arXiv:2305.04563v1 [cs.CC] 8 May 2023

# 有理交互式证明的结构复杂性

Daniil Musatov[1, 2, 3][0000−0002−1779−2513] 和
Georgii Potapov[1][0009−0002−2670−2206]

[1] 俄罗斯多尔戈普руд内市莫斯科物理技术学院[2] 俄罗斯莫斯科俄罗斯总统国民经济与公共管理学院[3] 俄罗斯迈科普市阿迪格国立大学高加索数学中心

**摘要**。 本文是提交给欧洲计算机可计算性会议（CiE 2023）的一篇论文的完整版，会议版本省略了所有证明。2012年，P. D. Azar 和 S. Micali 提出了一种新的交互式证明模型，称为“理性交互式证明”。在该模型中，证明者既不诚实也不恶意，而是以最大化其期望奖励为目标的理性参与者。本文探讨这一领域与经典复杂性结果之间的联系。

在本文的第一部分，我们重新审视计数层次与常数轮理性证明层次之间的联系。我们证明，能够访问 DRMA$[k]$ 预言机的多项式时间机器恰好判定 DRMA$[k]$ 中的语言，而这一等同性在计数层次的各个层级中尚未得到发现。
在第二部分中，我们研究单轮理性证明的通信复杂度。我们证明，由对数通信量的单轮理性证明所定义的类与 PP 一致。我们还证明，将 $\oplus$P 中的问题视为随机变量的黑盒采样器的单轮理性协议，至少需要线性数量的通信比特。

## 1 引言

计算技术的进步不仅改变了我们的世界，也为理论计算机科学的新领域铺平了道路。因此，在 20 世纪 60 年代和 70 年代，大规模计算机的出现推动了复杂性理论的发展和算法的设计。随后，在 20 世纪 80 年代和 90 年代，计算机网络的发展促成了交互式证明和密码学协议的诞生。2012 年，一个反映商业云计算特点的新领域逐渐形成，即理性交互式证明领域。

在云计算中，客户端向服务器发送一项计算任务，并接收某种响应。客户端如何确定该响应确实是所请求计算的结果？如果任务属于 NP 问题，服务器可以发送一份客户端能够验证的证书。但如果任务更难呢？理性证明的核心思想是创造经济激励，促使

服务器正确执行计算。为此，标准的交互式证明模型加入了由客户端支付给服务器、可通过多项式时间计算的概率性奖励。为了最大化预期奖励，服务器会揭示正确答案。

因此，虽然在标准的交互式证明和密码学模型中，证明者可以是诚实的，也可以是恶意的，但在这里我们只考虑一种证明者：经济理性的证明者。乍看之下，这对交互式证明影响不大：验证者只需为被接受的证明支付 1 美元，对被拒绝的证明支付 0 美元。但当我们考虑轮数和通信复杂度时，情况就大不相同了。在本文中，我们探讨了几个有关这些问题的具体问题。

### 1.1 历史与相关文献

交互式证明领域最初由 Babai（针对公共随机比特） [4] 以及 Goldwasser、Micali 和 Rackoff（针对私有随机比特） [15] 的研究提出。随后，Goldwasser 和 Sipser 证明 [16] ，可以将使用私有比特的协议转换为使用公共比特且轮数多两轮的协议。Babai 和 Moran 证明 [6] ，公共比特协议的轮数可以减半。综合这些结果可知，任何能由常数轮交互式证明系统识别的语言，实际上都能由两轮公共比特协议识别，因此属于 AM，进而属于多项式层次的第二层。开创性结果 IP = PSPACE [19,20,21] 表明，采用多项式数量的轮可将该类扩展至 PSPACE。多个证明者的情形也得到了分析，结果表明，相应的类 MIP 等于 NEXP [7,14,5]。

与此同时，Wagner 引入了 [23] 计数层次，这是一种多项式层次的类似结构，其中存在量词和全称量词被多数量词所取代。著名的 Toda 定理 [22] 表明，整个多项式层次都包含在计数层次的第二层中。

交互式证明与计数层次在 Azar 和 Micali 于 [2] 开创的理性交互式证明领域交汇。他们引入了理性证明的概念，定义了函数类 FRMA 和判定类 DRMA，并证明了具有常数轮复杂度的 DRMA 等于计数层次，从而展示了它与具有常数轮的 IP 之间的差异。另一方面，如果轮数是多项式的，那么相应的类（记为 RIP）仍然等于 PSPACE。

后续分析沿着多个方向展开。首先，理性证明的概念也扩展到了多个证明者的情形。由于证明者的收益彼此依赖，他们会相互进行某种博弈，结果取决于该博弈的规则。Chen、McCauley 和 Singh 考虑了合作 [10] 和非合作 [12] 两种方法，并证明相应的类别不仅比 RIP 更广，也比 MIP 更广（具体刻画取决于模型的细节）。因此，对于多个证明者而言，理性会扩大可识别语言的类别。

其次，研究者还考虑了各种证明者和/或验证者受到计算能力限制的模型。Azar 和 Micali 提出了 [3,1] 超高效理性证明，其中验证者的时间复杂度受对数级限制，且诚实证明者只需解决问题，无须进行更多计算。他们用这些概念刻画了类$\mathsf{TC}^0$, $\mathsf{P}^{\|\mathbf{NP}}$ 和 $\mathsf{P}^{\|\mathbf{MA}}$。他们还表明，验证者只需要多项式预算：偏离最优策略会导致显著损失。Guo 等人 [17] 将研究从 $\mathsf{TC}^0$ 推进到 $\mathsf{NC}^1$ ，Chen、McCauley 和 Singh [11] 则改进了效用差距的界。Campanelli 和 Gennaro 构造了一个顺序可组合协议 [8] ，以及另一个空间高效协议 [9]。Inasawa 和 Yasunaga 探索了 [18] 一种变体，其中证明者和验证者都是理性的。

### 1.2 结果阐述

在本文中，我们回到最初的 Azar-Micali 框架，并探讨计数层次与 DRMA 层次之间的关系。在 [2] 中证明了，可由 $k$ 轮理性证明识别的语言处于计数层次的第 $k$ 层与第 $(2k+1)$ 层之间。我们尝试阐明这些界限是否紧确。这两个层次有可能重合吗?

