arXiv:2611.31236v1 [quant-ph] 23 Nov 2026

量子交互式证明系统只需两条消息

Yupan Liu*[1]

[1]洛桑联邦理工学院计算机与通信科学学院

摘要

量子交互式证明系统可以通过并行化缩减至三条消息，这一点由Kitaev 和 Watrous（STOC 2000）证明，或许这是它们与经典对应系统之间最显著的区别。在这项工作中，我们证明任何量子交互式证明系统都可以进一步并行化为两条消息：验证者发送 EPR 对的一半（“量子公共随机币”），并在证明者响应后仅使用*stoquastic* 验证。具体而言，我们强化了量子交互式证明(3) =量子交互式证明 = PSPACE 这一结果，该结果由Jain、Ji、Upadhyay 和 Watrous（JACM，2011）提出；并通过证明以下结论，完整刻画了双消息量子交互式证明系统：

$$\text{qq-StoqAM} = \text{qq-QAM} = \text{QIP}(2) = \text{QIP} = \text{PSPACE}.$$

我们的主要技术贡献表明，接近均匀分布的像(CIUNIFORM——它自然属于*stoquastic* 版本的qq-QAM——是PSPACE困难的。我们将Shamir（JACM，1992年）和Shen（JACM，1992年）的求和检验协议转化为一个CIUNIFORM实例，其中包含一个高效采样器；当底层量化布尔公式为真时，对于某种输入分布，其像分布恰好是均匀分布。

1 引言

量子版交互式证明系统 [Bab85、GMR89]的研究始于 [Wat03]。对于一个承诺问题 $(\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$的量子交互式证明系统中，一名量子多项式时间验证者 与一名不可信的证明者 进行交互，证明者的计算能力不受限制，双方交换的消息数量至多为多项式级。给定输入 $x \in \mathcal{I}_{\text{yes}} \cup \mathcal{I}_{\text{no}}$，证明者断言 $x \in \mathcal{I}_{\text{yes}}$，随后双方执行一个交互协议，最终由验证者决定接受还是拒绝该断言。协议具有完备性 c，这意味着存在一种证明者策略，使验证者以至少 c 的概率接受是 实例 $x \in \mathcal{I}_{\text{yes}}$。协议还具有可靠性 s，这意味着对于 s 否 实例，无论证明者如何行动，验证者接受的概率至多为

著名的 量子交互式证明 = PSPACE [JJUW11] 以及 IP = PSPACE [LFKN92、Sha92] 定理确立了：当完备性与可靠性之间的差距 $c - s$ 至少为逆多项式时，量子交互式证明系统与其经典对应系统具有相同的计算能力。尽管如此，量子交互式证明系统仍呈现出一种称为

并行化：任何量子交互式证明系统都可以并行化，从而仅使用三条消息 [KW00], ，且验证者的唯一消息可以是单个公开硬币 [MW05]。相比之下，若将具有多项式多条消息的经典交互式证明系统并行化为常数条消息，则会使多项式时间层次坍缩至第二层 [BHZ87], ，因为所有常数消息经典交互式证明系统都可以并行化为两条消息 [Bab85，GS86]。

*电子邮件：yupan.liu@epfl.ch

1.1 主要结果

在本工作中，我们将三消息量子交互式证明系统，针对PSPACE [Wat03]，改进为两条消息，并回答 [Wat03第 4]节与 [VW16第4节中的开放问题。5]:

定理 1.1. qq-StoqAM$_1$ = qq-QAM = QIP(2) = QIP = PSPACE。

这里，下标 1 表示完美完备性。值得注意的是，QIP(2) 和 qq-QAM 的完美完备性都是直到最近才得到证明的，见 [LV26]。此外，将我们的包含关系 PSPACE ⊆QIP(2) 与三消息并行化 QIP ⊆ QIP(3) [KW00，KKMV09] 以及包含关系 QIP(3) ⊆ PSPACE [MW05，JJUW11] 结合起来可得

> 所有具有多项式数量消息的量子交互式证明系统都可以并行化为两条消息。

关于量子公共随机币的推论。 定理 1.1 所依据的双消息证明系统中，验证者发出的消息仅由 EPR 对的一半组成，这些消息称为 量子公共随机币，相应的复杂度类 qq-QAM 由 [KLN19]引入。因此，定理1.1改进了广义 Arthur–Merlin 证明系统的塌缩定理 [KLN19，定理 1。7], 在该定理中，验证者的消息包含 EPR 对的一半（“q”）或随机比特（“c”），将 四种类别缩减为三种:

推论 1.2 （关于广义阿瑟–梅林博弈的三分法定理）。 对于任意常数$m \geq 2$，下述三分法对 m 消息广义量子阿瑟–梅林博弈成立:

(1) 对于消息类型 t_1、 $\cdots$、 t_m 在 {c、q} 中的任意选择，若存在指标 $j \geq 2$ 使得 $t_j = \mathrm{q}$，则 $t_m \cdots t_1$-QAM(m) = PSPACE。

(2) c $\cdots$cq-QAM(m) = cq-QAM =: QAM。

(3) c $\cdots$c-QAM(m) = cc-QAM =: QCAM.

由于 QAM ⊆ BP ·PP [MW05，定理 4。7], 证明 QAM = qq-QAM 将使计数层级（CH）坍缩到第二层。因此，推论 1.2 表明

> 除非CH 坍缩，否则在双消息量子证明系统中，量子公共随机币比经典公共随机币严格更强。

对 stoquastic 交互式证明系统的推论。定理1.1 所依据的双消息证明系统中的验证者仅使用 *stoquastic* 验证，只允许使用 $|0\rangle$ 和 $|+\rangle$辅助量子比特、经典可逆电路，以及最后一次 Hadamard 基测量。如果验证者发送的消息仅限于经典公共随机币，在称为StoqAM的模型中，通过将StoqAM = 归约到 AM，可以看出这一点；具体做法是对固定公开挑战后得到的验证者应用 [BBT06第 5] 节中的平均化论证。由于单消息模型StoqMA 包含于AM [BBT06] ，且人们认为它会坍缩到MA [Liu21，AGL25], 定理1.1 还揭示了*stoquastic* 交互式证明系统的消息数存在鲜明的二分性:

- 一条消息：StoqMA 似乎并不比其经典对应类 MA 强大多少；
- 两条或更多消息：qq-StoqAM 与其完全量子版本 qq-QAM 一样强，因此涵盖了经典交互式证明系统的全部能力。

1.2 证明概述

为证明定理 1.1，特别是 PSPACE $\subseteq$ qq-StoqAM$_1$，我们引入接近均匀分布的像（CIUniform，见定义 3.1）。它是 [KLN19], 提出的“接近完全混合态的像”问题的一个特例，可作为 PSPACE 与 qq-StoqAM$_1$之间的桥梁。CIUniform 的一个实例由一个多项式规模的采样器 $\mathcal{S}$ 构成，它以 $(u,r) \in \{0,1\}^{m_{\text{in}}} \times \{0,1\}^{m_+}$ 为输入，其中 $r \sim U_{m_+}$ 为均匀随机的随机种子，并输出 $u' \in \{0,1\}^{m_{\text{out}}}$。相应的转移矩阵定义为 $M_{\mathcal{S}}(u',u) = 2^{-m_+}|\{r : \mathcal{S}(u,r) = u'\}|$。CIUniform$[\eta]$要求区分以下情况：

（是）存在某个输入分布 p，使给定采样器的输出 $M_{\mathcal{S}}p$ 恰好是均匀的；

（否）对于每个输入分布 p，$M_{\mathcal{S}}p$ η与均匀分布 $U_{m_{\text{out}}}$ 之间的全变差距离都至少为给定值。

为此，我们需要证明：(i) CIUniform 通过PSPACE-完全性归约，借助 [Sha92中使用的求和检验协议92]是 PSPACECIUniform 属于 qq-StoqAM$_1$。

回顾用于全称量化布尔公式**的求和检验协议**。我们先考虑真量化布尔公式(全称量化布尔公式)，它是PSPACE完全的 [SM73，定理 4。3]在一个量化布尔公式 $\Phi = Q_1 x_1 \cdots Q_m x_m\, \phi(x_1, \ldots\ldots, x_m)$中，每个量词 $Q_i \in \{\exists, \forall\}$ 都在 x_i上进行量化，且 $\{0,1\}$是一个无量词的布尔公式。

与 [Wat03第 3 节类似，1], 我们使用用于全称量化布尔公式 [的92], 求和检验协议，该协议使用一列多项式 $P_0, \ldots\ldots, P_T$，定义在 $m' = O(|\Phi|)$ 个变量上，取值于有限域 $\mathbb{F}_q$，其中 T 表示协议的轮次数。在端点处，常数 P_0 当且仅当1 当且仅当 Φ 为真时成立，而验证者可以直接计算 P_T。在任意中间轮次 $t < T$，验证者执行以下操作；每一轮的操作可以是全称量化、存在量化或降次：

