复合极限。我们证明，在关于测度的合理假设下，该极限会收敛。随后，我们给出一个关于随机化查询复杂度复合极限的出人意料的结果：我们证明 \mathrm{R}_0^*(f) =\mathrm{m}\mathrm{a}\mathrm{x}{\mathrm{R}^*(f), \mathrm{C}^*(f)}。这意味着，任何用于递归三数多数函数的有界错误随机化算法，都可以转化为解决同一任务的零错误随机化算法。我们的结果也适用于量子算法：对于递归复合函数，有界错误量子算法可以转化为一种能够以高概率找到证书的量子算法。

在此过程中，我们证明了测度和复合极限的各种组合性质。

目录

1 引言。 **2**
1 1 复合函数 .21.2 随机化查询复杂度.21.3 我们的结果 .31.4 我们的技术 .4

2 预备知识。 **5**
2 1 布尔函数、测度与复合极限 .52.2 决策树、证书与随机化算法 .62.3 敏感度与次数度量 .72.4 小 o 记号的细微之处 .8

3 测度的组合性质 **8**
3.1 基本性质.83.2 可切换函数及复合函数的归约 .103.3 块敏感度界 .13

4 递归复合的性质 **13**
4.1 合理有界度量 .134.2 收敛定理.154.3 复合极限的性质 .17

5 拉斯维加斯算法的复合极限 **18**

致谢 **21**

参考文献 **22**

1 引言

1.1 复合函数

复合是研究布尔函数的一个核心概念：许多值得关注的函数都可以表示为更简单函数的复合。对于布尔函数 $f\colon \{0,1\}^n \to \{0,1\}$和 $g\colon \{0,1\}^m \to \{0,1\}$，它们的复合（有时称为“块复合”）是布尔函数 $f \circ g\colon \{0,1\}^{nm} \to \{0,1\}$，其定义为：将 g应用于 n个独立输入，再将得到的 n比特字符串代入 f，从而获得一个 1 比特的答案。（这个定义可以推广到偏函数，它们定义在 $\{0,1\}^n$的一个子集上；参见定义 10。）

查询复杂度领域一项重要的研究方向，是试图为某些布尔函数的测度建立复合定理；这类定理旨在将复合函数的复杂度与原函数的复杂度联系起来，尤其关注下界方向。例如，一个著名的量子查询复杂度复合定理$\mathrm{Q}(f)$ 可由“负权重对抗界” [HLŠ07；Rei11；LMR+11；Kim13], 推出，并表明 $\mathrm{Q}(f \circ g) = \Theta(\mathrm{Q}(f)\,\mathrm{Q}(g))$。

在本文中，我们关注递归复合函数，有时也称为树函数。也就是说，用 f^k表示复合 $f \circ f \circ \cdots \circ f$（具有 k层 f），我们希望理解当 $k \to \infty$时 f^k 的极限行为。递归地复合一个布尔函数，已成为查询复杂度中的标准工具：以这种方式构造的函数通常用于展示不同查询复杂度度量之间的分离，此外还有许多其他用途。有关一些具体递归复合函数的示例，请参见 [SW86; WZ88; NW95; KRW95; Aar08; Tal13; G\"o\"o15; KRS15; Amb16; GSS16; ABK16; JK17; BKT18; BBG+21]。

还有一些研究从抽象层面探讨递归复合（或相关概念），包括 [San95；Tal13；GJ16；GSS16；EMP18]。这类研究通常会（显式或隐式地）考察布尔函数某种测度的复合极限。也就是说，若 $\mathrm{M}(f)$ 是布尔函数的一个实值测度（例如证书复杂度或随机化查询复杂度），则将其复合极限定义为

$$\mathrm{M}^*(f) \coloneqq \lim_{k\to\infty} \mathrm{M}(f^k)^{1/k}.$$

对于大多数我们感兴趣的测度 \mathrm{M}，\mathrm{M}(f^k) 通常会随 k 呈指数增长，因此这个极限（若存在）本身应当是 f的某种非平凡测度。对于某些 \mathrm{M}，例如量子查询复杂度 \mathrm{Q}(f) 和确定性查询复杂度 \mathrm{D}(f)，\mathrm{M}*(f) 的行为已得到充分理解（我们有 \mathrm{Q}*(f) = \mathrm{A}\mathrm{d}\mathrm{v}$^{\pm}$(f) [HL\u S07; Rei11; LMR+11; Kim13] 以及 \mathrm{D}*(f) = \mathrm{D}(f)[Tal13; Mon14]）。然而，对于其他测度 \mathrm{M}，\mathrm{M}* 的行为似乎极其复杂。

1.2 随机化查询复杂度

我们部分受到对复合函数随机化查询复杂度 $\mathrm{R}(f)$ 的研究启发。即使只有两个函数 f 与 g，其复合的随机化查询复杂度 $\mathrm{R}(f \circ g)$也表现复杂，并已成为大量研究的主题 [AGJ+18； BK18；GJPW18； GLSS19；BDG+20； BB20； BGKW20； GM21； BBGM22； San24]。对于递归复合函数，我们的理解要差得多。事实上，甚至下面这个问题也尚无答案：

开放问题 1. $\mathrm{R}^*(f)$ 是否可计算？也就是说，给定函数 f 的真值表，能否在图灵机上计算出$\mathrm{R}^*(f)$ 的值（达到指定精度）？

测度 $\mathrm{R}^*(f)$ 主要针对两种特定的 f 选择进行了研究。第一种是 $\mathtt{NAND}_2$,作用于 2 比特上的与非函数。在这种情况下， f^k 变成了“与非树”函数，也称为与或树或博弈树。这类函数 f^k 已知能够将 $\mathrm{R}(\cdot)$ 与 $\mathrm{D}(\cdot)$ 区分开来（事实上，在 [ABB+17] 之前，这是已知的全函数中最好的分离结果），因为

已知 \mathrm{R}^*(\ttN \ttA \ttN \ttD $1.686^k \approx 2^{k \log_2 1.686^2} = 2^k$ $\approx$) 的精确值为 $(1+\sqrt{33})/4 \approx 1.686$ [SW86; San95], , 因此 \mathrm{R}(\ttN \ttA \ttN \ttD $\frac{k}{2}$) ( ) ( ), 而 \mathrm{D}(\ttN \ttA \ttN \ttD $\frac{k}{2}$)。此外, 还已知 \mathrm{R}$_0^*$(\ttN \ttA \ttN \ttD $_2$) \mathrm{R} (\ttN \ttA \ttN \ttD $_2$), 其中 \mathrm{R}$_0(f)$ 是 f 的零错误（“拉斯维加斯”、“ \sansZ \sansP \sansP”）随机化查询复杂度。这最初促成了一个猜想：对于所有全布尔函数，\mathrm{R}$_0(f)$ = \Theta (\mathrm{R}(f)), 但这一猜想后来被 [ABB+17] 推翻。

第二个受到广泛关注的 f 、使得 \mathrm{R}^*(f) 的选择是 f = \ttM \ttA \ttJ $_3$, , 即 3 比特上的多数函数。尽管已有大量研究 [JKS03; MNS+15; Leo13; GJ16], , \mathrm{R}^*(\ttM \ttA \ttJ $_3$) 的值仍然未知！目前只知道其介于 2.596 和 2.650 之间。\mathrm{R}$_0^*$(\ttM \ttA \ttJ $_3$) 的值也尚未确定。我们指出，如果已知问题 1 中所述的算法，就可以用它直接计算 \mathrm{R}^*(\ttM \ttA \ttJ $_3$)，因为 \ttM \ttA \ttJ $_3$ 的真值表只有 8 个输入比特。

1.3 我们的结果

我们的主要结果如下。

定理 **m 1.** 对于所有（可能为偏）布尔函数 f，$\mathrm{R}_0^*(f) = \max\{\mathrm{R}^*(f), \mathrm{C}^*(f) \}$.

这里，\mathrm{R}$_0$ 表示零错误随机查询复杂度，\mathrm{R}表示随机化查询复杂度，而 \mathrm{C}表示证书复杂度（其中 $*$ 表示复合极限）。换言之，我们证明，对于递归复合函数，除非证书复杂度很大，否则可以将“蒙特卡洛”（又称有界错误，\sansB \sansP \sansP ）随机化算法转换为“拉斯维加斯”（又称零错误，\sansZ \sansP \sansP ）随机化算法，且不会增加额外成本。注意，由于零错误随机查询算法必须始终找到一个证书，因此很容易看出，\mathrm{R}$_0^*(f) \geq$ \mathrm{C}^*(f)；又由于有界错误算法可以模拟零错误算法，\mathrm{R}$_0^*(f) \geq$\mathrm{R}^*(f)。这意味着，定理 1 的下界方向很容易证明，而我们的主要贡献是给出 \mathrm{R}$_0^*(f)$ 的上界。

定理 1 特别蕴含，$\mathrm{R}_0^*(\mathtt{MAJ}_3) = \mathrm{R}^*(\mathtt{MAJ}_3)$。尽管针对这两种测度已有大量研究，甚至连这个特例此前也未得到证明 [JKS03; MNS+15; Leo13; GJ16]。

更一般地，定理 1 给出了一种策略，它只需使用有界错误算法，就能在递归复合函数中寻找证书。该策略也适用于将有界误差量子算法转化为寻找证书的量子算法。

定理2。 令$\mathrm{Q_C}(f)$ 表示以常数成功概率寻找 f的证书所需的量子查询次数。那么

$$\mathrm{Q}_{\mathrm{C}}^*(f) = \max\{\mathrm{Q}^*(f), \mathrm{C}^*(f)\}.$$

\mathrm{Q}$_{\mathrm{C}}(f)$ 的精确定义见第5节。我们注意到，我们的方法很可能也适用于其他计算模型：例如，很可能可以为递归复合函数构造一个次数仅为近似次数的证书查找多项式系统；本文不作此尝试，但可能的障碍仅在于定义上的技术细节。

在证明定理 1 和定理2时，我们会遇到一个或许令人意外的问题：证明诸如$\mathrm{R}^*(f)$、$\mathrm{R}_0^*(f)$和$\mathrm{Q}_{\mathrm{C}}^*(f)$这样的复合极限收敛，出人意料地棘手。为此，我们证明了一些关于一般测度的复合极限的结构性结果。

定理 *3*（非正式表述；见定理 *48*）。设 *|mathrm{M}* 是布尔函数的一个测度，满足对于所有的 f与 g，*|~|mathrm{M}($f \circ g$) = O (|mathrm{M}(f) |mathrm{M}(g))* 且 *|mathrm{M}($f \circ g$) = |Omega (|mathrm{M}(f))*。在对 *|mathrm{M}* 的一些温和良性条件下，极限 *|mathrm{M}^*(f) = |mathrm{l}|mathrm{i}|mathrm{m}*$_{k\to\infty}$ *|mathrm{M}(f^k)$^{1/k}$* 收敛。

该定理中的条件相对容易满足。因此，我们得到以下推论。

推论 4. 以下测度均具有收敛的复合极限 $:$

1. 确定性、随机化和量子查询复杂度 $\mathrm{D}(f)$、$\mathrm{R}(f)$、$\mathrm{Q}(f)$，以及它们的零错误和精确变体 $\mathrm{R}_0(f)$、$\mathrm{Q}_{\mathbb{C}}(f)$ 和 $\mathrm{Q}_E(f)$ *2.* 某些“局部”测度，例如敏感度 $\mathrm{s}(f)$、分数块敏感度 $\mathrm{fbs}(f)$ 和证书复杂度 $\mathrm{C}(f)$（也可由 [GSS16] 推出） *3.* 多项式次数度量，例如次数 $\mathrm{deg}(f)$ 和近似次数 $\widetilde{\mathrm{deg}}(f)$，即使对于偏函数也是如此 f。

便利定理。 我们还针对复合极限建立了其他结构性结果。例如，我们证明，诸如 $\mathrm{M}_1(f) \leq \mathrm{M}_2(f)$ 这样的测度间关系，会蕴含其复合极限之间相应的关系；并且我们证明，取复合极限时，低阶项往往会消失。我们还证明了 $(\mathrm{M}^*)^*(f) = \mathrm{M}^*(f)$（即复合极限的复合极限就是原来的复合极限），以及诸如 $\mathrm{M}^*(f \circ g) = \mathrm{M}^*(g \circ f)$ 和 $\mathrm{M}^*(f^k) = \mathrm{M}^*(f)^k$ 等其他结果。

组合约化。 为了证明测度满足定理 3的良性条件，我们研究测度的组合性质。若一个测度在指标重命名（以相同方式置换所有输入字符串）、比特复制（向每个输入添加一个新比特，该比特在函数的承诺下始终与另一个已有比特取相同的值）、添加冗余比特（向每个输入添加一个不用于确定函数值的比特）下保持不变，并且在限制到承诺时不增加，则称该测度为良态测度。另一种有用的不变性称为字母表重命名：对函数的所有输入中的一个比特取反。在字母表重命名下保持不变的良态测度称为强良态测度。

我们定义了函数间约化的概念，其实质是应用上述变换。我们证明了约化与复合之间相互作用的多种性质。我们的一个重要成果是定义了开关函数：这是函数 $\mathtt{S} : \{01,\ 10\} \to \{0,\ 1\}$，定义为 $\mathtt{S}(01) = 0$ 且 $\mathtt{S}(10) = 1$。我们证明，对于良态测度而言，开关函数是最简单的非恒定函数，具体来说：

定理 5。 对于所有（可能为偏）非恒定函数 f 与 g 以及所有良态测度$\mathrm{M}(\cdot)$，都有 $\mathrm{M}(f \circ g) \geq \mathrm{M}(f \circ \mathtt{S})$，且 $\mathrm{M}(f \circ g) \geq \mathrm{M}(\mathtt{S} \circ g)$。

我们还可以证明，一个函数的测度可以由块敏感度下界给出：将测度应用于承诺 OR 函数 $\mathtt{PROR}$（与开关复合），其规模等于块敏感度 $\mathrm{bs}(f)$。

定理 6。 对于任意（可能为偏）布尔函数 f 以及布尔函数上的任意良态测度$\mathrm{M}(\cdot)$，都有 $\mathrm{M}(f) \geq \mathrm{M}(\mathtt{PrOR}^{\mathrm{bs}(f)} \circ \mathtt{S})$。

1.4 我们的技术

从蒙特卡洛到拉斯维加斯。为证明定理 1，我们需要说明如何利用有界错误随机化算法 R 来处理 f^k，以便找到 f^k 的证书（假设 k 相较于 f的大小足够大）。函数 f^k 可以表示为一棵深度为 k 的树，其中每个节点有 n 个子节点，并对它们的值应用 f 门；树底部是长度为 n^k的输入。