我们以下列方式作出回答：要么这些层次彼此不同，要么它们的一致性将意味着一个长期悬而未决的问题得到解决。

**结果 1** （推论 3）：$\mathsf{P}^{\mathbf{DRMA}[k]}=\mathsf{DRMA}[k]$。

相反，等式 $\mathsf{P}^{C_k\mathbf{P}} = C_k\mathsf{P}$ 并不为人所知：例如，根据 Toda 定理，$\mathsf{PH} \subset \mathsf{P}^{\mathbf{PP}}$，但 $\mathsf{PH} \subset \mathsf{PP}$ 这一包含关系并不为人所知。

接下来的两个结果表明，DRMA 层次的各个层级之间的关系与计数复杂度类类似，但并不等同。

**结果2** （定理5）：$\mathsf{PP}^{\mathbf{DRMA}[k]} \subset \mathsf{DRMA}[k+1]$。

我们不知道这种包含关系是否成立为等式。相反，$\mathsf{PP}^{C_k\mathbf{P}} = C_{k+1}\mathsf{P}$ 只是 $C_{k+1}\mathsf{P}$ 的定义，因此始终成立。

我们也不知道等式 $\mathsf{DRMA}[k] = \mathsf{DRMA}[k+1]$ 是否意味着 $\mathsf{DRMA}[k+1] = \mathsf{DRMA}[k+2]$，但我们展示了这两个层次塌缩之间的如下联系。

**结果3** （推论5）：如果 $\mathsf{DRMA}[k] = \mathsf{DRMA}[k+1]$，那么计数层次至多在第 $(2k+1)$ 层坍缩。

最后，我们估计 1 轮证明的通信复杂度。

**结果 4** （推论 6）：$\mathsf{PP}$ 等于 $\mathsf{DRMA}[1, O(\log\ n)],$，也就是说，等于仅有一轮且发送 $O(\log n)$ 位的 DRMA。

因此，$\mathsf{PP}=\mathsf{DRMA}[1]$ 是否等价，取决于与对数位数相比，多项式数量的通信位是否会扩大该类。我们还简要讨论 $\oplus\mathsf{P}$ 与 $\mathsf{DRMA}[1]$ 之间的联系，以及我们方法的局限性。

### 1.3 路线图

在第 2 节中，我们给出计数层次和理性证明的形式化定义及基本事实。第 3 节和第 4 节分别阐述我们关于

DRMA 层次和通信复杂度的研究结果。在第 5 节中，我们给出总结性评论，并提出一些有待进一步研究的问题。

## 2 预备知识

### 2.1 计数层次

首先，我们回顾一些有关计数层次的基本定义。

**定义 1.** 类 **PP** 是满足以下条件的语言类 $A$：存在一个语言 $B \in \mathbf{P}$ 和一个多项式 $q$，使得对于所有 $x$

$$x \in A \iff \frac{1}{2^{q(|x|)}} \left|\left\{ y \in \{0,1\}^{q(|x|)} : (x,y) \in B \right\}\right| \geq \frac{1}{2}.$$

我们还将使用一种等价的定义，在该定义中，可接受证书所占的比例 $y$ 永远不会恰好等于 $1/2$。（为得到这一结果，需要额外添加 2 个随机比特，并人为地将接受概率微幅偏移。）

**定义 2.** 相对化类 $\mathbf{PP}^{\mathbf{C}}$ 的定义方式相同，但其中的 $B$ 是 $\mathbf{P}^C$ 中的某个语言，且对应某个 $C \in \mathbf{C}$。

**定义 3.** 计数层次递归定义如下：

- $C_0\mathrm{P} = \mathrm{P}$，
- $C_1\mathrm{P} = \mathrm{PP}$，
- $C_{k+1}\mathrm{P} = \mathrm{PP}^{C_k\mathbf{P}}$ 对于 $k \geq 1$，
- 计数层次 $= \bigcup_{k \geq 0} C_k\mathrm{P}$。

显然，如果 $C_k\mathrm{P} = C_{k+1}\mathrm{P}$，那么计数层次 $= C_k\mathrm{P}$。事实上，我们有 $C_{k+2}\mathrm{P} = \mathrm{PP}^{C_{k+1}\mathbf{P}} = \mathrm{PP}^{C_k\mathbf{P}} = C_{k+1}\mathrm{P}$，然后通过归纳法继续推导。

### 2.2 理性交互式证明

P. Azar 和 S. Micali 在 [2] 中引入了理性交互式证明。我们将证明者称为 Merlin，将验证者称为 Arthur。令有限字母表 $\Sigma$（例如 $\Sigma = \{0,1\}$）固定，并假设我们研究的是定义在 $\Sigma$ 上的语言。

我们从单轮协议及其相应的复杂性类的定义开始。

**定义 4。** 类 $\mathbf{FRMA}[1]$（来自 *1* 轮函数型理性 *Merlin-Arthur* 博弈）是所有函数 $f$：$\Sigma^* \to \Sigma^*$ 的集合，其中存在多项式时间可计算函数 $R$：$\Sigma^* \to [0,1]$ 和 $\varphi$：$\Sigma^* \to \Sigma^*$，使得对于所有 $x \in \Sigma^*$ 以及任意

$$m^* \in \mathrm{Argmax}_m \, \mathbb{E}_r R(x; m, r),$$

其中，$r$ 在 $\{0,1\}^{l(|x|)}$ 上均匀分布，对于某个多项式 $l$，有

$$f(x) = \varphi(x; m^*).$$

这里， $m$ 是 Merlin 给 Arthur 的提示， $r$ 是 Arthur 的随机性， $R$是 Arthur 支付给 Merlin 的奖励，以有限二进制小数表示； $\varphi$指定如何利用该提示计算 $f$。使期望奖励最大的消息 $m^*$ 必须是能引导 Arthur 得出 $f(x)$正确值的提示。

如果 $f(x)$ 仅取二进制值，就可以将其视为某个谓词的特征函数。由此可得到一个类似的语言类。

**定义 5.** 类 $\mathbf{DRMA}[1]$ （*Decisional RMA* 的缩写）是所有语言 $S \subset \Sigma^*$ 的集合，其特征函数 $\mathbb{I}_S(x) = \mathbb{I}\{x \in S\}$ 属于 $\mathbf{FRMA}[1]$。

Azar 和 Micali 明确或隐含地证明了以下结果：

**定理 1 ([2]).** #P $\subset$ FRMA$[1]$, PP $\subset$ DRMA$[1]$, $\oplus$P $\subset$ DRMA$[1]$.

现在我们将定义扩展到多轮协议。

**定义 6.** *A* $k$轮理性交互协议 $\Pi$ 由可在多项式时间内计算的函数 $V\colon \Sigma^* \to \Sigma^*$, $R\colon \Sigma^* \to [0,1]$ 和 $\varphi\colon \Sigma^* \to \Sigma^*$组成。对于字符串 $x \in \Sigma^*$，协议 $\Pi$ 在输入 $x$ 上的交互定义如下。

– 我们将 *Arthur* 的消息记作 $a_1, a_2, .., a_k$，将 *Merlin* 的消息记作$m_1, m_2, .., m_k$。所有消息的长度都必须是关于 $|x|$ 的多项式。– *Arthur* 的消息计算如下

$$a_{i+1} = V(x; m_1, a_1, m_2, \ldots, a_i, m_{i+1}; r_1, \ldots, r_{i+1}),$$

其中 $r_1, \ldots, r_k$是 *Arthur* 的私有随机字符串。– 我们称 $\varphi$ 为价值函数，并将值 $\varphi(x; m_1, a_1, .., m_k)$ 称为协议中计算出的值。– 我们称 $R$ 为奖励函数，并将值 $R(x; m_1, r_1, .., m_k, r_k)$称为奖励。

注释 *1.* 协议中计算的值不依赖于 Arthur 的最后一条消息，因为这种依赖关系可以包含在 $\varphi$ 中。我们说，奖励仅取决于 Merlin 的消息和 Arthur 的随机性，因为可以根据这些信息还原 Arthur 的消息。

备注 *2.* 在本文中，描述协议时，我们会谈到 Merlin 发送了哪些消息。这主要是为了让读者更清楚地理解协议的想法；应将其理解为对 Arthur 如何处理收到的字符串，以及 Merlin 应遵循何种格式的描述（我们假设，偏离所述格式的消息会导致奖励为 0）。