(1) 接收一个次数至多为二的单变量多项式 g 的系数，[1] 声称它是 P_{t+1} 在坐标 j_t 上的单变量限制，即 $g_\star(X) = P_{t+1}(\alpha_1, \ldots, \alpha_{j_t-1}, X, \alpha_{j_t+1}, \ldots, \alpha_{m'})$，其中本轮的运算作用于坐标 j_t，而 α 表示对 P_{t+1} 的赋值。(2) 根据第 t 轮运算，使用 $g(0)$ 和 $g(1)$ 检验当前声明 $P_t(\alpha) = \nu$。(3) 如果检验通过，则在从域中均匀随机选取的元素 $r \in \mathbb{F}_q$ 处计算 g，得到下一轮声明 $P_{t+1}(\alpha_1, \ldots, \alpha_{j_t-1}, r, \alpha_{j_t+1}, \ldots, \alpha_{m'}) = g(r)$。

重要的是，正如 [She92], 中所示，降次数操作确保真实限制$g_\star(X)$ 在第 t 轮具有相同的次数上界。如果当前声明是错误的且检验通过，那么 $g - g_\star$ 是一个次数至多为二的非零多项式，因此 $g(r) = g_\star(r)$ 至多对 $r \in \mathbb{F}_q$ 的两个取值成立。因此，下一轮声明正确的概率至多为 $2/q$。由此，[She92] 中求和检验协议的可靠性误差上界可由对所有 T轮次应用并合界得出；当多项式有足够大的界 q时，该结论成立。

CIUniform **是 PSPACE-困难（经由针对** 全称量化布尔公式**的求和检验）**。我们将 全称量化布尔公式归约到 CIUniform，而我们的证明构造现在与 [Wat03] 分道扬镳。在三消息量子证明系统（出处为 [Wat03，第 3 节）中，2], 验证者首先以叠加态接收完整的求和检验记录，然后检查 局部一致性 （即每条记录内相继求和检验断言的一致性）。相反，我们的构造检查 全局一致性 （跨各求和检验轮次）。

为此，我们基于单步求和检验转移构造了一个高效采样器 $\mathcal{S}$，它以元组（t，α，g）作为输入，该元组由轮次索引 t、求值点 $\alpha \in \mathbb{F}_q^{m'}$ 以及所断言的单变量多项式 g的三个系数组成，并输出一个元组（t'，α'，ν）

[1]在我们的 构造中，P_T 的多重线性以及次数归约确保该界在每一 ry 轮次；参见 引理 3.6。一项相关的个别次数界见于 [BF91，引理 9.2(a)]。

表示断言 $P_{t'}(\alpha') = \nu$。这种全局一致性给出了我们的qq-StoqAM$_1$ 证明系统所检验的条件：当底层量化布尔公式 Φ 为真时，存在一种输入分布，使得采样器的输出恰好是均匀的。

更具体地说，对于 Φ 为真的 是实例，均匀随机地选择一对 (t, α)，并取 $g = g_\star$，其中 $t < T$，而 $g = 0$。采样器从一个均匀元组 (t, α, ν) 开始，仅当 $\nu = P_t(\alpha)$ 时才将其替换为下一轮声明。若不发生替换，则 $(t', \alpha') = (t, \alpha)$。发生替换时，下一轮下标 t' 按循环顺序向前移动：

(i) 若 $t < T$，则下一轮为 $t' = t + 1$，而 α' 是通过将轮次 t 中使用的坐标 α_{j_t} 替换为均匀随机选取的 $r \in \mathbb{F}_q$ 得到的；(ii) 若 $t = T$，则采样器返回第 0 轮并保留 $\alpha' = \alpha$。

因此，数对 (t', α') 服从均匀分布。由于对于每个 (t, α)，替换发生的概率为$1/q$，并且即使采样器返回第 0 轮，下一轮声明仍然正确，因此下一轮声明与被替换的断言具有相同的分布。因此，采样器的输出仍然严格服从均匀分布。

对于 Φfalse 的非 实例，我们固定任意一个输入分布 p，并界定采样器的输出分布 $M_{\mathcal{S}}p$与均匀分布 $U_{m_{\text{out}}}$之间的全变差距离 TV($M_{\mathcal{S}}p$，$U_{m_{\text{out}}}$)。为此，我们考察在 $U_{m_{\text{out}}}$下的以下两个事件：

(i) 当从 $\{0, \ldots, T\} \times \mathbb{F}_q^{m'} \times \mathbb{F}_q$ 中均匀随机抽取 (t'，α'，ν) 时，选择轮次 T（$t' = T$）这一事件发生的概率为 $1/(T+1)$；(ii) 对每个固定的 t' 和 α'，$P_{t'}(\alpha') = \nu$ 这一事件发生的概率为 $1/q$。

令 (t'，α'，ν) $\sim M_{\mathcal{S}}p$。对这些事件在 $U_{m_{\text{out}}}$ 和 $M_{\mathcal{S}}p$ 下的概率差取相应的加权平均，其中每个概率差都至多为 TV($M_{\mathcal{S}}p$，$U_{m_{\text{out}}}$)，由此得到以下界

$$\mathrm{TV}(M_{\mathcal{S}}p, U_{m_{\text{out}}}) \geq \frac{1}{q+1}\left|\frac{1}{T+1} - \Pr\left[t' = T\right]\right| + \frac{q}{q+1}\left|\frac{1}{q} - \Pr\left[P_{t'}(\alpha') = \nu\right]\right|. \tag{1.1}$$

进一步分析我们的采样器构造，可得事件 (i) 对应的 $|1/(T+1) - \Pr[t' = T]|$ 的下界，以及事件 (ii) 对应的 $|1/q - \Pr[P_{t'}(\alpha') = \nu]|$ 的下界。将这些下界代入方程 (1.1)，可以看到，所得下界中的未知项 $\Pr[t = T]$ 会因方程 (1.1) 中的权重而抵消。取 $q = 8(T+1)$，我们便可得出结论：对于每个输入分布 p，TV($M_{\mathcal{S}}p, U_{m_{\text{out}}}$) $\geq 1/(4q(T+1))$。

剩下的挑战是确保所得的 $\mathrm{CIU}_{\mathrm{NIFORM}}[\eta]$ 实例具有逆多项式参数 $\eta = 1/(32(T+1)^2)$，这对于所得的 qq-StoqAM证明系统通过平行重复达到常数承诺间隙至关重要。[2] 利用 [She92], 中的降次，可以取 $T + 1 = O(|\Phi|^2)$，因此 $\eta = 1/O(|\Phi|^4) = 1/\mathrm{poly}(n)$，正如所需。

一个 qq-StoqAM 证明系统，用于 CIUniform。 给定一个 CIUniform$[\eta]$实例，我们有相应的采样器 $\mathcal{S}$：$\{0,1\}^{m_{\text{in}}} \times \{0,1\}^{m_+} \to \{0,1\}^{m_{\text{out}}}$及其可逆电路实现 $U_{\mathcal{S}}$，使得 $U_{\mathcal{S}}|u,\ r,\ w\rangle = |u,\ r,\ w \oplus \mathcal{S}(u,\ r)\rangle$ 对每个 $u \in \{0,1\}^{m_{\text{in}}}$、$r \in \{0,1\}^{m_+}$ 和$w \in \{0,1\}^{m_{\text{out}}}$。我们考虑以下 qq-StoqAM$_1$ 证明系统：

(1) 在寄存器 (B，B′) 之间制备 m_{out} EPR 对，并将 B′ 发送给证明者。

(2) 接收 m_{in} 量子比特的输入寄存器 A 和 m_+ 量子比特的种子寄存器 R，并对寄存器 (A,R, B) 应用 $U_{\mathcal{S}}^\dagger$。

[2]例如，对于具有指数基数的域，如 [Sha92，定理 6], TV($M_{\mathcal{S}}p$，$U_{m_{\text{out}}}$) 所示，因此 η将是指数级小的，从而所得的 qq-StoqAM 证明系统也只会具有指数级小的承诺间隙。

(3) 在寄存器 (R,B) 和 (R', B') 之间执行 SWAP 测试，由初始化为 $|+\rangle$ 的单量子比特寄存器 O 控制，其中 R' 和 B' 分别初始化为 $|+\rangle^{\otimes m_+}$ 和 $|0\rangle^{\otimes m_{\text{out}}}$。当且仅当 SWAP 测试接受时，才接受。

接下来，我们说明这一证明系统。对于是 实例，选择一个分布 p 使得$M_{\mathcal{S}}p = U_{m_{\text{out}}}$。收到 B″后，诚实证明者通过等距变换，将每个基态 $|u'\rangle$ 映射为与 $\sum_{(u,r):\mathcal{S}(u,r)=u'} \sqrt{p(u)}|u\rangle_{\mathsf{A}}|r\rangle_{\mathsf{R}}$ 成比例的量子态。由于对于每个 u'，$(M_{\mathcal{S}}p)(u') = 2^{-m_{\text{out}}}$，归一化因子对每个 u' 都相同。因此，应用 $U_{\mathcal{S}}^{\dagger}$ 后，验证者得到量子态 $(\sum_u \sqrt{p(u)}|u\rangle_{\mathsf{A}})|+\rangle^{\otimes m_+}{}_{\mathsf{R}}\,|0\rangle^{\otimes m_{\text{out}}}{}_{\mathsf{B}}$。由于 (R,B) 上的约化密度矩阵与 (R', B') 上的约化密度矩阵相同，SWAP 测试必定接受。