我们构造零错误算法的方法是，使用有界错误算法来计算树的根节点的 n 个子节点中的每一个；也就是说，我们对输入到最外层 f 副本中的每个 f^{k-1} 的 n 个副本，分别运行有界错误算法。我们放大每次运行，以降低错误率。这样就得到一个长度为 n 的字符串，其中包含对最外层 f 的输入值的最佳猜测；以很高的概率（但并非确定无疑），这个猜测字符串是正确的。

接下来，假设这个 n 比特字符串是真实输入，我们为它选择一个代价最低的证书 c forit。最后，我们在证书 c 所用到的每个 f^{k-1} 副本上递归调用零错误算法；该算法为每个副本生成一个证书，而这些证书合在一起就构成了外层 f 副本的证书，我们将其返回。

对该协议的分析最终会得到如下形式的界：

$$\mathrm{R}_0(f^k) \le \tilde{O}(n) \cdot \tilde{O}(\mathrm{R}(f) + \mathrm{C}(f))^k.$$

\~ 对两边取 $1/k$ 的幂，并令 $k \to \infty$ 取极限后， $O(n)$ 因子便消失了，于是 \~ 得到 \ mathrm{R}$_0^*(f)$ $\le O($\mathrm{R}(f) +\mathrm{C}$(f))$。这仍然是一个过大的界：\mathrm{R}$^*(f)$，尤其是 \mathrm{C}$^*(f)$，可能远小于 \mathrm{R}(f) 和 \mathrm{C}(f)。接下来的技巧或许有些反直觉：我们直接对不等式本身取复合极限。换句话说，我们对两边应用 $*$ 算子：

$$\mathrm{R}_0^{**}(f) \le \tilde{O}(\mathrm{R}(f) + \mathrm{C}(f))^*.$$

利用我们的便利定理，我们证明这个表达式可以大幅简化：\mathrm{R}$_0^{**}(f)$ 等于 \mathrm{R}$_0^*(f)$，对数因子消失，加法变成取最大值，而测度 \mathrm{R}(f) 和 \mathrm{C}(f) 则变成可能更小的测度 \mathrm{R}$^*(f)$ 和 \mathrm{C}$^*(f)$。因此，我们可以从对简单拉斯维加斯算法粗糙得多的分析中，提取出一个简洁而有力的上界：

$$\mathrm{R}_0^*(f) \le \max\{\mathrm{R}^*(f), \mathrm{C}^*(f)\}.$$

复合极限的收敛性。对于复合极限的收敛性（定理 3），粗略地说，我们构造一个子序列，使其同时收敛到序列 $\mathrm{M}(f^k)^{1/k}$ 的上极限和下极限。思路如下：我们将一个收敛到 k_1， k_3， $k_5 \ldots$ 序列 $\mathrm{M}(f^k)^{1/k}$ 上极限的序列与一个收敛到 k_2， k_4， k_6，.....序列 $\mathrm{M}(f^k)^{1/k}$ 下极限的序列交错排列。不过，我们会谨慎处理，逐个选取每个 k_i ，并使每个选取的数都远大于之前的数，从而使它在乘法意义下接近所有之前数的某个倍数。因此，我们可以对序列中的 k_i 进行取整，使每个数都恰好等于所有之前数的某个倍数；我们会谨慎地进行这一操作，以确保奇数指标仍收敛到上极限，偶数指标收敛到下极限。

最后，我们利用关于 \mathrm{M} 所作的复合性质假设，用下极限子序列给出上极限子序列的上界，从而迫使二者彼此趋近并收敛到同一个值。这足以证明原序列的极限存在。

2 预备知识

2.1 布尔函数、测度与复合极限

我们回顾查询复杂度中的一些基本定义。需要说明的是，其中一些细节（例如布尔函数上的一般测度的定义）未必是该领域的标准定义，因为通常无需在如此一般的情形下使用这类定义。

定义 7（布尔函数）。 $n \in \mathbb{N}$ 比特上的一个可能为偏的布尔函数，是一个函数f： $S \to \{0,1\}$，其中 $S \subseteq \{0,1\}^n$。我们也可以将 f写成函数 f： $\{0,1\}^n \to \{0,1,*\}$，其中

$f(x) = *$ 当 $x \notin S$ 时。 f的定义域为 $\mathrm{Dom}(f) := S$，输入规模为 $n(f) := n$。函数f称为全定义的，如果$\mathrm{Dom}(f) = \{0,1\}^{n(f)}$。

定义 8。 对于 $n \in \mathbb{N}$，令 $\mathcal{F}_n$ 表示定义在 n 个比特上的所有可能为偏的布尔函数的集合。令 $\mathcal{F} := \bigcup_{n=1}^{\infty} \mathcal{F}_n$ 表示所有（可能为偏的）布尔函数的集合。

定义 9 (测度)。 定义在子集 $\mathcal{A} \subseteq \mathcal{F}$ 上的测度 M 是函数 $M\colon \mathcal{A} \to [0,\infty)$.

定义 10 (复合)。 复合是作用于可能为偏的布尔函数上的二元运算 $\circ\colon \mathcal{F} \times \mathcal{F} \to \mathcal{F}$。对于两个函数 f、$g \in \mathcal{F}$，它们的复合 $f \circ g$ 是定义在长度为 $n(f) \cdot n(g)$ 的字符串上的函数，表示将 f 与函数 g 的 $n(f)$ 个独立副本进行复合。

形式上，长度为 $n(f) \cdot n(g)$ 的字符串 x 属于 $\mathrm{Dom}(f \circ g)$，当且仅当它可以写作 $x = y^1 y^2 \dots y^{n(f)}$，其中每个 $y^i \in$ 都属于 $\mathrm{Dom}(g)$，并且字符串 $g(y^1)g(y^2)\dots g(y^{n(f)})$ 属于 $\mathrm{Dom}(f)$。在这种情况下， $f \circ g(x)$ 的值定义为 $f(g(y^1)g(y^2)\dots g(y^{n(f)}))$。

注。 不难看出，复合满足结合律。记 $f \circ f$为 f^2， $f \circ f \circ f$为f^3，依此类推。用 I表示单比特上的恒等函数，我们注意到 $(\mathcal{F}, \circ)$ 构成一个幺半群，其单位元为 I，因为对所有 $f \in \mathcal{F}$都有 $f \circ I = I \circ f = f$。我们定义 f^0为 I。

定义 11（复合封闭类）。 子集 $\mathcal{A} \subseteq \mathcal{F}$ 称为复合封闭类，如果它是 $\mathcal{F}$ 的子幺半群；也就是说，它必须包含 I，并且对复合封闭。

定义 12（复合极限）。 对于任意 $f \in \mathcal{F}$ 以及定义在 $\{f$ 上的任意测度 M，令 f^2、$\dots\}$，定义

$$M^{\underline{*}}(f) := \liminf_{k\to\infty} M(f^k)^{1/k},$$

$$M^{\overline{*}}(f) := \limsup_{k\to\infty} M(f^k)^{1/k}.$$

若 $M^*(f) = \bar{} M^*(f)$，则将此量记作 $M^*(f)$；这称为将 M 应用于 f 的复合极限，且等于 $\lim_{k\to\infty} M(f^k)^{1/k}$。

2.2 决策树、证书与随机化算法

定义 13 (决策树)。 一个作用于 n 个比特的决策树是一棵有根二叉树，其内部节点标记为 $[n]$，叶节点标记为 $\{0、1\}$，弧标记为 $\{0、1\}$。此外，我们要求任意两个内部节点中，若一个是另一个的祖先节点，则它们的标记不同；这确保每个叶节点的高度至多为 n。树的高度定义为从根节点到叶节点的最大高度。

对于一个作用于 n 个比特的决策树 D，令 $D(x)$ 表示从根节点出发后到达的叶节点标记；对于每个标记为 i 的内部节点，我们沿着标记为 x_i 的弧向下遍历这棵树。对于一个可能是偏布尔函数的函数 $f \in \mathcal{F}$，如果对于所有 $x \in \mathrm{Dom}(f)$，都有 $n = n(f)$ 且 $D(x) = f(x)$，则称 D 计算了 f。确定性查询复杂度 $\mathrm{D}(f)$ 定义为计算 f 的决策树的最小高度。

定义 14（部分赋值）。 n 比特上的部分赋值是一个字符串 $p \in \{0,\ 1,\ *\}^n$。我们将 p 与有序对集合 $\{(i,\ p_i)\colon\ p_i \neq *\}$ 以及由该有序对集合定义的函数视为相同。若对于所有 $i \in [n]$，$p_i = q_i$ 成立，或者 p_i 和 q_i 中至少有一个为 $*$，则称部分赋值 p 与 q 一致。使用 $p \subseteq q$ 和 $|p|$ 等集合记号时，应将其理解为关于有序对集合的记号。

定义 15（证书）。设 $f \in \mathcal{F}$ 是一个可能为偏布尔函数的布尔函数。设 $x \in \mathrm{Dom}(f)$，并设 p 是 n（f）比特上的部分赋值。如果 $p \subseteq x$，且对于所有满足 $p \subseteq y$的 $y \in \mathrm{Dom}(f)$，都有 f（y）$= f$（x），则称 p 是 x 的一个证书。f在 x处的证书复杂度记为 C_x（f），定义为关于 f的 x 的证书的最小大小 $|p|$。

f 的证书复杂度记为 |*mathrm{C}(f)*，定义为 |*mathrm{C}(f)* := |*mathrm{m}|mathrm{a}|mathrm{x}*$_{x\in\mathrm{Dom}(f)}$ |*mathrm{C}*$_x$*(f)*。我们还定义 |*mathrm{C}*$_0$*(f)* := |*mathrm{m}|mathrm{a}|mathrm{x}*$_{x\in f^{-1}(0)}$ |*mathrm{C}*$_x$*(f)*，以及 |*mathrm{C}*$_1$*(f)* := |*mathrm{m}|mathrm{a}|mathrm{x}*$_{x\in f^{-1}(1)}$ |*mathrm{C}*$_x$*(f)*。

定义 16（随机化查询复杂度）。一个作用于 n 比特的随机化查询算法 R，是 n 比特上的决策树所构成的概率分布。对于每个字符串 $x \in \{0,\ 1\}^n$，我们将 $\mathrm{cost}(R,\ x)$定义为 $\mathbb{E}_{D\sim R}[\mathrm{cost}(D,\ x)]$,，其中，对于决策树 D，$\mathrm{cost}(D,\ x)$ 是从根节点到 x 所到达的叶节点的路径长度；换句话说，$\mathrm{cost}(R,\ x)$ 是 R 在 x 上运行时的期望查询次数。R 的高度定义为其支撑集中任意决策树的最大高度。

我们将 *R(x)* 定义为随机变量：当从 R 中采样 D 时，*D(x)* 的取值。若对所有 $x \in$ |*mathrm{D}|mathrm{o}|mathrm{m}(f)*，都有 |*mathrm{P}|mathrm{r}*$[R(x) = f(x)] \geq 1-\epsilon$，则称 R 以错误率 $\epsilon \in [0,1/2)$ 计算 f。当 $\epsilon > 0$ 时，我们将 |*mathrm{R}*$_\epsilon$*(f)* 定义为能够以错误率 ϵ 计算 f 的随机化查询算法 R 的最小高度。我们进一步将 |*mathrm{R}*$_\epsilon$*(f)* 定义为能够以错误率 ϵ 计算 f 的随机化查询算法 R 中，|*mathrm{m}|mathrm{a}|mathrm{x}*$_{x\in\mathrm{Dom}(f)}$ |*mathrm{c}|mathrm{o}|mathrm{s}|mathrm{t}(R,x)* 的最小值。当 $\epsilon = 1/3$ 时，我们省略它，记作 |*mathrm{R}(f)* 和 |*mathrm{R}(f)*。

当 $\epsilon = 0$ 时，测度 $\mathrm{R}_\epsilon(f)$ 变得与 $\mathrm{D}(f)$ 的测度相同，但测度 $\mathrm{R}_\epsilon(f)$ 仍然不同。按照文献中的惯例，我们将 $\mathrm{R}_0(f)$ 定义为 $\mathrm{R}_0(f)$。

以上定义在查询复杂度领域都是标准的。我们注意到，\mathrm{R}$_\epsilon$*(f)* 和 \mathrm{R}$_\epsilon$*(f)* 都可以通过放大来提升（重复运行算法几次，以降低错误率，同时增加成本）；这意味着，如果 ϵ 是 $(0, 1/2)$ 中的常数，且我们不关心乘法常数，那么它的取值并不重要。此外，这些测度关于 ϵ 单调不增，并且 \mathrm{R}$_\epsilon$*(f)* $\geq$\mathrm{R}$_\epsilon$*(f)*。可以使用马尔可夫不等式截断运行时间远超其期望值的算法；据此可以证明 $R(f) = O$(\mathrm{R}(*f*))，因此这两个测度在相差常数因子的意义下等价。我们还有 \mathrm{R}$_0$*(f)* $\geq$ \mathrm{R}(*f*) $=$ \Omega (\mathrm{R}(*f*))。

总之，当 ϵ为 0 或常数时，唯一不同的测度是 \mathrm{D}(*f*)、\mathrm{R}$_0$(*f*) 和 \mathrm{R}(*f*)，它们依次递减（相差至多一个常数因子）。它们分别对应复杂度类 \sansP 、\sansZ \sansP \sansP 和 \sansB \sansP \sansP 。

2.3 敏感度与次数测度

定义17 (块记号**)**。指标集合 $B \subseteq [n]$ 称为一个块。给定字符串 $x \in \{0、\ 1\}^n$和一个块 $B \subseteq [n]$，字符串 x^B 定义为将 x 中 B 对应的比特翻转后得到的字符串，即当 $i \notin B$ 时为 $x_i^B = x_i$，当 $i \in B$时为 $x_i^B = 1 - x_i$。如果 $B = \{i\}$ 只包含一个比特，我们用 x^i 作为 $x^{\{i\}}$的简写。

定义*18*（敏感度）。设 $f \in \mathcal{F}$ 且 $x \in$ |*mathrm{D}|mathrm{o}|mathrm{m}(f)*。若比特 $i \in [n]$ 满足 $x^i \in$ |*mathrm{D}|mathrm{o}|mathrm{m}(f)* 且 $f(x^i) \neq f(x)$，则称其对于 x相对于 f是敏感的。x相对于 f 的敏感度，记作 |*mathrm{s}*$_x$*(f)*，是对于 x敏感的比特 $i \in [n]$ 的数量。f 的敏感度定义为 |*mathrm{s}(f)* := |*mathrm{m}|mathrm{a}|mathrm{x}*$_{x\in\mathrm{Dom}(f)}$ |*mathrm{s}*$_x$*(f)*。