**定义 7。** 在一个具有奖励函数 $R$ 的 $k$ 轮理性交互协议 $\Pi$ 中，如果对所有 $i = 0, 1,$ ....., $k-1$ 都成立，则称 *Merlin* 是理性的。

$$m_{i+1} \in \mathrm{Argmax}_m \, \mathbb{E}_{a_{i+1}} \max_{m_{i+2}} \mathbb{E}_{a_{i+2}} \ldots \max_{m_k} \mathbb{E}_{a_k} \, R(x; m_1, \ldots, a_i, m, a_{i+1}, \ldots, m_k, a_k),$$

也就是说，理性 *Merlin* 总是会选择一条消息，使得在给定当前已获得信息的条件下，期望奖励最大。

**定义 8.** 如果对于所有 $x$，以及 *Merlin* 的任意理性行为，都有以下结论成立，则称函数 $f$ 是在理性交互协议 $\Pi$ 中计算的：

$$f(x) = \varphi(x; m_1, a_1, \ldots, m_k).$$

**定义 9.** 类 $\mathbf{FRMA}[k]$ 是由所有可通过某个$k$轮交互式协议计算的函数组成的集合。

**定义 10.** 类 $\mathbf{DRMA}[k]$ 是满足以下条件的语言类：$S$ 其特征函数 $\mathbb{I}_S(x) = \mathbb{I}\{x \in S\}$ 属于 $\mathbf{FRMA}[k]$。谈到$\mathbf{DRMA}[k]$-协议时，我们通常将相应的价值函数称为判定函数，并记作 $\pi$。

我们用 $\mathbf{DRMA}$ 表示所有这些类的并集：

$$\mathbf{DRMA} = \bigcup_{k \geq 0} \mathbf{DRMA}[k].$$

在开创性的论文 [2], 中，建立了计数层次与 DRMA 层次之间的以下联系。

**定理2.** $C_k\mathbf{P} \subseteq \mathbf{DRMA}[k]$，对所有 $k \geq 0$。

**定理3.** $\mathbf{DRMA}[k] \subseteq C_{2k+1}\mathbf{P}$，对于所有 $k \geq 0$。

这两个结果共同表明，计数层次 = DRMA。

以下记号可简化对 Merlin 理性性的推理。

**定义 11.** 给定一个理性交互协议 $\Pi$ 以及某个转录记录 $\mathcal{T}_i$,$\mathcal{T}_i = (x;\ m_1,\ a_1,\ \ldots\ldots,\ s)$ $s \in \{m_i, a_{i-1}\}$，该记录包含前 $i$ 轮（不一定是在与理性 *Merlin* 交互时获得），记 $E_i^{\Pi}(\mathcal{T}_i)$ 为 *Merlin* 在所有后续轮次中均采取理性行为时的最大奖励期望。

最后，为了构造和分析协议，我们需要以下概念。

**定义 12。** 给定一个理性交互协议 $\Pi$，记 $\Delta(\Pi)$ 为一个多项式时间可计算函数，它给出以下两者期望奖励之差的正下界：在 *Merlin* 首次偏离理性行为时，他所发送的最优消息和次优消息；也就是说，对所有 $x$

$$0 < \Delta(\Pi)(x) \leq \min_{\substack{i, \mathcal{T}_i;\ \text{where } \mathcal{T}_i \text{ is obtained in} \\ \text{an interaction with a rational Merlin,} \\ m' \notin \mathrm{Argmax}_m\, E_{i+1}^{\Pi}(\mathcal{T}_i, m)}} \left( \max_m E_{i+1}^{\Pi}(\mathcal{T}_i, m) - E_{i+1}^{\Pi}(\mathcal{T}_i, m') \right).$$

注 *3.* 在我们所研究的模型中，奖励应表示为有限二进制小数，且 Arthur 的随机比特均匀且相互独立地分布，因此期望奖励可以写成有限二进制小数之和（奖励值乘以其概率），其长度关于输入规模为多项式级。这使我们能够对某个依赖于 $\Pi$ 的多项式 $p$ 使用 $\Delta(\Pi)(x) = 2^{-p(|x|)}$。多项式 $p(n)$ 可以取为 $T_R(n) + l_r(n)$,

其中， $T_R(n)$ 是在 $x$ with$|x| = n$ 上计算奖励所需的最大时间（因此，奖励值可以表示为某个整数 $k$ 的 $\frac{k}{2^{T_R(n)}}$），而 $l_r(n)$ 是 Arthur 在长度为 $n$ 的输入上使用的随机比特数。在其他模型中（例如，奖励表示为两个整数之比的模型），应作出相应假设，确保存在可计算的 $\Delta(\Pi)$，并对定理陈述和证明作相应调整。还应注意，这类函数存在于 [2] 中的协议。

注 *4.* 函数 $\Delta(\Pi)$ 与奖励间隙并非同一概念，例如，其在 [17] 中的用法便是如此。

## 3 关于 DRMA 层次的结果

我们首先证明，Arthur 可以先与一位 Merlin 开始交互式证明，然后再与另一位 Merlin 继续进行。此外，在切换的时刻，还可以向第二位 Merlin 询问第一位 Merlin 的期望奖励。

**引理 1.** 对于任意整数 $i$， $j \geq 0$，对于任意用于计算函数 $f$ 的 $\mathbf{FRMA}[i+j]$-协议 $\widetilde{\Pi}$，都存在一个函数 $f$，使得：

*1.* 对于任意 $x$，根据输入 $x$ 上的协议 $\Pi$ 与理性 *Merlin* 进行交互的前 $i$ 轮所得到的任意记录 $\mathcal{T}_i$，将其映射为 $(E_i^{\Pi}(\mathcal{T}_i)\ f(x))$；*2.* 将任意 $i$ 轮的记录 $\mathcal{T}_i$ （即 *Arthur* 与任意证明者之间交互的记录）映射为 $(E_i^{\Pi}(\mathcal{T}_i)\ v)$，其中某个 $v$；*3.* 属于 $\mathbf{FRMA}[j]$。

该证明的思路是：对于一个可采样随机变量，存在一个用于确定其期望值的协议，并且可以通过缩小期望值协议中的奖励，将该协议与原始协议结合起来。完整证明见附录。

**推论 1.** 对于所有 $i$， $j \geq 0$，以下包含关系成立：

$$\mathbf{FRMA}[i+j] \subseteq \mathbf{FRMA}[i]^{(\mathbf{FRMA}[j])[1]} \subseteq \mathbf{FRMA}[i]^{||\mathbf{DRMA}[j]},$$

其中，第二类中的“[1]”表示只允许进行一次预言机查询。

证明。 $i = 0$ 或 $j = 0$ 的情况是平凡的。令 $\Pi$ 为某个函数 $f \in$ FRMA$[i+j]$的 FRMA$[i+j]$-协议。考虑一个新协议 $\Pi'$，它在 Merlin 于第 $i$轮发送消息之前与 $\Pi$ 一致。随后，Arthur 在协议 $\Pi$ 中计算其第$i$条消息，并将当前记录 $\mathcal{T}_i$ 发送给一个对应于引理 1 中某个函数的 FRMA$[j]$-预言机。Arthur 计算出的值和奖励就是从预言机获得的值和奖励。