对于 无 实例，对于每个输入分布 p，$\text{TV}(M_{\mathcal{S}}p, U_{m_{\text{out}}}) \geq \eta$。固定任意一种证明者策略，并令 $|\psi\rangle$ 表示验证者应用 $U_{\mathcal{S}}^{\dagger}$ 之前，$(\mathsf{A},\mathsf{R},\mathsf{B},\mathsf{Q})$ 上的联合纯态，其中 Q 表示证明者的私有寄存器。由于 B 是验证者的私有寄存器，且由 EPR 对的一半组成，因此对 $|\psi\rangle$ 中的 B 进行测量会得到 $U_{m_{\text{out}}}$。相反，考虑在 $(\mathsf{R},\mathsf{B},\mathsf{Q})$ 上的任意纯态$|\xi\rangle$：该态由应用 $U_{\mathcal{S}}$ 得到，其中 (R,B) 初始化为 $|+\rangle^{\otimes m_+}|0\rangle^{\otimes m_{\text{out}}}$，并允许 A 与 Q 纠缠。对 $|\xi\rangle$ 中的 B 进行测量会得到某个 p 所对应的 $M_{\mathcal{S}}p$。由于在计算基下测量不会增加迹距离，因此

$$\eta \leq \text{TV}(M_{\mathcal{S}}p, U_{m_{\text{out}}}) \leq \sqrt{1 - |\langle\psi|\xi\rangle|^2}.$$

因此，对于所有此类 $|\xi\rangle$，$|\langle\psi|\xi\rangle|^2 \leq 1 - \eta^2$ 均成立，而 SWAP 测试的接受概率至多为 $(1 + (1-\eta^2))/2 = 1 - \eta^2/2$，得证。

2 预备知识

我们假定读者熟悉量子信息与计算，教材 [NC10] 可作为良好的入门起点。我们推荐 [VW16] 作为量子交互式证明系统的自成体系综述。

本文中，所有对数均以 2 为底。我们用 U_ℓ 表示 ℓ 比特上的均匀分布，并用 $\mathbb{I}[E]$ 表示示性函数，当且仅当事件 E 发生时其取值为 1。对于集合 S上的任意概率分布 p_0 与 p_1，它们之间的全变差距离定义为 $\text{TV}(p_0, p_1) := \frac{1}{2}\sum_{x\in S}|p_0(x) - p_1(x)|$。

2.1 具有量子公共随机币的双消息量子证明系统

一个承诺问题 $\mathcal{I} = (\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$ 满足 $\mathcal{I}_{\text{yes}} \cap \mathcal{I}_{\text{no}} = \emptyset$ 且 $\mathcal{I}_{\text{yes}} \cup \mathcal{I}_{\text{no}} \subseteq \{0,1\}^*$。为方便起见，我们将 $x \in \mathcal{I}$ 记为 $x \in \mathcal{I}_{\text{yes}} \cup \mathcal{I}_{\text{no}}$。给定承诺问题 $\mathcal{I}$，我们将$(P \rightleftharpoons V)(x)$ 记为输入 $x \in \mathcal{I}$上的量子交互式证明系统。随后，我们回顾 [KLN19第 3]节中广义 Arthur–Merlin 证明系统的定义：

定义 *2.1*（*qq-QAM*）。设 $c(n)$ 和 $s(n)$ 是输入长度 n 的函数，满足 $= |x|$ 使得$0 \leq s(n) < c(n) \leq 1$。设 $\ell(n)$ 是取正整数值的函数，满足 $\ell(n) \leq poly(n)$。若存在一个高效的量子验证者 $V(x) = (V_1(x)\ V_2(x))$ 和一个多项式 p，使得承诺问题 $\mathcal{I} = (\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$ 属于 $qq\text{-}QAM[\ell, c, s]$，其中 V_1 制备 $p(n)$ 对 *EPR* 对，并将每对的第二个量子比特发送给证明者，将第一个量子比特存储在 V 中，而 V_2 作用于消息寄存器 M 和 V，且满足：

- **完备性**。对于每个 $x \in \mathcal{I}_{是}$，都存在一个证明者 $P(x)$，使得在收到 *EPR* 对的半边后，$P(x)$ 返回一个 $\ell(n)$量子比特态，并且

$$\Pr[(P \rightleftharpoons V)(x)\ accepts] \geq c(n).$$

- **可靠性**。对于任意 $x \in \mathcal{I}_{\text{no}}$ 以及任何返回 $\ell(n)$量子比特态的证明者 $P(x)$，

$$\Pr[(P \rightleftharpoons V)(x)\ accepts] \leq s(n).$$

由于 qq-QAM具有完美完备性 [LV26，定理 1。2] 并且允许误差缩减 [KLN19，引理 3。6], 我们采用以下约定

$$\text{qq-QAM} := \cup_{\ell(n)\le \text{poly}(n)} \text{qq-QAM}[\ell, 1, 1/2].$$

我们还在方便时省略参数 ℓ 并写作

$$\text{qq-QAM}[c, s] := \cup_{\ell(n)\le \text{poly}(n)} \text{qq-QAM}[\ell, c, s].$$

2.2 Stoquastic 算法工具包

我们需要以下来自 [LW26，定义 2。11]:

定义 *2.2*（*Stoquastic* 验证电路，隐含于 [*BBT06*，定义 4]）。我们称量子电路 Q 为 *stoquastic* 验证电路，如果 Q 作用于寄存器 (W, A_0, A_+)，在最终测量之前仅使用 *Toffoli*、*CNOT* 和 *X* 门，然后在 *Hadamard* 基中测量指定的输出量子比特。这里，工作空间寄存器 W 包含一个 m_w 量子比特态，辅助寄存器 A_0 和 A_+ 分别初始化为 $|0\rangle^{\otimes m_0}$ 和 $|+\rangle^{\otimes m_+}$。电路 Q 当且仅当最终测量给出结果 $+$时接受。

SWAP 测试最初是针对纯态在 [BCWdW01] 中提出的，后来被证明可推广到混合态 [KMY09]:

引理 2.3（混合态的 SWAP 测试，改编自 [KMY09，命题 9]）。设 ρ_0 和 ρ_1是两个 m量子比特量子态，它们通常可能是 混合态。那么存在一个 $(2m+1)$量子比特的 *stoquastic* 电路，其接受概率为 $(1+\text{Tr}(\rho_0\rho_1))/2$，并且只使用 ρ_0 和 ρ_1 各一个副本，以及 m 个 *Toffoli* 门和 $2m$ 个 *CNOT* 门。

3 CIUniform 是PSPACE-困难的

我们首先定义承诺问题“接近均匀分布的像”:

定义 3.1（接近均匀分布的像，CIUniform）。设 $\mathcal{S}$ 是一个多项式规模的布尔电路，其输入为一个 m_{in} 位字符串 u 和一个 m_+ 位随机种子 r，输出为一个m_{out}位字符串 u'。等价地，对于每个 $u \in \{0,1\}^{m_{\text{in}}}$，$\mathcal{S}$ 都是一个采样器，独立抽取 $r \sim U_{m_+}$并输出 $\mathcal{S}(u, r)$。对于输入分布 p，相应的转移矩阵和输出分布定义如下:

$$M_{\mathcal{S}}(u', u) = 2^{-m_+}\left|\{r : \mathcal{S}(u, r) = u'\}\right| \quad \text{and} \quad (M_{\mathcal{S}}p)(u') = \sum_{u\in\{0,1\}^{m_{\text{in}}}} M_{\mathcal{S}}(u', u)p(u).$$

令 $n := m_{\text{in}} + m_{\text{out}}$ 为输入长度，并令 $\eta(n)$ 为一个可高效计算函数，使得 $0 \le \eta(n) \le 1$。承诺问题 CIUniform$[\eta]$ 要求判定

（是）存在一个输入分布 p，使得 $M_{\mathcal{S}}p = U_{m_{\text{out}}}$。

（否）对于所有输入分布 p，均有 $\text{TV}(M_{\mathcal{S}}p, U_{m_{\text{out}}}) \ge \eta$。

在本 节中，我们将全称量化布尔公式归约到 CIUniform，从而证明 PSPACE-困难性 :

定理 引理 3.2 (CIUniform是 PSPACE-困难)。存在某个多项式 $p(n)$ 使得 t

$$\text{CIUniform}[1/p(n)] \textit{ is } \text{PSPACE-}\textit{hard}.$$

本节余下部分将首先在第 全称量化布尔公式3.1 节中回顾 3.1所需特定格式的求和检验协议，然后根据第 3.2节中协议的单步转移构造一个采样器。

3.1 全称量化布尔公式的求和检验协议

设 $\Phi = Q_1 x_1 \cdots Q_m x_m \, \phi(x_1, \ldots\ldots, x_m)$，其中 $m \geq 1$，是一个 TQBF 实例，其中每个 $Q_i \in \{\exists, \forall\}$ 都对 $\{0,1\}$ 上的 x_i 进行量化，而 ϕ 是由 AND 、 OR 和 NOT 构成的无量词公式。当且仅当 Φ 为真时，我们称 Φ 是一个是 实例。

在 全称量化布尔公式 的 [She92], 求和检验协议中，交互式验证者将关于 Φ 是否为真的断言，转化为它可以直接检验的多项式求值。设 T 为该协议的轮次数。对 Φ进行算术化后，验证者为一个多线性多项式 P_T 构造布尔电路，该多项式定义在 $\mathbb{F}_q$ 个 m' 变量上，并配有一列运算$\mathcal{O}_0$、……、$\mathcal{O}_{T-1}$。从 P_T开始，按逆序定义中间多项式：

$$\forall t \in \{T-1, \ldots, 0\}, \quad P_t := \mathcal{O}_t P_{t+1}. \tag{3.1}$$