定义 *19*（块敏感度）。设 $f \in \mathcal{F}$ 且 $x \in$ |*mathrm{D}|mathrm{o}|mathrm{m}(f)*。如果 $x^B \in$ |*mathrm{D}|mathrm{o}|mathrm{m}(f)* 且 $f(x^B) \neq f(x)$，则称块 $B \subseteq [n]$ 相对于 f对 x是敏感的。x 相对于 f的块敏感度，记为 |*mathrm{b}|mathrm{s}*$_x$*(f)*，是满足以下条件的最大数目 $k \in \mathbb{N}$：存在 k个块 B_1、.....、$B_k \subseteq [n]$，它们两两不相交，且都对 x敏感。f 的块敏感度定义为 |*mathrm{b}|mathrm{s}(f)* := |*mathrm{m}|mathrm{a}| x*$_{x\in\mathrm{Dom}(f)}$ |*mathrm{b}|mathrm{s}*$_x$*(f)*。

定义 20 （分数块敏感度）。设 $f \in \mathcal{F}$ 且 $x \in$ \mathrm{D}\mathrm{o\mathrm{m}}(f)。设 $\mathcal{B}$ 为 x 相对于 f 的敏感块集合。x 相对于 f 的分数块敏感度，记为 $\mathrm{fbs}_x(f)$，是可能的最大权重总和 $\sum_{B\in\mathcal{B}} w_B$，其中权重 $w_B \geq 0$ 受约束，满足 $\sum_{B\in\mathcal{B}:\ i\in B} w_B \leq 1$ 对所有 $i \in [n]$ 均成立。f 的分数块敏感度定义为 $\mathrm{fbs}(f) := \max_{x\in\mathrm{Dom}(f)} \mathrm{fbs}_x(f)$。

其他测度的定义，例如多项式次数和精确量子查询复杂度，可见 [BW02]。

2.4 小 o 记号的细微之处

由于小 o 记号经常出现在查询复杂度度量的指数中，我们在此花些时间明确说明这一记号的确切含义。这里的细节可能有些微妙。

定义 21（小 *o* 记号）。设 S 是一个无限集合，且 N、M：$S \to [0,\infty)$ 是函数。若 $M(x) \leq N(x)^{o(1)}$（关于 $x \in S$），则称 $M(x) = 0$，只要 $N(x) = 0$，并且对每个 $\epsilon > 0$，都存在 $C > 0$，使得只要 $M(x) \geq C$，就有 $M(x) \leq N(x)^{\epsilon}$。

我们以自然的方式扩展这个定义；例如，对于测度 $M\ N_1\ N_2\ \mathcal{F} \to$、~~、：），陈述 ( )~~ $[0,\infty$ $M\ f\circ g \leq N_1\ f\ ^{1+o(1)} N_2\ g\ ^{1+o(1)}$ $M\ f\circ g \leq$ $(\ )\ (\ )$ 与 $(\ )\ N_1(f)N_2(g)\ (N_1(f)N_2(g))^{o(1)}$（再加上条件：当分母 $N_1(f)N_2(g)$ 为 *0* 时，$M(f\circ g) = 0$）含义相同；此时两边都是从 $\mathcal{F}^2$ 到 $[0,\infty)$ 的函数（因此适用前述定义）。类似地，$M(f\circ g) \geq N_1(f)^{1-o(1)} N_2(g)^{1-o(1)}$ 与 $N_1(f)$ $N_2(g)\ M(f\circ g) \leq (N_1(f)N_2(g))^{o(1)}$（再加上条件：只要 $M(f\circ g) = 0$，就有 $N_1(f)N_2(f) = 0$）含义相同。

引理 22. 陈述 $M(x) \leq N(x)^{1+o(1)}$ 如 *定义 21* 中所定义的，与陈述 $N(x) \geq M(x)^{1-o(1)}$ 等价。

证明。请注意，这两个定义略有不同。前者表示，对于每个 $\epsilon > 0$，都存在 C_ϵ，使得只要 $M(x)/N(x) > C_\epsilon$，就有 $M(x)/N(x) \leq N(x)^{\epsilon}$；或者等价地，对于每个 $\epsilon > 0$，都存在 C_ϵ，使得对所有 x，$M(x) \leq$ \mathrm{m}\mathrm{a}\mathrm{x}$\{N(x)^{1+\epsilon}, C_\epsilon N(x)\}$。后者表示，对于每个 $\epsilon > 0$，都存在 C'_ϵ，使得只要 $M(x)/N(x) > C'_\epsilon$，就有 $M(x)/N(x) \leq M(x)^{\epsilon}$；或者等价地，对于每个 $\epsilon > 0$，都存在 C'_ϵ，使得对所有 x，$M(x) \leq$\mathrm{m}\mathrm{a}\mathrm{x}$\{N(x)M(x)^{\epsilon}, C'_\epsilon N(x)\}$。对于 $\epsilon < 1$，我们可以将后一条件改写为 $M(x) \leq$\mathrm{m}\mathrm{a}\mathrm{x}$\{N(x)^{1/(1-\epsilon)}, C'_\epsilon N(x)\}$。（两个陈述还都包含条件 $N(x) = 0 \Rightarrow M(x) = 0$，但由于两者都包含这一条件，在本证明中我们可以假设 $N(x) \neq 0$。）

因此，这两个条件的形式化版本之间唯一的区别是 $N(x)$ 上的指数：它要么是 $1+\epsilon$，要么是 $1/(1-\epsilon)$。对于 $\epsilon < 1$，我们只需采用不同的 ϵ 值，就能在两者之间转换，因此这两个条件是等价的。 □

3 测度的组合性质

3.1 基本性质

由于我们的目标是以高度一般化的方式研究布尔函数上的测度，我们将首先定义一些我们期望这类测度满足的基本条件。第一个这样的条件称为索引重命名，它表示测度 \mathrm{M}（例如 \mathrm{R}(f) 或 \mathrm{C}(f)）在对输入字符串的指标进行重命名时应保持不变（也就是说，对函数所有输入中的比特进行置换）。

定义 23 (索引重命名)。设 $f \in \mathcal{F}_n$ 是定义在 n 个比特上的一个（可能是部分）布尔函数，且 π：$[n] \to [n]$ 是一个置换。对于任意 $x \in \{0、1\}^n$，令 $x_\pi \in \{0、1\}^n$ 表示按照

对 x 的比特进行重排，即 $(x_\pi)_i := x_{\pi(i)}$。按照 π 对 f 进行的索引重命名 是定义在定义域 $\{x : x_\pi \in \mathrm{Dom}(f)\}$ 上的函数 f_π，其定义为 $f_\pi(x) := f(x_\pi)$。

我们称定义在 $\mathcal{A} \subseteq \mathcal{F}$ 上的测度 M 在索引重命名下保持不变，如果对于所有 $f \in \mathcal{A}$以及所有置换 π，都有 $f_\pi \in \mathcal{A}$，且 $\mathrm{M}(f_\pi) = \mathrm{M}(f)$。

下一个性质指出，向输入中添加不会影响函数输出的额外比特，不应改变 \mathrm{M}(f)。

定义 24 (冗余比特)。 设 $f \in \mathcal{F}$ 是定义在 n 个比特上的一个（可能是部分）布尔函数，且 $S \subseteq \{0,1\}^m$ 对某个 $m \in \mathbb{N}$成立。定义相对于 S 对 f 进行的冗余比特 修改为函数 f_S，该函数定义在 $\{xy : x \in \mathrm{Dom}(f)\ y \in S\}$上，通过 $f_S(xy) := f(x)$。

我们称定义在 $\mathcal{A} \subseteq \mathcal{F}$ 上的测度 M 具有<style id='4'>对冗余比特不变性，如果对于所有 $f \in \mathcal{F}$ 和 $S \subseteq \{0, 1\}^m$，都有 $f \in \mathcal{A}$ 当且仅当 $f_S \in \mathcal{A}$，并且如果 $f \in \mathcal{A}$，则 $\mathrm{M}(f_S) = \mathrm{M}(f)$。

上述两个性质几乎对所有我们感兴趣的查询测度都成立（某些技术细节除外，例如某些测度仅定义在全函数上，因此严格来说不满足对冗余比特不变的条件）。下一个性质表示，测度 M 应当对复制比特保持不变。大多数查询测度都满足这一性质；在我们于 第2节 中定义的测度里，唯一不满足该性质的是敏感度 $\mathrm{s}(f)$，因为敏感度关注各个比特，所以将一个比特变成一块相同的比特会改变敏感度。

定义 25 （比特复制）。 设 $f \in \mathcal{F}$ 是定义在 n 个比特上的一个（可能是部分）布尔函数，且令$i \in [n]$。定义 f 在比特 i 处的比特复制为定义在定义域 $\{xx_i : x \in \mathrm{Dom}(f)\}$上的函数 f_i，其定义为 $f_i(xx_i) = f(x)$，对所有 $x \in \mathrm{Dom}(f)$ 均成立。这里，xx_i 是将 x 与额外的比特 x_i 拼接而成的。

我们称定义在 $\mathcal{A} \subseteq \mathcal{F}$ 上的测度M 在比特复制下不变，如果对于所有 $f \in \mathcal{F}$ 和所有 $i \in [n] \cup \{0\}$，有 $f \in \mathcal{A}$ 当且仅当 $f_i \in \mathcal{A}$，并且若 $f \in \mathcal{A}$，则$\mathrm{M}(f_i) = \mathrm{M}(f)$。

接下来，我们定义“字母表重命名”性质，即分别将输入字母表中的“0”和“1”重命名为“1”和“0”。我们允许只对字符串的某些 n 个位置进行这种重命名。几乎所有我们感兴趣的测度都在这种重命名下保持不变，但遗憾的是，由复合定义的测度（例如复合极限 \mathrm{M}^*(f)）不具有这一性质。

定义 26 （字母表重命名）。 设 $f \in \mathcal{F}_n$ 是定义在 n 比特上的一个（可能是部分的）布尔函数，$z \in \{0, 1\}^n$ 是字符串。定义根据 z 对 f 进行的字母表重命名 为定义在 $\{x : x \oplus z \in \mathrm{Dom}(f)\}$ 上的函数 f_z，其定义为 $f_z(x) := f(x \oplus z)$，其中 $\oplus$ 表示两个字符串逐位异或。

我们称定义在 $\mathcal{A} \subseteq \mathcal{F}$ 上的测度 M 在字母表重命名下不变，如果对于所有$f \in \mathcal{A}$ 以及所有 $z \in \{0, 1\}^n$，都有 $f_z \in \mathcal{A}$，且 $\mathrm{M}(f_z) = \mathrm{M}(f)$。

有些测度是“双侧”的，这意味着它们不在意 f 的输出是否取反。另一些“单侧”测度，例如 \mathrm{C}_1(f)，则会在意这一点。由复合定义的测度通常不是双侧的。

定义 27 (双侧)。 设 $f \in \mathcal{F}_n$ 是定义在 n 个比特上的一个（可能是部分的）布尔函数。定义 f 的取反为函数 $\overline{f}$，该函数定义在 $\mathrm{Dom}(f)$ 上，其定义方式为 $\overline{f}(x) := 1 - f(x)$。

我们称定义在 $\mathcal{A} \subseteq \mathcal{F}$ 上的测度 M 具有双侧性，如果它在取负运算下保持不变：也就是说，对于所有 $f \in \mathcal{A}$，都有 $\overline{f} \in \mathcal{A}$，且 $\mathrm{M}(f) = \mathrm{M}(\overline{f})$。

最后，几乎所有测度都具有承诺尊重性，即限制到更小的承诺子域不会增加测度。

定义 28（承诺尊重性）。 我们称定义在 $\mathcal{A} \subseteq \mathcal{F}$ 上的测度 M 具有承诺尊重性，如果对于任意 $f \in \mathcal{A}$ 以及任意 $P \subseteq \mathrm{Dom}(f)$， f 在子域 P 上的限制 $f|_P$ 满足 $f|_P \in \mathcal{A}$，且 $\mathrm{M}(f|_P) \leq \mathrm{M}(f)$。

为方便起见，我们将上述定义汇总为一个定义。

定义 29（良态）。 定义在 $\mathcal{A} \subseteq \mathcal{F}$ 上的测度 M 称为弱良态，如果它在索引重命名、冗余比特和比特复制下保持不变，并且此外还遵守承诺。

如果此外它在字母表重命名下也保持不变，我们称 M 是强良态的（或简称为良态）。

定义 30（归约）。 对于（可能是部分的）布尔函数 f 和 g，如果我们可以通过索引重命名、冗余比特和比特复制（或其逆操作，例如移除重复比特），以及限制到某个承诺，利用这些操作将 g 转换为 f，则记作 $f \lesssim g$。如果可以结合字母表重命名（对输入比特取反）使用这些操作将 g 转换为 f，则记作 $f \lesssim' g$。

我们注意到， $\lesssim$ 和 $\lesssim'$ 是传递关系。它们也刻画了测度是否良态。

引理 31. 测度 M 弱良态，当且仅当对于所有 f和 g， $f \lesssim g \Rightarrow \mathrm{M}(f) \leq \mathrm{M}(g)$。类似地，$\mathrm{M}$ 强良态，当且仅当对于所有 f 和 g， $f \lesssim' g \Rightarrow \mathrm{M}(f) \leq \mathrm{M}(g)$。

证明。 根据定义可立即得出，良态测度尊重相应的归约。反过来，我们希望证明，假设 \mathrm{M} 尊重归约，则 \mathrm{M} 是良态的。良态意味着在限制到一个承诺时不增，并且在其他操作下保持不变。前一性质直接源于 \mathrm{M} 尊重归约这一事实（因为限制到一个承诺属于一种归约）。对于后一性质，考虑比特复制性质。我们需要证明，如果 f' 是 f的比特复制，那么 \mathrm{M}(f) =\mathrm{M}(f')。然而，如果 f'是 f的比特复制，那么 $f \lesssim f'$和 $f' \lesssim f$，因此我们知道 \mathrm{M}(f) $\leq$\mathrm{M}(f') 且 \mathrm{M}(f') $\leq$ \mathrm{M}(f)，所以 \mathrm{M}(f) =\mathrm{M}(f')，正如所需。由于良态定义中的所有其他性质都可以通过这种方式反向推导（限制到一个承诺除外），同样的论证适用于它们。 □