理性 Merlin 将遵循协议，因为

$$E_{i-1}^{\Pi'}(\mathcal{T}_{i-1}) = \max_m \mathbb{E}_r\, R\big((\mathcal{T}_{i-1}, m, r)\big) = \max_m \mathbb{E}_r\, E_i^{\Pi}\big((\mathcal{T}_{i-1}, m, r)\big) = E_i^{\Pi}(\mathcal{T}_i),$$

由此通过向下归纳法可得，对所有 $t < i$

$$E_t^{\Pi'}(\mathcal{T}_t) = \max_m \mathbb{E}_r\, E_{t+1}^{\Pi'}\big((\mathcal{T}_t, m, r)\big) = \max_m \mathbb{E}_r\, E_{t+1}^{\Pi}\big((\mathcal{T}_t, m, r)\big) = E_t^{\Pi}(\mathcal{T}_t),$$

这意味着，argmax 集合以及理性 Merlin 的策略对于 $\Pi$ 和 $\Pi'$ 都相同。这表示我们可以将协议 $\Pi'$ 的交互记录 $\mathcal{T}_i$ 视为与协议 $\Pi$ 中理性 Merlin 交互所获得的记录，因此根据引理 1，预言机也会返回 $f$ 的正确值。

第二个包含关系可以通过将预言机函数 $\sim f$ 替换为语言来轻松得到。

$$A_{\widetilde{f}} = \Big\{(x, i, b) \mid b \text{ is the } i\text{-th bit of } \widetilde{f}(x)\Big\}$$

~以及通过并行查询计算 $f(x)$ 的每一位，查询对象为 $A_{\widetilde{f}}$。

**推论 2.** 对于所有 $i,\ j \geq 0$, 以下包含关系成立:

$$\mathbf{DRMA}[i+j] \subseteq \mathbf{DRMA}[i]^{(\mathbf{FRMA}[j])[1]} \subseteq \mathbf{DRMA}[i]^{||\mathbf{DRMA}[j]},$$

其中，第二类中的“$[1]$”表示只允许进行一次预言机查询。

证明。 这显然由推论 1 得出，因为 DRMA$[k]$ 协议只是 FRMA$[k]$ 协议的一种特殊情况。对于第一个包含关系，DRMA$[i+j]$-协议是针对某个二值函数 $f$ 的 FRMA$[i+j]$- 协议。根据推论 1，存在一个 FRMA$[i]^{(\mathbf{FRMA}[j])[1]}$- 协议；由于它是针对二值函数的协议，因此构成了对应语言的 DRMA$[i]^{(\mathbf{FRMA}[j])[1]}$-协议。第二个包含关系也可以类似地证明。

现在我们将证明，推论 2 的上界至少对 $i = 0$ 是紧的。事实上，我们证明一个稍强一些的结果。

**定理 4.** $\mathbf{P}^{\mathbf{FRMA}[k]} = \mathbf{DRMA}[k]$ 对所有 $k \geq 0$。

这个思路同样是：对于那些取决于其他某些子问题答案的子问题，缩减其奖励。通过谨慎地进行归纳证明，我们可以看出，完全理性的 Merlin 没有动机在任何子问题中说谎。完整证明见附录。

**推论 3.** $\mathbf{P}^{\mathbf{DRMA}[k]} = \mathbf{DRMA}[k]$, 对于所有 $k \geq 0$。

证明。 由于 DRMA$[k]$-协议是 FRMA$[k]$-协议的特殊情况，根据定理 4 可得 $\mathbf{P}^{\mathbf{DRMA}[k]} \subseteq$DRMA$[k]$ 。另一个方向的包含关系是显然的。

这一推论表明，DRMA 层次和计数层次之间可能存在差异。例如，根据 Toda 定理，已知 $\mathbf{P}^{\mathbf{PP}}$ 包含 PH，而对于 PP 则尚无定论，因此 PP $\neq \mathbf{P}^{\mathbf{PP}}$ 很可能成立。

**定理5。** $\mathbf{PP}^{\mathbf{FRMA}[k]} \subseteq \mathbf{DRMA}[k+1]$, 对所有 $k \geq 0$。

证明。 如果 $A$ 是 $\mathrm{PP}^{\mathbf{FRMA}[k]}$中的一种语言，那么存在一种语言 $B \in \mathrm{P}^{\mathbf{FRMA}[k]}$ 和一个多项式 $q$，使得对于所有 $x$:

- $x \in A \Longrightarrow 2^{-q(|x|)} \left|\left\{y \in \{0,1\}^{q(|x|)} : (x,y) \in B\right\}\right| > \frac{1}{2}$,
- $x \notin A \Longrightarrow 2^{-q(|x|)} \left|\left\{y \in \{0,1\}^{q(|x|)} : (x,y) \in B\right\}\right| < \frac{1}{2}$.

根据定理 4，存在一个 DRMA$[k]$-协议 $\Pi$，其针对 $B$，具有奖励函数$R$ 和判定函数 $\pi$。现在我们描述一个针对语言 $A$的 DRMA$[k+1]$-协议 $\Pi'$。

1. 在第一轮中，Merlin 发送一位 $b$，该位应等于 $\mathbb{I}\{x \in A\}$。 2. 接着，Arthur 采样一个随机字符串 $y \sim \mathcal{U}_{q(|x|)}$ 并将其发送给 Merlin。 3. 接下来的 $k$ 轮对应协议 $\Pi$ 针对字符串 $(x,y)$ 的 $k$ 轮。 4. 最后，Arthur 计算值 $\Delta = \Delta(\Pi)((x,y))$，以及对应于 $(x,y)$ 的子协议的奖励$R$ 和判定比特 $\pi$，向 Merlin 支付奖励 $\frac{1}{2}R + \frac{\Delta}{4}\mathbb{I}\{b = \pi\}$，并且当且仅当 $b = 1$ 时接受 $x$。

理性 Merlin 不会偏离子协议 $\Pi$，因为偏离至少会使 $\frac{1}{2}R$ 减少 $\frac{1}{2}\Delta$，同时使 $\frac{\Delta}{4}\mathbb{I}\{b = \pi\}$ 最多增加 $\frac{\Delta}{4}$。因此， $\Pi'$ 中的理性 Merlin 将会复制协议 $\Pi$ 中理性 Merlin 的行为，在这种情况下， $\pi = \mathbb{I}\{(x,y) \in B\}$。因此，为了最大化 $\frac{\Delta}{4}\mathbb{I}\{b = \pi\}$ 的期望值，理性 Merlin 将在第一轮发送 $\mathbb{I}\{x \in A\}$。

定理5为 [2] 中的定理2提供了一个独立的证明。

**推论4**。 $C_k\mathbf{P} \subseteq \mathbf{DRMA}[k]$ 对所有 $k \geq 0$。

证明。 由 $k$ 进行直接归纳法。

下一个推论展示了这两个层次结构坍缩之间的联系。

**推论5**。 如果 $\mathbf{DRMA}[k] = \mathbf{DRMA}[k+1]$，那么计数层次将坍缩到第$(2k+1)$级。

证明。 我们将通过对 $l \geq 0$ 进行归纳法，证明 $C_{k+l}\mathrm{P} \subseteq \mathrm{DRMA}[k]$。基础情形由定理2给出。归纳步骤如下:

$$C_{k+(l+1)}\mathbf{P} = \mathbf{PP}^{C_{k+l}\mathbf{P}} \subseteq \mathbf{PP}^{\mathbf{DRMA}[k]} \subseteq \mathbf{DRMA}[k+1] = \mathbf{DRMA}[k],$$