每个运算 $\mathcal{O}_t$ 作用于一个坐标 j_t。对于求值点 $\alpha \in \mathbb{F}_q^{m'}$，我们用 $\alpha[j_t \leftarrow X]$表示将其第 j_t 个坐标 α_{j_t} 替换为 X后得到的元组。每个 $\mathcal{O}_t$ 属于以下三种类型之一：全称量化 A_{j_t}、存在量化 E_{j_t}或降次 R_{j_t}。对于第 t 轮，定义 $L_{t,\,\alpha}$: $\mathbb{F}_q^2 \to \mathbb{F}_q$ 如下：

$$L_{t,\alpha}(x,y) = \begin{cases} xy & \mathcal{O}_t = A_{j_t}, \\ x + y - xy & \mathcal{O}_t = E_{j_t}, \\ (1-\alpha_{j_t})x + \alpha_{j_t} y & \mathcal{O}_t = R_{j_t}. \end{cases}$$

对于任意多项式 P，第 t 轮对应的算子满足

$$(\mathcal{O}_t P)(\alpha) = L_{t,\alpha}(P(\alpha[j_t \leftarrow 0]), P(\alpha[j_t \leftarrow 1])).$$

我们将在引理 3.6 中稍后证明， P_0 等于 Φ的真值，并且每个 P_t 的个体次数至多为二。现在我们回顾 全称量化布尔公式 [She92]的协议 1。

协议 1： 全称量化布尔公式的求和检验协议。

---

1. 从 $\alpha = 0^{m'}$ 开始，提出断言 $P_0(\alpha) = 1$。

对于 第 $t \leftarrow 0$ **轮至** $T-1$ **：** 令 j_t 表示 $\mathcal{O}_t$ 作用的坐标。令 $P_t(\alpha) = \nu$ 表示当前声明。

2.a 接收单变量多项式 g 的三个系数，该多项式的次数至多为二，并声称 g 等于限制 $g_\star(X) = P_{t+1}(\alpha[j_t \leftarrow X])$。**2.b 如果** $\nu \neq L_{t,\,\alpha}(g(0)\ g(1))$ **：** 拒绝。**否则：** 抽取一个新的均匀随机 $r \in \mathbb{F}_q$，并继续提出断言 $P_{t+1}(\alpha[j_t \leftarrow r]) = g(r)$。

3. 在第 T 轮次中，当且仅当所断言的值等于 $P_T(\alpha)$ 时接受。

构造多项式。 我们现在构造多项式 P_T， P_{T-1}，……， P_0 由Φ。为使 P_T 成为多线性的，我们使用选择位来编码 ϕ 的求值（命题3.3），并应用插值将每个选择表示为一个多项式（命题 3.4）。具体而言，我们将否定下推到变量，并将无量词公式 ϕ 写成一棵树。每个内部节点都是一个二元与门或或门，以两个子节点作为输入，叶节点是文字x_i 或 $\neg x_i$，或布尔常量。对于每个内部门 h，我们引入一个选择位 z_h：从根开始， $z_h = 0$ 选择左输入， $z_h = 1$ 选择右输入，直到到达一个叶节点。

命题 3.3 （通过量化选择计算布尔公式，改编自 [Hin82，第 2]节）。 固定一个布尔赋值 α 到 x_1，……，x_m。考虑这样一个谓词：由选择位选中的叶节点在 1 下的值为 α。按照父节点在前、子节点在后的顺序，为选择位 z_h 赋予量词

，对于每个或门使用 $\exists$，对于每个与门使用 $\forall$。所得的量化谓词为真，当且仅当 ϕ 在1 下计算结果为 α。

命题 3.4（零点与一点插值，改编自 [BFL91，公式（4.15）和备注 4。5]）。设 P_L 和 P_R 是 $\mathbb{F}_q$上的多项式，并设 z 是一个新变量。唯一一个关于 z 呈仿射形式、且在 P_L 处取值为 $z=0$、在 P_R 处取值为 $z=1$ 的多项式是 $(1-z)P_L + zP_R$。若 P_L 和P_R 都是多线性多项式，则所得多项式在所有变量上也都是多线性的，即使这两个多项式含有共同变量。

为了针对每个 P_t 构造 $t<T$ 并保持次数有界，我们交替进行量词消去与降次 [She92]，使得每个 P_t 的个体次数至多为二：

引理 3.5（全称量化布尔公式的降次，改编自 [She92，第 2]节）。考虑一个量化公式 $Q_1x_1\cdots Q_{m'}x_{m'}[P=1]$，其中 P是一个 $\mathbb{F}_q$上的多线性多项式，在 $\{0,1\}^{m'}$上取布尔值。从 P开始，对于 $j=m'$，……，1 应用 R_1，……，R_{j-1} 然后在 A_j 时应用 $Q_j=\forall$，或者在 E_j 时应用 $Q_j=\exists$。[3] 每个中间多项式的个体次数至多为二。最终多项式是一个常数，等于该公式的真值。

有了命题 3.3 与 3.4 以及引理 3.5 之后，我们得到如下可高效构造的全称量化布尔公式 实例 Φ:

引理 *3.6*（全称量化布尔公式的高效算术化）。给定 Φ，可以在多项式时间内构造一个有限域 $\mathbb{F}_q$、多线性多项式 P_T 在 $\mathbb{F}_q$ 上关于$m'=O(|\Phi|)$个变量的布尔电路实现，以及 T个运算 $\mathcal{O}_t\in\{A_{j_t},E_{j_t},R_{j_t}\}$（由 $t\in\{0,\ldots,T-1\}$索引）的列表，其中 $T+1=O(|\Phi|^2)$是2的幂，并且 $q=8(T+1)$。由公式*(3.1)*定义的多项式的个体次数至多为二，且 $P_0=\mathbb{I}[\Phi$ 为真]。

证明。我们首先确定 P_T 中的所有变量。为此，我们将与选择位 z_h 相关联的量词附加到 Φ 的量词前缀上，如命题 3.3 所述。ϕ 的每个内部门对应一个选择位，因此扩展前缀有 $m'=O(|\Phi|)$ 个变量。

接下来，我们在任意有限域上，从 ϕ 的叶节点到根节点构造 P_T。分别用 x_i和 $1-x_i$表示文字 x_i和 $\neg x_i$，并用各自的布尔值表示每个常数。对于每个内部门 h，若其子多项式为 P_L 和 P_R，则使用 $(1-z_h)P_L+z_hP_R$。根据命题 3.4，根节点处的多项式是多线性的，并且在布尔输入上等于所选叶节点的值，从而得到一个用于 P_T 的算术电路，其中有 O个（$|\phi|$）门。固定 Φ中变量的任意布尔赋值α，并用 z 表示选择位组成的元组。根据命题 3.3，对 P_T（α，z）应用选择位量词 $=1$，得到 ϕ（α）的真值。因此，应用原量词 $Q_1x_1\cdots Q_mx_m$后，得到 Φ的真值。

接下来，我们将扩展前缀转换为轮次操作。将引理 3.5 应用于 P_T及这个扩展前缀。消去扩展前缀中位置 j上的变量，需要进行 $j-1$次降次和一次量词运算，总计 $\sum_{j=1}^{m'}j=m'(m'+1)/2$次运算。令 $T+1$为大于 $m'(m'+1)/2$的最小2的幂。因此，$T+1\le m'(m'+1)=O(|\Phi|^2)$。重复添加 R_1，直到列表包含 T 次运算。由于 R_1固定了最终常数，这种填充不会改变 $\mathbb{I}[\Phi$ 为真], 这一事实。对于 $k=1$，……，T，令 $\mathcal{O}_{T-k}$表示填充列表中的第 k次运算。然后，公式(3.1)给出 $P_0=\mathbb{I}[\Phi$ 为真], ，并且根据引理 3.5，每个 P_t 的个体次数至多为二。

最后，我们将所得的 P_T 算术电路实现为布尔电路。令 $q=8(T+1)$。我们将 $\mathbb{F}_q$ 表示为 $\mathbb{F}_2[X]/(f)$，其中 f 是次数为 $\log q$ 的首一不可约多项式。q 有 f 个首一候选多项式，且需要检验的较低正次数首一多项式作为因子的数量少于 q。因此，试除法能在关于 q 的确定性多项式时间内找到这样的 f，进而也能在关于 $|\Phi|$的确定性多项式时间内找到。将每个域元素表示为其余式的 $\log q$ 个二进制系数

[3]我们省略 R_j 中使用的 [她92] 在应用 A_j 或 E_j之前，因为 R_j 保留了通过设置 $x_j\in\{0,1\}$得到的两个限制，而这两个限制是 A_j 和 E_j 所依赖的。

模 f。在这种表示中，加法是按位异或，乘法则是多项式乘法后再模 f 约简。因此，P_T 电路中的每个算术门都可以用 $\mathrm{poly}(\log q)$ 个布尔门实现。

