arXiv:2302.02918v2 [quant-ph] 6 Jun 2024

有限与渐近情形下时间序列过程的优化

Mirjam Weilenmann, [1,2] Costantino Budroni, [3] 以及 Miguel Navascu´es[2]

[1] *Département de Physique Appliquée, Université de Genève, Genève, Switzerland*

[2] *Institute for Quantum Optics and Quantum Information–IQOQI Vienna,Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria*[3] *Department of Physics "E. Fermi" University of Pisa, Largo B. Pontecorvo 3, 56127 Pisa, Italy*

量子信息论中的许多问题都可以表述为：在受到不可预测的外部影响的动力系统中，对序贯结果进行优化。这类问题包括通过自适应测量进行多体纠缠检测、计算制备游戏在连续目标态集合上的最大平均得分，以及限定（量子）有限状态自动机的行为。在这项工作中，我们提出了这类优化问题的易处理松弛形式。为展示其性能，我们用它们来：（a）计算有限状态自动机输出给定比特序列的概率；（b）开发一种新的多体纠缠检测协议；（c）让计算机 *invent* 采用自适应协议进行魔态检测。我们还将进一步证明，无限多个时间步极限下序贯问题的最大得分通常是不可计算的。尽管如此，我们仍提供了用于界定这一量的通用启发式方法，并证明它们能在相关场景中给出有用的估计。

I. 引言

在量子物理中，我们通常关注如何操控量子系统：与它们相互作用，使其达到（或保持在）特定的量子态，或者对其进行测量，以观测或验证它们的某些性质。寻找以时间有序操作执行任务的新方法和更优方法，是当前量子信息科学研究的核心。量子计算依赖于将门操作依次施加于量子系统；借助量子系统的通信协议，则依赖于对这些系统执行操作并按特定顺序交换信息。在一些不那么显而易见的情形中，操作序列也至关重要，例如，为了读出超导量子比特，会施加特定的脉冲序列 [1]。

传统上，要找到完成特定任务的新方法（或操作序列），一直依赖科学家的 ingenuity，靠他们提出新的协议。近年来，这类问题也通过机器学习技术来解决：训练神经网络生成正确的操作序列。然而，目前仍缺乏一种能够优化序贯策略的通用方法，甚至也缺乏一种判据，用以判断某个序贯协议对于特定任务是否最优。

解决这些问题的部分难点在于，当操作按序执行时，协议可以是自适应的，即后续操作可能取决于先前操作的结果。自适应性可以带来巨大优势；例如，它能最大限度地减少纠缠认证 [2]和量子态探测 [3]中的统计误差。然而，它也增加了针对特定任务必须考虑的协议种类，从而提高了对这些协议进行优化的复杂性。事实上，尽管在单次执行或独立重复过程的背景下，优化技术已相当成熟（例如，在非局域性 [4, 5] 或纠缠见证 [6]的应用中），但为序贯协议开发这类技术仍是一项挑战。

在这项工作中，我们对这一问题取得了进展。具体而言，我们提出了一种通用技术，用于分析和优化一类我们称为序贯模型的时间序列过程。这类协议包含 N 轮，在每一轮中都会发生一次相互作用，并改变所关注系统的状态，而这一变化可能取决于未知或非受控变量。协议每一轮都会产生奖励，用以量化朝特定目标取得的进展；奖励也是我们优化过程的对象。

我们的首个结果是一种技术，它能够通过一套难度逐步递增的完整凸优化问题层级，对序贯模型在 N 轮中能够产生的最大总奖励给出上界。为展示该层级的性能，我们将其用于界定一种用于多体纠缠检测的自适应协议的第一类错误上界 [2, 7]。对于较大的系统规模（数量级为 $N \approx 100$），该技术给出的界看起来相当紧。

同样的技术也使我们能够深入研究由有限状态自动机 [8, 9]生成的时间关联。这些模型出现在量子基础和量子信息理论中的多个问题里，例如量子情境性的经典模拟 [10–13], 、经典随机过程的量子模拟 [14–16], 、纯度认证 [17], 、维度见证 [18–20], 、计时装置设计中的量子优势 [21–24], , 以及量子计算的经典模拟 [25]；更多详情请参阅近期一篇关于时间关联的综述 [26]。具体而言，我们关注最优时钟问题，即在能够使用具有 d 个内部状态的经典自动机的情况下，能构造出多好的时钟？利用我们的工具，我们解决了 d取较小值时的这一问题，给出了该自动机输出"单滴答序列"000...01的最大概率上界，这一序列曾在 [23, 24]中研究。这些上界与已知的最佳下界

在数值精度范围内相符。

除了有限长度的操作序列外，我们也常常关心让协议或过程无限期地运行，即我们希望刻画其在 $N \to \infty$ 时的渐近行为。例如，对于长时间持续演化的系统，或对于我们旨在探测大型系统的情形，这一点十分重要；在这些情况下，这个极限是很好的近似。

据我们所知，对于轮次数趋于无穷时的时间有序过程，目前人们知之甚少（假设检验中的渐近速率以及取特定极限时的结果 [27, 28]除外）。本文表明，这背后存在一个根本原因：某些序贯模型无法通过任何算法近似其渐近行为。这一点可由与有限状态自动机相关的不可判定性结果推出；具体而言，依据的是参考文献 [29, 30] 中的一种构造。尽管如此，我们仍提出了一种启发式方法，用于计算渐近行为的严格界。我们还发现，在所考虑的应用中，这些界接近预期的渐近行为，也接近我们能够计算出的下界，从而证实了我们方法的实用性。更具体地说，我们运用渐近方法，为上述多体纠缠检测协议在粒子数趋于无穷时的第一类错误给出上界。所得上界与实际数值的差距至多为 4×10^{-4}。我们的渐近方法还给出了在时间步数趋于无穷时，二状态自动机输出单滴答序列的概率上界 $O(10^{-2})$。

最后，在某些情况下，我们需要做的不是分析，而是寻找性能良好的序贯模型。也就是说，给定一组我们可以控制的参数——即策略——这些参数可能影响系统的演化以及奖励，我们要解决的问题是：确定哪种策略能在 N 轮次后使总奖励最大化。我们提出通过投影梯度方法解决这一问题，并展示如何将上界梯度的计算转化为一个易于处理的凸优化问题。利用这一方法，我们让计算机自行发现了一个双状态、六轮的制备游戏，用于检测单量子比特魔态。

本文结构如下。在第 II 节中，我们介绍量子信息论中的三个问题，并将在全文中用它们来阐释我们的方法。在第 III 节中，我们引入序贯模型这一抽象概念，并说明如何对其进行优化，随后在第 IV 节中应用该优化方法。在第 V 节中，我们证明，一般而言，序贯模型的渐近行为无法近似。我们还介绍了一种用于处理渐近问题的启发式方法，并在第 VI 节中应用该方法。在第 VII 节中，我们提出策略优化问题，并说明如何针对策略参数，计算第 III 节中推导的上界的梯度。我们使用梯度方法在第 VIII 节中求解一个策略优化问题。最后，我们在第 IX 节中给出结论。

II. 时间有序操作中的问题

涉及量子系统的各类问题中，有许多具有序贯性质。下面我们介绍三种由时间有序操作构成的情形；这些情形都给量子信息领域带来了具有挑战性的开放问题。

A. 时间关联

有限状态自动机（FSA）是一种数学结构，用于对具有有界记忆的自主计算设备建模。更正式地说，[8, 9], a d-状态自动机是在任意时刻由内部状态 $\sigma \in \Sigma$ 描述的设备，其中 $|\Sigma| = d$。在固定间隔（即轮次或时间步），自动机会更新其内部状态并生成结果 $b \in B$，这取决于其先前的内部状态 σ 以及输入端口的状态 $y \in Y$。这种同时改变状态并产生输出的转移由自动机的转移矩阵 $P(\sigma', b|\sigma, y)$支配，该矩阵表示：给定输入状态和先前状态分别为 y 和 σ时，自动机转移至内部状态 σ' 并输出 b的概率。总体而言，给定输入$\mathbf{y} = (y_1, \ldots, y_n)$时，输出$\mathbf{b} = (b_1, \ldots, b_n)$的概率可计算为

$$p(\mathbf{b}|\mathbf{y}) = \sum_{\sigma_0,\sigma_1,\ldots,\sigma_n} p(\sigma_0) P(\sigma_1, b_1|\sigma_0, y_1) \cdot P(\sigma_2, b_2|\sigma_1, y_2) \ldots P(\sigma_n, b_n|\sigma_{n-1}, y_n) \tag{1}$$

诸如式（1）所示的表达式，即由经典有限状态自动机生成的表达式，会出现在若干与时间量子相关性的经典模拟有关的问题中，例如，量子情境性的经典模拟 [10–12],经典随机过程的量子模拟 [14–16], 量子计算的经典模拟 [25],以及计时装置设计中的量子优势 [21–24]。

我们关注这样的情形：某个具有 d个状态的自动机经过 n 个时间步后的性能，由另一个自动机评估；更一般地，也可以由一个具有有界记忆的时变过程评估。我们希望对所有具有d 个状态的自动机的上述性能给出界。

这类问题包括，例如，计算一个拥有 d 个状态的自动机生成所谓“单滴答序列”00 . . . 01 的最大概率（这个名称源于将其解释为时钟的一个滴答所对应的时钟信号“1”）。这一优化问题是探讨能够生成时间信号的最优经典模型和量子模型的核心，由此也产生了量子优势，推动物理时钟的设计。不幸的是，目前还没有通用的优化方法可以给出经典模型性能的上界，并

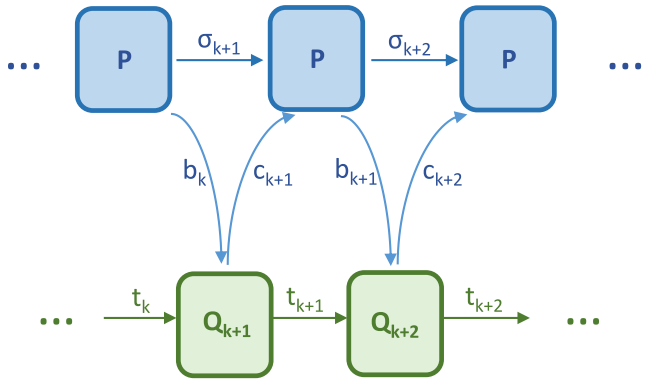


图1. **与过程 Q（绿色）耦合的自动机（蓝色）**。一般而言，过程可能因轮次而异。

从而证明量子优势。最优量子时钟问题已从理论角度（量子信息和量子热力学）进行了广泛研究 [21–24, 31–36], 也从实验角度进行了研究 [37]。

因此，考虑一个有限状态自动机 A，其状态记为 $\sigma \in \Sigma$，输入为 $y \in Y$，输出为 $b \in B$，其中 $|\Sigma| = d$。我们假设该自动机由（未知的）转移矩阵 $P(\sigma_{k+1}, b_k|\sigma_k, y_k)$ 描述。设 Q 为一个已知的时变过程，其内部状态记为 t，输入（输出）记为 z（c）。该过程在时间步 $k = 2, ..., N$的（已知）转移矩阵为 $Q_k(t_k, c_k|t_{k-1}, z_{k-1})$。过程的每个状态 t_k 都对应一个奖励 $\alpha_k(t_k)$。在时间步 1，状态和输出 t_1, c_1 由分布$Q_1(t_1, c_1)$生成。现在，我们按以下方式将 Q 与 A耦合（示意见图1）：在 Q 生成 t_1, c_1后，我们将 c_1 输入自动机 A，即令$y_1 = c_1$。随后，自动机经由 P 转移至状态 σ_1，并输出 b_1。接着，将该输出作为输入送入过程 Q（令 $z_1 = b_1$），过程再通过 Q_2生成 t_2, c_2，依此类推。在时间步 N，我们考虑所有奖励之和，

$$\sum_{k=1}^{N} \alpha_k(t_k). \tag{2}$$

我们的目标是在所有 d状态自动机 A中最大化总奖励的期望值。注意，利用凸性，最佳策略是将自动机初始化为特定状态 $\sigma_0 = \bar{\sigma}_0$，而非其上的某种分布 [38]。因此，固定初始状态后，最优自动机完全由使期望奖励最大的转移矩阵 P 刻画。

这个问题可以用一种数学方式重新表述，这种表述在后文会很有用。具体而言，耦合系统 A 和 Q 可以视为一个单一的动力系统，其在时间步 k的内部状态 s_k 对应于三元组的概率分布 (t_k, c_k, σ_k)，即 $s_k := p_k(t_k, c_k, \sigma_k)$。该系统从一个时间步演化到下一个时间步时遵循运动方程

$$\begin{aligned} p_{k+1}(t_{k+1}, c_{k+1}, \sigma_{k+1}) &= \sum_{c_k, t_k, \sigma_k, b_k} p_k(t_k, c_k, \sigma_k) P(\sigma_{k+1}, b_k|\sigma_k, c_k) \\ &\quad \cdot Q_{k+1}(t_{k+1}, c_{k+1}|t_k, b_k) \\ &=: f_k(s_k, \lambda). \end{aligned} \tag{3}$$

注意，此处的演化由状态 s_k 和未知演化参数 λ 的多项式 f_k给出：$=(P(\sigma', c|\sigma, z): z \in Z, c \in C, \sigma \in \Sigma)$。在这种问题表述中，时间步 k 的奖励 r_k 为

$$r_k(s_k) := \sum_{t_k, c_k, \sigma_k} p_k(t_k, c_k, \sigma_k)\alpha(t_k). \tag{4}$$

注意，此处奖励不依赖于 λ（除了通过 p_k之外）：不过，可以通过使用不同的奖励函数 $r_k(s_k, \lambda)$ 引入这种依赖。在这一表述中，我们的任务是在所有可能的演化参数 λ 中最大化总奖励。

B. 多体系统的纠缠认证

给定一个 N 部分量子系统，我们经常需要判断其状态是否为纠缠态。原则上，可以通过找到合适的纠缠见证，并估计其在当前状态下的取值来解决这一问题。然而，除了从理论上找到此类见证属于 NP难 [39], 之外，对其取值的估计还可能需要对N部分状态的多个子系统进行联合测量，而这在实验上可能无法实现。通常，若以基于局域测量统计的估计取代此类联合测量，则需要进行 $\mathrm{Exp}[N]$ 次态制备，因此，对于规模适中的N，相应协议将变得不可行（例如，协议要求进行完整的量子态层析时）。

避免这些问题的一种方法，即进行单系统测量并减少态制备次数，是执行自适应协议 [2]。该方案按如下方式进行。我们依次测量构成 N粒子系综的粒子，使后续测量取决于先前的测量以及先前的结果。完成最后一次测量后，我们猜测底层状态是否为纠缠态。

为了选择如何测量每个系统并作出最终猜测，我们使用一个动力系统 Q。该过程具有内部状态 $t_k \in T$，其在时间 $k = 1, ..., N-1$ 的转移矩阵形式为$Q_k(t_{k+1}, y_{k+1}|t_k, b_k)$，其中 $b_k \in B$ 表示时间 k 的测量结果，y_{k+1} 则标记将在第 $(k+1)$ 个粒子上进行的测量。

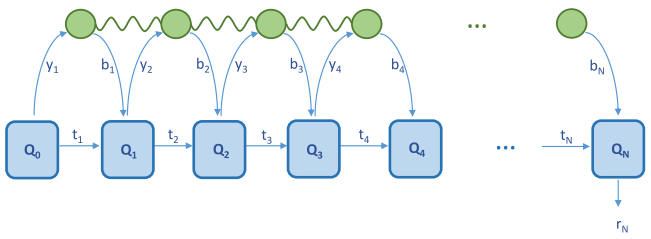


图 2. **纠缠检测的序贯模型**。 一个 N方状态（绿色）的粒子依次逐个进行测量。第 k 次测量 y_k 取决于有限状态自动机的内部状态，而测量结果 b_k 则会根据 Q_k影响自动机的状态转移。

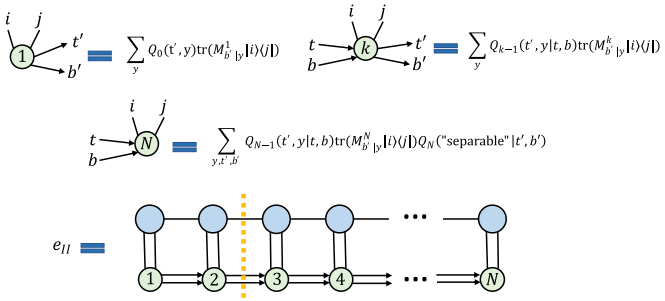


图 3. **第二类错误的高效计算**。 蓝色圆圈表示构成 MPO 目标态的张量，其中两条竖直边分别表示每个粒子的 bra 和 ket 指标，两条维度为 D 的水平边——即键维数——用于表征目标态的关联。按照图中所示定义绿色张量后，它们与蓝色张量的收缩结果等于相应纠缠检测协议的第二类错误。正如橙色虚线所示，这一收缩可通过乘以维度为 $|T||B|D$ 的矩阵来计算。