其中，最后一个等式由推论的假设得出。根据定理3，我们有 $\mathrm{DRMA}[k] \subseteq C_{2k+1}\mathrm{P}$，因此

$$C_{2k+2}\mathbf{P} = C_{k+(k+2)}\mathbf{P} \subseteq \mathbf{DRMA}[k] \subseteq C_{2k+1}\mathbf{P},$$

所以 $C_{2k+1}\mathrm{P} = C_{2k+2}\mathrm{P}$，且计数层次 $= C_{2k+1}\mathrm{P}$。

请注意，我们不知道 $\mathrm{DRMA}[k] = \mathrm{DRMA}[k+1]$ 是否蕴含 $\mathrm{DRMA}[k+1] = \mathrm{DRMA}[k+2]$，但我们仍可由此推论得出，$\mathrm{DRMA}[k] = \mathrm{DRMA}[k+1]$ 蕴含 DRMA 层次在某个更高层级上坍缩。

## 4 单轮证明的通信复杂度

本节研究形如 DRMA$[1,c]$ 的类，也就是由 Merlin 最多发送 $c$ 位的 DRMA$[1]$ 协议所识别的语言类。我们还假设 Merlin 使用二进制字母表。

首先，让我们将问题简化为二进制奖励的情形。

**引理2**。 每个$\mathbf{DRMA}[1,c]$-协议都等价于一个$\mathbf{DRMA}[1,c]$-协议，其奖励函数取值于 $\{0,1\}$。

证明。 Arthur 应在计算给定协议中的奖励 $R$ 后，不发送数值 $R$作为奖励，而是以概率 $2^{-i}$ 发送 $R$ 的第 $i$ 位（这可以在有限时间内完成，因为对于所有足够大的 $i$， $R$ 的第 $i$ 位都将为 0）。这样，Arthur 实质上会以概率 $R$ 发送 1。

注意，这种变换可应用于任何 DRMA 协议，且不会增加其轮数或通信复杂度。

**引理3.** 对于任意两个电路 $C_0, C_1$，它们计算从 $\{0,1\}^n$到 $\{0,1\}$的函数，判定 $\mathbb{E}_{x\sim\mathcal{U}_n} C_0(x) \le \mathbb{E}_{x\sim\mathcal{U}_n} C_1(x)$ 是否属于 $\mathbf{PP}$的问题也属于 $PP$。换言之，该语言

$$\mathsf{Compare-Expectations} = \Big\{ (C_0, C_1) \mid C_i : \{0,1\}^n \to \{0,1\}, \\ \mathbb{E}_{r\sim\mathcal{U}_n} C_0(r) \le \mathbb{E}_{r\sim\mathcal{U}_n} C_1(r) \Big\}$$

属于 $\mathbf{PP}$。

这里使用电路，是为了方便地描述参数化函数。在我们的应用中，带有固定参数的多项式时间可计算函数由多项式规模电路表示。证明的思路是对两个电路都进行采样，并优先选择取值较大的那个；若取值相同，则随机打破平局。证明见附录。

以下引理在 [2], 中是隐含的，但为完整起见，我们给出证明。

引理4. $\mathbf{PP} \subseteq \mathbf{DRMA}[1,1]$。

证明。 众所周知，对于任意语言 $A \in$ PP，都存在一个多项式时间算法 $V$，使得 $\Pr_y[V(x,y) = 1]$ 对 $x \in A$ 严格大于 $1\,2$，而对 $x \notin A$严格小于 $1\,2$。

考虑以下协议。

1. Merlin 发送一位比特 $b$，该比特应为 $\mathbb{I}\{x \in A\}$；2. Arthur 在随机 $y$ 上运行 $V(x,y)$，并向 Merlin 支付 $\mathbb{I}\{b = V(x,y)\}$，当且仅当 $b = 1$ 时接受 $x$。

由于不存在平局，理性 Merlin 会发送正确的比特 $b$。

最后，为了证明本节的主要结果，我们将用到 Fortnow 和 Reingold 提出的以下定理。

**定理 6 ([13])**。如果 $A \leq_{tt} B$ 且 $B \in \mathbf{PP}$，那么 $A \in \mathbf{PP}$。

接下来给出本节的主要结果。

**定理 7.** $\mathbf{DRMA}[1, O(\log n)] \subseteq \mathbf{PP}$。

证明。设 $A$ 是 DRMA$[1, O(\log n)]$ 中的一种语言，$\Pi$ 是其对应的协议，其中 $A$ 的奖励函数为 $R$，判定函数为 $\pi$。由于 Merlin 发送的消息长度仅为 $O(\log n)$，因此可能的消息总数至多为 $p(n) = 2^{O(\log n)} = \text{poly}(n)$。

考虑一种算法：给定输入 $x$，它遍历 Merlin 的所有可能消息，并找出使值 $\mathbb{E}_r\, R(x;\, m, r)$ 最大的消息 $m^*$。可以通过一场淘汰赛找出获胜者：将消息 $m_0$ 和 $m_1$ 组成一对，并将 $(R(m_0, \cdot)\ R(m_1, \cdot))$ 输入 Compare $-$ 期望值预言机进行比较。最后，当且仅当 $\pi(m^*) = 1$时，接受 $x$。显然，该算法给出了从 $A$ 到 Compare $-$ 期望值 $\in$ PP 的多项式时间真值表归约。因此，根据定理 6，我们有 $A \in$ PP。

**推论 6**。$\mathbf{PP} = \mathbf{DRMA}[1, O(\text{对数}\ n)]$。

证明。直接由引理4和定理 7 得出。

现在我们讨论 DRMA[1]-协议中 $\oplus$P 的通信复杂度下界。推论 6 表明，$\oplus \text{P} \not\subseteq \text{DRMA}[1, O(\log n)]$ 将意味着 $\oplus\text{P} \neq \text{PP}$；而 $\oplus\text{P} \subseteq \text{DRMA}[1, \text{poly}(n)]$ 成立（定理 1），因此，研究 $\oplus$P 中问题的 DRMA[1]-协议的通信复杂度很有意义。到目前为止，在所有给出的证明中，我们都将用于确定计数复杂度类包含关系的证书验证算法视为伯努利分布的采样器。现在我们将证明，这种方法无法得到通信复杂度为次线性的 DRMA[1]-协议。

*定理 8.* 不存在多项式时间可计算函数 $R:\ \{0,1\}^* \to [0,1]$ 以及 $\varphi:\ \{0,1\}^* \to \{0,1\}$，使得对于任意 $n$ 和 $0 \leq k \leq 2^n$，$\varphi(1^n, m^*)$ 的值等于 $k$ 的奇偶性，其中 $m^* \in \mathit{Argmax}_m\, \mathbb{E}_{a,r} R(1^n, m, a, r)$，$|m^*| < \alpha n$ 对某个常数 $\alpha \in (0, 1)$ 成立，$a \sim \mathcal{U}_s$ 满足 $s = \mathit{poly}(n)$，且 $r \in \{0,1\}^d$ 满足 $d = \mathit{poly}(n)$，并且 $r$ 的各位从 $\mathit{Bern}\left(\frac{k}{2^n}\right)$ 中独立采样。