□

协议 1 的分析。固定一个轮次 $t < T$ 和一个求值点 α。根据引理 3.6，协议 1 中的限制 $g_\star$ 的次数至多为二。根据 $L_{t,\,\alpha}$ 的定义以及方程（3.1），可得 $L_{t,\,\alpha}(g_\star(0)\ g_\star(1)) = (\mathcal{O}_t P_{t+1})(\alpha) = P_t(\alpha)$。如果 Φ 为真，则初始断言 $P_0(0^{m'}) = 1$ 是正确的。只要当前声明正确，回复 $g = g_\star$ 就会通过验证者的检查，并且对每个 r都给出正确的下一轮声明，因为 $g_\star(r) = P_{t+1}(\alpha[j_t \leftarrow r])$。因此，最终断言是正确的，验证者必然接受。

现在固定任意一个错误的当前声明 $P_t(\alpha) = \nu$ 以及任意一个通过验证者检查的回复 g。于是，我们得到矛盾

$$L_{t,\alpha}(g(0), g(1)) = \nu \neq P_t(\alpha) = L_{t,\alpha}(g_\star(0), g_\star(1)).$$

因此，$g - g_\star$ 是一个次数至多为二的非零多项式。验证者在收到 g后，均匀随机地抽取 $r \in \mathbb{F}_q$，因此下一轮声明正确的概率为

$$\Pr_{r \sim U_{\log q}}[g(r) = g_\star(r)] = \frac{|\{r \in \mathbb{F}_q \colon (g - g_\star)(r) = 0\}|}{q} \leq \frac{2}{q}. \tag{3.2}$$

如果 Φ为假，则初始声明为假，而要被接受，终端声明必须正确。因此，求和检验协议的一次接受执行必然包含某一轮：错误的当前声明得出了正确的下一轮声明。根据公式（3.2），即使条件是已知截至证明者回复为止的转录记录，每一轮发生此类转移的概率也至多为 $2/q$。对 T 轮应用并合界，得到接受概率至多为

$$2T/q = T/(4(T+1)) < 1/4.$$

3.2 从单步求和检验转移构造采样器

固定一个 TQBF 实例 Φ，并令 $\mathcal{S} = \mathcal{S}_\Phi$。输入 $u \coloneqq (t,\ \alpha,\ g)$ 指定一个轮次索引 $t \in \{0, \ldots, T\}$、一个求值点 $\alpha \in \mathbb{F}_q^{m'}$，以及一个次数至多为二的单变量多项式$g$的三个系数。在 $t = T$ 处，采样器忽略 g。采样器的输出 $u' \coloneqq (t',\ \alpha',\ \nu)$ 表示声明 $P_{t'}(\alpha') = \nu$。令 $r \in \mathbb{F}_q$ 为均匀随机选取的值，并定义表示当前声明 $C_{\mathrm{now}}(u)$ 和下一轮声明 $C_{\mathrm{next}}(u,\ r)$ 的元组如下

$$C_{\mathrm{now}}(u) \coloneqq \begin{cases} (t, \alpha, L_{t,\alpha}(g(0), g(1))), & t < T \\ (T, \alpha, P_T(\alpha)), & t = T \end{cases}, \tag{3.3a}$$

$$C_{\mathrm{next}}(u, r) \coloneqq \begin{cases} (t+1, \alpha[j_t \leftarrow r], g(r)), & t < T \\ (0, \alpha, 1), & t = T \end{cases}. \tag{3.3b}$$

对于 $t < T$，$C_{\mathrm{now}}(u)$ 中所断言的值，恰好是使回复 g 通过验证者在协议 1 中检查的那个值。在 $t = T$ 处，$C_{\mathrm{now}}(u)$ 使用值 $P_T(\alpha)$，而 $C_{\mathrm{next}}(u, r)$ 带着断言 $P_0(\alpha) = 1$ 返回第 0 轮。在式 (3.3) 的环绕情形 $t = T$ 中，我们保持求值点 α 不变，因为 P_0 是常数。

均匀随机地选择 $v \in \mathbb{F}_q$，并构造元组 $(t,\ \alpha,\ v)$。仅当该元组等于当前声明时，才将其替换为下一轮声明。因此

$$\mathcal{S}_\Phi(u; r, v) = \begin{cases} C_{\mathrm{next}}(u, r), & (t, \alpha, v) = C_{\mathrm{now}}(u) \\ (t, \alpha, v), & (t, \alpha, v) \neq C_{\mathrm{now}}(u) \end{cases}. \tag{3.4}$$

对于每个固定输入和每个 r，替换发生的概率为 $1/q$。因此，对于

任意输入分布和输出事件 E，

$$\Pr\big[u' \in E\big] = \Pr[(t,\alpha,v) \in E] + \frac{\Pr[C_{\text{next}}(u,r) \in E] - \Pr[C_{\text{now}}(u) \in E]}{q}. \tag{3.5}$$

写作 $\ell = \log(T+1)$，电路参数为 $m_{\text{in}} = \ell + (m'+3)\log q$，$m_+ = 2\log q$，以及$m_{\text{out}} = \ell + (m'+1)\log q$。每个指定长度的比特串都编码一个有效输入或输出。根据 3.6 引理，域运算、轮次操作 $\mathcal{O}_t$ 及其坐标 j_t，以及 P_T 的布尔电路，都可以在多项式时间内构造出来。这些足以实现 $\mathcal{S}_\Phi$。

接下来，我们分析采样器 $\mathcal{S}_\Phi$ 在协议 1 中的证明者诚实（引理3.7）或量化布尔公式 Φ 为假（引理3.8）时的行为。

引理 3.7（诚实证明者回复的输出分布）。令 p 为 $u=(t,\alpha,g)$ 的概率分布，按如下方式获得：从 $\{0,\dots,T\}\times\mathbb{F}_q^{m'}$ 中均匀随机地选取 (t,α)，并令 $g := \begin{cases} g_\star, & t = T, \\ 0 & \text{。} \end{cases}$ 那么，输出分布 $M_{\mathcal{S}}p$ 满足以下条件：

- 如果 Φ 为真，那么 $M_{\mathcal{S}}p = U_{m_{\text{输出}}}$。
- 如果 Φ 为假，那么 $\text{TV}(M_{\mathcal{S}}p, U_{m_{\text{输出}}}) = 1/(q(T+1))$。

证明。初始元组 (t,α,v) 是均匀随机选取的。当前声明 $C_{\text{now}}(u)$ 有一个随机均匀选取的对 (t,α)，以及正确的声明值 $P_t(\alpha)$。$C_{\text{next}}(u,r)$ 的轮次按循环顺序推进，其求值点要么保持不变，要么有一个坐标被独立、均匀随机选取的域元素替换。因此，$C_{\text{next}}(u,r)$ 的前两个坐标联合服从 $\{0,\dots,T\}\times\mathbb{F}_q^{m'}$ 上的均匀分布。对于 $t<T$，下一轮声明是正确的，因为 $g = g_\star$。对于 $t=T$，其第 0 轮的声明值为 1。

如果 Φ 为真，$P_0 = 1$，因此 $C_{\text{now}}(u)$ 和 $C_{\text{next}}(u,r)$ 具有相同的分布。根据方程 (3.5)，采样器的输出因此服从均匀分布。如果 Φ 为假，$P_0 = 0$，而 $C_{\text{now}}(u)$ 与 $C_{\text{next}}(u,r)$ 的分布之间唯一的差异出现在第 0 轮，该轮在两种分布中的概率均为 $1/(T+1)$。此处的求值点具有相同的均匀分布，但声明值从 0 变为 1。由于替换的概率为 $1/q$，采样器恰好将总概率的 $1/(q(T+1))$ 从值为 0 的对应输出转移到值为 1 的对应输出，因此得到所声明的距离，证毕。

□

Le引理 3.8 (与均匀分布的分离)。若 Φ 为假，则每个输入分布 p 都满足 s

$$\text{TV}(M_{\mathcal{S}}p, U_{m_{\text{out}}}) \geq \frac{1}{4q(T+1)}.$$

证明。固定任意输入分布 p。从 p 中抽取 $u=(t,\alpha,g)$，并令 (t',α',ν) 为采样器的输出。我们对以下两个事件的概率差进行界定：[4]

(i) 选择第 T 轮（$t'=T$）；当从 $\{0,\dots,T\}\times\mathbb{F}_q^{m'}\times\mathbb{F}_q$ 中均匀随机抽取 (t',α',ν) 时，该事件发生的概率为 $1/(T+1)$；

(ii) $P_{t'}(\alpha') = \nu$；对每个固定的 t' 和 α'，该事件发生的概率为 $1/q$。

事件(i) 和 (ii) 对应以下两个事件概率的绝对差。由于每个差都至多为 $\text{TV}(M_{\mathcal{S}}p, U_{m_{\text{out}}})$，因此它们的任意加权平均（权重之和为一）也至多为 $\text{TV}(M_{\mathcal{S}}p, U_{m_{\text{out}}})$。出于下文将会明了的原因，我们分别选取权重 $1/(q+1)$ 和 $q/(q+1)$，并得到以下断言：

$$\text{TV}(M_{\mathcal{S}}p, U_{m_{\text{out}}}) \geq \frac{1}{q+1}\left|\frac{1}{T+1} - \Pr\big[t'=T\big]\right| + \frac{q}{q+1}\left|\frac{1}{q} - \Pr\big[P_{t'}(\alpha')=\nu\big]\right|. \tag{3.6}$$