3.2 复合函数的可切换性与归约

定义32（开关函数）。 若函数 f 满足 switchable，则称其为可切换函数；若 $f \lesssim' f$，则称其为强可切换，即 $f \leq \overline{f}$。

我们还将开关函数定义为$\mathtt{S}$: $\{01, 10\} \to \{0, 1\}$，其定义为$\mathtt{S}(01) = 0$且$\mathtt{S}(10) = 1$。

注。 许多常见函数，例如 MAJ 和 Parity，都是可切换的（对于多数函数，将其所有比特取反会使输出取反；对于奇偶校验函数，将单个比特取反会使输出取反）。强可切换的自然函数较少，不过我们将在引理35 中看到，与开关函数复合会产生这类函数。像\ttA \ttN \ttD 和 或 这样的函数似乎不可切换（这里不予证明）。

引理 33。 f 是（强）可切换的，当且仅当 f 是（强）$\overline{\ }$ 可切换的。

证明。 假设 f是可切换的。那么 $f \lesssim^{\top} f$。考虑将这一约简应用于 f，而不是应用于 f。注意，约简中的操作（例如添加/移除重复位）并不依赖于

f的输出值；事实上，所有操作都与否定 $\underline{f}$的输出值可交换。因此，将约简应用于 f 等同于将其应用于 f，再对所得结果的输出值取反；但这会得到函数 $\underline{\ } f$，所以 $\underline{f} \lesssim' f$，这意味着 f是可切换的。反向结论可通过交换 f 和 f的角色得到。对于强可切换函数，证明完全相同。

□

推论34。 如果M 是强良态，且 f 可切换，那么$\mathrm{M}(f) = \mathrm{M}(f)$。如果$\mathrm{M}$ 是弱良态，且 f 强可切换，那么我们也有$\mathrm{M}(f) = \mathrm{M}(f)$。

引理35。对于 e　任意（可能是部分的）布尔函数 f，以下是$\mathsf{S} \circ f$ 的性质　d:

1. $\mathsf{S} \circ f \lesssim f$*2.* $\mathsf{S} \circ f$ 是强可切换的 *3.* f 可切换当且仅当 $f \lesssim' \mathsf{S} \circ f$*4.* f 强可切换当且仅当 $f \lesssim \mathsf{S} \circ f$。

证明。 为证明\ttS $\circ f \lesssim f$，从 f开始，添加 $n(f)$个冗余比特，它们可以取\mathrm{D}\mathrm{o}\mathrm{m}(f)中的任意值（这里 $n(f)$是 f的输入规模），并施加承诺：对于新定义域中的每个字符串xy， $f(x) \neq f(y)$。这样就得到了函数\ttS $\circ f$。

要看出 \ttS $\circ f$ 是强可切换的，只需注意到，交换 \ttS $\circ f$ 的两个块会使该函数的输出值取反（而这个取反后的函数实际上等于 \ttS $\circ f$）。

对于第三项，若 f 可切换，则有 $f \lesssim' f$。将此归约应用于 \ttS $\circ f$ 的第一个块（由一半的比特组成）。由于函数 \ttS $\circ f$ 始终等于将 f 应用于第一个块，归约后，新函数等于将 f 应用于第一个块，也等于将 f 应用于第二个块；除两个块具有相同的 f值这一条件外，它们彼此独立。现在施加两个块相同的承诺，并移除由此产生的重复位。这样便得到函数 f。由于 f 可切换，我们可以将其转换为f，因此 $f \lesssim'$\ttS $\circ f$。同样的证明也适用于说明，若 f强可切换，则 $f \lesssim$\ttS $\circ f$。

最后，假设 $f \lesssim'$\ttS $\circ f$。我们将证明 $f \lesssim' f$，这意味着根据引理 33， f是可切换的。根据当前引理的第一部分，我们有 \ttS $\circ f \lesssim f$。此外，很容易看出，\ttS $\circ f \lesssim$\ttS $\circ f$，因为 \ttS $\circ f$ 与 \ttS $\circ f$之间的唯一差异在于两个块的顺序，因此只需重新排列比特即可在二者之间转换。由于我们假设 $f \lesssim'$\ttS $\circ f$（并且由于 $\lesssim$是比 $\lesssim'$更强的性质），由传递性可得 $f \lesssim' f$。类似地，如果 $f \lesssim$\ttS $\circ f$，同样的论证给出$f \lesssim f$。证明完毕。 □

引理 36。 对于任意（可能是部分的）布尔函数 f、 g、 f'、 g'，我们有：

1. 如果 $g' \lesssim g$，那么 $f \circ g' \lesssim f \circ g$*2.* 如果 $f' \lesssim f$，那么 $f' \circ g \lesssim f \circ g$*3.* 如果 $g' \lesssim' g$，那么 $f \circ g' \lesssim' f \circ g$*4.* 如果 $f' \lesssim' f$与 g可切换，那么 $f' \circ g \lesssim' f \circ g$*5.* 如果 $f' \lesssim' f$与 g强可切换，那么 $f' \circ g \lesssim f \circ g$。

证明。 第一项和第三项都很直接：不难看出，重排 g 的比特会重排 $f \circ g$ 的比特，将 g 限制为一个承诺会将 $f \circ g$ 限制为一个承诺，复制 g 的比特会复制 $f \circ g$ 的比特（因此，删除 g 中的重复位会删除 $f \circ g$ 中的重复位），添加或移除 g 中的冗余比特会添加或移除 $f \circ g$ 中的冗余比特，而对 g 的比特取反会对 $f \circ g$ 的比特取反。

对于第二项，我们需要证明，如果我们可以通过添加/删除重复或冗余的比特、重新排列比特以及限制到一个承诺，将 f 转换为 f'，那么我们也可以使用这些操作将 $f \circ g$ 转换为$f' \circ g$。显然，重新排列 f的比特相当于重新排列 $f \circ g$的比特，而将 f限制到一个承诺相当于将 $f \circ g$限制到一个承诺。此外，向 f 添加冗余比特会向 $f \circ g$添加冗余比特，而从 f 删除冗余比特会从 $f \circ g$删除冗余比特（这里，若一组比特 $S \subseteq [n]$ 满足函数 $f(x)$ 的值仅取决于 $x_{[n]\setminus S}$，即除 S以外各比特上的部分赋值，并且对于任意此类部分赋值 $x_{[n]\setminus S}$，承诺中符合条件的 x_S 可能赋值始终相同，则称这组比特为冗余比特）。

剩下要处理的是重复比特的添加和删除。假设我们向 f添加比特复制，得到 f_i，并考虑 $f_i \circ g$。我们可以从 $f \circ g$ 构造它：添加一组多余的比特（对应于 g 的另一个输入，而该输入会被忽略），然后施加一个承诺（确保所添加比特块的 g值与 g的第 i 个输入相同）。因此 $f_i \circ g \lesssim f \circ g$。反过来，假设我们删除一个重复比特，从 f_i 得到 f。这一次，我们从 $f_i \circ g$出发，希望构造 $f \circ g$。函数 $f_i \circ g$ 在 g处有一个额外输入；我们将施加承诺，要求这个额外输入与 g的第 i 个输入相同。这样一来，这些额外输入比特就是重复比特，随后我们便可从所得函数中删除这些重复比特。第二项的证明至此完成。

对于最后两项，我们需要说明如何处理 f的比特取反。注意，对 f 的比特取反相当于切换 $f \circ g$各块的 g值。如果 g 是（强）可切换的，我们可以通过上述操作将其转换为 g （强可切换g的情况除外，因为其中不包括比特取反）。对单个块应用此操作，会翻转复合 $f \circ g$中外函数 f 对应的比特。所需结论由此得证。 □

推论 37. 设 f 和 g 是（可能为部分的）布尔函数。那么

1. 如果 f 是强可切换的，那么 $f \circ g$也是。
2. 如果 f 和 g 均可切换，那么 $f \circ g$也可切换。
3. 如果 f 可切换且 g 强可切换，那么 $f \circ g$ 强可切换。

证明。 如果 f强可切换，那么 $f \lesssim f, \neg$因此根据 引理 36 可得 $f \circ g \lesssim \neg f \circ g$。由于 $f \circ g$与$\neg f \circ g$ 是同一个函数，第一个结论成立。类似地，根据 引理 36 可得后两个结论。 □

我们注意到，\mathrm{M}($f \circ g$)可以视为 f 的测度（固定 g），也可以视为 g 的测度（固定 f）。由此可得以下性质。

推论 38. 假设$\mathrm{M}(f)$ 在复合封闭的 $\mathcal{A}$ 上是弱良态的。那么$\mathrm{M}(f \circ g)$ 是 f 的弱良性测度，也是 g的弱良性测度。

此外，如果 $\mathrm{M}(f)$ 是强良态的，那么 $\mathrm{M}(f \circ g)$ 作为 g 的函数也是强良态的；如果进一步而言， g 是可切换的，那么 $\mathrm{M}(f \circ g)$ 作为 f 的函数也是强良态的。

证明。 这可由引理 36和 引理 31立即推出。 □

3.3 块敏感度界

定义 39。 对于 $n \in \mathbb{N}$，令“承诺-或”函数 $\mathtt{PrOR}_n$ 为定义在 n 个比特上的函数，其\mathrm{D}\mathrm{o}\mathrm{m}}(\mathtt{PrOR}_n) $= \{x\colon\ |x| = 0$ 或 $|x| = 1\}$ 定义为 $\mathtt{PrOR}_n(0^n) = 0$，以及当 $|x| = 1$ 时，$\mathtt{PrOR}_n(x) = 1$。

定理 40。 对于任意（可能是部分的）布尔函数 f，$\mathtt{PrOR}^{\mathrm{bs}(f)} \circ \mathtt{S} \lesssim f$。因此，如果 M 是任意弱良态测度，那么 $\mathrm{M}(f) \geq \mathrm{M}(\mathtt{PrOR}^{\mathrm{bs}(f)} \circ \mathtt{S})$。

证明。令 $k =$\mathrm{b}\mathrm{s}(f)，并令 $n = n($f$)$ 为 f 的输入规模。回忆 $k =$ \mathrm{m}\mathrm{a}\mathrm{x}$^{x\in\mathrm{Dom}(f)}$\mathrm{b}\mathrm{s}$_x($f$)$。令 $x \in$ \mathrm{D}\mathrm{o}\mathrm{m}}(f) 满足 \mathrm{b}\mathrm{s}$_x($f$) = k$，并令 B_1，B_2，…，B_k 为 x 的互不相交的敏感块。将 f 限制在承诺集合 $\{x\} \cup \{x^{B_j}$ 上：$\ j \in [k]\}$，也就是说，该字符串 x 连同对 x 的块翻转（总共 $k+1$ 个字符串）。任何不属于任何块的比特在限制到该承诺后都将是常量，因此是多余的；移除所有此类比特。此外，在每个块 B_j 内，字符串 x 中取值为 0 的所有比特都是重复位，取值为 1 的所有比特也都是重复位；移除重复位后，块 B_j 的规模变为 1 或 2。如果块 B_j 变成单个比特，我们可以向输入中加入一个多余比特，并添加承诺：该新比特始终等于 B_j 中这个单比特的否定；这样便归结为 B_j 具有两个比特，且它们始终为 01 或 10 的情形。

最后，我们可以重新排列这些比特，使所有块都连续排列，并且在原先为 x 的输入中，所有块都呈现为 01。这意味着输入 x 变为 $(01)^k = 010101\ldots01$，而每个输入 x^{B_j} 都变为同一个字符串，只是第 j 对 01 变为 10。这正是函数 \ttP \ttr \ttO \ttR$_k \circ$ \ttS，因此我们如愿证明了 \ttP \ttr \ttO \ttR$_k \circ S \lesssim f$。

□

引理 41。 对于所有 $n \in \mathbb{N}$，$\mathtt{I} \lesssim \mathtt{PrOR}_n$。我们还有 $\mathtt{I} \lesssim' \mathtt{S}$。

证明。第一个结论可通过将范围限制在承诺 $\{0^n, 10^{n-1}\}$ 并移除 $n-1$ 个常量（多余）比特而得出。对于第二个结论，将 \ttS 的第二个比特取反；这样两个比特就相同了，移除重复位即可得到 \ttI。

□

推论 42。 设 f 和 g 是非常值（可能是偏）函数，且 M 是弱良态的。那么

1. *|mathrm{M}($f \circ g$) $\geq$ |mathrm{M}($f \circ$|ttP |ttr |ttO |ttR$^{\mathrm{bs}(g)} \circ$|ttS) $\geq$ |mathrm{M}($f \circ$ |ttS)*
2. *|mathrm{M}($f \circ g$) $\geq$ |mathrm{M}(|ttP |ttr |ttO |ttR$^{\mathrm{bs}(f)} \circ$|ttS $\circ g$) $\geq$ |mathrm{M}(|ttS $\circ g$)*
3. 若 *|mathrm{M}* 是强良态的，则 *|mathrm{M}($f \circ g$) $\geq$ |mathrm{M}($f \circ$ |ttP |ttr |ttO |ttR$^{\mathrm{bs}(g)}$) $\geq$ |mathrm{M}(f)* 4. 若 *|mathrm{M}* 是强良态的，且 g 是可切换的，则 *|mathrm{M}($f \circ g$) $\geq$ |mathrm{M}(|ttP |ttr |ttO |ttR$^{\mathrm{bs}(f)} \circ g$) $\geq$ |mathrm{M}(g)*。

证明。这些结论都可由 定理 40、引理 36 和 引理 41轻易推出 . □

注。 推论 42 表明，对于良态测度而言，开关函数 $\mathtt{S}$ 在相当强的意义下是最简单的非恒定函数（具体而言，$\mathrm{M}(f \circ g) \geq \mathrm{M}(f \circ \mathtt{S})$ 且 $\mathrm{M}(f \circ g) \geq \mathrm{M}(\mathtt{S} \circ g)$对所有非恒定的 f 和 g）。

4 递归复合的性质

4.1 合理有界度量

我们介绍一些关于测度复合行为的定义。

定义43 (合理上界有界（RUBO、RUBI）)。 设 $\mathcal{A} \subseteq \mathcal{F}$ 是一个复合封闭的函数类，且 M 是 $\mathcal{A}$ 上的测度。若存在某个测度 $\mathrm{N}\colon \mathcal{A} \to [0,\infty)$，使得对于所有 f、$g \in \mathcal{A}$，都有 $\mathrm{M}(f \circ g) \leq \mathrm{N}(f)\,\mathrm{M}(g)$，则称 M 在外部是合理上界有界（RUBO）。