其思路是：固定 $n$、$m$ 后，奖励函数是关于非均匀比特取值为 1 的概率的多项式。如果 $m$ 较短，那么这些多项式中必有两个多项式次数有限的多项式在指数多个点上相交。详细内容见附录。

## 5 后续研究

在本文中，我们展示了计数层次与 DRMA 层次之间的若干有趣联系。但主要问题仍未解决：二者是否相同，还是彼此不同？如果二者不同，一个自然的下一步是构造一个属于 DRMA$[k]$ 、但似乎不属于 $C_k$P 的语言。

## 参考文献

1. Azar, P.D.：超高效理性证明。博士学位论文，麻省理工学院电气工程与计算机科学系（2014年）2. Azar, P.D., Micali, S.：理性证明。载于：第四十四届 ACM 计算理论年度研讨会论文集。第1017–1028页。ACM（2012年）3. Azar, P.D., Micali, S.：超高效理性证明。载于：第十四届 ACM 电子商务会议论文集。第29–30页（2013年）4. Babai, L.：以群论换取随机性。载于：第17届 ACM 计算理论年度研讨会论文集，1985年5月6日至8日，美国罗得岛州普罗维登斯。第421–429页（1985年）5. Babai, L., Fortnow, L., Lund, C.：非确定性指数时间具有双证明者交互协议。《计算复杂性》**1**(1)，3–40（1991年）6. Babai, L., Moran, S.：Arthur-Merlin博弈：一种随机化证明系统与复杂性类层次。《计算机与系统科学杂志》**36**(2)，254–276（1988年）7. Ben-Or, M., Goldwasser, S., Kilian, J., Wigderson, A.：多证明者交互式证明：如何消除难解性假设。载于：第二十届 ACM 计算理论年度研讨会论文集。第113–131页。ACM（1988年）8. Campanelli, M., Gennaro, R.：可顺序组合的理性证明。载于：安全决策与博弈论：第六届国际会议 GameSec 2015，英国伦敦，2015年11月4日至5日，论文集6。第270–288页。Springer（2015年）9. Campanelli, M., Gennaro, R.：针对空间受限计算的高效理性证明。载于：安全决策与博弈论：第八届国际会议 GameSec 2017，奥地利维也纳，2017年10月23日至25日，论文集。第53–73页。Springer（2017年）10. Chen, J., McCauley, S., Singh, S.：具有多个证明者的理性证明。载于：2016年 ACM 理论计算机科学创新会议论文集。第237–248页（2016年）11. Chen, J., McCauley, S., Singh, S.：具有强效用差距保证的高效理性证明。载于：算法博弈论：第十一届国际研讨会 SAGT 2018，中国北京，2018年9月11日至14日，论文集11。第150–162页。Springer（2018年）12. Chen, J., McCauley, S., Singh, S.：非合作理性交互式证明。载于：第27届欧洲算法研讨会（ESA 2019）。Schloss Dagstuhl-Leibniz 信息学中心（2019年）13. Fortnow, L., Reingold, N.：PP 在真值表归约下封闭。《信息与计算》**124**(1)，1–6（1996年）14. Fortnow, L., Rompel, J., Sipser, M.：多证明者交互协议的能力。《理论计算机科学》**134**(2)，545–557（1994年）15. Goldwasser, S., Micali, S., Rackoff, C.：交互式证明系统的知识复杂性。《SIAM计算杂志》**18**(1)，186–208（1989年）16. Goldwasser, S., Sipser, M.：交互式证明系统中的私有随机币与公开随机币之争。载于：第18届 ACM 计算理论年度研讨会论文集，1986年5月28日至30日，美国加利福尼亚州伯克利。第59–68页（1986年）17. Guo, S., Hubáček, P., Rosen, A., Vald, M.：理性论证：具有次线性验证的单轮委托。载于：第五届理论计算机科学创新会议论文集。第523–540页。ITCS '14，计算机协会，美国纽约州纽约市（2014年）18. Inasawa, K., Yasunaga, K.：针对理性验证者的理性证明。《电子、通信与计算机科学基础IEICE汇刊》**100**(11)，2392–2397（2017年）

19. Lund, C., Fortnow, L., Karloff, H.J., Nisan, N.：交互式证明系统的代数方法。《美国计算机协会会刊》**39**(4)，859–868（1992） 20. Shamir, A.：IP=PSPACE。载于：第31届计算机科学基础年会论文集，圣路易斯，密苏里州，美国，1990年10月22日至24日，第I卷。第11–15页（1990） 21. Shen, A.：IP=PSPACE：简化证明。《美国计算机协会会刊》**39**(4)（1992） 22. Toda, S.：PP与多项式时间层次一样难。《SIAM计算杂志》**20**(5)，865–877（1991） 23. Wagner, K.W.：简洁输入表示下组合问题的复杂性。《信息学学报》**23**(3)，325–356（1986）

## 引理 1 的证明

证明。 用 $R$ 表示 $\Pi$ 中的奖励函数，用 $\varphi$ 表示其中的价值函数。 $i=0$ 或 $j=0$ 的情形显然成立，因此我们假设 $i,j\geq 1$。考虑以下 $\widetilde{}$ 协议 $\Pi$：在第一轮中，给定输入 $x$ 和一份部分对话记录 $\mathcal{T}$，Merlin 发送 $E=E_i^{\Pi}(\mathcal{T})$，以及 Merlin 在协议 $\Pi$中会发送的第 $(i+1)$ 条消息；其他所有消息则与理性 Merlin 在 $\Pi$ 中发送的消息完全相同。最后，Arthur 向 Merlin 支付

$$\widetilde{R}=\frac{1}{2}R(\mathcal{T})+\frac{1}{4}\Delta(\Pi)(x)\Big(1-\big(E-R(\mathcal{T})\big)^2\Big),$$

否则，如果 Merlin 的消息格式不符合协议规定的格式（例如，值 $E$ 不在范围 $[0,1]$ 内），则支付 0。注意 $\widetilde{}$， $R$ 是多项式时间可计算的，因为根据定义，$R$ 和 $\Delta(\Pi)(\cdot)$ 都是多项式时间可计算的（我们可以使用形如 $2^{-\operatorname{poly}(|x|)}for\Delta(\Pi)$ 的函数）。由于奖励是 $[0,1],$ 中的一个值，$(E-R(\mathcal{T}))^2$ 的值也属于 $[0,1],$。这意味着，如果 Merlin 在某一步偏离协议 $\Pi$的“后续协议”，那么 $\frac{1}{2}R(\mathcal{T})$ 的期望值至少会降低 $\frac{1}{2}\Delta(\Pi)(x)$，而 $\frac{1}{4}\Delta(\Pi)(x)\Big(1-\big(E-R(\mathcal{T})\big)^2\Big)$ 的期望值增加幅度不会超过 $\frac{1}{4}\Delta(\Pi)(x)$。这意味着理性 Merlin 只能通过在第一轮发送不正确的 $E$ 来偏离协议。