对于每个 $y \in Y_k$，都存在一个正算子值测度 (POVM) $\{M^k_{b|y}\}_b$。最终猜测通过函数 $Q_N(t_{N+1}|t_N, b_N)$ 生成，其中 $t_{N+1} \in${‘纠缠的’，‘可分态’}。过程的初始状态以及 y_1 第一个粒子的测量设置由分布 $Q_0(t_1, y_1$给出。如图2所示。

如果目标态 ρ ——我们希望通过实验检测其纠缠的目标态——可以高效地分解为矩阵乘积算子（MPO） [40]，那么就能高效地计算该过程输出结果“可分态”的概率，见图3。这一概率通常称为第二类错误，或称为假阴性。

接下来要计算由Q编码的纠缠检测协议的第一类错误，即假阳性：这对应于输入为完全可分离量子态时，过程输出“纠缠”的最大概率。在计算这一最大值时，根据凸性，我们可以假设玩家制备了一个纯积量子态。也就是说，在每个时间步 k，我们测量某个纯量子态 ρ_k。尽管经过了这一简化，计算该方案的第一类错误仍需要对一个规模为$O(N)$的输入的多线性函数进行最大化。随着 N 增长，这个问题会变得更加困难。

与计算所有 d 状态自动机的最大性能这一问题类似，在可分态集合上最大化第一类错误，也可以表述为对确定性动力系统的序贯输出进行优化。在这种情况下，动力系统在时间步 k 的内部状态 s_k 对应于 t_k，y_k 的分布 P_k 。系统的运动方程为

$$P_{k+1}(t_{k+1}, y_{k+1}) = \sum_{t_k, y_k, b_k} P_k(t_k, y_k)\mathrm{tr}(M^k_{b_k|y_k}\rho_k) \cdot Q_k(t_{k+1}, y_{k+1}|t_k, b_k), \quad (5)$$

其中，量子态 ρ_k 可以解释为影响系统演化的非受控外部变量 h 。在时间步 N，系统输出确定性结果

$$r_N(s_N) = \sum_{t_N, y_N, b_N} P_N(t_N, y_N)\mathrm{tr}(M^N_{b_N|y_N}\rho_N) \cdot Q_N(t_{N+1}|t_N, b_N)\delta_{t_{N+1},\text{‘entangled’}}. \quad (6)$$

C. 量子制备博弈中的独立同分布（IID）制备策略

制备博弈这一概念旨在刻画一般（可能具有自适应性）的协议结构，其中量子系统会被依次探测 [2]。更准确地说，量子制备博弈是一项包含 N轮、由玩家和裁判参与的任务。在每一轮中，玩家制备一个量子态，随后由裁判对其进行探测。在第 k轮中，裁判执行测量之前，他当前对玩家所用源的了解由变量 $t_k \in T_k$表示，其中 $|T_k| < \infty$，该变量称为博弈配置。此变量与以往的测量历史和测量结果密切相关：每一轮中，它都会引导裁判决定下一步执行哪种测量，并根据测量结果发生变化。博弈配置的这双重作用可以编码在裁判该轮使用的 POVM 中。也就是说，假设测量前的博弈配置为$t \in T_k$，新的博弈配置为 $t' \in T_{k+1}$ 的概率为 $\mathrm{tr}(\rho_k M^k_{t'|t})$，其中 ρ_k 是玩家第 k次态制备；而 $\{M^k_{t'|t} : t' \in T_{k+1}\}$，则是博弈配置为 t时裁判实施的 POVM。在制备博弈结束时，裁判会根据适用于 $t \in T_{N+1}$的某种计分系统 $g(t)$生成得分 $g(t_{N+1})$，其中 t_{N+1} 表示最终博弈配置。

在某些情况下——例如，在玩家试图（诚实地）制备特定纠缠态的纠缠检测协议中——考虑遵循独立同分布（IID）策略的玩家是合理的，这意味着玩家在每一轮都制备相同的状态 ρ 。

因此，考虑这样一个问题：对于固定的计分系统，计算采用如下形式的制备策略时 $\rho^{\otimes N}$，且满足 $\rho \in C$ 的情况下，能够达到的最高游戏得分，其中 C 是某个状态集合。参考文献 [2], 展示了当可行制备集合 C 的基数有限时，如何计算独立同分布策略下制备博弈的最高得分。本文考虑 C 为连续集合的情形。

这个问题可以通过一个动力系统来建模，其内部状态 s_k 在时间 k 对应于$P_k(t_k)$，即第 k轮开始时的博弈配置分布。该系统的运动方程为

$$P_{k+1}(t') = \sum_{t\in T_k} P_k(t)\mathrm{tr}(\rho M^k_{t'|t}), \tag{7}$$

其中，未知演化参数 $\lambda := \rho \in C$对应于玩家的制备。该动力系统在时间 N输出奖励，即

$$r_N(s_N,\lambda) = \sum_{t'\in T_{N+1}} g(t') \sum_{t\in T_k} P_N(t)\mathrm{tr}(\rho M^N_{t'|t}). \tag{8}$$

因此，我们的目标是对演化参数 λ的所有可行取值进行优化，使系统的奖励最大化，也就是对所有 $\rho \in C$进行优化。

顺带一提，在某些情况下，有必要计算对抗玩家能够达到的最大平均游戏得分。对抗玩家可以获知当前的博弈配置，因此能够据此调整每一轮的制备。有趣的是，这个问题比优化独立同分布策略更简单；事实上，文献 [2] 给出了一般解。尽管如此，我们将在下文展示，在自适应策略下计算制备游戏的最大游戏得分，也可以视为本文所讨论的序贯问题中的一个特定类别。

III. 序贯模型及其优化

上述描述的三个问题——尽管从物理角度来看差异颇大——在结构上却非常相似。事实上，它们都是我们将在下文以更抽象方式引入的那类问题的实例。考虑这样一种情形：在时间步 k ，动力系统的状态由变量 $s_k \in S_k$ 完整描述。在时间步 k 和 $k+1$ 之间，系统从 s_k 转变为另一状态 s_{k+1} ，具体取决于 s_k 、若干个非受控变量 $h_k \in H_k$

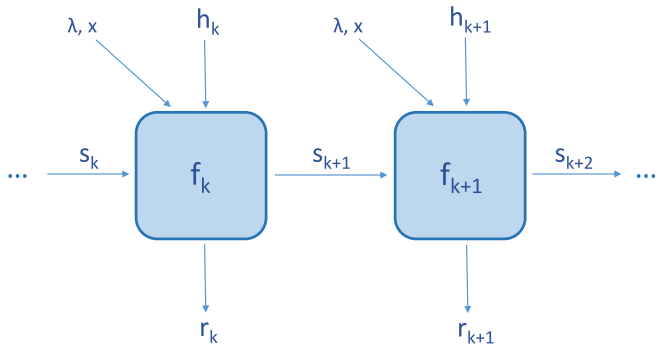


图 4. **序贯模型的示意图**。请注意，运动方程本身可能涵盖多种相互作用，也可能由多个步骤构成（例如，对量子系统进行测量后，更新有限状态自动机）。

以及若干个未知的演化参数 $\lambda \in \Lambda$。描述这一转变的运动方程为

$$s_{k+1} = f_k(s_k, h_k, \lambda), \tag{9}$$

其中， S_k、 H_k $\forall k$ 和 Λ 是参数值的集合。

我们的目标是根据具体问题给定的某种评价指标，对这类系统进行优化。我们通过假设系统在每个时间步都会产生奖励（或惩罚）来对此建模$r_k(s_k,\ h_k,\ \lambda)$ 。请注意，对于某些 k，该奖励可以是零函数，因此，只关心最终结果的问题也作为一种特殊情况包含在内。下文将此类系统称为序贯模型（见图 4）。

我们的目标是估计所有可能的 λ、 h_1、……、 h_N取值下的最大总奖励 $\nu^\star$。也就是说，我们希望求解以下问题

$$\begin{aligned} \nu^\star \ := \ \max_{\lambda,h} \quad & \sum_{k=1}^{N} r_k(s_k,h_k,\lambda) \\ \text{such that} \quad & \lambda\in\Lambda,\ h\in \times_{k=1}^{N} H_k \\ & s_{k+1} = f_k(s_k,h_k,\lambda)\ \ \forall k. \end{aligned} \tag{10}$$

我们通常假设初始状态 s_1 已知；否则，可以将其纳入 λ 的定义中，具体做法是增加一个时间步来生成初始状态。若没有 λ，上述问题在数学上等价于一个确定性马尔可夫决策问题，只需将 h 视为一个动作 [41]。

A. 序贯模型优化问题的重新表述

为计算最优值 $\nu^\star$，我们考虑一种基于动态规划方法 [41]的方法。

该方法通过定义 值函数 $V_k(s_k,\ \lambda)$ 来实现。这些函数表示在假设演化参数取值为 λ 的情况下，从状态 s_k 出发，在所有可能的 $h_k,\ \ldots\ldots h_N$ 取值中，从时间步 k 到 N 之间可实现的最大奖励。通过用多项式近似这些函数，并调用关于半代数集上正多项式的已知刻画，我们得以推导出关于 $\nu^\star$ 的单调收敛的、易于处理的上界序列。我们注意到，类似的思想已在连续时间最优控制问题的背景下得到探索；这类问题可以表述为一个无限维线性规划，而针对该规划，基于已有多项式优化技术；参见文献 [42]及其中的参考文献。

用奖励函数表示，值函数为

$$\begin{aligned} V_N(s_N,\lambda) &= \max_{h_N\in H_N} r_N(s_N,h_N,\lambda),\\ V_k(s_k,\lambda) &= \max_{h_k\in H_k} r_k(s_k,h_k,\lambda)+V_{k+1}(f_k(s_k,h,\lambda),\lambda) \end{aligned} \tag{11}$$

并且在最后一步，我们将 $\nu^\star$ 还原为

$$\nu^\star = \max_{\lambda\in\Lambda} V_1(s_1,\lambda). \tag{12}$$

因此，求解 $\nu^\star$ 的问题可化简为

$$\begin{aligned} \min_{V_1,\ldots,V_N,\nu}\quad & \nu \\ \text{such that}\quad & V_N(s_N,\lambda)\geq r_N(s_N,h,\lambda)\quad \forall h\in H_N,\ s_N\in S_N,\ \lambda\in\Lambda \\ & V_k(s_k,\lambda)\geq r_k(s_k,h,\lambda)+V_{k+1}(f_k(s_k,h,\lambda),\lambda)\quad \forall h\in H_k,\ s_k\in S_k,\ \lambda\in\Lambda \\ & \nu\geq V_1(s_1,\lambda)\quad \forall\lambda\in\Lambda. \end{aligned} \tag{13}$$

事实上，一方面，方程（13）中给出的问题的任一可行点，都为 $\nu^\star$ 提供了一个上界。另一方面，根据方程（ V_1，……，V_N）、$\nu^\star$（11）、（12）定义的这些量也是（13）的一个可行点。因此，方程（13）中给出的问题的解为 $\nu^\star$。

遗憾的是，除非其定义域是有限的，否则没有通用方法可以对任意函数进行优化。可行的做法是在假设 $\{V_k(s_k,\lambda)\}_k$ 属于一个由有限个参数描述的函数类 $\mathcal{F}$ 的前提下，求解方程（13）中给出的问题。一般而言，最优函数 $V_k(s_k,\lambda)$ 可能不属于 $\mathcal{F}$，因此 $\bar{\nu}$ 此类优化所得的结果是该问题实际解的一个上界 $\nu^\star$。多项式函数类 $\mathcal{F}$ 非常实用，因为它在复合运算下封闭，并且相对于一致范数，在连续函数集合中稠密。本文采用的正是这一函数类。

因此，在本文余下部分，我们假设对于所有 $k\in\{1,2,\ldots,N\}$，$f_k(s_k,\ h_k,\ \lambda)$ $r_k(s_k,\ h_k,\ \lambda)$，它们都是定义在 $s_k,\ h_k,\ \lambda$ 上的多项式，并且集合 $S,\ H_k$ 和 Λ 是某个度量空间中的有界集，可由有限个多项式不等式描述。请注意，在这些假设下，值函数在 s_k 和 λ上连续。

于是，将 $\nu^n\geq\nu^\star$ 式（13）在约束 $\{V_k(s_k,\ \lambda)\}_k$ 为给定次数的多项式 n时所得的结果称为。由于定义在有界集上的任意连续函数都可以用多项式任意精确地逼近，因此可得 $\lim_{n\to\infty}\nu^n=\nu^\star$。

此外，求解（13）还会带来额外的困难，需要施加如下形式的正性约束

$$p(x)\geq 0,\forall x\in X, \tag{14}$$

其中 $p(x)$ 是向量变量 $x\in\mathbb{R}^m$上的多项式，而 X 是由有限个多项式不等式定义的 $\mathbb{R}^m$ 有界区域（即基本半代数集）。值得庆幸的是，存在若干完备的（无限）充分判据层级，可用于证明多项式在半代数集 [43–46]上的正性。在代数几何中，这类判据层级称为正性定理。

两种重要的正值定理¨是 Schm¨udgen 的[45] 和 Putinar 的 [46]。这两种层级有一个独特之处：对于固定的指标 k，所有满足第 k个准则的多项式集合都可以通过半定规划表示。将 Schm¨udgen 和 Putinar 的正值定理应用于多项式优化，由此得到两个完备的半定规划松弛层级。基于 Putinar 正定性定理的半定规划松弛称为 Lasserre-Parrilo 层级 [47, 48]。两种层级的介绍见附录 A。虽然基于 Schm¨udgen 正值定理的层级比 Lasserre-Parrilo 层级计算开销更大，但收敛更快。以下数值计算中，我们采用两者的混合方法。

在对次数为 n 的多项式值函数进行优化时，使用给定正值定理的 k^{th} （充分）正性检验，可得到关于 ν^n 的上界ν_k^n，且 $\lim_{k\to\infty}\nu_k^n=\nu^n$。对我们而言，关键结论是：对于所有 $k,\ n$ 均有 $\nu_k^n\geq\nu^\star$，并且 $\lim_{n\to\infty}\lim_{k\to\infty}\nu_k^n=\nu^\star$。

我们通过指出，多项式用于近似值函数并没有什么

特别之处。事实上，还存在其他完备的函数族可用于求解公式（13）中给出的问题。其中，一个很有前景的类别是符号多项式，即指数函数的线性组合；关于这类函数，文献中也存在一些积极的结果¨ [49, 50]。在这种情况下，相应的正多项式集合无法用半定规划表示，但仍然是易于处理的凸集。因此，它们适用于优化。

B. 量子制备博弈作为序贯模型

序贯模型刻画了各种类型的时间序列过程的结构，其中包括第II节介绍的三种过程。在这里，我们指出，序贯模型实际上相当通用：量子制备博弈中对对抗策略的优化，也可以建模为序贯问题。事实上，通过值函数求解这些问题，可以重新推导出该主题的既有结果 [2]。

设 $\mathcal{S}$ 为一组量子态，并考虑这样一种制备博弈：玩家在每一轮 k都可以根据当前博弈配置 t_k制备任意量子态 $\rho(t_k) \in \mathcal{S}$ 。该制备博弈可以解释为一个序贯模型，其中包含 $\Lambda = \emptyset$、$s_k = p_k(t_k)$、 $h_k = (\rho^k(t) : t \in T_k)$以及运动方程

$$p_{k+1}(t') = \sum_{t \in T_k} p_k(t) \mathrm{tr}(\rho^k(t) M^k_{t'|t}). \tag{15}$$

我们考虑最大化平均博弈得分（或奖励）的问题

$$r_{N+1}(p_{N+1}) = \sum_{t \in T_{N+1}} p_{N+1}(t) g(t), \tag{16}$$

其中， g 是博弈 [2]的得分函数。

原则上，我们可以像公式（13）那样表述这个问题。注意， $V_{N+1} = r_{N+1}$ 关于 p_{N+1}是线性的。这促使我们考虑用线性值函 $V_k(p_k)$ 作为该问题的试探解。也就是说，我们旨在假设

$$V_k(p_k) = \sum_{t \in T_k} \mu_k(t) p_k(t), \tag{17}$$

对于某个向量 $(\mu_k(t) : t \in T_k)$ 。条件$V_k(p_k) \geq V_{k+1}(p_{k+1})$ 于是转化为

$$\begin{aligned} \sum_{t \in T_k} \mu_k(t) p_k(t) &\geq \max_{\{\rho^k(t)\}_t} \sum_{t' \in T_{k+1}} \mu_{k+1}(t') \sum_{t \in T_k} p_k(t) \mathrm{tr}(\rho^k(t) M^k_{t'|t}) \\ &= \sum_{t \in T_k} p_k(t) \max_{\rho^k(t)} \mathrm{tr}\left(\rho^k(t) \sum_{t' \in T_{k+1}} V_{k+1}(t') M^k_{t'|t} \right). \end{aligned} \tag{18}$$