类似地，如果存在某个测度 N，使得对所有 f、$g \in \mathcal{A}$，都有 M 是合理上界有界（RUBI），即 $\mathrm{M}(f \circ g) \leq \mathrm{M}(f)\,\mathrm{N}(g)$。

如果测度 N 满足 $\mathrm{N}(f) \leq \mathrm{M}(f)^{1+o(1)}$，我们就称相应的界近似线性。

我们还希望将合理下界测度定义为满足 \mathrm{M}($f \circ g$) $\geq$\mathrm{N}(f) \mathrm{M}(g) 的测度。然而，如果 \mathrm{N}(f) $= 0$，这个定义就变得平凡；但我们不能总是要求 \mathrm{N}(f) > 0，因为 \mathrm{M}($f \circ g$) 可能等于 0。为了使定义不平凡，我们要求除非 \mathrm{M}($f \circ g$) 为零，否则 \mathrm{N}(f) 非零。

定义 44 （合理下界有界（RLBO、RLBI））。 设 $\mathcal{A} \subseteq \mathcal{F}$ 是一个复合封闭的函数类，并设 M 是 $\mathcal{A}$ 上的一个测度。若存在 $\mathcal{A}$ 上的某个测度 N，使得对所有 f、$g \in \mathcal{A}$，$\mathrm{M}(f \circ g) \geq \mathrm{N}(f)\,\mathrm{M}(g)$，并且 $\mathrm{N}(f) = 0$ 蕴含 $\mathrm{M}(f \circ g) = 0$ 对所有 f、$g \in \mathcal{A}$ 均成立，则称 M 是外部合理下界有界（RLBO）。

类似地，若存在某个测度N，使得$\mathrm{M}(f \circ g) \geq \mathrm{M}(f)\,\mathrm{N}(g)$，且$\mathrm{N}(g) = 0 \Rightarrow \mathrm{M}(f \circ g) = 0$ 对所有 f、$g \in \mathcal{A}$ 均成立，则称M 是内部合理下界有界（RLBI）。

如果测度 N满足 $\mathrm{N}(f) \geq \mathrm{M}(f)^{1-o(1)}$，我们就说相应的界近似线性成立。

注意，RLBI 对所有良态测度都成立。

引理 45. 假设 M是强良态的，且对所有常函数 f，$\mathrm{M}(f) = 0$。那么M 满足 *RLBI*。

证明。回顾推论 42，其中指出只要 g 不是常数，就有 \mathrm{M}($f \circ g$) $\geq$\mathrm{M}(f)。于是我们可以定义 \mathrm{N}(g)：对于所有常数 g，其值为 0；对于所有非恒定 g，令 \mathrm{N}(g) $= 1$；则 \mathrm{M}($f \circ g$) $\geq$\mathrm{M}(f) \mathrm{N}(g)。最后，如果 \mathrm{N}(g) $= 0$，那么 g 是常数，因此 $f \circ g$ 是常数，这意味着 \mathrm{M}($f \circ g$) $= 0$。 □

我们还有以下结论。

定理46。 测度 $\mathrm{D}(f)$、$\mathrm{R}(f)$、$\mathrm{R}_0(f)$、$\mathrm{Q}(f)$、$\mathrm{s}(f)$、$\mathrm{fbs}(f)$、$\mathrm{C}(f)$、$\deg(f)$和$\deg(f)$均满足 *RLBI*，且都以近似线性的方式满足 *RUBO*。

证明。 不难验证，除 $\mathrm{s}(f)$ 之外，这些测度都具有强良态性，并且对常函数均等于 0；因此根据引理 45，它们都满足 RLBI。不难验证，$\mathrm{s}(f \circ g) \geq \mathrm{s}(f)$ 当 $\mathrm{s}(g) > 0$ 时成立，因此 s 也满足 RLBI。

算法测度 \mathrm{D}、\mathrm{R}、\mathrm{R}$_0$, 和 \mathrm{Q} 都可以通过运行计算 f 的算法来计算 $f \circ g$；每当该算法查询 f 的一个比特时，就运行相应的 g 算法。带有错误率的测度 \mathrm{R} 和 \mathrm{Q} 需要对用于 g 的子程序进行误差缩减，将错误率分别降至 o(1/\mathrm{R}(f)) 和 o(1/\mathrm{Q}(f))；这分别需要 O(\mathrm{l}\mathrm{o}\mathrm{g} \mathrm{R}(f)) 和 O(\mathrm{l}\mathrm{o}\mathrm{g} \mathrm{Q}(f)) 的开销。由此不难看出，\mathrm{D}($f \circ g$) $\leq$\mathrm{D}(f) \mathrm{D}(g)，\mathrm{R}$_0$($f \circ g$) $\leq$\mathrm{R}$_0$(f) \mathrm{R}$_0$(g)，\mathrm{R}($f \circ g$) $\leq O$(\mathrm{R}(f) \mathrm{l}\mathrm{o}\mathrm{g} \mathrm{R}(f)) $\cdot$\mathrm{R}(g)，以及 \mathrm{Q}($f \circ g$) $\leq O$(\mathrm{Q}(f) \mathrm{l}\mathrm{o}\mathrm{g} \mathrm{Q}(f)) $\cdot$\mathrm{Q}(g)；因此，这些测度近似线性地满足 RUBO。对于次数度量 \mathrm{d}\mathrm{e}\mathrm{g} 和 \mathrm{d}\mathrm{e}\mathrm{g}，类似的策略同样适用，因为多项式可以复合，而且多项式的误差缩减与算法的误差缩减类似。

这对证书也成立，因为要证明 $f \circ g$，只需证明外函数 f，然后对证书中的每个比特，证明内函数 g；因此 $\mathrm{C}(f \circ g) \leq \mathrm{C}(f)\,\mathrm{C}(g)$。对于分数块敏感度 fbs，我们使用其对偶形式，即分数证书复杂度 [Aar08;

KT16]。我们可以通过选取 $f \circ g$ 的一个分数证书，并将其与 f 的一个分数证书复合，来为 g指定一个分数证书，因此 $\mathrm{fbs}(f \circ g) \leq \mathrm{fbs}(f)\,\mathrm{fbs}(g)$。最后，可以直接证明 $\mathrm{s}(f \circ g) \leq \mathrm{s}(f)\,\mathrm{s}(g)$，因为对于 $f \circ g$的任意输入，只有那些敏感比特才对应于 g 某个输入的敏感比特，而后者又对应于 f 输入的一个敏感比特。这就完成了证明。 □

注。 上述列表中明显缺少了块敏感度 $\mathrm{bs}(f)$，它不满足近似线性的 RUBO。块敏感度的复合行为已在 [Tal13；GSS16] 中进行了研究。

以上内容引出了以下定义。

定义 47 (复合有界)。 复合封闭 $\mathcal{A}$ 上的测度M 称为复合有界，如果它满足 *RLBI*，且近似线性地满足 *RUBO*。

根据此定义，上述所有测度（\mathrm{b}\mathrm{s}(f) 除外）都是复合有界的。

4.2 收敛定理

定理 48。 设 $\mathcal{A} \subseteq \mathcal{F}$ 在复合下封闭，且 M 是 $\mathcal{A}$ 上的复合有界测度。那么，对于所有 $f \in \mathcal{A}$， $M^*(f)$ 均收敛。

为了证明这个定理，我们需要下面的引理。

引理 49. 假设 M 合理上界有界（在外部或内部）且合理下界有界（在外部或内部）。那么存在一个正整数序列 $k_1, k_2, \ldots$，满足以下条件：

1. 该序列递增：对于所有 $\ell \in \mathbb{N}^+$，都有 $k_\ell < k_{\ell+1}$
2. 这些整数彼此整除：对于所有 $\ell \in \mathbb{N}^+$，都有 $k_\ell | k_{\ell+1}$
3. 该序列的偶数项满足 $M(f^{k_{2\ell}})^{1/k_{2\ell}} \to M^*(f)$ 当 $\ell \to \infty$
4. 该序列的奇数项满足 $M(f^{k_{2\ell+1}})^{1/k_{2\ell+1}} \to M^*(f)$ 当 $\ell \to \infty$。

证明。 我们将逐个构造无限序列 $k_1, k_2, \ldots$。首先从一个长度为 0 的序列开始。现在假设在某个中间步骤中，序列里已有 $k_1, k_2, \ldots, k_{n-1}$（这些是彼此整除的递增整数）。对于任意固定的 $\epsilon > 0$，我们说明如何添加 k_n，使得 $k_n > k_{n-1}$, $k_{n-1} | k_n$，并且 \mathrm{M}(f^{k_n})$^{1/k_n} \geq$\mathrm{M}^*(f)$(1-\epsilon)$。同样，我们也会说明如何添加 k_n，使得 \mathrm{M}(f^{k_n})$^{1/k_n} \leq$\mathrm{M}^*(f)$(1+\epsilon)$。然后，我们可以交替向序列中添加 \mathrm{M}^*(f) 或 \mathrm{M}^*(f) 的一个近似值，并随着推进逐渐减小 ϵ。

要加上 k_n with \mathrm{M}(f^{k_n})$^{1/k_n} \geq$\mathrm{M}^*(f)$(1-\epsilon)$，我们首先注意到，存在无穷多个整数 k，使得 $|$\mathrm{M}(f^k)$^{1/k} -$\mathrm{M}^*(f)$| < \epsilon/2$。对于任意这样的 $k \geq 2k_{n-1}$，写作 $k = ck_{n-1} + r$ with$r \in [0, k_{n-1} - 1]$。那么，\mathrm{M}($f^{ck_{n-1}+r}$) 与 \mathrm{M}($f^{ck_{n-1}}$) 相差不超过因子 \mathrm{N}(f)^r，因此 \mathrm{M}($f^{ck_{n-1}}$)$^{1/ck_{n-1}}$ 与 \mathrm{M}(f^k)$^{1/(k-r)}$ 相差不超过因子 \mathrm{N}(f)$^{r/ck_{n-1}}$；而后者本身与 \mathrm{M}(f^k)$^{1/k}$ 相差不超过因子 \mathrm{M}(f^k)$^{1/(k-r)-1/k} =$(\mathrm{M}(f^k)$^{1/k})^{r/(k-r)}$。表达式 (\mathrm{M}(f^k)$^{1/k})^{r/(k-r)}$ 比 (\mathrm{M}(f^k)$^{1/k})^{1/c}$ 更接近 1，而 \mathrm{N}(f)$^{r/ck_{n-1}}$ 比 \mathrm{N}(f)$^{1/c}$ 更接近 1。这些又分别比 (\mathrm{M}(f^k)$^{1/k})^{1/(k-k_{n-1})}$ 和 \mathrm{N}(f)$^{1/(k-k_{n-1})}$ 更接近 1。注意，\mathrm{M}(f^k)$^{1/k} \geq$\mathrm{M}^*(f)$-\epsilon/2$；如果 \mathrm{M}^*(f) > 0，并且 ϵ 足够小，这意味着 \mathrm{M}(f^k)$^{1/k}$ 被两个正数界定，因此，只要选取足够大的 k，就能使 (\mathrm{M}(f^k)$^{1/k})^{1/(k-k_{n-1})}$ 任意接近 1，\mathrm{N}(f)$^{1/(k-k_{n-1})}$ 也一样。因此，通过选取足够大的 k，我们可以令 $k_n = ck_{n-1}$，并得出结论：\mathrm{M}(f^{k_n})$^{1/k_n}$ 与 \mathrm{M}^*(f) 的差在 ϵ 以内。在−

另一方面，如果 $\overline{\mathrm{M}}^*(f) = 0$，那么 $\mathrm{M}(f^k)^{1/k}$ 可以任意接近 0。在这种情况下，$\mathrm{M}(f^k)^{1/k} \cdot (\mathrm{M}(f^k)^{1/k})^{\pm 1/(k-k_{n-1})} = (\mathrm{M}(f^k)^{1/k})^{1\pm 1/(k-k_{n-1})}$ 也可以任意接近 0，而 $\mathrm{N}(f)^{1/(k-k_{n-1})}$ 可以任意接近 1。因此，我们仍然可以选取 $k_n = ck_{n-1}$，使其以误差 ϵ 逼近 $\overline{\mathrm{M}}^*(f)$。

这些论证同样适用于 $\underline{\mathrm{M}}^*(f)$，因此我们总能找到一个值 k，它是任意指定数值的倍数，并且能以任意选定的错误率 ϵ，逼近 $\overline{\mathrm{M}}^*(f)$ 或 $\underline{\mathrm{M}}^*(f)$。通过在序列中交替加入对 $\overline{\mathrm{M}}^*(f)$ 和 $\underline{\mathrm{M}}^*(f)$ 的近似值，并将所选的 ϵ 值逐渐减小至 0，我们便能构造出所需的序列。

□

定理 48 的证明。我们先讨论几个边界情形。首先，考虑对于无穷多个 k 值，$\mathrm{M}(f^k) = 0$ 的情形。在这种情况下，我们断言，对于所有 $k \geq 1$，$\mathrm{M}(f^k) = 0$。为此，反设结论不成立，并设 $k_1 < k_2$ 满足 $\mathrm{M}(f^{k_1}) > 0$ 且 $\mathrm{M}(f^{k_2}) = 0$。现在，由于 M 是 RLBI，存在一个测度 N，使得对于所有 f 和 g，$\mathrm{M}(f \circ g) \geq \mathrm{M}(f)\,\mathrm{N}(g)$；以 f^{k_2-1} 和 f 作为两个函数，可得 $M(f^{k_2}) \geq \mathrm{M}(f^{k_2-1})\,\mathrm{N}(f)$，反复应用便得到 $\mathrm{M}(f^{k_2}) \geq \mathrm{N}(f)\,\mathrm{M}(f^{k_2-1}) \geq \mathrm{N}(f)^2\mathrm{M}(f^{k_2-2}) \geq \cdots \geq \mathrm{N}(f)^{k_2-k_1}\mathrm{M}(f^{k_1})$。由于 $\mathrm{M}(f_2^k) = 0$ 且 $\mathrm{M}(f^{k_1}) > 0$，可知 $\mathrm{N}(f) = 0$。然而，定义 44 的条件指出，$\mathrm{N}(f) = 0$ 蕴含对于所有 g（包括 $g = \mathrm{I}$），$\mathrm{M}(f \circ g) = 0$。特别地，我们必须有对于所有 $k \geq 1$，$\mathrm{M}(f^k) = 0$，这意味着 $\overline{\mathrm{M}}^*(f)$ 收敛到 0。