但随后他将需要选择 $E$ 以使泛函最小化

$$\mathbb{E}\Big[(E-R(\mathcal{T}))^2\Big|\mathcal{T}_i\sqsubseteq\mathcal{T}\Big],$$

其中， $\mathcal{T}_i\sqsubseteq\mathcal{T}$ 表示 $\mathcal{T}$ 是 $\mathcal{T}_i$ 的后续协议。该值通过以下方式最小化：

$$E=\mathbb{E}\left[R(\mathcal{T})\mid\mathcal{T}\sqsubseteq\mathcal{T}_i\right]=E_i^{\Pi}(\mathcal{T}_i),$$

其中，最后一个等式成立是因为，正如我们已经证明的，协议 $\Pi$ 中的 $\widetilde{}$理性 Merlin 将会像协议 $\Pi$中的理性 Merlin 一样行动。

最后，Arthur 返回值 $\widetilde{\varphi}=(E,\varphi(\mathcal{T}'))$，其中 $\mathcal{T}'$ 只是去掉对 $E$的提及后的 $\mathcal{T}$。根据理性 Merlin 已确立的行为，立即可知 $E=E_i^{\Pi}(\mathcal{T}_i)$；此外，如果 $\mathcal{T}_i$ 是在与理性 Merlin 的交互中产生的，那么 $\varphi(\mathcal{T}')=f(x)$。

## B 定理的证明4

证明。 包含关系 DRMA$[k] \subseteq$P$^{\mathbf{FRMA}[k]}$ 是显然的。

为证明另一个包含关系，令 $A$ 为 P$^{\mathbf{FRMA}[k]}$ 中的一种语言，对于其个 $f \in$ FRMA$[k]$，并令 $\Pi$ 为 $f$ 的 DRMA$[k]$ 协议。再令 $M$ 为一台多项式时间图灵机，它可以访问预言机 $f$ 并识别 $A$。现在考虑针对输入字符串 $x$的以下$k$轮协议 $\widetilde{\Pi}$，用于 $A^f$。

1. 在第一轮中，Merlin 发送一条消息 $m_1$，其中包含一个数字 $l$、一块由 $l$ 个字符串组成的内容 $y_1, y_2, \ldots, y_l$，以及一块由 $l$ 个字符串组成的内容 $m_1^{(1)}, m_1^{(2)}, \ldots, m_1^{(l)}$：

$$m_1 = \left(l; y_1, \ldots, y_l; m_1^{(1)}, \ldots, m_1^{(l)}\right).$$

2. Arthur 随后在输入 $x$ 上模拟机器 $M$，使用字符串 $y_i$ 作为对预言机查询 $x_1$, $\ldots, x_l$ 的回答，并将字符串 $m_1^{(j)}$ 解释为 Merlin 在针对 $x_i$ 的协议 $\Pi$ 中的第一条消息（如果对 $M$ 的模拟未恰好进行 $l$ 次查询，则最终奖励设为 0）。

3. 在以下所有轮中，Merlin 发送格式为 $m_i = \left(m_i^{(1)}, \ldots, m_i^{(l)}\right)$ 的消息，而 Arthur 发送格式为 $a_i = \left(a_i^{(1)}, \ldots, a_i^{(l)}\right)$ 的消息，其中 Arthur 将每个 $a_i^{(j)}$ 计算为对 transcript 的响应。

$$\mathcal{T}_i^{(j)} = \left(x_j; m_1^{(j)}, a_1^{(j)}, \ldots, m_i^{(j)}\right),$$

而 Merlin 预计也会表现出类似的行为。

4. 在全部 $k$ 轮结束后，Arthur 计算 $\Delta = \min_j \Delta(\Pi)(x_j)$，并为每个“子协议”奖励 $R_j$；如果 Merlin 没有明显偏离协议，则向他支付。

$$R = \frac{1}{2}R_1 + \frac{\Delta}{4}R_2 + \ldots + \frac{\Delta^{l-1}}{2^l}R_l + \frac{\Delta^l}{2^{l+1}}.$$

Arthur 当且仅当收到字符串 $y_j$ 作为对查询 $x_j$ 的回答、且 Merlin 在每个“子协议”中都已证明 $f(x_j) = y_j$ 的机器 $M$ 接受 $x$ 时，才接受 $x$。

让我们证明，一个多项式时间随机化 Arthur 能够遵循所描述的协议。在该协议中，查询的数量以及每个查询 $x_j$ 的长度均受机器 $M$ 在输入 $x$ 上运行所用时间的限制，因此对于每个 $j$，我们有 $|x_j| =$poly($|x|$) 和 $l =$poly($|x|$)。这意味着每个 $y_j$、每条消息 $a_i^{(j)}$、$m_i^{(j)}$ 以及每条组合消息 $a_i$、$m_i$ 的长度也都是 poly($|x|$)。根据定义，值 $\Delta(\Pi)(x_j)$ 是多项式时间可计算且长度为多项式的值。计算 $R$ 需要对长度为多项式的有理数执行多项式数量的基本算术运算，因此也可以在多项式时间内完成。

现在我们证明，理性 Merlin 不会偏离协议。由于$R$ 是一个严格正值，理性 Merlin 没有动机违反

消息格式，也不会提供与模拟 $M$ 中的查询次数不符的 $l$ （这会导致奖励为 0）。

通过对 $j$ 进行归纳法，我们将证明对所有 $j$:

**(a)** 模拟中的第 $j$ 个查询 $x_j$ 等于实际机器 $M$ 在访问 $f$时的第 $j$ 个查询，该模拟由 $M$ 进行；**(b)** 对于所有 $i = 1, 2, \ldots, k$，字符串 $m_i^{(j)}$ 是相应“子协议”中理性 Merlin 的最优选择；**(c)** $y_j = f(x_j)$。

为了在假设对所有 $j' < j$ 都已证明的情况下证明 $j$ 的**(a)**，注意到，对所有 $j' < j$ 而言，**(a)**和**(c)** 意味着，由于 $M$ 是一台确定性图灵机，其模拟在向预言机发出第 $j'$ 个查询之前（包括该查询），都以与 $M^f$ 相同的方式运行。

现在我们在假设对所有 $j' < j$ 都已证明的情况下，证明 $j$ 的**(b)** 。假设理性 Merlin 在第 $j$ 个子协议中直到第 $i$ 轮都没有偏离。令 $\widetilde{m}_i^{(j)}$ 为第 $j$ 个子协议中的最优第 $i$ 条消息，令 $\widehat{m}_i^{(j)}$ 为对第 $j$ 个子协议而言次优的一条消息，并令 $\widehat{m}_i$ 为相应的不诚实消息。根据归纳法假设，理性 Merlin 会在所有先前的子协议中选择最优消息，因此