令 $p_k(t) = \delta_{t,\, j}$，对于 $j \in T_k$，我们得到递推关系：

$$\begin{aligned} &\mu_{N+1}(t) = g(t), \\ &\mu_k(t) = \max_{\rho^k(t)} \mathrm{tr}\left(\rho^k(t) \sum_{t' \in T_{k+1}} \mu_{k+1}(t') M^k_{t'|t} \right), \end{aligned} \tag{19}$$

这使我们能够计算 $V_1(t_0)$ 。原则上，这个量是公式（13）中问题实际解的一个上界，因为我们额外施加了值函数为线性的约束。然而，这个上界是紧的；只需计算公式（19）中问题的最大化解 $\bar{\rho}^k(t)$ 所给出的制备策略下，制备游戏的平均得分即可看出这一点。事实上，以上所有推导不过是为了得到参考文献 [2] 中给出的递推关系，以计算制备游戏的最高得分。

IV. 时间序列过程优化的应用

原则上，本研究中考察的所有序贯问题都可以通过直接应用 Lasserre-Parrilo 层级来求解（或至少进行近似） [47, 48]。然而，此类问题中的多项式次数会随步骤数线性增长 N，因此，当迭代次数超过少数几次时，相应的半定规划便难以求解。另一方面，我们将序贯优化问题重新表述为式（13）的形式，从而能够避开这一问题，并针对更大的 N值优化序贯模型。

A. 有限状态自动机上的优化：概率界

本节研究经典有限状态自动机生成给定输出序列的最大概率。针对输入输出序列 [12], 以及仅含输入的序列 [23, 24]，这一问题已得到广泛研究。特别地，我们考察所谓的单滴答序列 *00.....01*；该序列在最优时钟问题的背景下由文献 [23] 引入。对于总长度为 L的序列，我们采用紧凑记法 $0^{L-1}1$。在这里，我们运用第III节提出的一般方法来处理这一问题。注意，这是第IIA节所介绍的问题类型的一个实例。

考虑一个具有 d 个状态、无输入且具有二进制输出的自动机，即 $Y = \emptyset$, $B = \{0, 1\}$。我们希望计算该自动机输出单滴答序列 $0^{L-1}1$ 的最大概率，记为 $P^{\mathrm{d}}_{\max}(L)$。为此，我们构造一个简单的过程 Q ，使其与自动机耦合后产生的期望奖励等于 $P(0^{L-1}1)$。 Q 具有两个内部状态，即，

$t_k \in \{0,1\}$ 且没有输出（$C = \emptyset$）。其初始状态为$t_1 = 1$，其转移矩阵如下：

$$Q_k(t_{k+1}|t_k, b_k) = \delta_{t_{k+1}, t_k(1-b_k)}, \text{ for } k = 1, ..., L-1,$$
$$Q_L(t_{L+1}|t_L, b_L) = \delta_{t_{L+1}, t_L b_L}. \tag{20}$$

对于时间步 $k = 1, ..., L-1$，只要自动机输出 0，过程 Q 就会持续处于状态 1；如果自动机输出任何一个 1，过程的状态就会变为 0，并一直保持到博弈结束。在时间步 L，过程 Q 会收到输出b_L。如果 $b_L = 0$或 $t_L = 0$，则 $t_{L+1} = 0$；否则，$t_{L+1} = 1$。因此，自动机产生序列 $0^{L-1}1$ 的概率对应于 $t_{L+1} = 1$的概率。这对应于一个奖励函数

$$\alpha_k(t_k) = 0, \text{ for } k = 1, ..., L-1,$$
$$\alpha_{L+1}(t_{L+1}) = \delta_{t_{L+1}, 1}. \tag{21}$$

利用第III节中提出的技术，我们将此问题映射为一个多项式优化问题。鉴于奖励的选择（以及过程 Q），我们可以看到，式（3）中运动方程所包含的项，只有与正确的 b_k对应的项会对最终奖励产生贡献。这使模型得以进一步简化。

首先，将序贯模型的内部状态重新定义为由以下向量

$$s_k = (p_k(t_k = 1, \sigma_{k+1}))_\sigma, \tag{22}$$

参数 d s_k^σ 描述，并满足约束 $s_k^\sigma \geq 0$ 对于$\sigma = 0, ..., d-1$，以及$1 - \sum_\sigma s_k^\sigma \geq 0$。接下来，我们将未知演化参数 λ 重新定义为维度为d^2的参数，形式如下： $\lambda := (P(\sigma', b = 0|\sigma) : \sigma, \sigma' = 0, 1)$，并满足约束

$$P(\sigma', b = 0|\sigma) \geq 0, \text{ for all } \sigma, \sigma' = 0, \ldots, d-1$$
$$1 - \sum_{\sigma'} P(\sigma', b = 0|\sigma) \geq 0, \text{ for } \sigma = 0, \ldots, d-1. \tag{23}$$

对于 $k = 1, ..., L-1$，该序贯模型的运动方程为

$$p_{k+1}(t_k = 1, \sigma_{k+1}) = \sum_{\sigma_k} p_k(t_{k-1} = 1, \sigma_k) P(\sigma_{k+1}, 0|\sigma_k), \tag{24}$$

而奖励函数为

$$r_k = 0, \text{ for } k = 1, ..., L-1;$$
$$r_L(s_L, \lambda) = \sum_\sigma p_L(t_L = 1, \sigma) \left(1 - \sum_{\sigma'} P(\sigma', b = 1|\sigma)\right). \tag{25}$$

现在，我们应用半定规划松弛 `（Lasserre 方法）[47]，以求得以下情形下序贯问题解的上界： $d = 2$ 和 $d = 3$。在

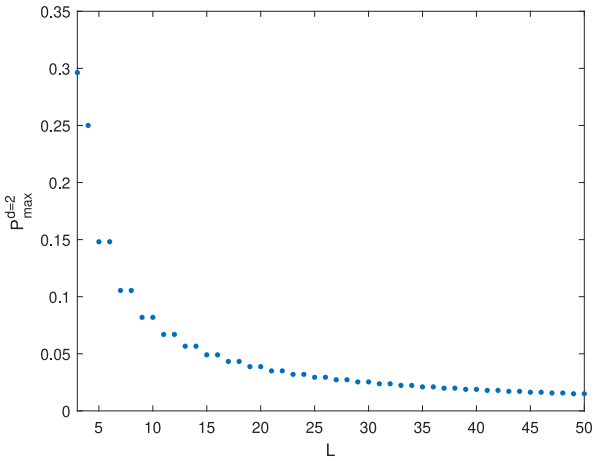


图 5. **双状态自动机上的优化**。上界（红色）呈现出一种规律：从 $L = 5$ 开始，连续成对的数值相同。此外，我们的界与参考文献 [23] 中给出的显式自动机在数值精度范围内一致，因此得到了紧界，并证明了参考文献 [23, 24]中所发现模型的最优性。优化使用 MOSEK [51] 和 CVXPY [52]完成。我们对求解器给出的每个解都进行了检验，以确认线性约束和正性约束在数值精度范围内均得到满足。

后一种情形此前尚无非平凡的解析上界 [23, 24]。关于精确实现的详情，请参阅附录B1。图5 和6 展示了用此方法计算出的上界。我们发现，在所有情形下，所得上界都与参考文献 [23, 24]，中提出的自动机的输出概率在数值精度范围内一致。这意味着计算出的上界均为紧界。除 $L = d + 1$这一情形外，这些序列的最优模型都对应于所谓的循环模型 [23]。该模型由状态之间的确定性转移构成，且只有在最后一个状态下发射 1 的概率才非零。因此，界仅取决于 $\lfloor L/d \rfloor$，对应于图5 和6中观察到的 2 周期和 3 周期平台。

为了将我们的算法与此前已知的方法（即 Lasserre-Parrilo 层级）的性能进行比较，[47, 48]，我们也采用后者对问题进行了数值优化。我们的方法能够达到 $L = 50$（当 $d = 2$ 时），并且达到 $L = 10$ （当 $d = 3$ 时），而 Lasserre-Parrilo 层级无法超越 $L = 7$ （当 $d = 2$ 时）的情况。性能的大幅提升并不意外，因为 Lasserre-Parrilo 层级中的多项式次数随步数 L线性增长，而我们的方法中则保持不变。更多详情见附录 A 和B。

除了 $P_{\max}^{\mathrm{d}}$ 的数值之外，我们还可以从优化过程中提取值函数

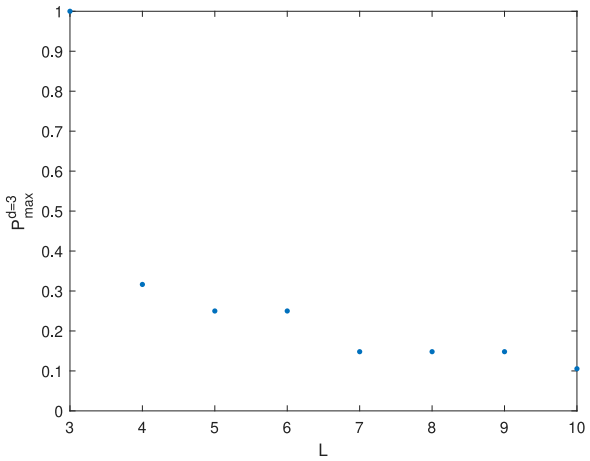


图 6. **对三状态自动机进行优化**。 我们的方法还允许对三状态自动机进行优化。同样，我们在数值精度范围内恢复了参考文献 [23, 24], 中显式模型计算出的界，证明了我们的界是紧的，且先前找到的模型是最优的。优化使用 SCS [53] 和 CVXPY [52] 完成。我们对求解器给出的每个解都进行了检验，以确认线性约束和正性约束在数值精度范围内均得到满足。

并利用这些值函数以解析方式证明我们的界。在推导出这些值函数后，我们还可以进一步利用它们为当前问题找到最优自动机。

在提取值函数时，首先要注意，从数值解中可以直接提取多项式 V_k 的系数，因为它们是该问题的优化变量。然而，值函数可能并不唯一，从数值结果中提取系数合适（有理数或整数）的多项式则更具挑战性。附录 B2中详细阐述了进一步简化这些值函数的方法。

这里采用的序贯模型优化方法，使我们能够用值函数表示上界，而无需显式处理模型的实际变量——在本例中为 $\{p_k\}_k$ 和 P ——[54]。先验地，因此，解并未告诉我们实现这些界的最优动力系统可能取哪些值，即使这些界是紧的。不过，我们可以通过先从优化问题中提取值函数，再进行第二次优化来解决这一问题；这一次固定值函数，并针对序贯模型的变量进行优化，在此处即$\{p_k\}_k$ 和 P。更确切地说，如果我们找到了一个最优上 $\nu^\star$界，那么所有值函数不等式都必须取等号，并且存在一个能够达到该界的最优动力系统。现在，如果我们能找到一个使所有不等式都取等号的系统，那么它就自动是最优的。因此，要找到这样的模型，我们可以

考虑该优化问题

$$\begin{aligned}&\max_{s_k,\lambda,h_k} V_1(s_1,\lambda)\\ \text{such that } &V_N(s_N,\lambda)=r_N(s_N,h_N,\lambda)\\ &V_k(s_k,\lambda)=r_k(s_k,h_k,\lambda)+V_{k+1}(f_k(s_k,h_k,\lambda),\lambda)\\ &h_k\in H_k\ \forall k,\ s_k\in S_k\ \forall k,\ \lambda\in\Lambda\end{aligned}\tag{26}$$

这又是一个可以通过半定规划松弛求解的多项式优化问题。在以下示例中，我们使用 YALMIP 的 SOLVEMOMENT 功能 [55] ，在第 4 级调用求解器 MOSEK [51] 来求解该问题。[56] 我们发现，在这些情况下，问题是可行的，并提取出最优自动机。

- 在上述 $d=2$ 和 $L=3$ 的情况下，我们得到

$$\begin{aligned}V_1(s_1,\lambda)=&(P(0,0|0)q_1(0)+P(0,0|1)q_1(1))P(b=1|0)\\&+(P(1,0|0)q_1(0)+P(1,0|1)q_1(1))P(b=1|1),\end{aligned}\tag{27}$$

其中 $q_k(\sigma):=p_k(1,\sigma)$。请注意，在这种情况下，这正是人们为解决当前问题而直接构造的自然优化问题；然而，对于更高的 L ，值函数的分解有所不同。现在，利用最终奖励为

$$r_2=P(b=1|0)q_2(0)+P(b=1|1)q_2(1),\tag{28}$$

以及可转化为以下形式的状态转移规则

$$q_2(0)=P(0,0|0)q_1(0)+P(0,0|1)q_1(1),\tag{29}$$
$$q_2(1)=P(1,0|0)q_1(0)+P(1,0|1)q_1(1),\tag{30}$$

我们立即看到， $V_1(s_1,\lambda)-r_2(s_2(s_1)\ \lambda)=0$。此外，我们可以推导出关于 $V_1(s_1(s_0)\ \lambda)$的上界。根据状态转移规则，我们有 $q_1(0)=P(0,0|0)$ 和 $q_1(1)=P(1,0|0)$（因为初始状态为 $q_0(1)=1, q_0(2)=0$），因此

$$\begin{aligned}V_1(s_1(s_0),\lambda)=&(P(1,0|1)^2+P(2,0|1)P(1,0|2))P(b=1|1)\\&+(P(1,0|1)P(2,0|1)+P(2,0|1)P(2,0|2))P(b=1|2).\end{aligned}\tag{31}$$

这为解给出了一个多项式上界；通过对 P, q_k上的值函数进行数值最大化可知，该上界确实不超过 0.29630。优化还表明，这一最大值由一个自动机取得，其满足 $P(0,0|0)=P(1,0|1)=\frac{1}{3}$, $P(1,0|0)=\frac{2}{3}$, $P(0,0|1)=0$, 从而确认该值是最优紧上界。[57]这也与 [23]中提出的最优自动机一致。

- 对于 $d=2$ 和 $L=4$ ，我们得到两个值函数[58]

$$W_2(s_2,\lambda)=V_1(s_2,\lambda)\tag{32}$$
$$\begin{aligned}W_1(s_1,\lambda)=&0.25(1+q_1(0)(q_1(0)-P(0,0|0))\\&+q_1(1)(q_1(1)-P(1,0|0)))\end{aligned}\tag{33}$$

现在，我们可以看到，0.25 是W_1（s_1，λ）的上界，因为状态更新规则以及本例中的 q_0（0）$=1$ 和q_0（1）$=0$ 意味着 q_1（0）$=P$（0，0|0）以及q_1（1）$=P$（1，0|0）。作为最后一个关系，我们 [59] 必须检查

$$W_1(s_1,\lambda) - W_2(s_2(s_1),\lambda) \geq 0. \tag{34}$$

数值优化证实了这一多项式不等式。在对s_1 和 s_2 施加约束的条件下，要求 $W_1(s_1,\ \lambda) = W_2(s_2(s_1)\ \lambda)$，同时最大化 $W_1(s_1,\ \lambda)$，可得到自动机 $P(1,\ 0|0) = 1$，$P(0,\ 0|0) = 0$和 $P(0,\ 0|1) = \frac{1}{2}$,$P(1,\ 0|1) = 0$的最优解。[60] 这再次与 [23] 中针对 $L = 4$的自动机一致。

请注意，通常有许多不同的值函数都可以解决该问题。不过，从优化问题中提取项数较少且系数为整数或分数的值函数，需要进行一些调整（见附录 B2）。随着变量数量增加，这一过程会变得更加繁琐。因此，这里不提供更大 L 对应的值函数。我们指出，尽管如此，始终可以从优化中提取出有效的值函数。

B. 多体系统中的纠缠检测：自动机引导的 GHZ 游戏

为展示我们的半定规划松弛在求解多体系统纠缠认证问题上的性能，我们重点关注 N 量子比特的 Greenberger-Horne-Zeilinger（GHZ）态

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}\right) \tag{35}$$

最大为 $N = 35$。这项研究恰逢其时，因为目前已经能够制备多达 20 个量子比特的 GHZ 态 [61–63]。设计这类协议的主要目标，是获得一种所需状态制备次数尽可能少的流程，从而可靠地认证纠缠。本节提出这样一种单次协议，并证明遵循此流程确实比基于影子层析的一类协议所需的重复次数更少 n 。 [64]

我们方法的主要特点是采用假设检验框架。这意味着，我们还能够证明协议在最坏情形可分态下的性能界（对应于第一类错误）；而这类界难以计算，在估计保真度时通常也不会给出。我们的方法还有一个优点：仅依赖单量子比特量子操作（例如，参考文献 [61] 中的 18 量子比特示例不仅在制备阶段，也在解纠缠阶段使用了双量子比特门，而我们的方法无需如此），并且还适用于自适应协议（见第 IVC节），（相比之下，确定某个算符的期望值例如奇偶性，或通过固定测量 [62, 63], 来评估贝尔不等式 [65]）。后一特点通常使我们能够减少协议的重复次数。