接下来，考虑引理 49 中的序列 $k_1, k_2, \ldots$。注意，由于 M 的 RUBO/RLBI 性质，可得 $\overline{\mathrm{M}}^*(f) \leq \overline{\mathrm{N}}(f)$，且 $\underline{\mathrm{M}}^*(f) \geq \mathrm{N}'(f)$，其中测度 N 和 N' 可能不同，因此特别地，这两个值都有限。于是，要证明 $\overline{\mathrm{M}}^*(f)$ 收敛，只需证明 $\overline{\mathrm{M}}^*(f) = \underline{\mathrm{M}}^*(f)$；这等价于证明序列 $[\mathrm{M}(f^{k_i})^{1/k_i}]_{i=1}^{\infty}$ 的偶数项和奇数项收敛到相同的值。

由于我们可以假设 $\mathrm{M}(f^k)$ 仅在有限多个时候为零，因此可以取足够大的 i，使得对所有 $j \geq i$，都有 $\mathrm{M}(f^{k_j}) > 0$。于是，对所有 $j \geq i$，k_j 都是 k_i 的倍数。令 $g = f^{k_i}$；那么序列 $[\mathrm{M}(f^{k_j})^{1/k_j}]_{j=i}^{\infty}$ 可以写成 $[\mathrm{M}(g^{m_\ell})^{1/k_i m_\ell}]_{\ell=0}^{\infty}$，其中 $m_\ell = k_{\ell+i}/k_i$。由此不难看出，$\overline{\mathrm{M}}^*(f)$ 收敛当且仅当 $\overline{\mathrm{M}}^*(g)$ 收敛；如有必要，用 g 替换 f，我们可以假设对所有 $k \geq 1$，都有 $\mathrm{M}(f^k) > 0$，并且仍然有一个如引理 49 中所述的有效序列 $k_1, k_2, \ldots$，只是这一次所有值 $\mathrm{M}(f^{k_i})$ 都非零。

只需证明，对于任意固定的 $\epsilon > 0$，$\overline{\mathrm{M}}^*(f) \leq \mathrm{M}^*(f) + \epsilon$。由近线性的 RUBO 性质可知，对于所有 $k \geq 2$，有 $\mathrm{M}(f^k) \leq \mathrm{M}(f)^{1+o(1)}\mathrm{M}(f^{k-1})$。取足够小的 $\delta > 0$，使得 $(\mathrm{M}^*(f) + \epsilon/3)^{1+\delta} \leq \underline{\mathrm{M}}^*(f) + 2\epsilon/3$。根据定义 21，取 $C \geq 1$，使得当 $k \geq 2$，$1 \leq \ell \leq k-1$ 且 $\mathrm{M}(f^k) > C\mathrm{M}(f^\ell)\,\mathrm{M}(f^{k-\ell})$ 时，$\mathrm{M}(f^k) \leq \mathrm{M}(f^\ell)^{1+\delta}\mathrm{M}(f^{k-\ell})$。于是，对每个 $k \geq 2$，都有 $\mathrm{M}(f^k) \leq \mathrm{M}(f^\ell)\,\mathrm{M}(f^{k-\ell})\,\mathrm{max}\{C, \mathrm{M}(f^\ell)^\delta\}$。类似地，$\mathrm{M}(f^{k-\ell}) \leq \mathrm{M}(f^\ell)\,\mathrm{M}(f^{k-2\ell})\,\mathrm{max}\{C, \mathrm{M}(f^\ell)^\delta\}$。综上，当 ℓ 整除 k 时，我们得到

$$\begin{aligned}
\mathrm{M}(f^k) &\leq \mathrm{M}(f^\ell)\,\mathrm{M}(f^{k-\ell})\max\{C, \mathrm{M}(f^\ell)^\delta\} \\
&\leq \mathrm{M}(f^\ell)^2\,\mathrm{M}(f^{k-2\ell})\max\{C, \mathrm{M}(f^\ell)^\delta\}^2 \\
&\leq \ldots \\
&\leq \mathrm{M}(f^\ell)^{k/\ell}\max\{C, \mathrm{M}(f^\ell)^\delta\}^{k/\ell}.
\end{aligned}$$

因此，只要 ℓ 整除 k，我们就可以写成

$$\mathrm{M}(f^k)^{1/k} \leq \mathrm{M}(f^\ell)^{1/\ell}\max\{C^{1/\ell}, (\mathrm{M}(f^\ell)^{1/\ell})^\delta\}.$$

现在，取一个足够大的偶数项 k_i，使得 $\mathrm{M}(f^{k_i})^{1/k_i} \leq \underline{\mathrm{M}}^*(f) + \epsilon/3$，并且使得 $C^{1/k_i}(\overline{\mathrm{M}}^*(f) + \epsilon/3) \leq \overline{\mathrm{M}}^*(f) + 2\epsilon/3$。此外，取一个大于 k_i 的奇数项 k_j，且足够大，使得 $\mathrm{M}(f^{k_j})^{1/k_j} \geq$

\mathrm{M}^{*}(f) $-\epsilon/3$。然后在上文中令 $k=k_j$ 和 $\ell=k_i$，并写作

$$\begin{aligned}\mathrm{M}^{\overline{*}}(f) &\le \mathrm{M}(f^k)^{1/k}+\epsilon/3\\ &\le \epsilon/3+\mathrm{M}(f^\ell)^{1/\ell}\max\{C^{1/\ell},(\mathrm{M}(f^\ell)^{1/\ell})^\delta\}\\ &\le \epsilon/3+\max\{C^{1/\ell}(\mathrm{M}^{\underline{*}}(f)+\epsilon/3),(\mathrm{M}^{\underline{*}}(f)+\epsilon/3)^{1+\delta}\}\\ &\le \epsilon+\mathrm{M}^{\underline{*}}(f).\end{aligned}$$

由于 ϵ 是任意的，我们必有 \mathrm{M}^{*}(f) $=$ \mathrm{M}^{*}(f)，如所求。 □

4.3 复合极限的性质

我们列出复合极限的一些基本性质。

引理 50. 若M 是弱良性测度，且 M^* 收敛，那么M^* 也弱良态。

证明. 我们需要证明，若 $f'\lesssim f$，则 \mathrm{M}^{*}(f') $\le$\mathrm{M}^{*}(f)（见引理 31）。只需证明，对所有 $k\in\mathbb{N}$，\mathrm{M}((f')^{k}) $\le$\mathrm{M}(f^{k})。利用引理 36，我们可以逐个将 $f^k=f\circ f\circ\cdots\circ f$ 中的每个 f 替换为 f'，直到得到 $(f')^k=f'\circ\cdots\circ f'$。每次将 f 替换为 f'，得到的函数都小于或等于前一个函数（按 $\lesssim$ 序）。因此 $(f')^k\lesssim f^k$，所求结论得证。 □

引理 51。 如果 $\mathrm{M}^*(f)$ 收敛，那么对每个 $k\in\mathbb{N}$，$\mathrm{M}^*(f^k)$ 都收敛，并且 $\mathrm{M}^*(f^k)=\mathrm{M}^*(f)^k$。

证明。 我们有

$$\mathrm{M}^*(f^k)=\lim_{n\to\infty}\mathrm{M}((f^k)^n)^{1/n}=\lim_{n\to\infty}(\mathrm{M}(f^{kn})^{1/kn})^k=(\lim_{n\to\infty}\mathrm{M}(f^{kn})^{1/kn})^k=\mathrm{M}^*(f)^k,$$

这里我们将极限与连续函数 x^k 交换，并用到了这样一个事实：收敛序列的子序列收敛于同一个极限。 □

推论 52。 如果 $\mathrm{M}^*(f)$ 收敛，那么 $\mathrm{M}^{**}(f)$ 也收敛，并且 $\mathrm{M}^{**}(f)=\mathrm{M}^*(f\quad)$.

证明。我们有 \mathrm{M}^{**}(f) $=$\mathrm{l}\mathrm{i}\mathrm{m}_{k\to\infty}\mathrm{M}^{*}(f^{k})^{1/k}，但根据引理 51，\mathrm{M}^{*}(f^{k}) $=$\mathrm{M}^{*}(f)^{k}，所以这是常数序列 \mathrm{M}^{*}(f)，它收敛于 \mathrm{M}^{*}(f)。□

引理 53. 假设 M 在复合封闭类 $\mathcal{A}\subseteq\mathcal{F}$ 上复合有界。那么$\mathrm{M}^*(f\circ g)=\mathrm{M}^*(g\circ f)$ 对所有 $f,g\in\mathcal{A}$ 均成立。

证明. 假设 \mathrm{N}(f) $\neq 0$，其中 \mathrm{N} 是 RLBI 性质中的测度。记

$$\mathrm{M}((f\circ g)^k)=\mathrm{M}(f\circ(g\circ f)^{k-1}\circ g)\le\frac{\mathrm{M}(f)^{1+o(1)}}{\mathrm{N}(f)}\mathrm{M}((g\circ f)^k),$$

这里，我们使用近线性 RUBO 性质来给 \mathrm{M}(f\circ(g\circ f)^{k-1}\circ g) $\le$\mathrm{M}(f)^{1+o(1)} \mathrm{M}((g\circ f)^{k-1}\circ g) 提供上界，并使用 RLBI 性质来给 \mathrm{M}((g\circ f)^{k-1}\circ g\circ f) $\ge$ \mathrm{M}((g\circ f)^{k-1}\circ g) \mathrm{N}(f) 提供上界。将两边提升到 $1/k$ 次幂并取极限，即得所需结果。

接下来，假设 \mathrm{N}(g) $\neq 0$。我们可以使用相同的证明，只需从 \mathrm{M}((g\circ f)^{k}) 开始，而不是从 \mathrm{M}((f\circ g)^{k}) 开始。

最后，假设 \mathrm{N}(f) $=$\mathrm{N}(g) $=0$。那么对于所有 $h\in\mathcal{A}$，\mathrm{M}(h\circ f) $=0$，特别是对于所有 k，\mathrm{M}((g\circ f)^{k}) $=0$。类似地，对于所有 k，\mathrm{M}((f\circ g)^{k}) $=0$。这意味着 \mathrm{M}^{*}(g\circ f) $=0=$\mathrm{M}^{*}(f\circ g)，如所求。 □

引理 54。 如果$\mathrm{M}(f) \leq \mathrm{N}(f)^{c+o(1)}$对某个常数 c成立，并且$\mathrm{M}^*(f)$和$\mathrm{N}^*(f)$都收敛，且$\mathrm{M}^*(f) \geq 1$，那么$\mathrm{M}^*(f) \leq \mathrm{N}^*(f)^c$。

证明。根据小 o 记号的定义 21，对于任意固定的 $\delta > 0$，存在一个常数 $C > 0$，使得对所有 f，\mathrm{M}(f) \leq \mathrm{m}\mathrm{a}\mathrm{x}{\mathrm{N}(f)^{c+\delta}, C} 成立。于是 \mathrm{M}(f^k)^{1/k} \leq\ mathrm{m}\mathrm{a}\mathrm{x}{\mathrm{N}(f^k)^{(c+\delta)/k}, C^{1/k}}，取极限可得 \mathrm{M}^*(f) \leq \mathrm{m}\mathrm{a}\mathrm{x}{\mathrm{N}^*(f)^{c+\delta}, 1}。由于这对所有 $\delta > 0$ 都成立，我们得到 \mathrm{M}^*(f) \leq \mathrm{m}\mathrm{a}\mathrm{x}{\mathrm{N}^*(f)^c, 1}，证毕。 □

引理 *55.* *如果对所有 f 和 g，|mathrm{M}(f \circ g) \leq|mathrm{N}(f) |mathrm{M}(g)，并且 |mathrm{M}^*(f) 收敛，那么 |mathrm{M}^*(f) \leq |mathrm{N}(f)。类似地，如果对所有 f 和 g，|mathrm{M}(f \circ g) \leq|mathrm{M}(f) |mathrm{N}(g)，那么 |mathrm{M}^*(f) \leq|mathrm{N}(f)。*

下界方向也成立：如果对所有 f 和 g，$\mathrm{M}(f \circ g) \geq \mathrm{N}(f)\,\mathrm{M}(g)$；或者对所有 f 和 g，$\mathrm{M}(f \circ g) \geq \mathrm{M}(f)\,\mathrm{N}(g)$，那么只要 $\mathrm{M}(f^k)$ 并非始终为 0（且 $\mathrm{M}^*(f)$ 收敛），就有 $\mathrm{M}^*(f) \geq \mathrm{N}(f)$。

证明。如果 \mathrm{M}(f \circ g) \leq\mathrm{N}(f) \mathrm{M}(g)，那么 \mathrm{M}(f^k) \leq\mathrm{N}(f) \mathrm{M}(f^{k-1}) \leq\ mathrm{N}(f)^2\mathrm{M}(f^{k-2}) \leq \cdots \leq\mathrm{N}(f)^k\mathrm{M}(\ttI)。于是 \mathrm{M}(f^k)^{1/k} \leq\mathrm{N}(f) \mathrm{M}(\ttI)^{1/k}。由于 $k \to \infty$，\mathrm{M}(\ttI)^{1/k}要么收敛于 0，要么收敛于 1，而在这两种情况下我们都得到 \mathrm{M}^*(f) \leq\mathrm{N}(f)，证毕。当 \mathrm{M}(f \circ g) \leq\mathrm{M}(f) \mathrm{N}(g) 时同样成立。

对于下界，同样的论证表明，对于任意 $k \geq \ell$，\mathrm{M}(f^k) \geq\mathrm{N}(f)^{k-\ell}\mathrm{M}(f^\ell)。取满足 \mathrm{M}(f^\ell) \neq 0 的 ℓ。于是 \mathrm{M}(f^k)^{1/k} \geq\mathrm{N}(f)^{1-\ell/k}\mathrm{M}(f^\ell)^{1/k}，并且由于 $k \to \infty$，我们得到 \mathrm{M}^*(f) \geq\mathrm{N}(f)，如所需。 □

推论 *56.* *|mathrm{R}^*(f) = O(|mathrm{R}(f) |mathrm{l}|mathrm{o}|mathrm{g} |mathrm{R}(f))。此外，|mathrm{R}^*(f) =|Omega (|mathrm{n}|mathrm{o}|mathrm{i}|mathrm{s}|mathrm{y}|mathrm{R}(f) +|mathrm{L}|mathrm{R}(f))，其中测度 |mathrm{n}|mathrm{o}|mathrm{i}|mathrm{s}|mathrm{y}|mathrm{R}(f) 和 |mathrm{L}|mathrm{R}(f) 分别定义于 [BB20]和 [BBGM22]。*