[4]任意的凸 组合，特别是权重为 $1/(q+1)$ 的两个绝对差 d $q/(q+1)$，g 为每个分布 p 给出了全变差距离的下界。

对于事件 (i)，即 $t' = T$，采样器要么以 $1 - 1/q$ 的概率停留在 $t = T$，要么以 $1/q$ 的概率替换 $t = T - 1$ 处的当前声明。那么，可以得出

$$\Pr[t' = T] = \left(1 - \frac{1}{q}\right) \Pr[t = T] + \frac{1}{q} \Pr[t = T - 1] \le \Pr[t = T] + \frac{1}{q}. \tag{3.7}$$

在 $U_{m_{\text{out}}}$下，该轮次为 T 的概率是 $1/(T+1)$，因此公式 (3.7) 给出

$$\left| \frac{1}{T+1} - \Pr[t' = T] \right| \ge \frac{1}{T+1} - \Pr[t = T] - \frac{1}{q}. \tag{3.8}$$

现在考虑事件 (ii)，即 $P_{t'}(\alpha') = \nu$。若 $t = T$，采样器要么保留 $v \ne P_T(\alpha)$，要么回到第 0 轮，并带有断言 $P_0(\alpha) = 1$。这两个断言都是错误的，因此不会对该事件作出贡献。我们只需考虑以下两种情况：(a) 对每个满足 $t < T$ 的输入，均匀随机选取的初始值 v 满足 $v = P_t(\alpha)$ 的概率为 $1/q$；(b) 只有当替换操作移除一个错误的当前声明 $v \ne P_t(\alpha)$，并产生一个正确的下一轮声明 $P_t(\alpha') = \nu$ 时，才会提高这一概率。若当前声明是错误的，则替换以概率 $1/q$ 发生；根据公式 (3.2)，下一轮声明在此条件下正确的概率至多为 $2/q$，因为 r 与 v相互独立。结合这两种情况，我们得到

$$\Pr[P_{t'}(\alpha') = \nu] \le \Pr[t < T,\, v = P_t(\alpha)] + \Pr[t < T,\, v \ne P_t(\alpha),\, P_{t'}(\alpha') = \nu] \tag{3.9a}$$

$$\le \underbrace{\Pr[t < T] \cdot \frac{1}{q}}_{\text{(a) initial claim correct}} + \underbrace{\Pr[t < T] \cdot \frac{1}{q} \cdot \frac{2}{q}}_{\text{(b) false claim replaced by a correct claim}} \tag{3.9b}$$

$$\le \frac{1 - \Pr[t = T]}{q} + \frac{2}{q^2}. \tag{3.9c}$$

在 $U_{m_{\text{out}}}$ 条件下，该值以 $1/q$ 的概率正确，因为每一轮和每个求值点都恰有一个正确值。因此，我们得到

$$\left| \frac{1}{q} - \Pr[P_{t'}(\alpha') = \nu] \right| \ge \frac{\Pr[t = T]}{q} - \frac{2}{q^2}. \tag{3.10}$$

将方程（3.8）和（3.10）中事件(i) 和(ii)的界代入方程（3.6）后，选定的权重 $1/(q+1)$ 和 $q/(q+1)$ 消去了未知项$\Pr[t = T]$。由于$q = 8(T+1)$ 根据引理3.6成立，我们得到

$$\mathrm{TV}(M_{\mathcal{S}^p}, U_{m_{\text{out}}}) \ge \frac{1}{q+1}\left(\frac{1}{T+1} - \frac{3}{q}\right) = \frac{5}{8(q+1)(T+1)} \ge \frac{1}{4q(T+1)} = \frac{1}{32(T+1)^2}. \qquad \square$$

定理3.2的证明。由于全称量化布尔公式是PSPACE完全的 [SM73，定理 4。3]，因此，只需给出一个从全称量化布尔公式到CIUNIFORM的 Karp归约。给定一个全称量化布尔公式实例 Φ，输出方程（ $\mathcal{S}_\Phi$ 3.4）中定义的采样器的布尔电路。根据引理3.6，域运算、轮次操作以及 P_T 所用的电路 $\mathcal{S}_\Phi$ 都能在关于$|\Phi|$的多项式时间内构造出来。

令 $n = m_{\text{in}} + m_{\text{out}}$如定义 3.1中所述。输出长度 $m_{\text{out}} = \log(T+1) + (m'+1)\log q$给出 $n \ge m' + 1$。因此，在引理 T的证明中选择 3.6 可得 $T+1 \le m'(m'+1) \le n^2$。

若 Φ 成立，则引理 3.7 给出一个输入分布 p 满足 $M_{\mathcal{S}_\Phi} p = U_{m_{\text{out}}}$。若 Φ 不成立，则引理 3.8 以及 $q = 8(T+1)$ 对每个输入分布 p给出：

$$\mathrm{TV}(M_{\mathcal{S}_\Phi} p, U_{m_{\text{out}}}) \ge \frac{1}{4q(T+1)} = \frac{1}{32(T+1)^2} \ge \frac{1}{32n^4}.$$

因此，$\Phi \mapsto \mathcal{S}_\Phi$ 分别将真公式和假公式映射为 CIUniform$[1/(32n^4)]$, 的是和否实例。

$\square$

4 CIUniform 属于 qq-StoqAM

我们首先定义 qq-QAM 的 stoquasti 版本：

定义 *4.1*（*qq-StoqAM*）。设 $c(n)$ 和 $s(n)$ 是关于输入长度 $n := |x|$ 的函数，满足 $0 \le s(n) < c(n) \le 1$。设 $\ell(n)$ 是取正整数值的函数，满足 $\ell(n) \le poly(n)$。如果存在一个高效的量子验证者 $V(x) = (V_1(x)\ V_2(x))$ 和一个多项式 p，使得 V_1 制备 $p(n)$ 个 *EPR* 对并将其第二半发送给证明者，同时将第一半存储在 V 中，且 V_2 是如定义 *2.2* 中所述、作用于消息寄存器 M 和 V 上的 *stoquastic* 验证电路，那么承诺问题 $\mathcal{I} = (\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$ 属于 *qq-StoqAM*$[\ell, c, s]$：

- **完备性**。对于每个 $x \in \mathcal{I}_{\text{是}}$，都存在一个证明者 $P(x)$，使得在收到 *EPR* 对的各半后，$P(x)$ 返回一个 $\ell(n)$量子比特态，并且

$$\Pr[(P \rightleftharpoons V)(x)\ \ accepts] \ge c(n).$$

- **可靠性**。对于任意 $x \in \mathcal{I}_{\text{否}}$以及任意证明者 $P(x)$，其返回一个 $\ell(n)$量子比特态 e，

$$\Pr[(P \rightleftharpoons V)(x)\ \ accepts] \le s(n).$$

如定义2.1中所述，我们省略回复长度 ℓ 并记作

$$\text{qq-StoqAM}[c, s] := \cup_{\ell(n) \le \text{poly}(n)} \text{qq-StoqAM}[\ell, c, s].$$

为采用约定 qq-StoqAM $:=$ qq-StoqAM$[1, 3/4]$，我们需要对 qq-StoqAM进行平行重复，证明推迟至第A节：

引理 4.2（qq-StoqAM的平行重复）。设 $c(n)$ 与 $s(n)$ 为阈值函数，使得 $1/2 \le s(n) < c(n) \le 1$，并设 $r(n) \ge 1$ 为一个取正整数值且多项式有界的可高效计算函数。则

$$\text{qq-StoqAM}[c, s] \subseteq \text{qq-StoqAM}\left[\frac{1 + c^r}{2}, \frac{1 + s^r}{2}\right].$$

注记 4.3（非负联合态可能是次优的）。考虑一个验证者，它在（B，B′）上制备一个 EPR 对，将 B′ 发送给证明者，并接收一个量子比特 A。它在 A $= 1$的控制下将 B 与一个新的 $|0\rangle$ 交换，然后在 Hadamard 基中测量 B，并在 $+$时接受。对于（B，A）上的联合态 ρ，令 $\sigma_b = (I \otimes \langle b|)\rho(I \otimes |b\rangle)$。边缘条件给出$\sigma_0 + \sigma_1 = I/2$，因此接受概率为 $\text{Tr}(|+\rangle\langle+|\sigma_0) + \frac{1}{2}\text{Tr}(\sigma_1) = \frac{1}{2} + \frac{1}{2}\text{Tr}(X\sigma_0) \le \frac{3}{4}$。此处 $\text{Tr}(X\sigma_0) = \langle+|\sigma_0|+\rangle - \langle-|\sigma_0|-\rangle \le 1/2$。对 B′ 施加 Hadamard 变换并将其返回，得到$\sigma_0 = |+\rangle\langle+|/2$ 并达到 $3/4$。若 ρ 在计算基下逐项非负，则 σ_0 与 σ_1 的非对角元非负且和为零。于是 $\text{Tr}(X\sigma_0) = 0$，从而接受概率为 $1/2$。

对于 CIUniform$[\eta]$，我们按照定义 $n = m_{\text{in}} + m_{\text{out}}$，以 3.1 中的方式，以 $\eta(n) > 0$ 为指标，分别标记承诺问题和验证者的可靠性。我们取该值，使承诺问题的两种情况互不相交。