值得指出的是，在任何 旨在检测纯 GHZ 态的单次纠缠检测协议中，第一类和第二类错误 e_I，e_{II}将满足以下关系

$$e_I + e_{II} \geq \frac{1}{2}. \tag{36}$$

为了解释这一点，记 M 为与宣布系统“纠缠”相关联的 N量子比特有效 POVM 元素（视协议而定，相应的 POVM 可以是全局的、局域操作与经典通信的，或单向局域操作与经典通信的），并令 σ 为可分状态

$$\sigma = \frac{1}{2}(|0\rangle\langle 0|^{\otimes N} + |1\rangle\langle 1|^{\otimes N}). \tag{37}$$

那么我们有

$$\begin{aligned} 1 - e_{II} - e_I(\sigma) &= \mathrm{tr}\{M(|GHZ\rangle\langle GHZ| - \sigma)\} \\ &\leq \frac{1}{2}\,\||GHZ\rangle\langle GHZ| - \sigma\|_1 \\ &= \frac{1}{2}, \end{aligned} \tag{38}$$

其中 $e_I(\sigma)$ 是宣布 σ “纠缠”的概率。由于 $e_I \geq e_I(\sigma)$，我们得到式（36）。

我们接下来提出的协议在36式的关系在极限 $N \to \infty$下达到饱和。从这个意义上说，尽管我们的协议仅依赖单量子比特测量，但它在渐近意义下是最优的。

接下来，我们来描述用于纠缠检测的协议。该协议受 GHZ 游戏启发，相关研究此前见参考文献 [66, 67], ，其中记忆的作用由经典有限状态自动机承担。因此，我们称该协议为自动机引导的 *GHZ* 游戏。具体来说，设想一种用于多体纠缠验证的协议：对于前 $N-1$ 个粒子中的每一个，以概率$_1$ $_2$执行以下两种测量之一：

$$\begin{aligned} M_1 &= \{M_{1|1} = |+\rangle\langle +|,\ M_{2|1} = |-\rangle\langle -|\}\ , \\ M_2 &= \{M_{1|2} = |+i\rangle\langle +i|,\ M_{2|2} = |-i\rangle\langle -i|\}, \end{aligned}$$

其中 $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ 和 $|\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$。此过程用于更新四态自动机的状态，该自动机初始化于状态 $t_1 = 1$，如图 7所示。对于最后一个粒子，我们为自动机的状态 $t_N = \pm 1$ 选择测量 1，为 $t_N = \pm i$选择测量 2。如果额外测量的结果 b_N为 $b_N = 1$（当 $t_N \in \{1, i\}$）或为 $b_N = 2$（当 $t_N \in \{-1, -i\}$）时，则认为纠缠态验证成功，此时我们将 t_{N+1} 更新为“纠缠态”；否则更新为“可分态”。

对于任意维度的 GHZ态，该协议均以概率 1 成功。事实上，考虑一个 k 方

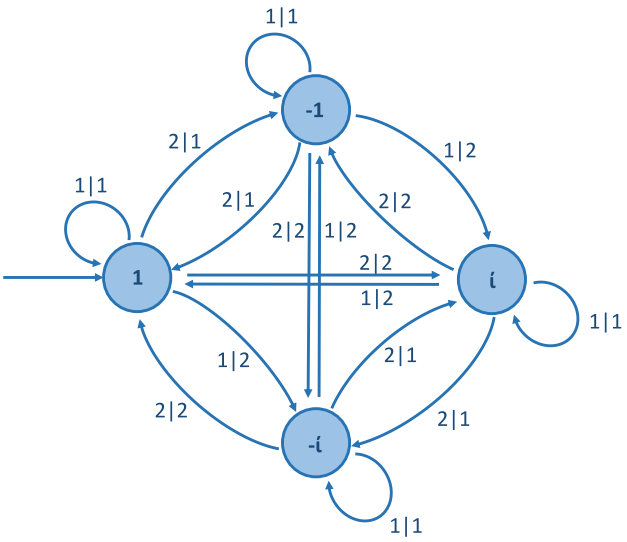


图7. **GHZ 游戏中四状态自动机的记忆更新**。状态之间的转移由 b 和 y 确定性地决定，并以 $b|y$ 标记边。在相关序贯模型的每一轮中，这会更新自动机状态 $t \in \{1, -1, i, -i\}$。

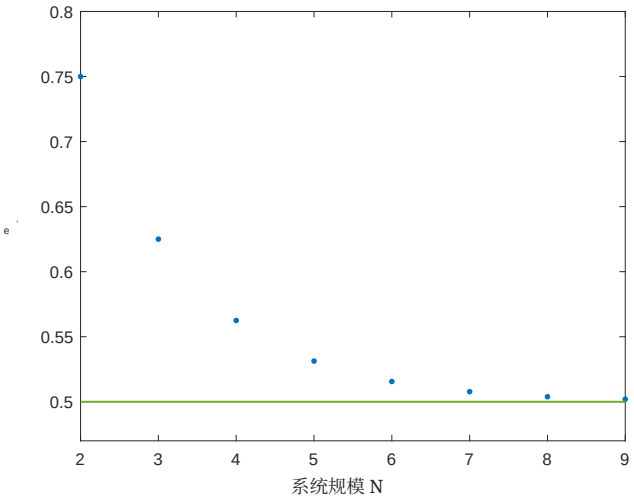


图 8。**GHZ 游戏中最佳可分态获胜概率的上界**。我们观察到，获胜概率（蓝色）迅速下降并趋近于 0.5（绿色线）。出于美观考虑，图中仅展示了截至 $N = 9$ 的上界。事实上，我们已经验证，使用此方法可以推导出截至 $N = 35$ 的上界。借助渐近层级（见第 VIB节），我们进一步确认渐近值的上界为 0。5004，即 $N \to \infty$。

GHZ 类状态，其形式为

$$\frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes k} + \alpha|1\rangle^{\otimes k}\right). \tag{39}$$

其中 $\alpha \in \{1, -1, i, -i\}$。假设我们在基 $\{|+\rangle, |-\rangle\}$ ($\{|i\rangle, |-i\rangle\}$) 中测量一个量子比特态，得到结果 $|\pm\rangle$ ($|\pm i\rangle$)。那么，最终后选态是一个（$k-1$）部分态，其形式如式（39）所示，但此时相位为 $\pm\alpha$ ($\mp i\alpha$)。

由于其转移矩阵，图7中的自动机内部状态会跟踪 GHZ 类态的相位，随着其量子比特依次被测量，即 $t = \alpha$。奖励函数只需验证最后一个量子比特的状态是否对应于 $\frac{1}{\sqrt{2}}(|0\rangle + \alpha|1\rangle)$。

第III 节中介绍的过程使我们能够推导出可分态所能达到的最大成功概率的上界，也就是最坏情况下的第一类错误 e_I。我们在图中展示了不同系统规模 n 下的上界。8。需要注意的是，优化问题的规模使我们能够处理的轮次数高达 $N = 35$。读者可以看出， e_I 似乎在极限 $_{1\ 2}$ 下收敛至 $N \to \infty$，从而使式（ 36 ）中的不等式取等。实现细节（包括精度问题以及如何在此情形下解决这些问题）见附录 B3。

我们还将自动机引导的 GHZ 游戏的检测性能与一类基于影子层析的纠缠检测协议进行比较 [64], ， 下文称为 影子协议。

影子层析有多种不同的协议，具体取决于对量子比特进行的测量类型。由于在自动机引导的 GHZ 游戏中，我们只允许对每个量子比特单独进行测量，因此我们选择采用在三个泡利基上进行随机测量的影子协议。

因此，我们用于纠缠检测的影子协议系列按如下方式工作：

1. 对每个量子比特，在某个泡利基中进行随机测量，并记录测量结果和所用的基。对于 n 个实验轮次（或态制备）重复此过程。 2. 随后使用得到的经典影子，生成一个估计量 f ，用于估计量子态相对于 GHZ 态的保真度。 3. 如果 f 大于阈值 $0 \le \theta \le 1$, 则协议输出“纠缠的”；否则，输出“可分态”。

因此， θ 的每个取值都对应一个影子协议。

计算这类协议的第二类错误 $e_{II}(\theta)$ 很简单——但计算 $e_I(\theta)$ 却并非如此，因为需要在可分输入态集合上优化协议输出“纠缠的”的概率。为此，我们将对所有可分态的最大化替换为对三个可分态 $|0\rangle^{\otimes N}$、$|+\rangle^{\otimes N}$和 $|+i\rangle^{\otimes N}$ 的最大化。因此，所得量 $\tilde{e}_I(\theta)$ 是实际 $e_I(\theta)$ 的一个下界，即 $e_I(\theta) \ge \tilde{e}_I(\theta)$。由于我们的目标是证明自动机引导的 GHZ 游戏优于影子协议，因此低估后者的误差就足够了，因为这为我们观察到的自动机引导的 GHZ 游戏的优势提供了一个下界。

对于不同的 θ值，我们估计了影子协议在五方GHZ态下的第一类和第二类错误 $\tilde{e}_I(\theta)$ $e_{II}(\theta$，具体见 $n = 50$ 实验轮次 [68]。为了将这些数值与单轮自动机引导的 GHZ 游戏的性能进行比较，我们通过以下方式将后者扩展为 n 实验重复：

1. 运行自动机引导的 GHZ 游戏 n 个实验轮次，并记录协议输出“纠缠的”的次数 n_e 。2. 如果 $\frac{n_e}{n}$ 超过阈值 $0 \leq \phi \leq 1$，则判定该状态为纠缠态；否则判定为可分态。

两类协议的数值对（e_I， e_{II}）绘于图9中。注意，自动机引导的 GHZ 博弈曲线完全位于影子协议曲线之下。事实上，对于某些阈值 ϕ ，自动机引导的 GHZ 游戏会出现满足 $e_I \approx e_{II} = 0$ 的数值。这是意料之中的。实际上，设 $\bar{e}_I \approx 0.53$ 为单次 GHZ 博弈的第一类错误。那么，对于 $\phi = 1$，GHZ态的纠缠仍能以概率 1 被检测到（因此$e_{II} = 0$）。此外，可分态被误标为纠缠态的概率至多为 $e_I = \bar{e}_I^{50} \approx 0$。

人们或许会认为，当系统规模 N较大时，基于影子的协议更占优势。然而，从图8中可以清楚地看出，自动机引导协议的（$e_I(\phi)$ $e_{II}(\phi)$）曲线会随着 N的增大而改善。基于影子的 GHZ 保真度估计则并非如此（见文献 [64]）。因此，随着 N增大，我们的自动机引导的 GHZ 游戏将更具优势。最后，我们指出，我们将自动机引导的 GHZ 游戏与文献[64]中的基于影子的 GHZ 保真度估计进行了比较。不过，采用不同的抽样规则，例如按照文献 [69]的思路，从稳定子群中选取泡利算符，可以得到更好的 GHZ 保真度估计。

C. 多体系统中的纠缠检测：比特序列协议

为了说明我们的方法如何能够优化真正具有自适应性的协议，我们在此考虑以下一族 N 轮博弈，并将其称为比特序列协议。

在第一轮中，我们以相同的概率进行以下每一种测量，并记录结果：

$$M_1 = \{M_{1|1} = |0\rangle\langle 0|,\ M_{2|1} = |1\rangle\langle 1|\}\ ,$$
$$M_2 = \{M_{1|2} = |+\rangle\langle +|,\ M_{2|2} = |-\rangle\langle -|\}.$$

在接下来的每一轮 $N-1$ 中，我们都会采用以下流程。在第 k 轮，我们将第 $k-1$ 轮的测量结果（1 或 2）作为新的测量选择。我们进行相应的测量，并记录新的结果。在第 N 轮的最后一次测量后，我们检查最终结果是否为 2；若是，则奖励为 1；否则奖励为 0。

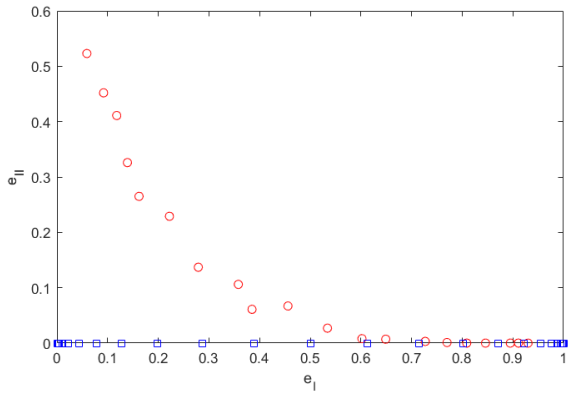


图 9. **第一类错误与第二类错误。** 蓝色方块表示自动机方法；红色圆点表示影子协议。对于某些阈值 ϕ，自动机方法几乎完美。

对于每个 N，比特序列协议定义一个 N 量子比特算符，该算符作用于我们旨在认证其纠缠的 N 量子比特态。接下来，我们将考虑一个 N 量子比特态 ρ_N，它是由 N 轮协议定义的该算符最大本征值对应的本征态。

在图 10中，我们比较使用 $S_{\max}$得到的得分 ρ_N 与使用可分态所能获得的最高得分。可分态的得分采用第III节中的方法计算，见附录 B4。

在该协议中，可分态所能达到的最大得分，与第IVB 节协议中的情况一样，对应于最大第一类错误 e_I；而纠缠态 ρ_N的得分对应于 $1 - e_{II}(\rho_N)$。

我们观察到，ρ_N 的得分与我们为可分态得到的上界之间存在严格差距。这表明，比特序列协议可以认证这一类状态的纠缠。我们还可以进一步将单次协议转化为 n 轮协议，例如借鉴参考文献 [2], 中的元博弈思路，以扩大这一差距。

V. 序贯模型的渐近行为

在某些情形下，所考虑的序贯问题可以自然地推广到任意多个轮次或时间步 N。在这种情况下，我们也可能关注总奖励的渐近行为，即当 $N \to \infty$时。不过，正如我们将在下文（第VA节）看到的，有些序贯模型的近似-

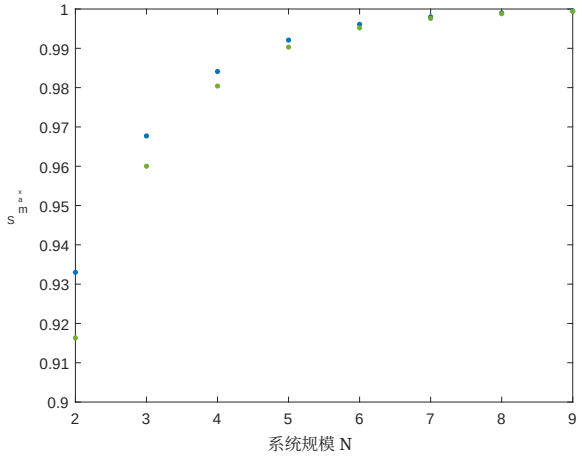


图 10. **与单次操作中相比，最佳可分态的获胜概率上界** ρ_N 。绿色圆点给出了比特序列博弈中可由可分态获得的得分上界。我们观察到，该值严格低于使用状态 ρ_N （蓝色）所得到的值。

近似计算渐近最大奖励（或惩罚）是一个不可判定问题。因此，我们所能期望的最佳结果是找到在实践中表现良好的启发式方法。在第 VB 节中，我们将介绍此类启发式方法，并在第 VI节中证明，这些方法能为我们在第 IV A 节和第 IVB节所研究的有限情形问题提供有用的界。

A. 渐近行为不可计算的序贯模型

为了说明存在一些序贯模型，其渐近最大奖励无法得到良好近似，我们借助 [30], 中提出的一项中间结果；该文构造了特定的概率有限状态自动机，其渐近行为无法得到良好近似。

考虑一个有限状态自动机 $\mathcal{A}$ ，它具有（有限的）状态集合和输入集合 Σ 和 X、初始状态 $\sigma_0 \in \Sigma$ ，且没有输出。如果存在一个输入 $x_0 \in X$ ，使自动机保持在相同的内部状态，则称该自动机为可冻结的。将某个子集 $A \subset \Sigma$ 称为接受状态集合。于是，我们可以考虑通过适当选择输入词 $(x_1, ..., x_n) \in X^{\times n}$，经过 n 个时间步将自动机的状态从 σ_0 转移到某个接受状态的概率。定义

$$\mathrm{val}_n(\mathcal{A}) = \max_{\bar{x}\in X^{\times n}} \mathrm{Prob}\left(\sigma_n \in A\right). \tag{40}$$

自动机的取值 $\mathrm{val}(\mathcal{A})$ 定义为 $\sup_n \mathrm{val}_n(\mathcal{A})$。注意，如果 $\mathcal{A}$ 是可冻结的，那么函数 $\mathrm{val}_n(\mathcal{A})$ 关于 n 单调不减。在这种情况下，

$$\mathrm{val}(\mathcal{A}) = \lim_{n\to\infty} \mathrm{val}_n(\mathcal{A}). \tag{41}$$

给定一个可冻结的无输出自动机 $\mathcal{A}$，考虑序贯模型，其中 S_k 是 Σ、 $H_k = X$、 $\Lambda = \emptyset$ 和 $s_1 = \sigma_0$ 上的概率分布集合。运动方程为

$$P_{k+1}(\sigma') = \sum_{\sigma} P_k(\sigma) P_{\mathcal{A}}(\sigma'|\sigma, h), \tag{42}$$

其中， $P_{k+1} \in S_{k+1}$， $P_k \in S_k$和 $P_{\mathcal{A}}$ 表示该自动机的转移矩阵。

在一个包含 n 轮次的序贯问题中，我们将系统的奖励定义为 $r_k = 0 \ \forall \ k < n$, $r_n(s_n) = \sum_{\sigma\in A} P_n(\sigma)$。由以上内容可知，系统的最大总奖励对应于$\nu_n^\star := \mathrm{val}_n(\mathcal{A})$。因此，$\lim_{n\to\infty} \nu_n^\star = \mathrm{val}(\mathcal{A})$。

计算这类序贯模型的渐近总奖励有多困难？下一个结果给出了一个非常悲观的答案。[70]

引理1 (引理1，出自 [30])。 对于任意有理数 $\lambda \in (0, 1]$, ，存在一个由 $\mathcal{T}_\lambda$ 个可冻结概率有限状态自动机构成的族，其字母表大小为 $|X| = 5$ ，具有$|\Sigma| = 62$ 个状态，使得对于所有 $\mathcal{A} \in T_\lambda$,

(a) $\mathrm{val}(\mathcal{A}) \geq \lambda$ *or* $\mathrm{val}(\mathcal{A}) \leq \frac{\lambda}{2}$.