证明。这由引理 55 得出，再结合以下观察：\mathrm{R}(f \circ g) = O(\mathrm{R}(f) \mathrm{l}\mathrm{o}\mathrm{g} \mathrm{R}(f)· \mathrm{R}(g))、\mathrm{R}(f \circ g) =\Omega (\mathrm{n}\mathrm{o}\mathrm{i}\mathrm{s}\mathrm{y}\mathrm{R}(f) \mathrm{R}(g)) [BB20],以及 \mathrm{R}(f \circ g) =\Omega (\mathrm{R}(f) \mathrm{L}\mathrm{R}(g)) [BBGM22],，这些观察对所有偏函数 f 和 g均成立。 □

引理 57。 设M 和N 是具有收敛的复合极限的测度，且设 $c > 0$ 为常数。则

1. $c\,\mathrm{M}$具有收敛的复合极限，且$(c\mathrm{M})^* = \mathrm{M}^*$
2. M^c 具有收敛的复合极限，并且$(\mathrm{M}^c)^* = (\mathrm{M}^*)^c$
3. $\mathrm{M} + \mathrm{N}$具有收敛的复合极限，并且$(\mathrm{M} + \mathrm{N})^* = \max\{\mathrm{M}^*, \mathrm{N}^*\}$
4. $\mathrm{M} \cdot \mathrm{N}$具有收敛的复合极限，并且$(\mathrm{M} \cdot \mathrm{N})^* = \mathrm{M}^* \cdot \mathrm{N}^*$。

证明。所有这些结论都直接源自极限的性质。最棘手的是 (\mathrm{M} + \mathrm{N})^* =\mathrm{m}\mathrm{a}\mathrm{x}{\mathrm{M}^*, \mathrm{N}^*}，这等价于证明 \mathrm{l}\mathrm{i}\mathrm{m}_{k\to\infty}(\mathrm{M}(f^k) +\mathrm{N}(f^k))^{1/k} = \mathrm{m}\mathrm{a}\mathrm{x}{\mathrm{M}^*(f), \mathrm{N}^*(f)}。利用 \mathrm{M}(f^k) +\mathrm{N}(f^k) \leq 2 \mathrm{m}\mathrm{a}\mathrm{x}{\mathrm{M}(f^k), \mathrm{N}(f^k)}，即可不难证明这一点。 □

5 拉斯维加斯算法的复合极限

定义测度 \mathrm{Q}c(f) 为找到证书所需的量子算法查询次数。也就是说，量子算法必须输出一个证书 c，以证明输入 x 的值 $f(x)$，并且必须以至少 $1/2$ 的概率成功生成 c（如果失败，则应输出失败符号 $\perp$）。这个定义有一点需要注意：我们要求输出的证书大小计入成本；也就是说，返回证书 c 的成本应为所使用的量子查询次数，加上 $|c|$，即由 c 揭示的比特数。其直观含义是，一个

经典算法将使用额外的 $|c|$ 次查询来验证返回的证书。请注意，这确保了 \mathrm{Q}_{\mathrm{C}}(f) $\geq$ \mathrm{C}(f)。

我们注意到，由于此类算法在失败后可以重复运行，因此可以用它来构造一个针对 f 的拉斯维加斯式量子算法，其期望查询次数至多为 2 \mathrm{Q}_{\mathrm{C}}(f)。我们还注意到，这种测度的随机化版本与 \mathrm{R}_0(f) 仅相差常数因子，因为众所周知，零错误的随机化查询算法必须在输入中找到一个证书。（要理解这一点，可以注意到，如果某次运行某种 \mathrm{R}_0(f) 类型的算法在未找到证书的情况下终止，并声称知道输入 x 上 $f(x)$ 的值，那么根据证书的定义，在 f 的定义域中存在某个 y-输入，它与已查询的比特一致，且满足 $f(y) \neq f(x)$；那么，如果在 x上运行同一算法，而非在 y上运行，它就有非零概率到达同一个叶节点并给出相同的输出，这与零错误性质相矛盾。）

因此，这些寻找证书的量子算法是定义零错误量子算法的一种可能方式。

引理 58。 $\mathrm{Q}_{\mathrm{C}}(f)$ 是强良态、复合有界的，并且对于所有（可能是部分的） f，$\mathrm{Q}^*_{\mathrm{C}}(f)$ 都收敛。

证明。 很容易看出，\mathrm{Q}_{\mathrm{C}}(f) 是强良态的：如果返回的证书是最小的，那么证书大小和算法所用的查询次数在重命名指标、添加冗余比特、复制比特以及进行字母表重命名（将比特从 0 翻转为 1）时均保持不变；此外，限制到承诺后，测度不会增加。

另请注意，如果 f 是常数，则 \mathrm{Q}_{\mathrm{C}}(f) $= 0$ 。这是因为我们总能返回空证书（不进行任何查询）。由引理 45 可知，\mathrm{Q}_{\mathrm{C}}(f) 满足 RLBI。接下来只需证明它以近似线性的方式满足 RUBO，这使其复合有界，因此根据定理 48，\mathrm{Q}^*_{\mathrm{C}}(f) 收敛。换言之，我们必须证明 \mathrm{Q}_{\mathrm{C}}(f \circ g) $\leq$ \mathrm{Q}_{\mathrm{C}}(f)^{1+o(1)} \mathrm{Q}_{\mathrm{C}}(g)。

这可以由量子算法的常规复合得到，具体如下：从一个针对 \mathrm{Q}_{\mathrm{C}}(g) 的最优算法开始，将其重复运行 O(\mathrm{l}\mathrm{o}\mathrm{g} \mathrm{Q}_{\mathrm{C}}(f)) 次以放大其效果，从而将失败概率降至例如 (10 \mathrm{Q}_{\mathrm{C}}(f))^{-10}。然后，用这个放大后的算法替代 g 中针对输入比特的量子预言机调用，并运行 \mathrm{Q}_{\mathrm{C}}(f) 的算法（为放大目的重复运行两次）。以这种方式运行 \mathrm{Q}_{\mathrm{C}}(f) 的算法时，我们确保对最终找到的 f 的证书，进行经典查询（调用那些量子 g 子程序）。由于每个 g 子程序都会返回该副本 g 的证书，我们最终得到 f 的证书；对于其中的每个比特，还能得到对应副本 g 的证书。这些证书合在一起，就构成了 $f \circ g$ 的证书，我们随后将其返回。

由于针对 g 的子程序失败概率极低，因此在针对 g 的子程序上运行时，针对 f 的算法所产生的工作态与在干净预言机查询上运行针对 f 的算法所得的工作态之间的迹距离很小。由此很容易看出，所得算法的总失败概率至多为 $1/4 + o(1) \leq 1/2$ （ $1/4$ 是因为我们将 \mathrm{Q}_{\mathrm{C}}(f) 运行了两次，且每次失败的概率均为 $1/2$； $o(1)$ 则是 g 子程序失败所导致的贡献）。因此，所用查询的总数为 O(\mathrm{Q}_{\mathrm{C}}(f) \mathrm{Q}_{\mathrm{C}}(g) \mathrm{l}\mathrm{o}\mathrm{g} \mathrm{Q}_{\mathrm{C}}(f))。这给出了 \mathrm{Q}_{\mathrm{C}}(f \circ g) 所需的上界，证明得证。 □

现在我们证明主要结果。

定理 59。

$$\mathrm{R}^*_0(f) = \max\{\mathrm{R}^*(f), \mathrm{C}^*(f)\},$$
$$\mathrm{Q}^*_{\mathrm{C}}(f) = \max\{\mathrm{Q}^*(f), \mathrm{C}^*(f)\}.$$

证明。我们对 \mathrm{Q}c(f) 证明这一点。对于随机化查询复杂度，论证将类似。固定一个定义在 n 比特上的（可能是部分）布尔函数 f。不妨设 $n \geq 2$，因为 $n = 1$ 情形是平凡的。我们还假设 f 不是常数。

我们递归地定义一个量子算法，用于寻找 f^k 的证书；对于每个 k，将其记为 A_k。每个这样的算法 A_k 找到 f^k 的证书的概率至少为 $1/2$。A_k 使用的最坏情况下的查询次数记为 q_k。基本情形为 $k = 1$；对于函数 $f^1 = f$，我们只需给出 $q_1 \leq n$ 的上界。

现在假设 $k > 0$ 和 A_{k-1} 已经定义。算法 A_k 的工作方式如下。考虑复合 f^k 中最顶层的 f 副本；该副本有 n 个比特，每个比特都是将 f^{k-1} 应用于互不相交的输入得到的。对于其中的每个 n 个 f^{k-1} 副本，我们首先使用蒙特卡洛算法估计其输出值。具体来说，我们使用针对 f^{k-1} 的最佳有界错误量子算法，该算法使用 \mathrm{Q}(f^{k-1}) 次查询；然后通过重复运行多次并取多数函数来放大该算法，直到其最坏情况下的错误率从 $1/3$ 降至 $1/4n$。每个 f^{k-1} 副本需要使用 O(\mathrm{Q}(f^{k-1}) \mathrm{l}\mathrm{o}\mathrm{g} n) 次量子查询，而这样的副本共有 n 个。注意，由于 $n \geq 2$，我们有 \mathrm{l}\mathrm{o}\mathrm{g} $n > 0$，并且可以认为大 O 记号中的常数是乘法常数。换言之，存在一个通用常数 C（与 f、k 和 n 无关），使得使用至多 C\mathrm{Q}(f^{k-1})n \mathrm{l}\mathrm{o}\mathrm{g} n 次查询，我们就能估计输入到最顶层 f 副本的所有 n 个输入。此外，每个估计出的比特出错的概率至多为 $1/4n$；根据并集界，它们全部正确的概率至少为 $1/4$。

令 $x \in \{0,1\}^{n^k}$ 表示 f^k 的输入，并令 $z \in \{0,1\}^n$ 表示对 f 最顶层副本输入的估计值。如果 z不属于 \mathrm{D}\mathrm{o}\mathrm{m}(f)，算法 A_k则声明失败并终止（输出$\perp$）。如果 $z \in$ \mathrm{D}\mathrm{o}\mathrm{m}(f)，算法会找到一个与 z一致、大小至多为 \mathrm{C}(f) 的 f 的证书 c。证书 c 至多揭示 \mathrm{C}(f) 个比特。对于其中每个比特，算法 A_k 随后会在 f^{k-1} 的对应副本上应用 A_{k-1}；如果算法 A_{k-1} 输出 $\perp$，则重复执行，最多重复$1 + \lceil$ \mathrm{l}\mathrm{o}\mathrm{g} \mathrm{C}(f)$\rceil \leq 2 +$\mathrm{l}\mathrm{o}\mathrm{g} \mathrm{C}(f) 次，以确保失败概率降至至多 $1/4$\mathrm{C}(f)。接着，我们检查所有得到的证书。如果这些副本的函数值与预测值（来自证书 c）一致，我们就将所有得到的证书合并成一个关于 f^k 的大证书并返回（这是有效证书，因为我们已经验证了顶层副本 f 的证书 c 中的所有比特）。否则，如果某个函数值与证书 c 所预测的比特不符，我们就返回 $\perp$。至此，A_k 的定义完成。

注意，A_k 生成错误预测的概率只有 $1/4$ z，而该预测针对的是 f的最顶层输入。此外，如果 z正确，那么假设 $x \in$\mathrm{D}\mathrm{o}\mathrm{m}(f^k)，我们必有 $z \in$\mathrm{D}\mathrm{o}\mathrm{m}(f)，且c 是 z的有效证书。在这种情况下，算法唯一可能失败的方式，就是 A_{k-1}的某次运行在经过 $1 + \lceil$ \mathrm{l}\mathrm{o}\mathrm{g} \mathrm{C}(f)$\rceil$ 次重复后仍然失败。对于这些运行中的任意一次，在所有重复中都失败的概率至多为 $1/4$\mathrm{C}(f)；因此，这些运行（对应证书 c的不同比特）全部失败的概率至多为 $1/4$。根据并集界，A_k 输出 $\perp$ 的概率至多为 $1/2$，因此它是一个有效的证书查找算法。

现在我们来分析它的查询复杂度。第一部分中，当我们找到猜测字符串 z 时，最多使用 C\mathrm{Q}(f^{k-1}) n\mathrm{l}\mathrm{o}\mathrm{g} n 次查询。第二部分中，我们对 \mathrm{C}(f) 个比特中的每一个重复执行 A_{k-1}，每个重复 $2 +$\mathrm{l}\mathrm{o}\mathrm{g} \mathrm{C}(f) 次；为此使用的查询数为 q_{k-1} \mathrm{C}(f)(2 +\mathrm{l}\mathrm{o}\mathrm{g} \mathrm{C}(f))。由此得到递推关系

$$q_k \leq C\,\mathrm{Q}(f^{k-1}) n \log n + \mathrm{C}(f)(2 + \log \mathrm{C}(f)) q_{k-1}.$$

令 $a = Cn$\mathrm{l}\mathrm{o}\mathrm{g} n 且 $b =$\mathrm{C}(f)(2 + \mathrm{l}\mathrm{o}\mathrm{g} \mathrm{C}(f))。那么

$$q_k \leq a\,\mathrm{Q}(f^{k-1}) + b q_{k-1} \leq a\,\mathrm{Q}(f^{k-1}) + ab\,\mathrm{Q}(f^{k-2}) + b^2 q_{k-2} \leq \dots$$

$$\leq a\,\mathrm{Q}(f^{k-1}) + ab\,\mathrm{Q}(f^{k-2}) + ab^2\,\mathrm{Q}(f^{k-3}) + \dots + ab^{k-2}\,\mathrm{Q}(f^1) + b^{k-1} q_1.$$

现在我们使用 $q_1 = n \le a$ 与 \mathrm{Q}(f^ℓ) $\le d$\mathrm{Q}(f)$^\ell$，其中常数为 $d \ge 1$，且对所有 ℓ 均成立。这使我们能够用几何级数来界定 q_k：

$$q_k \le da\,\mathrm{Q}(f)^k \sum_{i=1}^{k-1} \left(\frac{b}{\mathrm{Q}(f)}\right)^i.$$

现在，如果 $b \ge$ \mathrm{Q}(f)/2，那么将 b 替换为 $4b$，就会得到一个几何级数，每次至少增大为原来的 2 倍，因此其上界为最大项的两倍；在这种情况下 $q_k \le 2da$ \mathrm{Q}(f)($4b$)$^{k-1} \le da$($4b$)^k，或者

$$\mathrm{Q_C}(f^k) \le C' n \log n \cdot (5\,\mathrm{C}(f) \log(4\,\mathrm{C}(f)))^k$$