$$
\begin{aligned}
E_{i-1}^{\widetilde{\Pi}}(\mathcal{T}_{i-1}) &\geq \sum_{j'<j} \frac{\Delta^{j'-1}}{2^{j'}} E_{i-1}^{\Pi}\left(\mathcal{T}_{i-1}^{(j')}\right) + \frac{\Delta^{j-1}}{2^{j}} E_i^{\Pi}\left(\left(\mathcal{T}_{i-1}^{(j)}, \widetilde{m}_i^{(j)}\right)\right) \\
&\geq \sum_{j'<j} \frac{\Delta^{j'-1}}{2^{j'}} E_{i-1}^{\Pi}\left(\mathcal{T}_{i-1}^{(j')}\right) + \frac{\Delta^{j-1}}{2^{j}} \left(E_i^{\Pi}\left(\left(\mathcal{T}_{i-1}^{(j)}, \widehat{m}_i^{(j)}\right)\right) + \Delta(\Pi)(x_j)\right) \\
&\geq \sum_{j'<j} \frac{\Delta^{j'-1}}{2^{j'}} E_{i-1}^{\Pi}\left(\mathcal{T}_{i-1}^{(j')}\right) + \frac{\Delta^{j-1}}{2^{j}} E_i^{\Pi}\left(\left(\mathcal{T}_{i}^{(j)}, \widehat{m}_i^{(j)}\right)\right) + \frac{\Delta^{j}}{2^{j}} \\
&> \sum_{j'<j} \frac{\Delta^{j'-1}}{2^{j'}} E_{i-1}^{\Pi}\left(\mathcal{T}_{i-1}^{(j')}\right) + \frac{\Delta^{j-1}}{2^{j}} E_i^{\Pi}\left(\left(\mathcal{T}_{i}^{(j)}, \widehat{m}_i^{(j)}\right)\right) + \sum_{j<j'\leq l+1} \frac{\Delta^{j'-1}}{2^{j'}} \\
&\geq E_i^{\widetilde{\Pi}}\left(\mathcal{T}_i, \widehat{m}_i\right),
\end{aligned}
$$

这里所有不等式都由定义直接得到，最后一个不等式则由 **(b)** 的归纳假设以及几何级数的上界得出（注意所有值 $R'_j$ 均不超过 1）：根据 **(b)** 的归纳假设，$(\mathcal{T}, \widehat{m}_i)$ 的期望奖励是部分对话记录 $\left(\mathcal{T}(\,{}_{i-1}^{j'}\,)\right)$ 对应的期望奖励、部分对话记录 $\left(\mathcal{T}_i^{(j)}, \widehat{m}_i^{(j)}\right)$ 的期望奖励以及其余子协议的期望奖励的组合，而后者均不超过 1。

~最后，**(c)** 对 $j$ 成立，是由**(b)** 对 $j$成立推出的，因为 $\Pi$ 中的理性Merlin在第 $j$ 个子协议中的行为，就像一个理性 Merlin 在 $\Pi$ 中的行为一样。

## C 引理3的证明

证明。 我们将描述概率多项式时间算法，该算法以至少 $1/2$ 的概率判定语言 Compare – Expectations。

输入 $(C_0, C_1)$ 时，算法独立地采样两个长度为 $n$ 的均匀分布字符串 $r, r'$，并计算两个比特： $c_0 = C_0(r)$ 和比特 $c_1 = C_1(r')$。如果 $c_0 < c_1$ （即 $c_0 = 0$ 和 $c_1 = 1$），则算法接受该输入；如果 $c_0 > c_1$，则拒绝。如果 $c_0 = c_1$，算法以概率 $1/2$ 接受，否则拒绝该输入。

对于 $i = 0$，1，记 $\mathbb{E}_{r\sim\mathcal{U}_n} C_i(r)$ 的值为 $E_i$。那么

$$\Pr[\ \textit{the algorithm accepts}\ ] = \Pr[c_0 < c_1] + \frac{1}{2}\Pr[c_0 = c_1] =$$
$$= \Pr[c_0 = 0, c_1 = 1] + \frac{1}{2}\big(\Pr[c_0 = c_1 = 0] + \Pr[c_0 = c_1 = 1]\big) =$$
$$= (1 - E_0)E_1 + \frac{1}{2}\big((1 - E_0)(1 - E_1) + E_0E_1\big) =$$
$$= \frac{1}{2} + \frac{E_1 - E_0}{2},$$

当且仅当 $(C_0, C_1)$ 时，该值至少为 $1\,2$。比较期望值。由于我们假设方案的大小至少与其输入大小相同，因此该算法在多项式时间内终止。

## D 定理 8 的证明

证明。 假设存在这样的函数 $R$ 和 $\varphi$ 以及常数 $\alpha < 1/2$。对于每个 $m$，考虑多项式

$$Q_m(p) = \frac{1}{2^s}\sum_{a\in\{0,1\}^s}\sum_{r\in\{0,1\}^d} R(1^n, m, a, r)p^{|r|_1}(1 - p)^{|r|_0},$$

其中， $|r|_b$ 是 $r$ 中等于 $b \in \{0, 1\}$的比特数。注意，对于所有 $m$，我们都有 deg $Q_m \le |r|_1 + |r|_0 = |r| = d = \text{poly}(n)$。显然，对于所有 $m$，我们也有 $\mathbb{E}_{a,\ r}R(1^n, m, a, r) = Q_m\left(\frac{k}{2^n}\right)$。

根据我们的假设，存在一个（不一定可计算的）函数$m_*\colon \{0, 1, \ldots, 2^n\} \to \{0, 1\}^{<\alpha n}$，使得对于每个 $k$:

1. $\varphi(1^n, m_*(k)) = (k \text{ 模 } 2)$，2. $Q_{m_*(k)}\left(\frac{k}{2^n}\right) > Q_{\widetilde{m}}\left(\frac{k}{2^n}\right)$ 对于任意满足 $\varphi(1^n, \widetilde{m}) \neq (k \text{ 模 } 2)$ 的 $\widetilde{m}$。

根据鸽巢原理，存在一个字符串 $m_0, m_1$，使得对于至少 $\frac{2^n}{2^{\alpha n+1}}$ 个偶数值的 $k$， $m_0 = m_*(k)$ 成立。由于这些数全都是偶数，因此至少有 $\frac{2^n}{2^{\alpha n+1}} - 1$ 个奇数与 $m_*^{-1}(m_0)$ 交错。再次应用鸽巢原理可知，存在一个字符串 $m_1$，使得 $m_*^{-1}(m_1)$ 中至少有 $\frac{\frac{2^n}{2^{\alpha n+1}}-1}{2^{\alpha n+1}} > 2^{(1-2\alpha)n-3}$ 个奇数与

某个 $m_*^{-1}(m_0)$ 的子集交错。令 $k_0 < k_1 < \ldots < k_N$ 表示 $m_*^{-1}(m_0)$ 和 $m_*^{-1}(m_1)$ 的交错子集，其中对于 $i$ 的偶数值，$k_i \in m_*^{-1}(m_0)$ 成立；对于 $i$ 的奇数值，$k_i \in m_*^{-1}(m_1)$ 成立。

$\mathrm{LQ}(\widehat{k_i})$ 表示差值所有偶数 $i$ 以及 $Q$ 注意到 $\widehat{Q}(k_i) = 0$ 对于所有奇数 $i$，由介值定理可知，$Q$ 至少有 $N-1$ 个不同的零点。由于 $N = \Omega(2^{(1-2\alpha)n})$，而 $\deg \widehat{Q} \leq \widehat{d} = \mathrm{poly}(n)$，因此我们有 $Q \equiv 0$；而对于所有 $i$，都有 $Q(k_i) \neq 0$。由此得到的矛盾证明了所声称的结果