(b) 无法判定属于哪种情况。

现在，考虑渐近值存在且属于$[0, 1]$的序贯问题类 $\mathcal{C}$ 。该类包含计算 $\mathcal{T}_1$ 中任意自动机的值这一序贯问题。因此，不存在通用算法，能够将 $\mathcal{C}$ 中任意序贯问题的渐近值计算到误差严格小于 $1/4$。否则，我们就可以用它区分 $\mathcal{T}_1$ 中值为 $1/2$的自动机和数值为 1 的自动机，这与上述引理矛盾。

B. 用于计算序贯模型渐近行为上界的启发式方法

对于任意 $N \to \infty$ ，通过推导一个函数$\nu(N)$，使其为对应的、规模为 N 的序贯问题的解提供上界，并取其极限，即可获得序贯模型渐近值的上界。实现这一点的一种方法是通过函数约束，对定义任意高 N下值函数的递推关系进行编码。为便于说明，我们考虑这样一个序贯模型：对于 $k \neq N$ 和 f_k， $r_k = 0$，且 S_k和 H_k 独立于 k。[71]

接下来，我们将展示如何在 $\frac{1}{N}$ 上呈多项式收敛的情况下，以及在 N 下呈指数衰减的情况下推导渐近界。即使序贯问题的解发散，也可以使用类似方法为其求界。例如，这些方法可用于证明 $\nu(N) \leq 4N^3$ （不过，在这种情况下，将相应的约束化简为对有界变量函数的优化，可能需要某种正则化技巧（例如： $V_k \to V_k/k^3$）。

1. *Sequential models with polynomial speed of convergence in* $\frac{1}{N}$

假设对于较大的 N， $\nu(N) \approx \bar{\nu} + \frac{A}{N}$，我们希望计算 $\bar{\nu}$。例如，当我们想研究量子制备博弈 [2]的渐近第一类错误时，就可能遇到这个问题。为简化记号，我们使用负指标 $-j$ 表示 $N-j$。根据式（13）的表述，为了得到规模为N的序贯问题的解的上界，我们需要找到 ν、 $\{V_{-j}(s、\ \lambda)\}_{j=0}^{N-1}$，使得

$$V_0(s,\lambda) \geq r(s,h,\lambda), \tag{43}$$

$$V_{-(j+1)}(s,\lambda) \geq V_{-j}(f(s,h,\lambda),\lambda), \forall j \in \{0,\ldots,N-1\} \tag{44}$$

$$\nu \geq V_{-(N-1)}(s_1,\lambda). \tag{45}$$

根据式（ V_{-j} 13）得到的值函数通常会因问题规模 N 而异，因此无法帮助我们解决渐近问题。

在值函数中引入一个额外参数，以便考虑 j 的增加，不过这样一来，我们就能从某个 k 起使用同一个值函数。为此，假设我们能够证明存在函数 $\{W_{-j}(s,\ \lambda)\}_{j=0}^{k}$、 $W(\alpha,\ s,\ \lambda)$，使得

$$W_0(s,\lambda) \geq r(s,\lambda,h), \tag{46}$$

$$W_{-j}(s,\lambda) \geq W_{-(j-1)}(f(s,h,\lambda)\ \lambda)\ \forall j \in \{1,\ldots,k\}, \tag{47}$$

$$W\left(\frac{1}{k},s,\lambda\right) \geq W_{-k}(s,\lambda), \tag{48}$$

$$W\left(\frac{\alpha}{\alpha+1},s,\lambda\right) \geq W(\alpha,f(s,h,\lambda),\lambda),\ \forall \alpha \in \left[0,\frac{1}{k}\right] \tag{49}$$

那么，函数

$$V_{-j}(s,\lambda) := \begin{cases} W_{-j}(s,\lambda) & j=0,\ldots,k, \\ W\left(\frac{1}{j},s,\lambda\right) & j=k+1,\ldots,N-1 \end{cases} \tag{50}$$

满足方程 (43) 和 (44) 中的约束。直观地说，在方程 (48) 和 (49) 中，变量 α 应理解为表示 $\frac{1}{j}$，此时 $\frac{\alpha}{\alpha+1}$ 对应于 $\frac{1}{j+1}$。因此，方程 (49) 中的约束意味着，对于所有 $j \geq k$，方程 (44) 中的递推关系均成立；而 $j < k$ 的情形则由方程 (47) 处理。注意， α的值有界；如果我们希望使用多项式优化方法来施加方程 (49) 中的不等式约束，这一点很重要（参见第VI节）。

此外，若对于某些实数 B， C.....，满足额外条件

$$\bar{\nu} + A\alpha + B\alpha^2 + C\alpha^3 + ... \geq W(\alpha,s_1,\lambda),\ \forall \alpha \in \left[0,\frac{1}{k}\right], \tag{51}$$

，则根据方程（45），函数 $\bar{\nu} + A\alpha + B\alpha^2 + C\alpha^3 + ...$ 给出了序贯问题解的上界。要为极限 $\lim \bar{\nu}^\star$ 给出上界$_{N\to\infty}\nu$（N），一种启发式方法是最小化 $\bar{\nu}$，并满足约束 [72]方程（46）-（49）以及（51）。

预计在以下情形中，前述方案能够给出良好的上界：当 N 较大时，问题式（13）中的最优值函数 V_0、...、$V_{-(N-1)}$ 满足 $V_{-(N-1)} \approx \bar{V} + \frac{V}{N}$，其中 $\bar{V}$、V 为某些函数。也就是说，只要 $\lim_{N\to\infty} V_{-(N-1)}$ 存在，它们就能发挥良好作用。不过，动力系统的经验表明，即使序列问题的解趋于某个给定值 $\bar{\nu}$，序列 $(V_{-(N-1)})_N$ 也可能在渐近意义下趋近于一个极限环。这意味着，对于许多问题，只有每 $\mathcal{C}$ 个值函数中的一个遵循所要求的模式：在这种情况下，存在一个自然数 $\mathcal{C}$ （即周期）以及函数 V^0、...、$V^{\mathcal{C}-1}$，使得当 N 足够大时， $V_{-N} \approx V^R$，其中 $R = N$（模 $\mathcal{C}$）。因此，我们需要构造一族这样的递推关系，而不是式（49）中的单个递推关系。

因此，可以通过考虑满足以下条件的函数 $\{W_{-j}(s,\ \lambda)\}_{j=0}^{k}$、$\{W^{j}(\alpha,\ s,\ \lambda)\}_{j=0}^{\mathcal{C}-1}$ 来处理这种情况：

$$\begin{aligned}
W_0(s,\lambda) &\geq r(s,\lambda,h),\\
W_{-j}(s,\lambda) &\geq W_{-(j-1)}(f(s,h,\lambda),\lambda),\ j=1,\ldots,k,\\
W^0\left(\frac{1}{k},s,\lambda\right) &\geq W_{-k}(s,\lambda),\\
W^1\left(\frac{\alpha}{\alpha+1},s,\lambda\right) &\geq W^0(\alpha,f(s,h,\lambda),\lambda),\ \forall\alpha\in\left[0,\frac{1}{k}\right],\\
&\vdots\\
W^{\mathcal{C}-1}\left(\frac{\alpha}{\alpha+1},s,\lambda\right) &\geq W^{\mathcal{C}-2}(\alpha,f(s,h,\lambda),\lambda),\ \forall\alpha\in\left[0,\frac{1}{k+\mathcal{C}-1}\right],\\
W^0\left(\frac{\alpha}{\alpha+1},s,\lambda\right) &\geq W^{\mathcal{C}-1}(\alpha,f(s,h,\lambda),\lambda),\ \forall\alpha\in\left[0,\frac{1}{k+\mathcal{C}}\right].
\end{aligned} \tag{52}$$

2. Sequential models with exponential speed of convergence in N

假设序贯模型的收敛速度呈指数级，即对于 $\gamma<1$，$\nu(N)\approx\bar{\nu}+A\gamma^N$。为简便起见，假设 $\lim_{N\to\infty}V_{-(N-1)}$ 存在，我们该如何估计 $\bar{\nu}$ 和 γ?

验证假定的收敛率成立的一种方法，是确认存在函数 $\{W_{-j}(s,\lambda)\}_{j=0}^{k}$、$W(\alpha,s,\lambda)$，使得

$$\begin{aligned}
W_0(s,\lambda) &\geq r(s,\lambda,h),\\
W_{-j}(s,\lambda) &\geq W_{-(j-1)}(f(s,h,\lambda),\lambda),\ j=1,...,k,\\
W\left(\gamma^k,s,\lambda\right) &\geq W_{-k}(s,\lambda),\\
W(\gamma\alpha,s,\lambda) &\geq W(\alpha,f(s,\lambda,h),\lambda),\ \forall\alpha\in\left[0,\gamma^k\right]
\end{aligned} \tag{53}$$

和式（51）成立。上述方程的最后一行是归纳约束，此处 α 应解释为 γ^j。与之前一样，我们根据 j 定义了 α，使前者有界。要在凸优化的形式体系下处理这个问题，可以尝试针对不同的γ值，最小化 $\bar{\nu}$。每次这样的最小化若可行，就会得到一个上界 $\nu(N$，作为满足 $\nu(N)\approx\bar{\nu}+O(\gamma^N)$ 的序贯问题的解。

C. 适应有限数值精度

在标准数值优化中，计算机输出的值函数只能近似满足方程 (43-51) 中的正性约束。更一般地，形式为 $\bullet\geq 0$的条件会放宽为$\delta+\bullet\geq 0$，其中 $1\gg\delta\geq 0$。

当 δ较小时，方程（43-48）和（51）中的条件并不构成问题，因为这些不等式中任一项仅有轻微不满足时，值函数就会相应地增加一个常数量。这就是

为何在求解方程（13）时，我们迄今尚未明确考虑数值精度问题。事实上，令$\{\delta_j\}_{j=k+1}$ 满足

$$\begin{aligned}
&W_0(s,\lambda)+\delta_0\geq r(s,\lambda,h),\\
&W_{-j}(s,\lambda)+\delta_j\geq W_{-(j-1)}(f(s,h,\lambda),\lambda),\forall j\in\{1,\ldots,k\}\\
&W_{-k}(s,\lambda)\leq W\left(\frac{1}{k},s,\lambda\right)+\delta_{k+1},\\
&W\left(\alpha,s_1,\lambda\right)\leq\bar{\nu}+A\alpha+B\alpha^2+C\alpha^2+...+\delta_\infty.
\end{aligned} \tag{54}$$

于是，函数 $\tilde{W}_{-j}:=W_{-j}+\sum_{i=0}^{j}\delta_i$ 和 $\tilde{W}:=W+\sum_{i=0}^{k+1}\delta_i$ 满足方程 (43-48) 中的条件。如果原函数还满足方程 (49) 中的条件，那么

$$\bar{\nu}+\sum_{j=0}^{k+1}\delta_k+\delta_\infty \tag{55}$$

是该博弈渐近值的可靠上界。

然而，如果方程 (49) 中的关系仅近似成立，即

$$W\left(\frac{\alpha}{\alpha+1},s,\lambda\right)+\hat{\delta}\geq W(\alpha,f(s,h,\lambda),\lambda). \tag{56}$$

在这种情况下，对于 $N>k$，第 N 轮游戏的最优奖励上界为

$$\bar{\nu}+\sum_{j=0}^{k+1}\delta_k+\delta_\infty+\hat{\delta}(N-k). \tag{57}$$

也就是说，该界随 N 线性增长。在这种情况下，数值获得的渐近上界 $\bar{\nu}$ 只能被视为对 $N\ll O\left(\frac{1}{\delta}\right)$ 有效。

VI. 时间序列过程渐近优化的应用

在本节中，我们利用第 V节的技术，对第 IV A 节和第 IV B节中分别在有限情形下讨论过的时间序列过程的渐近行为给出界。前者是 $\frac{1}{N}$ 中多项式收敛速度的一个例子，而后者展示了指数情形下的技术。

A. 有限状态自动机的渐近行为

二状态自动机生成长度为 L 的单滴答序列的概率似乎随着 $O(1/L)$趋于 0。还可以验证，这是参考文献 [23] 中所找到的最优模型的收敛速率。事实上，该模型给出的单滴答序列的概率为

$$p(2k) = \frac{1}{k}\left(1-\frac{1}{k}\right)^{k-1} \approx \frac{1}{\mathrm{e}k}, \text{ for } k \to \infty, \tag{58}$$

其中 e 是自然对数的底，且 $p(2k-1) = p(2k)$。这个明确的例子给出了 $\nu(L)$收敛速率的上界，即 $\nu(L)$不可能比 $2/\mathrm{e}L$更快地趋于零。与该模型类似，通过数值计算得到的序贯博弈的值 $\nu(L)$ 满足：从 $k=2$ 起，$\nu(2k) = \nu(2k-1)$。这表明我们应采用式（52）中的松弛，其中 $\mathcal{C}=2$。

记住，$s_k := (p_k(0)\ p_k(1))$，其中 $p_k(t)$ 表示自动机目前已产生结果 0 且处于状态 t 的概率，而 $\lambda := (P(\sigma', 0|\sigma) : \sigma, \sigma')$ 是自动机的转移矩阵。我们允许离散值函数 $W_{-k}(s,\lambda)$ 为所有形如 $s^a\lambda^b$ 的单项式的线性组合，其中 $a, b = 0$ 取 1、2。连续值函数 W^1, W^2 是单项式 $s^a\lambda^b\alpha^c$ 的线性组合，其中 $a, b, c = 0$ 取 1、2。通过将整个表达式乘以 $(1+\alpha)^2$，即可将正性约束（例如公式（52）最后一行中的约束）映射为一个多项式问题。

为了解决这个问题，我们使用了半正定规划求解器 MOSEK [51], 并结合 YALMIP [55]。经过 28 次迭代后，MOSEK 返回的上界为 0。0265，同时给出了 UNKNOWN 消息。然而，MOSEK 找到的解几乎可行，参数为 PFEAS= 4×10^{-7}; DFEAS= 8.6×10^{-7} GFEAS= 7.5×10^{-11} 和 MU= 1.3×10^{-7}。因此，可以合理地认为[73] 半定规划的实际解确实接近 2×10^{-2}，只是由于某种原因 MOSEK 未能找到该解。这个数值确实大于猜测的零渐近值，但仍是一个非平凡的上界。

B. 纠缠检测协议的渐近行为

我们观察到，对于较小的 N，$p_{\max}^{\mathrm{sep}}$ 表现为

$$p_{\max}^{\mathrm{sep}} \approx \frac{1}{2} + \frac{1}{2^N}. \tag{59}$$

这一数值 p^{sep} 也可以通过制备可分态 $|+\rangle^{\otimes N}$来实现。为完整起见，我们在附录C中对此进行了说明。这表明，对于有限8的 N 情形，图 8 中的界是紧的（在数值精度范围内）。

式（59）中的行为也意味着，我们预计渐近值为1 2。按照第V B2节中用于确定渐近行为上界的方法进行实现后，我们确认了上界为 0。5004；随后，使用 YALMIP [55]和求解器 MOSEK [51]时遇到了精度问题。对于该实现，我们在附录C所述方法的基础上，加入了第V B2节中的额外关系。注意，取值1 2 相当于随机猜测状态是否纠缠；对于任意 N，采用式（37）中的状态即可实现这一取值。因此，这是 e_I的下界。注意，GHZ 态的成功概率为 1，而最坏情形可分态的成功概率约为1 2，两者之间的差距几乎达到此类差距的最大可能值1 2 （如式（38）所述）。这表明，多轮 GHZ 博弈在认证 GHZ 态纠缠这一任务中基本达到了最优表现。