对于 $C' = dC$ （5 来自额外加上的一个 \mathrm{C}(f^k) $\le$ \mathrm{C}(f)^k 因子，该因子根据 \mathrm{Q}$_\mathrm{C}$(f^k) $= q_k +$\mathrm{C}(f^k) 的定义得出）。或者，如果 $b \le$\mathrm{Q}(f)/2，那么几何级数每次都会缩小为原来的 1/2，因此其上界为首项的两倍；在这种情况下 $q_k \le 2dab$\mathrm{Q}(f)$^{k-1} \le da$ \mathrm{Q}(f)^k，或者

$$\mathrm{Q_C}(f^k) \le C' n \log n \cdot \mathrm{Q}(f)^k + \mathrm{C}(f)^k.$$

在两种情况下，我们得到

$$\mathrm{Q_C}(f^k) \le C' n \log n \cdot \left((5\,\mathrm{C}(f) \log 4\,\mathrm{C}(f))^k + \mathrm{Q}(f)^k\right).$$

将两边取 $1/k$ 次幂，并令 $k \to \infty$ 时的极限趋于，我们得到

$$\mathrm{Q^*_C}(f) \le \max\{5\,\mathrm{C}(f) \log 4\,\mathrm{C}(f), \mathrm{Q}(f)\}.$$

最后，我们对两边取星号。根据 推论 52，我们有 $\mathrm{Q^{**}_C}(f) = \mathrm{Q^*_C}(f)$。根据 引理 54，对测度 $*$取 $5\,\mathrm{C}(f) \log 4\,\mathrm{C}(f)$ 可得 $\mathrm{C}^*(f)$。由此可知

$$\mathrm{Q^*_C}(f) \le \max\{\mathrm{Q}^*(f), \mathrm{C}^*(f)\}.$$

相应的下界很容易得到：根据证书查找算法的定义，任何为 f^k 查找证书的算法，其成本都至少为 \mathrm{C}(f^k)。此外，任何证书查找算法都可以轻松转换为有界错误算法，而无需增加成本（如果证书查找算法输出 $\perp$，只需随机猜测输出即可）。这表明 \mathrm{Q}*(f) 和 \mathrm{C}*(f) 的下界正如所需。

随机化算法的情况完全相同，只有最后的递推关系有所不同；在那里，我们对某个常数 d 使用了 \mathrm{Q}(f^ℓ) $\le d$\mathrm{Q}(f)$^\ell$，但这对随机化算法不成立。我们改为对某个常数 d 使用 \mathrm{R}(f^ℓ) $\le$(d\mathrm{R}(f) \mathrm{l}\mathrm{o}\mathrm{g} \mathrm{R}(f))$^\ell$。于是，最终的界为

$$\mathrm{R_C}(f^k) \le C' n \log n \cdot \left((5\,\mathrm{C}(f) \log 4\,\mathrm{C}(f))^k + (d\,\mathrm{R}(f) \log \mathrm{R}(f))^k\right),$$

证明的其余部分类似地进行（首先将两边取 $1/k$ 次方，然后取极限 $k \to \infty$，得到上界 O(\mathrm{C}(f) \mathrm{l}\mathrm{o}\mathrm{g} 4 \mathrm{C}(f) $+$\mathrm{R}(f) \mathrm{l}\mathrm{o}\mathrm{g} \mathrm{R}(f))，接着对两边取星号，将其改进为上界 \mathrm{m}\mathrm{a}\mathrm{x}{\mathrm{C}*(f), \mathrm{R}*(f)}）。我们注意到 \mathrm{R}$^*_\mathrm{C}$(f) $=$\mathrm{R}$^*_0$(f)，因为 \mathrm{R}$_\mathrm{C}$(f) 和 \mathrm{R}$_0$(f) 相差常数因子（并使用引理 57）。 □

致谢

这项研究部分得到了加拿大自然科学与工程研究委员会（NSERC）、DGECR-2019-00027 和 RGPIN-2019-04804 的支持。[1]

参考文献

[Aar08] Scott Aaronson。量子证书复杂度。《计算机与系统科学杂志》（2008年）。此前版本发表于2003年计算复杂性会议。doi：10.1016/j.jcss.2007.06.020。arXiv：1506.04719（第2、14页）。[ABB+17] Andris Ambainis、Kaspars Balodis、Aleksandrs Belovs、Troy Lee、Miklos Santha和Juris Smotrovs。基于指针函数的查询复杂度分离。《ACM学报》（2017年）。此前版本发表于2016年STOC。doi：10.1145/3106234。arXiv：1506.04719（第2、3页）。[ABK16] Scott Aaronson、Shalev Ben-David和Robin Kothari。使用备忘单的查询复杂度分离。第48届ACM SIGACT计算理论研讨会（STOC）论文集。2016年。doi：10 . 1145 / 2897518 . 2897644。arXiv：1511.01937（第2页）。[AGJ+18] Anurag Anshu、Dmitry Gavinsky、Rahul Jain、Srijita Kundu、Troy Lee、Priyanka Mukhopadhyay、Miklos Santha和Swagato Sanyal。随机化查询复杂度的复合定理。第37届IARCS软件技术基础与理论计算机科学年会（FSTTCS）论文集。2018年。doi：10.4230/LIPIcs.FSTTCS.2017.10。arXiv：1706.00335（第2页）。[Amb16] Andris Ambainis。精确量子算法的超线性优势。《SIAM计算杂志》（2016年）。此前版本发表于2013年STOC。doi：10.1137/130939043。arXiv：1211.0721（第2页）。[BB20] Shalev Ben-David和Eric Blais。偏函数随机化查询复杂度的紧复合定理。第61届IEEE计算机科学基础研讨会（FOCS）论文集。2020年。doi：10.1109/focs46700.2020.00031。arXiv：2002.10809（第2、18页）。[BBG+21] Kaspars Balodis、Shalev Ben-David、Mika G\"o\"os、Siddhartha Jain和Robin Kothari。无歧义析取范式与Alon-Saks-Seymour猜想。第62届IEEE计算机科学基础研讨会（FOCS）论文集。16, 2021年。doi：10.1109/ FOCS52979.2021.00020。arXiv：2102.08348（第2页）。[BBGM22] Shalev Ben-David、Eric Blais、Mika Goos和Gilbert Maystre。随机化复合与小偏差极小极大。第63届IEEE计算机科学基础研讨会（FOCS）论文集。2022年。doi：10.1109/focs54457.2022.00065。arXiv：2208.12896（第2、18页）。[BDG+20] Andrew Bassilakis、Andrew Drucker、Mika G\"o\"os、Lunjia Hu、Weiyun Ma和Li-Yang Tan。查询复杂度中多样本的力量。第47届自动机、语言与编程国际学术讨论会（ICALP）论文集。2020年。doi：10.4230/LIPIcs.ICALP.2020.9。arXiv：2002.10654（第2页）。

[1]本研究由加拿大自然科学与工程研究理事会（CRSNG）资助，项目编号为 DGECR-2019-00027 和 RGPIN-2019-04804。

[BGKW20] Shalev Ben-David、Mika G\"o\"os、Robin Kothari和Thomas Watson。随机化查询复杂度中复合何时需要放大？第24届随机化与计算国际会议（RANDOM）论文集。2020年。doi：10.4230/LIPICS.APPROX/RANDOM.2020.28。arXiv：2006.10957（第2页）。[BK18] Shalev Ben-David和Robin Kothari。受破坏函数与复合函数的随机化查询复杂度。《计算理论》（2018年）。此前版本发表于2016年ICALP。doi：10.4086/toc.2018.v014a005。arXiv：1605.09071（第2页）。[BKT18] Mark Bun、Robin Kothari和Justin Thaler。多项式方法卷土重来：通过对偶多项式获得紧量子查询界。第50届ACM SIGACT计算理论研讨会（STOC）论文集。2018年。doi：10.1145/ 3188745.3188784。arXiv：1710.09079（第2页）。[BW02] Harry Buhrman和Ronald de Wolf。复杂度测度与决策树复杂度：综述。《理论计算机科学》（2002年）。doi：10.1016/S0304-3975(01) 00144-X（第8页）。[EMP18] Jeff Edmonds、Venkatesh Medabalimi和Toniann Pitassi。语义只读分支程序的函数复合难度。第33届计算复杂性会议（CCC）论文集。2018年。doi：10.4230/LIPICS.CCC. 2018.15（第2页）。[GJ16] Mika G\"o\"os和T. S. Jayram。锥形合取的复合定理。第31届计算复杂性会议（CCC）论文集。2016年。doi：10.4230/ LIPIcs.CCC.2016.5。eccc：2015/167（第2、3页）。[GJPW18] Mika G\"o\"os、T. S. Jayram、Toniann Pitassi和Thomas Watson。随机化通信与划分数的比较。《ACM计算理论汇刊》（2018年）。此前版本发表于2017年ICALP。doi：10.1145/3170711。eccc：2015/169（第2页）。[GLSS19] Dmitry Gavinsky、Troy Lee、Miklos Santha和Swagato Sanyal。通过最大冲突复杂度得到的随机化查询复杂度复合定理。第46届自动机、语言与编程国际学术讨论会（ICALP）论文集。2019年。doi：10.4230/LIPICS.ICALP.2019.64。arXiv：1811.10752（第2页）。[GM21] Mika G\"o\"os和Gilbert Maystre。随机化查询复杂度的多数函数引理。第36届计算复杂性会议（CCC）论文集。2021年。doi：10.4230/LIPICS.CCC.2021.18。eccc：2021/024（第2页）。[G\"o\"o15] Mika G\"o\"os。团与独立集的下界。第56届IEEE计算机科学基础研讨会（FOCS）论文集。2015年。doi：10.1109/FOCS.2015.69。eccc：2015/012（第2页）。[GSS16] Justin Gilmer、Michael Saks和Sudarshan Srinivasan。一些布尔函数复杂度测度的复合极限与分离示例。《组合数学》（2016年）。此前版本发表于2013年计算复杂性会议。doi：10.1007/s00493- 014- 3189- x。arXiv：1306.0630（第2、4、15页）。[HL\u S07] Peter H\o yer、Troy Lee和Robert \u Spalek。负权使对手方法更强。第39届ACM SIGACT计算理论研讨会（STOC）论文集。2007年。doi：10.1145/1250790.1250867。arXiv：quant-ph/0611054（第2页）。[JK17] Stacey J effery和Shelby Kimmel。图连通性与公式求值的量子算法。《Quantum》（2017年）。doi：10 . 22331 / q - 2017 - 08 - 17 - 26。arXiv：1704.00765（第2页）。

[JKS03] T. S. Jayram、Ravi Kumar 和 D. Sivakumar。信息复杂度的两个应用。《第35届 ACM SIGACT计算理论研讨会论文集》（STOC）。2003年。doi: 10.1145/780542.780640（第3页）。[Kim13] Shelby Kimmel。量子对手（上）界。《芝加哥理论计算机科学杂志》（2013年）。早期版本见 ICALP 2012。doi: 10.4086/cjtcs.2013. 004。arXiv: 1101.0797（第2页）。[KRS15] Robin Kothari、David Racicot-Desloges 和 Miklos Santha。将决策树复杂度与子立方体划分复杂度区分开。《第18届随机化与计算国际会议论文集》（RANDOM）。2015年。doi: 10.4230/LIPIcs.APPROX-RANDOM.2015.915。arXiv: 1504.01339（第2页）。[KRW95] Mauricio Karchmer、Ran Raz 和 Avi Wigderson。通过通信复杂度中的直和获得超对数深度下界。《计算复杂性》（1995年）。doi: 10.1007/BF01206317（第2页）。[KT16] Raghav Kulkarni 和 Avishay Tal。关于分数块敏感度。《芝加哥理论计算机科学杂志》（2016年）。doi: 10 . 4086 / cjtcs . 2016 . 008。eccc: 2013/168（第15页）。[Leo13] Nikos Leonardos。递归多数函数的随机化决策树复杂度的改进下界，《自动机、语言与编程国际学术讨论会第40届会议论文集》（ICALP）。2013年。doi: 10.1007/978-3-642- 39206-1_59。eccc: 2012/099（第3页）。[LMR+11] Troy Lee、Rajat Mittal、Ben W. Reichardt、Robert \u Spalek 和 Mario Szegedy。状态转换的量子查询复杂度。《第52届 IEEE计算机科学基础研讨会论文集》（FOCS）。2011年。doi: 10.1109/FOCS.2011.75。arXiv: 1011.3020（第2页）。[MNS+15] Fr\'ed\'eric Magniez、Ashwin Nayak、Miklos Santha、Jonah Sherman、G\'abor Tardos 和 David Xiao。递归多数函数的随机化决策树复杂度的改进界。《随机结构与算法》（2015年）。早期版本见 ICALP 2011。doi: 10.1002/rsa.20598。arXiv: 1309.7565（第3页）。[Mon14] Ashley Montanaro。决策树复杂度的一个复合定理。《芝加哥理论计算机科学杂志》（2014年）。doi: 10 . 4086 / cjtcs . 2014 . 006。arXiv: 1302.4207 （第 2 页）。[NW95] Noam Nisan 和 Avi Wigderson。关于秩与通信复杂度。《组合数学》（1995年）。早期版本见 FOCS 1994。doi: 10.1007/BF01192527（第2页）。[Rei11] Ben W. Reichardt。量子查询算法的反射。《第22届 ACM-SIAM离散算法研讨会论文集》。2011年。doi: 10.1137/1. 9781611973082.44。arXiv: 1005.1601（第2页）。[San24] Swagato Sanyal。随机化查询复合与乘积分布。《第41届计算机科学理论方面研讨会论文集》（STACS）。2024年。doi: 10.4230/LIPICS.STACS.2024.56。arXiv: 2401.15352（第2页）。[San95] Miklos Santha。一次读取公式的蒙特卡罗布尔决策树复杂度。《随机结构 \& 算法》（1995年）。doi: 10.1002/rsa.3240060108（第2、3页）。

[SW86] Michael Saks 和 Avi Wigderson。概率布尔决策树及博弈树求值的复杂度。 第*27*届 *IEEE* 计算机科学基础年度研讨会论文集（*FOCS*）。1986年。 DOI： 10.1109/SFCS.1986.44 （第2、3页）。[Tal13] Avishay Tal。布尔函数复合的性质与应用。 第*4*届理论计算机科学创新会议论文集（*ITCS*）。2013年。DOI： 10.1145/2422436.2422485。 ECCC： 2012/163 （第2、15页）。[WZ88] Ingo Wegener 和 Laszlo Z\'adori。 关于临界复杂度与敏感度复杂度之间关系的注记。1988年（第2页）。