定理 4.4. CIUniform$[\eta] \in$ qq-StoqAM$[1, 1 - \eta^2/2]$。

定理 1.1 的证明。由定理 3.2 和定理 4.4，从全称量化布尔公式得到的归约给出了一个完美完备的 qq-StoqAM 验证器，其可靠性至多为 $1 - \eta(n)^2/2$，其中 $\eta(n) = 1/(32n^4)$。在引理 4.2 中取 $r = 2/\eta(n)^2$ 个副本，可保持完美完备性，并使可靠性至多为 $(1 + (1 - 1/r)^r)/2 < 3/4$。采样器宽度 n 关于公式长度呈多项式有界，因此得到 PSPACE $\subseteq$qq-StoqAM$_1$。

对于可靠性为 1 StoqAM$_1$ 验证者，可靠性为 s 的 QAM 验证者可以并行运行多项式数量的副本，并在所有副本均接受时接受。根据公式（A.1），k 个副本的可靠性至多为 $s^k \le 1/2$（对于 $k \ge 1/(1 - s)$），且保持完美完备性。因此，利用 QIP $=$PSPACE [JJUW11], ，我们得到

$$\text{PSPACE} \subseteq \text{qq-StoqAM}_1 \subseteq \text{qq-QAM} \subseteq \text{QIP}(2) \subseteq \text{QIP} = \text{PSPACE}. \qquad \square$$

4.1 面向CIUNIFORM的qq-StoqAM 证明系统

我们将 [KLN19 引理 4 中的像测试1] 特化到采样器 $\mathcal{S}$，并通过 SWAP 测试实现验证者的最终测量。令 $U_{\mathcal{S}}$ 为该采样器的经典可逆实现，它作用于输入、种子和输出寄存器 (A，R，B) 如下：

$$U_{\mathcal{S}}|u,r,w\rangle = |u,r,w \oplus \mathcal{S}(u,r)\rangle.$$

验证者将 $\mathcal{S}(u,r)$ 计算到新的零态量子比特中，通过按位异或将结果加到 B，并在这些新量子比特上逆转该计算。由此使用多项式多个 Toffoli 门、CNOT 门和 X 门得到 $U_{\mathcal{S}} = U_{\mathcal{S}}^{\dagger}$。

协议 2： 一个用于 CIUniform$[\eta]$ 的双消息 stoquastic 验证者

---

1. 在寄存器 (B,B′) 上制备 m_{out} 个 EPR 对，并将 B″ 发送给证明者。**2.** 接收 m_{in} 量子比特的输入寄存器 A 和 m_+ 量子比特的种子寄存器 R。对寄存器 (A,R, B) 施加 $U_{\mathcal{S}}^{\dagger}$。**3.** 在 (R, B) 与初始化为$|+\rangle^{\otimes m_+}|0\rangle^{\otimes m_{\text{out}}}$的新参考寄存器 (R′,B′) 之间执行 SWAP 测试，并使用初始化为 $|+\rangle$ 的控制量子比特 O。当且仅当在 Hadamard 基中测量 O 得到结果 $+$ 时接受。

验证者通过对 $|+\rangle|0\rangle$施加 CNOT 来制备每个 EPR 对2.3。结合引理 $U_{\mathcal{S}}$ 的可逆实现可得到一个符合定义 4.1的多项式时间一致 stoquastic 验证者。验证者可以将两条消息填充至固定的多项式长度，并忽略多余的寄存器。

4.2 协议 2 的分析

定理 *4.4* 的证明。 设 ρ 是在验证者于协议 (A,R,B) 上施加$U_{\mathcal{S}}^{\dagger}$ 之前的联合态，协议编号为 2。

接受概率。 记 $|\omega\rangle = |+\rangle^{\otimes m_+}|0\rangle^{\otimes m_{\text{out}}}$ 为参考态，记 $\Pi = U_{\mathcal{S}}(I_{\mathsf{A}} \otimes |\omega\rangle\langle\omega|)U_{\mathcal{S}}^{\dagger}$为验证者所测试子空间上的投影算符。施加 $U_{\mathcal{S}}^{\dagger}$后，(R, B) 上的状态为 $\sigma = \mathrm{Tr}_{\mathsf{A}}(U_{\mathcal{S}}^{\dagger}\rho U_{\mathcal{S}})$。根据引理 2.3中的 SWAP 测试，接受概率为

$$p_{\text{acc}} = \frac{1}{2}\big(1 + \langle\omega|\sigma|\omega\rangle\big) = \frac{1}{2}\big(1 + \mathrm{Tr}[(I_{\mathsf{A}} \otimes |\omega\rangle\langle\omega|)U_{\mathcal{S}}^{\dagger}\rho U_{\mathcal{S}}]\big) = \frac{1}{2}\big(1 + \mathrm{Tr}(\Pi\rho)\big). \tag{4.1}$$

完美完备性。 假设对于某个输入分布 p，$M_{\mathcal{S}}p = U_{m_{\text{out}}}$。收到 B″ 后，证明者将每个 $|u'\rangle$ 映射为 (A,R) 上的以下状态，并返回这些寄存器：

$$|k_{u'}\rangle = 2^{(m_{\text{out}}-m_+)/2} \sum_{(u,r):\,\mathcal{S}(u,r)=u'} \sqrt{p(u)}\,|u\rangle_{\mathsf{A}}|r\rangle_{\mathsf{R}}.$$

对于每个 u'，我们有 $\||k_{u'}\rangle\|^2 = 2^{m_{\text{out}}}(M_{\mathcal{S}}p)(u') = 1$。不同的输出对应互不相交的原像集合，因此向量 $|k_{u'}\rangle$ 两两正交，该映射是一个等距变换。对得到的联合态应用 $U_{\mathcal{S}}^{\dagger}$ 后，得到

$$\begin{aligned} U_{\mathcal{S}}^{\dagger}\left(2^{-m_{\text{out}}/2}\sum_{u'}|k_{u'}\rangle_{\mathsf{AR}}|u'\rangle_{\mathsf{B}}\right) &= 2^{-m_+/2}\sum_{u,r}\sqrt{p(u)}\,|u\rangle_{\mathsf{A}}|r\rangle_{\mathsf{R}}|0\rangle_{\mathsf{B}}^{\otimes m_{\text{out}}} \\ &= \left(\sum_{u}\sqrt{p(u)}|u\rangle_{\mathsf{A}}\right)|\omega\rangle_{\mathsf{RB}}. \end{aligned}$$

SWAP 测试比较 $|\omega\rangle$ 的两个副本，并以确定性接受。

可靠性 *s.* 假设对于每个输入分布 p，都有 TV($M_{\mathcal{S}}p$，$U_{m_{\text{out}}}$) $\geq \eta$。固定任意一种证明者策略 y

并使用私有寄存器 Q 将 ρ 纯化为 $|\psi\rangle$。证明者只对 B″ 和私有寄存器进行操作，因此验证者的寄存器 B 仍处于最大混合态。在$|\psi\rangle$上对 B 进行计算基测量，得到 $U_{m_{\text{out}}}$。

为界定 $|\psi\rangle$ 在 $\Pi\otimes I_{\mathsf{Q}}$的像上的投影，取该像中的任意单位向量 $|\xi\rangle$。根据 Π的定义，将 $U_{\mathcal{S}}^{\dagger}$ 作用于 $|\xi\rangle$，会在(R,B)上得到 $|\omega\rangle$，并在(A,Q)上得到一个单位向量 $\sum_u |u\rangle_{\mathsf{A}}|\chi_u\rangle_{\mathsf{Q}}$。因此 $p(u) = \||\chi_u\rangle\|^2$ 定义了一个输入分布。再次应用 $U_{\mathcal{S}}$，会对每一对(u,r)将 $\mathcal{S}(u,r)$写入B。由于不同的对在(A,R)中彼此正交，对 $|\xi\rangle$ 测量B将以如下概率得到 u'

$$2^{-m_+} \sum_{(u,r):\,\mathcal{S}(u,r)=u'} p(u) = (M_{\mathcal{S}}p)(u').$$

测量不能增大迹距离。比较这两个分布并使用纯态的迹距离公式，可得

$$\eta \le \mathrm{TV}(M_{\mathcal{S}}p, U_{m_{\text{out}}}) \le \frac{1}{2}\||\psi\rangle\langle\psi| - |\xi\rangle\langle\xi|\|_1 = \sqrt{1-|\langle\psi|\xi\rangle|^2}.$$

因此 $|\langle\psi|\xi\rangle|^2 \le 1-\eta^2$ 对每一个这样的 $|\xi\rangle$。与子空间中单位向量的最大平方重叠等于到该子空间的正交投影的范数平方。代入式（4.1）可得

$$p_{\text{acc}} = \frac{1}{2}\big(1 + \|(\Pi\otimes I_{\mathsf{Q}})|\psi\rangle\|^2\big) \le 1 - \frac{1}{2}\eta^2. \qquad \square$$

致谢

作者获得了瑞士教育、研究与创新国务秘书处（SERI）的部分资助。本研究还通过 ChatGPT 学术研究人员计划，获得了使用 OpenAI 模型的权限资助。

AI 使用情况披露

在准备本手稿的各个阶段，均以交互方式使用了大语言模型工具：从最初的探索性研究阶段，到最终的阐述和撰写阶段。作者对最终手稿进行了大幅修订，并对所有数学断言、证明、参考文献和结论承担全部责任。