VII. 具有保证最低奖励的策略

让我们稍微扩展一下序贯模型，加入一个策略。其思路是，描述我们策略的参数 x 也会影响系统的演化，即

$$s_{k+1} = f_k(s_k, h_k, \lambda, x) \tag{60}$$

以及每个时间步获得的奖励 $r_k(s_k,\ h_k,\ \lambda,\ x)$。

理想情况下，我们希望找到使最大惩罚最小的策略 x。也就是说，我们希望求解以下问题

$$\min_x \max_{h,\lambda} \sum_{k=1}^{N} r_k(s_k, h_k, \lambda, x), \tag{61}$$

假设式（60）成立，且我们知道初始状态 s_1。

不过，对于固定的 x，计算最小期望奖励可能难以实现。因此，一个更现实且实用的目标是找到一个策略 x，并为其最大奖励（或惩罚）$\nu^\star(x)$ 求得一个足够小的上界 ν。下一节将讨论这一主题。

A. 策略优化

对于任意 x，令 $\nu(x)$ 表示 $\nu^\star(x)$ 的一个上界，该上界通过对式（13）中给出的问题进行某种松弛得到。我们提出使用标准梯度下降方法或其某种变体（如 Adam [74], ）来确定一个策略 $x^\star$，使其具有可接受的最低奖励保证 $\nu(x^\star)$。

更具体地，令 X 表示可容许策略集合，并假设 X 是凸集。从对最优策略的某个初始猜测$x^{(0)}$ 出发，给定一个非负递减数列（ϵ_k）$_k$，投影梯度下降 通过应用以下迭代方程来进行

$$x^{(k+1)} = \pi_X\left(x^{(k)} - \epsilon_k \nabla_x \nu(x^{(k)})\right), \tag{62}$$

其中，π_Z（x）表示向量 x 在集合 Z上的投影，即在欧几里得范数下距 x 最近的向量 $z \in Z$。对于 $k \gg 1$，我们期望策略 $x^{(k)}$ 在保证奖励 ν（$x^{(k)}$）方面接近最小值。

使用梯度方法需要估计$\nabla_x \nu(\bar{x})$，适用于任意策略 $\bar{x}$。鉴于迄今为止，我们通过对式（ $\nu(x)$ 的松弛，在数值上得到了界 x）（针对固定的 13），这项工作还需要额外的理论见解。因此，本节余下部分将致力于构建一个优化问题，以估计 $\nu(x)$ 的梯度。

为简单起见，假设 x 仅由一个实参数组成，即我们希望计算$\frac{d}{dx}\nu(\bar{x})$。固定策略为 $\bar{x}$，令 $\delta x \overline{>} 0$，并考虑式（13）所给出的问题。为了得到一个易于处理的问题，通常会考虑如下类型的简化：

$$\begin{aligned}
&\nu(\bar{x}) := \min_{V_1,\ldots,V_N,\nu} \nu \\
&\text{s.t. } V_N(s_N,\lambda) \geq_Q r_N(s_N,h,\lambda,\bar{x}), \\
&\quad V_k(s_k,\lambda) \geq_Q r_k(s_k,h,\lambda,\bar{x}) + V_{k+1}(f_{k+1}(s_k,h_k,\lambda),\lambda), \\
&\quad \nu \geq_Q V_1(s_1,\lambda).
\end{aligned} \tag{63}$$

这里，关系 $a \geq_Q b$ 表示表达式$a-b$在变量 Q 上的概率分布集合的某个凸超集 $\{s_k,h_k\}_k$ λ上取值时非负。本文所考虑的多项式问题中，这个超集 Q 实际上与用于施加正性约束的正值定理互为对偶。对于 Putinar 正定性定理，Q 对应于单项式平均值的集合 $\{\langle z_{i_1}\ldots z_{i_N}\rangle\}$；这些平均值以特定方式排列后会构成半正定矩阵（详见 [47]）。

由于 Q 包含所有概率分布，$a \geq_Q b$意味着 $a \geq b$，因此式（63）的解是式（13）的一个可行点，从而给出上界 ν（$\bar{x}$） $\nu^\star$（$\bar{x}$）。暂且假设式（63）所给问题的极小化解 V_1，……，V_N对于策略 $\bar{x}$是唯一的。稍后我们将去掉这一假设。

现在，我们来考察将 $\bar{x}$ 替换为 $\bar{x}+\delta x$时，式（63）所给问题会如何变化。我们不仅假设解满足 ν（$\bar{x}+\delta x$） $\approx \nu$（$\bar{x}$） $+\mu\delta x$，还假设最优松弛变量 V_1，……，V_N也发生无穷小变化，即：

$$V_k(s_k,\lambda) \to V_k(s_k,\lambda) + \hat{V}_k(s_k,\lambda)\delta x. \tag{64}$$

也就是说，不仅解是可微的，优化问题的极小化解也是可微的。

忽略式 $o(\delta x)$ 中形如64的所有项，显然，$\nu+\mu\delta x$ 是 $\nu^\star(\bar{x}+\delta x)$ 的上界，当且仅当

$$V_N(s_N,\lambda) + \hat{V}_N(s_N,\lambda)\delta x \geq_Q r_N(s_N,h,\lambda,\bar{x}) + \frac{\partial}{\partial x} r_N(s_N,h,\lambda,\bar{x})\delta x, \tag{65}$$

$$\begin{aligned}
V_k(s_k,\lambda) + \hat{V}_k(s_k,\lambda)\delta x \geq_Q\ & r_k(s_k,h,\lambda,\bar{x}) + \frac{\partial}{\partial x} r_k(s_k,h,\lambda,\bar{x})\delta x + V_{k+1}(s_{k+1},\lambda) + \hat{V}_{k+1}(s_{k+1},\lambda)\delta x \\
&+ \delta x \sum_\sigma \frac{\partial V_{k+1}}{\partial s^\sigma_{k+1}} \frac{\partial f^\sigma_k(s_k,h_k,\lambda,x)}{\partial x}
\end{aligned} \tag{66}$$

$$\nu + \mu\delta x \geq_Q V_1(s_1,\lambda) + \hat{V}_1(s_1,\lambda)\delta x. \tag{67}$$

此处，符号 σ 用于表示 s_{k+1}的坐标。

现在，我们的目标是将其转化为一个优化问题，以便求出 μ。为此，可以利用这样一个事实：松弛变量 $\{V_k\}_k$ 是 optimal，即它们不仅满足问题中方程（63）给出的条件，而且所有不等式都必须取等号。也就是说，对于每个 k，都存在 $q \in Q$ 满足

that

$$\langle V_k(s_k,\lambda) - r_k(s_k,h_k,\lambda) - V_{k+1}(s_{k+1},\lambda)\rangle_q = 0. \quad (68)$$

接下来，我们需要以下引理，它使我们能够用量 V_k 来表述方程（65）-（67）中的约束。

引理 2. 设 $a \geq_Q 0$，且集合 $Q' := \{q : q \in Q, \langle a\rangle_q = 0\}$ 非空。那么，对于 $\delta x \to 0^+$， $a + \hat{a}\delta x \geq_Q 0$ 当且仅当 $\hat{a} \geq_{Q'} 0$。

证明。 $Q' \subset Q$，因此 $a + \hat{a}\delta x \geq_Q 0$ 意味着 $\hat{a} \geq_{Q'} 0$。为证明逆向蕴含，注意对于 $q \in Q \setminus Q'$，$\langle a\rangle_q > 0$，因此 $\lim_{\delta x\to 0^+}\langle a + \hat{a}\delta x\rangle_q > 0$。要确定在极限 $\delta x \to 0^+$ 中，对于所有 $q \in Q$， $\langle a + \hat{a}\delta x\rangle_q \geq 0$ 是否成立，只需检查该性质对 $q \in Q'$ 成立，即 $a \geq_{Q'} 0$。 □

根据对偶性，条件 $\hat{a} \geq_{Q'} 0$ 等价于

$$\xi a + \hat{a} \geq_Q 0, \text{ for some } \xi \in \mathbb{R}. \quad (69)$$

由上式及等式（68）中的关系可知（假设极小化解 V 在 $\bar{x}$ 处可微且唯一），极限 $D^+\nu(\bar{x}) \equiv \lim_{\delta x\to 0^+} {}^{\nu(\bar{x}+\delta x)}{}_{-\nu(\bar{x})\ \delta x}$ 等于

$$\begin{aligned}
&\min_{\mu,\hat{V},\xi}\ \mu \\
\text{such that}\ \ &\hat{V}_N(s_k,\lambda) \geq_Q \frac{\partial}{\partial x} r_N(s_N,h_N,\lambda,\bar{x}) + \xi_N\left(V_N(s_k,\lambda) - r_N(s_N,h_N,\lambda,\bar{x})\right), \\
&\hat{V}_k(s_k,\lambda) \geq_Q \frac{\partial}{\partial x} r_k(s_k,h,\lambda,\bar{x}) + \hat{V}_{k+1}(s_{k+1},\lambda) + \sum_\sigma \frac{\partial V_{k+1}(s_{k+1},\lambda)}{\partial s^\sigma_{k+1}} \frac{\partial f^\sigma_k(s_k,h_k,\lambda,x)}{\partial x} + \\
&\qquad + \xi_k\left(V_k(s_k,\lambda) - r_k(s_k,h_k,\lambda,\bar{x}) - V_{k+1}(s_{k+1},\lambda)\right), \\
&\mu \geq_Q \hat{V}_1(s_1,\lambda) + \xi_1\left(\nu - V_1(s_1,\lambda)\right).
\end{aligned} \quad (70)$$

此外，如果集合

$$\begin{aligned}
&Q'_k := \{q \in Q : q\left(V_k(s_k,\lambda) - r_k(s_k,h_k,\lambda,\bar{x}) - V_{k+1}(s_{k+1},\lambda)\right)) = 0\}, k = 1,...,N, \\
&Q'_0 := \{q \in Q : q\left(\nu - V_1(s_1,\lambda)\right)) = 0\}
\end{aligned} \quad (71)$$

各自的基数均为 1，即 $Q'_k = \{q_k\}$，那么待求解的问题就更加简单，即:

$$\begin{aligned}
&\min_{\mu,\hat{V},\xi}\ \mu \\
\text{such that}\ \ &q_N\left(\hat{V}_N(s_k,\lambda)\right) = q_N\left(\frac{\partial}{\partial x} r_N(s_N,h_N,\lambda,\bar{x})\right), \\
&q_k\left(\hat{V}_k(s_k,\lambda)\right) = q_k\left(\frac{\partial}{\partial x} r_k(s_k,h,\lambda,\bar{x}) + \hat{V}_{k+1}(s_{k+1},\lambda) + \sum_\sigma \frac{\partial V_{k+1}(s_{k+1},\lambda)}{\partial s^\sigma_{k+1}} \frac{\partial f^\sigma_k(s_k,h_k,\lambda,x)}{\partial x}\right), \\
&\mu = q_0\left(\hat{V}_1(s_1,\lambda)\right).
\end{aligned} \quad (72)$$

式（70）的推导依赖于这样一个假设：策略 $V := \{V_k\}_k$ 对应的最优松弛变量 $x = \bar{x}$ 是唯一的。若这一假设不成立，则计算 $D^+\nu(\bar{x})$ 的过程需要求解一个非凸优化问题。读者可在附录D中找到该问题，以及解决该问题的一种启发式方法。

现在，让我们回到多变量策略 x 的情形。如果梯度 $\nabla_x\nu(\bar{x})$ 存在，那么它的第 i 个分量对应于以下极限

$$\lim_{\delta x\to 0^+} \frac{\nu(\bar{x} + \delta x|i\rangle) - \nu(\bar{x})}{\delta x}. \quad (73)$$

这些条目都可以依次通过上述概述的步骤计算。这需要求解一个复杂度与计算 $\nu(\bar{x})$ 相当的优化问题。此外，对于 x 的每个坐标，都可以分别进行此类优化。也就是说，计算 $\nu(\bar{x})$ 的梯度这一过程可以并行化。借助式（62），只要我们有足够的资源来计算 $\nu(\bar{x})$，便可以优化包含任意多个参数的策略。

VIII. 应用：魔态检测自适应协议的优化

魔态，即无法表示为稳定子态凸组合的状态，是量子计算中已知的一种资源：它们与 Clifford 门结合，使我们能够高效地执行通用量子操作 [75]。因此，如何认证给定的状态源是否能够制备魔态，便成了一个问题[76]。

对于量子比特，魔态是指无法表示为三个 Pauli矩阵的特征向量的凸组合的状态。等价地，魔态的布洛赫向量 $\vec{n}$ 至少违反以下不等式之一：

$$\left\{ \sum_{j=1}^{3} n_j a_j \leq 1 : a_1, a_2, a_3 \in \{-1, 1\} \right\}, \qquad (74)$$

（示意图见图11）。

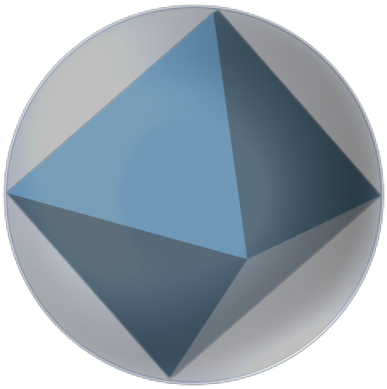


图 11. **量子比特魔态**。 在 Bloch球中表示时，量子比特的魔态就是所有位于蓝色八面体之外的状态。本节的目标是验证一个一般状态是否为魔态。

我们希望设计一种 N 轮自适应测量协议，以判断给定的源是否正在制备魔态。具体而言，如果该源只能产生非魔法态，我们希望协议以较低的概率判定该源为“魔法态” e_I （即协议的第一类错误）。然而，如果该源实际上正在制备任意一种违反上述不等式之一且违反幅度大于或等于 δ的量子态的独立副本，我们希望协议以较低的概率判定该源为“非魔法态” e_{II} （即协议的第二类错误），见图 12。

为此，我们将该协议表述为一个与时间无关的制备游戏 [2]。也就是说，在每个

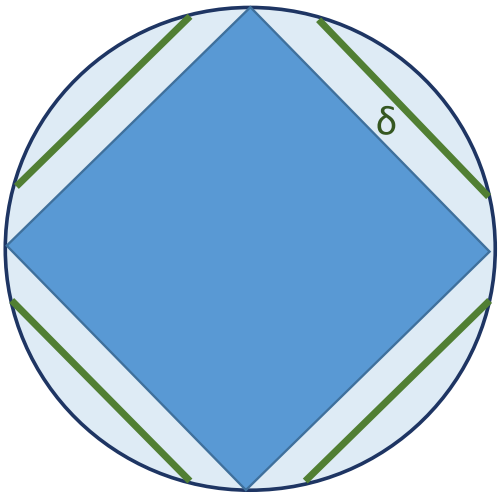


图 12. **魔态检测示意图**。我们展示了 Bloch球的一个截面，其中标出了非魔法态（蓝色方块）和魔态（方块外的区域）。目标是设计一种 N轮协议，能够可靠地将状态分类为魔态或非魔法态，前提是所考虑的魔态与非魔法态之间至少相距 δ。下文推导的协议基于一个双状态自动机，适用于非魔法态方块外的某个区域。

测量轮次 k 中，我们对状态的魔力的了解由博弈配置 $t \in T$ 编码，其中 $|T| < \infty$。随后，源制备的状态通过具有元素 $(M_{t'|t}\colon t' \in T) \subset B(\mathbb{C}^2)^{\times|T|}$ 的 POVM 进行测量。此次测量的结果 t' 是博弈的新配置。当测量轮次总数超过 n 时，我们必须根据当前博弈配置，猜测状态源是否具有魔力。为简单起见，若 $t \in A \subset T$，我们便将该源判定为具有魔力，其中$|A| = \left\lfloor \frac{|T|}{2} \right\rfloor$。博弈的初始状态 t_1的选取满足 $t_1 \notin A$。

因此，该博弈由以下 POVM 定义

$$\{M_{t'|t} \quad t' \in : \quad 。$$

$T\}_t$ e_I

为计算，我们假设这位声称能够制备魔态、但实际上不能的“不诚实”玩家，在每一轮都知道当前的博弈配置。因此，他们可以相应地调整其态制备，以增大第一类错误。如第IIIB节所述，在自适应策略下计算制备游戏的最大得分，可以表述为一个具有 $h_k := (\rho_k(t)\colon\ t \in T_k$的序贯问题。在此情况下，可行态集合 C由以下各项的凸组合生成 $\{\psi_i\}_{i=1}^{6}$，即三个 Pauli矩阵的特征向量：因此，在线性最大化中，只需在这六个“顶点”上进行最大化。综合起来，计算该博弈的第一类错误等价于应用以下递推关系

关系：

$$\mu_N(t) = \max_i \sum_{t' \in A} \mathrm{tr}(|\psi_i\rangle\langle\psi_i| M_{t'|t}),$$
$$\mu_k(t) = \max_i \sum_{t'} \mathrm{tr}(|\psi_i\rangle\langle\psi_i| M_{t'|t}) \mu_{k+1}(t'),$$
$$e_I = \mu_1(t_1). \tag{75}$$

假设上述所有最大化都有唯一的最大化解，并将 i $(k,\ t)$ 称为与第 k 轮及博弈配置 t相对应的最大化解。那么， e_I 关于 POVM 元素 $M_{\tau'|\tau}$ 的梯度满足以下递推关系：

$$\vec{\nabla}\mu_N(t) = \delta_{\tau,t} |\psi_{i(N,\tau)}\rangle\langle\psi_{i(N,\tau)}|,$$
$$\vec{\nabla}\mu_k(t) = \sum_{t'} \mathrm{tr}(|\psi_{i(k,t)}\rangle\langle\psi_{i(k,t)}| M_{t'|t}) \vec{\nabla}\mu_{k+1}(t')$$
$$+ \delta_{\tau,t}\mu_{k+1}(\tau') |\psi_{i(k,\tau)}\rangle\langle\psi_{i(k,\tau)}|,$$
$$\vec{\nabla} e_I = \vec{\nabla}\mu_1(t_1). \tag{76}$$

因此，可以按照测量轮次的数量高效地计算它。

现在，考虑独立同分布策略下第二类错误的计算，其作为序贯问题的表述可见第 IIC 节。我们首先聚焦于集合 $\mathcal{S}_a$ 中具有布洛赫向量 $\vec{n}$ 且满足$\sum_j a_j n_j \geq 1+\delta$的量子比特态，其中 a_1， a_2， $a_3 \in \{-1, 1\}$。对于始终产生相同状态 $\rho \in \mathcal{S}$的源，可以通过序贯模型对魔态检测协议进行建模；在时刻 s_k ，即第 k 轮测量之前，该模型的内部状态由博弈配置 P_k（t）上的概率分布给出。源制备的状态 $\rho \in \mathcal{S}$ 应与演化参数 λ对应，因为该模型的运动方程为：

$$P_{k+1}(t') = \sum_t \mathrm{tr}(\rho M_{t'|t}) P_k(t). \tag{77}$$

为计算第二类错误，我们为模型赋予奖励 $r_k = 0$，对于 $k = 1$、..... $N-1$ 以及

$$r_N(P_N, \rho) = \sum_t P_N(t) \sum_{t' \in A} \mathrm{tr}(\rho M_{t'|t}). \tag{78}$$

因此，我们可以通过式（ $e_{II}(\mathcal{S}_a$13）的半定规划松弛，计算在类别 $\mathcal{S}_a$ 中的状态所能达到的最大第二类错误 的上界；并通过式（70）计算其关于 POVM 元素 $M_{t'|t}$的梯度。[77] 我们假设式（13）所给问题的解是唯一的，因此无需使用附录D 中的技巧。

然而，我们原本的问题是计算所有至少有一个魔多胞体面被违反了 $\geq \delta$ 的状态的第二类错误。因此，我们有e_{II} $= \max_a e_{II}(\mathcal{S}_a)$。该函数的梯度（更准确地说，是次梯度）为 $\vec{\nabla} e_{II}(\mathcal{S}_{a^\star})$，其中$a^\star$ 是 $\max_a e_{II}(\mathcal{S}_a)$ 的自变量。

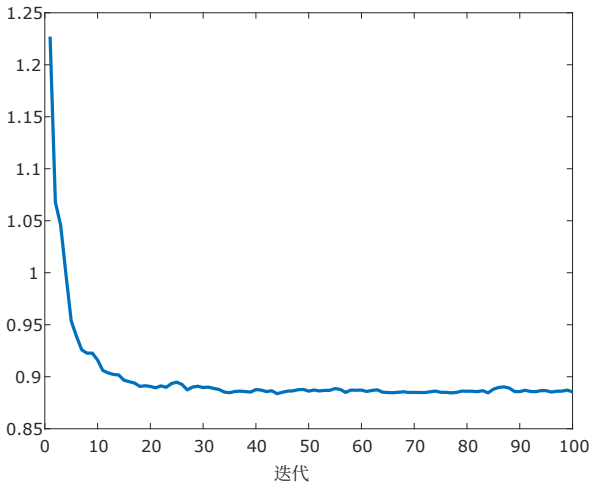


图 13. **上界 $e_I + e_{II}$ 随梯度迭代次数的变化。** 从一个随机制备博弈出发，我们使用 Adam 算法[74] 来降低魔态检测协议中第一类错误与第二类错误之和。对于此计算，我们将算法的学习率设为 0。01。

现在，我们可以使用梯度下降来最小化合并误差 $e_I + e_{II}$。我们采用了梯度方法 Adam [74], ，并在每次迭代后将结果投影到协议的（凸）集合 $\{M_{t'|t} \quad t' \in : , T\}_{t \in T}$ $M_{t'|t} \geq 0\ \forall t\ t' \in T\ \sum_{t'} M_{t'|t} = \mathbb{I}\ \forall t \in T$ 其中，，，，。对于 $|T| = 2$， $n = 6$，梯度下降收敛到一个值$e_I + e_{II} \approx 1$，这或许表明，无法用二状态自动机检测所有魔态。不过，如果我们将问题限制为检测满足不等式 $\sum_i n_i \geq 1 + \delta$的那些状态，就会得到图 13所示的曲线。

读者可以看到，经过几次迭代后，算法成功找到了一个策略，其 $e_I + e_{II} <$ 为 1。超过 50 次迭代后，目标值似乎不再显著下降。应将此曲线视为一个原理验证，表明梯度方法有助于设计制备博弈。请注意，对于一般的制备博弈，梯度的分量数为 $4|T|^2$。因此，对具有较高 $|T|$ 的制备博弈进行优化，将受益于使用并行处理来计算整个梯度向量。

九、结论

我们提出了一种放宽涉及有限轮次的序贯问题的方法。借助该方法，我们能够求解以往凸优化技术无法处理的规模的优化问题。此外，该方法的一种变体可以在轮次数趋于无穷的渐近极限下，为问题的解生成上界。

我们展示了该方法的实际应用，

通过解决一个未解决的问题：具体而言，我们计算了某一固定维度下任意有限状态自动机生成特定序列的最大概率，从而证明参考文献 [23, 24] 中猜想的数值是最优的（在数值精度范围内）。我们还进一步说明了如何将此类界转化为解析结果。

正如我们所展示的，这些方法同样适用于量子系统性质的认证，尤其是纠缠检测。具体而言，我们的方法能够为多轮方案以及渐近极限下可分态的误分类误差给出界。我们通过一个受 GHZ 博弈启发的协议来说明这一点，并且还证明了我们的界是紧的。

最后，我们解释了如何将这些方法与梯度下降技术相结合，以优化序贯模型，并认证其最大奖励。借助这一方法，计算机生成了一个用于魔法态检测的自适应协议。

在一些优化问题中，我们发现，即使是原本表现良好的半定规划求解器，例如 MOSEK[51], , 有时也无法给出可靠的结果。这种异常行为的原因尚不明确，我们也没有解决这一问题的通用方案。尽管如此，数值优化的结果仍使我们能够在大多数情况下从优化中提取并确认可靠的界。

在所考虑的两项应用中，我们为关注的量找到了紧上界。这或许表明，至少在相当简单的情形下，我们的层级方法在较低的复杂度层级上便会收敛。探究在如此低的层级上实现收敛的条件是一个有趣的问题，我们将其留待今后研究。

量子技术目前正处于构建计算设备的前沿，这些设备将可用于纯学术目的以外的领域。这类设备涉及的粒子数不止几个，因此，如何认证中等规模系统的性质已成为当前的关键问题。这不仅关系到构建设备的公司，也关系到希望独立测试设备的用户。从某种程度上说，这一进展与认证研究的现状存在张力，例如在纠缠理论中，相关方法仍主要适用于少粒子情形。我们的 GHZ 游戏表明，自动机引导协议或许能够弥合这一差距：通过序列过程对单向局域操作与经典通信协议进行建模，或可认证大类多体系统，从而为基于影子层析的协议提供一种替代方案 [64, 78]。

此外，我们的方法还能够认证超越线性范围的系统；而认证系统时，通常采用的见证算子类型仅适用于线性范围。从数学角度来看，这些见证算子本质上是通过寻找分离超平面来区分凸集。正如魔态的例子所示，超越这一范围的技术也意味着我们能够同时分析更多一般类别的系统。事实上，我们预计，只要有限状态自动机的维度足够大，就能检测出与非魔法态集合至少相距一定距离的任意状态。随着优化方法不断改进，我们预计这类通用协议会越来越普遍，因为即使对相关系统的状态知之甚少，它们也同样适用。

最后，量子信息理论中遇到的许多不同问题都具有与本文所分析的问题相似的序贯结构。因此，我们预计，我们的方法很快就会应用于本研究之外的领域。在这方面，将我们的技术用于分析量子通信协议将会很有意思。另一个自然的研究方向是扩展我们的方法，以对与不断演化的量子系统（而非（经典）有限状态自动机）的交互进行建模。

致谢

本研究全部或部分由奥地利科学基金（FWF）资助，项目编号为 10.55776/M3109（莉泽·迈特纳）、10.55776/ZK3（Zukunftskolleg）、10.55776/F71（BeyondC）和 10.55776/P35509]；另获瑞士国家科学基金会资助（Ambizione PZ00P2 208779）。

附录 A：Lasserre-Parrilo 层级及其变体

Lasserre-Parrilo 方法提供了一套完整的层级充分条件，用于证明当在由有限个多项式不等式定义的紧致区域内求值时，多项式非负 [47, 48]。给定若干多项式 $g_1(z)$……，$g_u(z)$ $\tilde{g}_1(z)$……，$\tilde{g}_v(z)$，我们将区域 $Z \subset \mathbb{R}^n$ 定义为

$$Z = \{z \in \mathbb{R}^n : g_1(z), ..., g_u(z) \geq 0, \tilde{g}_1(z) = ... = \tilde{g}_v(z) = 0\} \tag{A1}$$

设 $p(z)$ 为一个多项式，并考虑证明对于所有 $z \in Z$，$p(z) \geq 0$ 的问题。一个充分条件是 $p(z)$可以表示为

$$p(z) = \sum_i \tilde{g}_i(z)\tilde{f}_i(z) + \sum_i f^i(z)^2 + \sum_{i,j} f^i_j(z)^2 g_j(z), \tag{A2}$$

其中，$\tilde{f}_i(z)$ $f_i(z)$ $f_{ij}(z)$是关于向量变量 z的多项式。上述形式称为多项式 $p(z)$的平方和（*SOS*）分解。判断 $p(z)$是否存在由有界次数的多项式 $\tilde{f}_i(z)$ $f_i(z)$ $f_{ij}(z)$构成的 SOS，可以转化为一个半定规划（SDP） [47]。此外，如 [47], 所示，只要 Z 是有界集，且 $p(z)$在 Z上严格为正，这样的分解就始终存在 [79]。

一种较弱的正性判据是要求存在一个分解[80]

$$p(z)=\sum_i \tilde{g}_i(z)\tilde{f}_i(z)+\sum_i f^i(z)^2+\sum_{i,j} f^i_j(z)^2 g_j(z)+\sum_i\sum_{j>k} f^i_{jk}(z)^2 g_j(z)g_k(z)+\sum_i\sum_{j>k>l} f^i_{jk}(z)^2 g_j(z)g_k(z)g_l(z)+\ldots \tag{A3}$$

如果 t 中的所有项 分解中的变量次数均不超过 n，则称 $p(z)\in SOS^n$ 为 g，$\tilde{g}$.

下面简要说明如何应用这两个层级中的任一个来处理正文中的问题 (13)。设 $(g^k,\tilde{g}^k)$ 是定义集合 S_k，S_{k+1}，H_k，Λ 以及条件 $s_{k+1}=f_k(s_k,h_k,\lambda)$ 的多项式。取一个充分大的自然数n，并考虑以下半定规划：

$$\begin{aligned}\nu^n := &\min_{V_1,\ldots,V_N,\nu}\ \nu\\ \text{subject to } &V_1,\ldots,V_N,\text{polynomials of degree } n,\\ &V_N(s_N,\lambda)-r_N(s_N,h,\lambda)\in SOS^n(g^N,\tilde{g}^N)\\ &V_k(s_k,\lambda)-r_k(s_k,h,\lambda)-V_{k+1}(f_k(s_k,h,\lambda),\lambda)\in SOS^n(g^k,\tilde{g}^k),\\ &\nu-V_1(s_1,\lambda)\in SOS^n(g^1,\tilde{g}^1).\end{aligned} \tag{A4}$$

由上述讨论 可知 $\nu^n\geq\nu^\star$。此外，如果 S_k，H_k，Λ 有界，则 $\lim_{n\to\infty}\nu^n=\nu^\star$.

通过要求函数$\{W_{-j}\}_{j=0}^k$、W为 α，s，λ的多项式，可以使用同样的思路对正文中的约束 (47) 和 (49) 建模。由于我们对 α的定义方式，该变量是有界的，因此 Lasserre-Parrilo 层级必然收敛。对于正文中形如 (45) 的约束，其中一个多项式在 $\frac{\alpha}{\alpha+1}$ 处求值，可以通过引入表示 $\frac{\alpha}{\alpha+1}$ 的新变量 β 来处理，并加入多项式约束$\beta(\alpha+1)=\alpha$。后者又可以通过条件 $\beta(\alpha+1)-\alpha\geq 0$、$\alpha-\beta(\alpha+1)\geq 0$ 建模。

为了在半定规划中表示方程（A2）和（A3）中的条件，我们需要用向量形式表示多项式。例如，可以固定一个由所有单项式组成的基 $\{m_i(z)\}_{i=1}^N$，其次数不超过描述问题中多项式所需的次数。将此基记为 $\mathrm{MB}_{\mathrm{in}}$。于是，每个多项式都是这些单项式的线性组合。这使我们能够将平方和条件写成半定规划形式，例如：

$$\sum_i f^i(z)^2 g(z)=\sum_{k,l} Z_{kl}m_k(z)m_l(z)g(z) \tag{A5}$$

其中 Z 是适当选取的半正定矩阵。类似地，我们有

$$\tilde{g}(z)\tilde{f}(z)=\sum_i \alpha_i g(z)m_i(z), \tag{A6}$$

对于某个向量 α。随后，必须将这些运算的结果用向量形式重新表示，并以新的单项式基表示，我们将其记为 $\mathrm{MB}_{\mathrm{out}}$。这两个基 $\mathrm{MB}_{\mathrm{in}}$ 和 $\mathrm{MB}_{\mathrm{out}}$ 使我们能够将所有约束表示为线性约束和半正定约束。更多详情请参见 [47]；有关该优化问题的具体实现，请参见后续章节。

附录 B：序贯模型优化的实现

1. 单滴答序列的概率界

为了实现式（A4）中的优化问题，我们首先需要确定用于描述该问题的相关变量。为使符号简洁，我们讨论 $d=2$的情形；$d=3$ 的情形可轻易视为其推广。为描述自动机的状态，我们使用以下变量

$$s_k=(p_k(t_k=1,\sigma_{k+1}))_\sigma, \tag{B1}$$

满足约束 s_k^0，$s_k^1\geq 0, 1-s_k^0-s_k^1\geq 0$，这使得每个 k 对应两个变量。注意，无需描述 $t_k=0$ 的情况，因为这不会对计算成功输出单滴答序列的概率有贡献。

同样，对于转移参数 λ，只有四个变量：$\lambda:=(P(\sigma',\ b=0|\sigma):\ \sigma,\ \sigma'=0,\ 1)$，因为在 $b=1$ 的情况下，我们无需追踪内部状态，且可通过归一化条件恢复概率。它们满足以下约束

$$\begin{aligned}&P(\sigma',b=0|\sigma)\geq 0,\ \text{for all } \sigma,\sigma'=0,1,\\ &1-\sum_{\sigma'}P(\sigma',b=0|\sigma)\geq 0,\ \text{for } \sigma=0,1.\end{aligned} \tag{B2}$$

最后，还有来自运动方程的等式约束

$$p_{k+1}(t_k=1,\sigma_{k+1})=\sum_{\sigma_k}p_k(t_{k-1}=1,\sigma_k)P(\sigma_{k+1},0|\sigma_k), \tag{B3}$$

对于 $k=1,\ \ldots,\ L-1$。最后，初始状态固定为 $s_1=(1,\ 0)$。

这使得在每个时间步（初始和最终时间步除外），状态 s_k^0、s_k^1、s_{k+1}^0、s_{k+1}^1 有四个变量，转移参数 $\{\lambda_{\sigma,\sigma'}\}_{\sigma,\ \sigma'=0,\ 1}$则有四个变量。这些变量构成了方程（A1）中多项式的基础。