参考文献

[AGL25] Dorit Aharonov、Alex B. Grilo 和 Yupan Liu。StoqMA 与 MA：错误约简的力量。《Quantum》。9:1853。2025年。doi:10.22331/Q-2025-09-11-1853。arXiv:2010.02835。出现次数：2[Bab85] László Babai。以随机性换取群论。载于《第17届ACM年度计算理论研讨会论文集》。第421–429页。1985年。doi: 10.1145/22145.22192。出现次数：1[BBT06] Sergey Bravyi、Arvid J. Bessen 和 Barbara M. Terhal。Merlin–Arthur博弈与随机矩阵复杂性。2006年。预印本。arXiv:quant-ph/0611021。出现次数：2, 6[BCWdW01] Harry Buhrman、Richard Cleve、John Watrous 和 Ronald de Wolf。量子指纹识别。《物理评论快报》。87(16):167902。2001年。doi:10.1103/ PhysRevLett.87.167902。arXiv:quant-ph/0102001。出现次数：6

[BF91] László Babai 和 兰斯·福特诺。算术化：结构复杂性理论中的一种新方法。《计算复杂性》。1(1):41–66。1991年。doi:10.1007/ BF01200057。初步版本发表于 FOCS 1990。出现次数：3[BFL91] László Babai、兰斯·福特诺 和 卡斯滕·伦德。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。doi:10.1007/BF01200056。出现次数：8[BHZ87] 拉维·B·博帕纳、约翰·霍斯塔德 和 斯塔西斯·扎科斯。co-NP 是否具有简短的交互式证明？《信息处理快报》。25(2):127–132。1987年。doi: 10.1016/0020-0190(87)90232-8。出现次数：1[GMR89] 沙菲·戈德瓦瑟、西尔维奥·米卡利 和 查尔斯·拉科夫。交互式证明系统的知识复杂性。《SIAM计算杂志》。18(1):186–208。1989年。doi:10.1137/0218012。初步版本发表于 STOC 1985。出现次数：1[GS86] 沙菲·戈德瓦瑟 和 迈克尔·西普瑟。交互式证明系统中的私有随机币与公开随机币。载于《第18届ACM年度计算理论研讨会论文集》。第59–68页。1986年。doi:10.1145/12130.12137。出现次数：1[Hin82] 雅各·欣蒂卡。博弈论语义学：洞见与展望。《圣母大学形式逻辑杂志》。23(2):219–241。1982年。doi:10.1305/ndjfl/1093883627。出现次数：7[JJUW11] 拉胡尔·贾恩、季正丰、萨尔瓦吉亚·乌帕迪亚耶 和 John Watrous。QIP = PSPACE。《ACM会刊》。58(6):30:1–30:27。2011年。doi:10.1145/2049697.2049704。初步版本发表于 STOC 2010。arXiv:0907.4737。出现次数：1, 2, 12[KKMV09] 朱莉娅·肯佩、小林弘忠、松本圭司 和 Thomas Vidick。在量子多证明者交互式证明中使用纠缠。《计算复杂性》。18(2):273–307。2009年。doi:10.1007/s00037-009-0275-3。初步版本发表于 CCC 2008。arXiv:0711.3715。出现次数：2[KLN19] 小林弘忠、弗朗索瓦·勒加尔 和 西村治道。广义量子阿瑟–梅林博弈。《SIAM计算杂志》。48(3):865–902。2019年。doi:10.1137/17M1160173。初步版本发表于 CCC 2015。arXiv:1312.4673。出现次数：2, 3, 5, 6, 13[KMY09] 小林弘忠、松本圭司 和 山上知之。量子梅林–阿瑟证明系统：多个梅林能为阿瑟提供更多帮助吗？《芝加哥理论计算机科学杂志》。2009:1–19。2009年。doi:10.4086/ cjtcs.2009.003。初步版本发表于 ISAAC 2003。arXiv:quant-ph/0306051。出现次数：6[KW00] 阿列克谢·基塔耶夫 和 John Watrous。量子交互式证明系统的并行化、放大与指数时间模拟。载于《第32届ACM年度计算理论研讨会论文集》。第608–617页。ACM。2000年。doi:10.1145/335305.335387。出现次数：1, 2[LFKN92] 卡斯滕·伦德、兰斯·福特诺、霍华德·卡洛夫 和 诺姆·尼桑。交互式证明系统的代数方法。《ACM会刊》。39(4):859–868。1992年。doi:10.1145/146585.146605。初步版本发表于 FOCS 1990。出现次数：1[Liu21] Yupan Liu。StoqMA 与分布检验相遇。载于《第16届量子计算、通信与密码学理论会议论文集》。

LIPIcs 第197卷。第 4:1–4:22 页。Schloss Dagstuhl – Leibniz 信息学中心。2021年。doi:10.4230/LIPIcs.TQC.2021.4。arXiv:2011.05733。出现位置：2[LV26] Yupan Liu 和 Thomas Vidick。为单消息和双消息量子证明系统实现完美完备性。2026年。arXiv:2609.15926。出现位置：2, 6[LW26] Yupan Liu 和 Pei Wu。无破坏性干涉时非纠缠性的威力。2026年。即将发表于 SODA 2027。arXiv:2604.27886。出现位置：6, 17[MW05] Chris Marriott 和 John Watrous。量子 Arthur–Merlin 博弈。《计算复杂性》。14(2):122–152。2005年。doi:10.1007/s00037-005-0194-x。初步版本发表于 CCC 2004。arXiv:cs/0506068。出现位置：1, 2[MW12] Abel Molina 和 John Watrous。运用相关量子策略对冲赌注。《皇家学会会刊 A 辑》。468(2145):2614–2629。2012年。doi:10.1098/rspa.2011.0621。arXiv:1104.1140。出现位置：17[NC10] Michael A. Nielsen 和 Isaac L. Chuang。《量子计算与量子信息》。剑桥大学出版社。十周年纪念版。2010年。doi:10.1017/CBO9780511976667。出现位置：5[Sha92] Adi Shamir。IP = PSPACE。《ACM会刊》。39(4):869–877。1992年。doi:10.1145/146585.146609。初步版本发表于 FOCS 1990。出现位置：1, 3, 4[She92] Alexander Shen。IP =PSPACE：简化证明。《ACM会刊》。39(4):878–880。1992年。doi:10.1145/146585.146613。出现位置：3, 4, 7, 8[SM73] Larry J. Stockmeyer 和 Albert R. Meyer。需要指数时间的字问题（初步报告）。载于《第五届 ACM 计算理论年会论文集》。第 1–9 页。ACM。1973年。doi:10.1145/800125.804029。出现位置：3, 11[VW16] Thomas Vidick 和 John Watrous。量子证明。《理论计算机科学前沿与趋势》。11(1-2):1–215。2016年。doi:10.1561/0400000068。arXiv:1610.01664。出现位置：2, 5[Wat03] John Watrous。PSPACE 具有常数轮次的量子交互证明系统。《理论计算机科学》。292(3):575–588。2003年。doi:10.1016/S0304-3975(01)00375-9。初步版本发表于 FOCS 1999。arXiv:cs/9901015。出现位置：1, 2, 3

两消息stoquastic证明系统的平行重复

引理 4.2 (qq-StoqAM 的平行重复StoqAM)。 设 $c(n)$ 和 $s(n)$ 是阈值函数，满足 $1/2 \leq s(n) < c(n) \leq 1$；并设 $r(n) \geq 1$ 是一个可高效计算函数，其取值为正整数且有多项式上界。那么

$$\mathrm{qq\text{-}StoqAM}[c, s] \subseteq \mathrm{qq\text{-}StoqAM}\left[\frac{1+c^r}{2}, \frac{1+s^r}{2}\right].$$

证明。 固定一个 qq-StoqAM$[c, s]$ 证明系统，以及一个长度为 n 的输入 x 。记 $\omega(x)$ 为对 x 的最大接受概率，并令 $r = r(n)$。验证者制备 r 份相互独立的 EPR挑战副本，在一条消息中发送所有第二半，然后对联合应答和存储的 EPR一半运行每份副本的可逆门。接着，它执行一次

在 r 未测量的输出量子比特与一个新寄存器之间进行 SWAP 测试，寄存器处于 $|+\rangle^{\otimes r}$中，如 [LW26的定理 3.14 和图 2]所示。根据引理 2.3，这最后一步只需使用 Toffoli 门、CNOT 门以及一次 Hadamard 基测量。由于 r 是多项式有界且可有效计算的，因此重复验证器是多项式时间一致的。

对于任意联合证明者策略 P，令 σ_P 为 r 个输出量子比特在 SWAP 测试之前的状态。若验证者在 Hadamard 基中测量每个输出，则获得 $+$于每个副本的概率为 $a(P) = \mathrm{Tr}[\sigma_P(|+\rangle\langle+|)^{\otimes r}]$。因此，SWAP 测试以概率 $(1 + a(P))/2$ 接受，依据引理 2.3。

这些单独的测量是相互独立的验证器测试，而 P 可在全部r 个副本上联合作用。应用关于指定结果最大概率的乘积规则 [MW12，第 4(a) 节] ，针对每个副本中的结果 $+$ ，可得

$$\max_P a(P) = \omega(x)^r. \tag{A.1}$$

因此，重复验证器的最大接受概率为 $(1+\omega(x)^r)/2$。在是实例上， $\omega(x) \geq c(n)$ 给出的完备性至少为 $(1 + c(n)^r)/2$。在否实例上， $\omega(x) \leq s(n)$ 给出的可靠性至多为 $(1 + s(n)^r)/2$。

□