为了施加问题中的约束，我们需要在$_{\text{in}}$ 和$_{\text{out}}$ 中讨论的A两个单项式基 g_i、$\tilde{g}_i$ 。这些基使我们能够将约束条件在公式（A1）中出现的多项式 g_i，$\tilde{g}_i$ 以及公式（A2）和（可能还有）公式（A3）中的多项式表示为向量。对于正文图 5 和图 6 中单滴答序列概率的具体计算，使用 Putinar 正定性定理，即公式（A2），就足够了。输入基和输出基的单项式选取如下。

- 构造三个集合：变量（s_k^0，s_k^1）中的二次单项式、变量（s_{k+1}^0，s_{k+1}^1）中的二次单项式，以及变量 $\{\lambda_{\sigma\sigma'}\}_{\sigma\sigma'}$ 中的二次单项式。

- 将这三个集合合并，并添加形如 $s_k^i\lambda_{\sigma\sigma'}$ 的单项式，其中 σ，σ'，$i=0$，1；以及形如 $s_{k+1}^i\lambda_{\sigma\sigma'}$ 的单项式，其中 σ，σ'，$i=0$，1。此操作完成输入基 MB$_{\text{in}}$ 的构造。

- 以类似方式构造另外两个基 MB$_k$和 MB$_{k+1}$，定义如下。MB$_k$ 由变量中分别为 (s_k^0, s_k^1) 和 $\{\lambda_{\sigma\sigma'}\}_{\sigma\sigma'}$ 的二次单项式，以及形如 $s_k^i\lambda_{\sigma\sigma'}$、满足 $\sigma,\sigma',i=0,1$ 的单项式组成。MB$_{k+1}$ 的构造方式相同，只需将 s_k^i 替换为 s_{k+1}^i。换句话说，这些基的定义方式与 MB$_{\text{in}}$ 相同，但这次排除了所有包含 s_{k+1} 或包含 s_k 的单项式。

- 输出基由三个输入基的副本的张量积给出。换句话说，此列表中的每个单项式都是输入列表中出现的三个单项式的乘积。由此完成输出基 MB$_{\text{out}}$的构造。

有了这些基之后，我们希望实现这些约束

$$V_k(s_k,\lambda) - V_{k+1}(s_{k+1},\lambda) \in SOS^{\ell}(g_i,\tilde{g}_i), \qquad \text{(B4)}$$

其中，$SOS^{\ell}(g_i,\tilde{g}_i)$表示平方和约束被实现到 ℓ 这一层级，该层级取决于上述输入（以及可能的输出）基的选择。函数 $V_k(s_k,\lambda)$是一个多项式，由列表 MB$_k$ 中单项式的线性组合给出。类似地，$V_{k+1}(s_{k+1},\lambda)$是 MB$_{k+1}$ 中元素的线性组合。属于 $SOS^{\ell}(g_i,\tilde{g}_i)$的条件意味着，$V_k(s_k,\lambda)$ $-V_{k+1}(s_{k+1},\lambda)$可以按照式（A2）的形式表示，其中多项式~ ~$f_i$、$f_i$、$f_{ij}$经过适当选取。在我们的实现中，$f_i$、$f_i$、$f_{ij}$ 是 MB$_{\text{in}}$ 基中单项式的凸组合。按照 MB$_{\text{out}}$ 的选取方式，由 f_i、f_i、f_{ij} 与 $\tilde{g}_i$、g_i 的乘积产生的所有可能单项式~都会出现在 MB$_{\text{out}}$中。

对于 $d=2$的情况，半定规划使用 CVXPY [52]和 MOSEK [51] 运行至 $L=50$。所得数值与 [23] 中给出的显式模型一致，精确到小数点后五位。对于 $d=3$的情况，半定规划使用 CVXPY[52] 和 SCS [53] 运行至 $L=10$。数值解与 [23]中给出的最优模型以及 [24]，中明确报告的数值一致，精确到小数点后四位。对于求解器提供的每个显式解，我们都验证了线性约束和正性约束确实满足数值精度要求。

2. 提取单刻序列的值函数并寻找最优自动机

为了提取适合进一步处理的值函数，最好先简化多项式优化的输出（见附录 B1）。此时，施加任何对称性并加入关于当前问题结构的其他知识都会有所帮助。例如，这或许能让我们规定某些单项式具有相同的系数，从而减少独立变量的数量。

如果涉及冗余变量，我们还可以通过检查值函数来进一步实现这一点。例如，假设我们选择的问题实现还涉及变量$P(0,1|0)$ 和 $P(0,1|1)$，我们就可以找到不包含这些变量及包含它们的单项式的值函数。反过来，我们可以确认，实现附录 B1所用到的所有变量确实都是必需的。更确切地说，虽然在 $P(0,0|1)$ 或 $P(1,0|1)$ 的 $d=2$，$L=3$ 情况下，我们可以去掉这些变量，但对于更高的 L，它们是必需的。

由于数值优化往往会为所有优化变量赋予非零值，因此还可以通过消除无关单项式（即将其系数设为零）来简化值函数。事实证明，对于当前问题，采用以下启发式过程效果良好：先计算最优值 $P_{\max}^{d*}$，然后重复执行以下两步：

- 设定阈值 ν，并在下一次优化中将小于 ν 的 V_k的所有系数设为零。如果没有这样的系数，则增大 ν。

- 求解优化 P_{dmax} 的问题，并检查最优值是否仍为 $P_{\text{d*max}}$。如果不是，则逐步恢复系数，直到重新得到 $P_{\text{d*max}}$。

经过这一过程后，还可以进一步手动调整这些多项式，例如要求某些系数相等。

3. 自动机引导的 GHZ 游戏中的纠缠检测

a. Implementation of a polynomial optimization problem to bound the performance of separable states in the automaton-guided GHZ game

自动机引导的 GHZ 态通过一个四状态自动机来实现，该自动机在每一轮中通过测量一个量子比特态进行更新。由于归一化的原因，这意味着对于四状态自动机，我们需要使用 3 个变量的多项式， $\{p_k(t)\}_{t\in\{1,-1,i\}}$ ；对于每一轮中该状态的布洛赫向量，则需要使用 2 个变量， n_1， n_2，其中$n=(n_1,\ n_2,\ n_3)$表示第 k轮中该状态的布洛赫向量（最后一轮除外；在最后一轮中，我们以 s_{N+1} 的函数形式生成奖励，并通过与每种情况下最后一次测量的成功概率相乘来更新该量。由于归一化的丧失，最后一步因此还需要一个额外的多项式变量）。

值函数是根据式 (A3) 中 Schm¨udgen 正值定理的一种改写构造的。多项式 V_k 取为混合次数 2，即包含阶数最高为 $p_k(t)p_k(t')n_sn_{s'}$, $t,t'\in\{1,-1,i\}$, $s,s'\in\{1,2\}$的项。这意味着，对于涉及 V_k 和 V_{k+1} 的不等式，我们考虑在每个 $\{p_k(t)\}_{t\in\{1,-1,i\}}$, $\{p_{k+1}\ t\ \}_{t\in\{1,-1,i\}}$ n_1 n_2 n_1' n_2' n $=()$, , , , （其中 (n_1,n_2,n_3) 表示第 k 轮状态的布洛赫向量，而 $n'=(n_1',n_2',n_3')$ 是第 $k+1$轮的布洛赫向量）中次数最高为 2 的多项式。这意味着我们考虑如下形式的单项式：$p_k(t)p_k(t')p_{k+1}(t'')p_{k+1}(t''')n_sn_{s'}n'_{s''}n'_{s'''}$。这里的多项式 g_i 由自动机的概率正性（$p_k(t=1)\geq 0, p_k(t=-1)\geq 0, p_k(t=i)\geq 0$, $1-p_k(t=1)-p_k(t=-1)-p_k(t=i)\geq 0$, p_{k+1}亦然）以及 $(1-n_1^2-n_2^2\geq 0$ 和 $1-n_1'^2-n_2'^2\geq 0)$ 的布洛赫向量归一化给出。此例的运动方程（见正文中的式 (5)）定义了 $\tilde{g}_i$。

在这种情况下，运动方程关于 p_k、p_{k+1}、 ρ_k 的次数为 1，因此，为了用尽可用次数，我们可以将它与关于 p_k、p_{k+1}、 ρ_k 的一次多项式以及关于 ρ_{k+1} 的二次多项式相乘。乘在乘积 $g=g_jg_kg_l\ldots$ 上的平方多项式，选为关于不属于 g 的变量的次数至多为 1 的线性组合。

b. Resolution of numerical problems in the optimization of the automaton-guided GHZ game

我们使用 YALMIP 实现了上述问题 [55] ，并使用求解器 MOSEK [51]来求解半定规划。为了确认我们的结果在较大 N时仍然可信，我们进一步从解中提取了所有值函数，然后分别检查了每个不等式 $V_N\geq r_N$, $V_k-V_{k+1}\ \forall k$, $\nu\geq V_1$ 。为此，我们建立了一个受约束的多项式优化问题（受正性约束和运动方程约束），以分别最大化每个不等式的违反程度。与原始优化问题的情形不同，我们没有手动建立半定规划形式，而是在这一步使用了 YALMIP 的 SOLVEMOMENT 功能（设置 level=3 ，但 k=30 除外，此处我们使用 level=2），并使用 MOSEK 求解器。各项违反程度之和给出了我们结果的误差估计（另见正文第 VC 节）。

对于 $N=35$ ，我们得到的值为 0。5025，其中上界是按照过程 (50)，针对有限 N 情形并结合 $\nu=0.5002$ 计算得出的。

4. 通过比特序列协议进行纠缠检测

比特序列协议通过一个双状态自动机执行，该自动机在每一轮测量一个量子比特态后更新。这个自动机保存上一次测量的结果，并据此决定下一次测量。由于归一化，对于双状态自动机，我们需要关于 1 个变量的多项式，即 $\{p_k\ (t)\ \}_{t\in\{1\}}$；对于每一轮中状态的布洛赫向量，则需要关于 2 个变量的多项式，即 n_1， n_3，其中 $n=(n_1,\ n_2,\ n_3)$ 表示第 k [81] 轮中状态的布洛赫向量。

值函数按照式（A3）中 Schm¨udgen 正值定理的一种改写方式构造。多项式 V_k 取混合次数 2，即包含阶数最高为 $p_k(t)p_k(t')n_sn_{s'}$, $t,t'=1$,$s,s'\in\{1,2\}$ 的项。这意味着，对于涉及 V_k 和 V_{k+1} 的不等式，我们考虑关于每个 $\{p_k(t)\}_1$, $\{p_{k+1}(t)\}_1$, n_1, n_2, n_1', n_2' 的次数最高为 2 的多项式（其中，$n=(n_1,n_2,n_3)$ 表示第 k 轮状态的布洛赫向量，而 $n'=(n_1',n_2',n_3')$ 表示第$k+1$轮的布洛赫向量）。这意味着我们考虑如下形式的单项式：$p_k(t)p_k(t')p_{k+1}(t'')p_{k+1}(t''')n_sn_{s'}n'_{s''}n'_{s'''}$。这里，多项式 g_i 由自动机的概率的正性（$p_k(t=1)\geq 0, 1-p_k(t=1)\geq 0$, 以及对 p_{k+1}同样如此）和（$1-n_1^2-n_2^2\geq 0$ 与 $1-n_1'^2-n_2'^2\geq 0$的）布洛赫向量归一化给出。这个例子的运动方程（见正文中的式（5））定义了 $\tilde{g}_i$。

附录 C：具有可分态的自动机引导的 GHZ 游戏中的最大获胜概率下界

N轮 GHZ 游戏中的获胜概率可以通过计算任意 N 方可分态的得分来确定下界。下面我们将展示，最优可分策略在于制备状态 $|+\rangle^{\otimes n}$，这确实恢复了我们的界（达到数值精度范围内）。

对于这个状态，每一轮中，测量 1 的测量结果都是 1，而对于测量 2，两个

结果出现的概率均为1 2。这意味着,⌜ 自动机在第 k 轮的状态具有如下概率：$\mathbf{p_k} = (p_k(1)\ p_k(-1)\ p_k(i)\ p_k(-i)) = (1/4 + 1/2^n, 1/4 - 1/2^n, 1/4, 1/4)$，其计算方式为$\mathbf{p}_k = M^{k-1}\mathbf{p_1}$„ 其中$\mathbf{p_1} = (1,0,0,0)$是序贯模型的初始状态，且

$$M = \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{4} & \frac{1}{4} \\ 0 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{2} & 0 \\ \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{2} \end{pmatrix}.$$

最终获胜概率为 $p^{\text{sep}}(|+\rangle) = p_N(1) + 1\,2(p_N(i) + p_N(-i))$。–

附录D：最优值函数不唯一时的梯度计算

从正文中的公式 (66) 推导时，依赖于这样一个假设：策略 $x = \bar{x}$ 的最优松弛变量 $V := \{V_k\}_k$ 是唯一的。在这种情况下，自然会假定它们在 $x = \bar{x}$ 处可微，即具有策略 $x = \bar{x} + \delta x$ 的扰动问题的最优松弛变量应具有正文中公式 (60) 的形式。

不过，如果主文中的问题 (59) 存在多个极小化解，那么自然可以假设至少存在一个 可微的极小化解。然而，没有理由认为该极小化解的值应与数值求解器返回的值一致。换言之，给定 (59) 的一个极小化解 V，优化问题 (66) 通常返回的是 $D^+\nu(\bar{x})$ 的上界，而非其精确值。

为处理最优松弛变量 V 可能不唯一的情况，对于固定的 ξ，考虑问题 (66) 的以下变体：

$$\begin{aligned}
&\min_{\mu, V, \hat{V}} \mu \\
\text{such that } &\hat{V}_N(s_k, \lambda) \geq_Q \frac{\partial}{\partial x} r_N(s_N, h_N, \lambda, \bar{x}) + \xi_N \left(V_N(s_k, \lambda) - r_N(s_N, h_N, \lambda, \bar{x})\right), \\
&\hat{V}_k(s_k, \lambda) \geq_Q \frac{\partial}{\partial x} r_k(s_k, h, \lambda, \bar{x}) + \hat{V}_{k+1}(s_{k+1}, \lambda) + \sum_\sigma \frac{\partial V_{k+1}(s_{k+1}, \lambda)}{\partial s^\sigma_{k+1}} \frac{\partial f^\sigma_k(s_k, h_k, \lambda, x)}{\partial x} + \\
&+ \xi_k \left(V_k(s_k, \lambda) - r_k(s_k, h_k, \lambda, \bar{x}) - V_{k+1}(s_{k+1}, \lambda)\right), \\
&\mu \geq_Q \hat{V}_1(s_1, \lambda) + \xi_1 \left(\nu - V_1(s_1, \lambda)\right), \\
&V_N(s_N, \lambda) \geq_Q r_N(s_N, h, \lambda, \bar{x}), \\
&V_k(s_k, \lambda) \geq_Q r_k(s_k, h, \lambda, \bar{x}) + V_{k+1}(f_k(s_k, h_k, \lambda), \lambda), \\
&\nu(\bar{x}) \geq_Q V_1(s_1, \lambda).
\end{aligned} \tag{D1}$$

该问题的优化对象不仅包括 $\hat{V}$，还包括问题 (59) 的极小化解 V。

因此，计算极限 $D^+\nu(\bar{x})$ 的一种基于坐标下降的启发式方法如下：给定$V^{(j)}$ 未扰动问题的一个极小化解，我们求解问题 (66)，从而得到松弛变量 $\xi^{(j)}$。接着，我们求解方程 (D1) 中的问题以求得 $\xi = \xi^{(j)}$，从而得到新的未扰动问题解 $V^{(j+1)}$。从未扰动问题的初始解 $V^{(0)}$ 出发，由此生成问题 (59) 的一系列极小化解 $V_{(1)}V_{(2)}\ldots$。相应的问题 (66) 解序列（其中 $V = V_{(1)}V_{(2)}\ldots$）显然是递减的；如果初始种子 $V^{(0)}$ 足够接近最优解——度，人们会预期它收敛到 $D^+\nu(\bar{x})$。

由于估计 $D^+\nu(\bar{x})$ 需要求解一个非凸优化问题，因此通过坐标下降得到的解可能并非最优。要验证坐标下降是否陷入了局部极小值，一种简单的自洽性检查方法是计算反向极限 $D^-\nu(\bar{x}) := \lim_{\delta_x \to 0^+} {}^{\nu(\bar{x}) - \nu(\bar{x} - \delta|i\rangle)}, \delta x$ 并查看两个量是否相等（如果 $\nu(x)$ 关于 $x = \bar{x}$ 可微，则它们应该相等）。利用方程 (66)、(D1) 的推导来估计 $D^-\nu(\bar{x})$，而非 $D^+\nu(\bar{x})$，并不困难。

[1] A. Wallraff、D. I. Schuster、A. Blais、L. Frunzio、J. Ma- jer、M. H. Devoret、S. M. Girvin 和 R. J. Schoelkopf，《通过色散读出实现对超导量子比特的近乎完美可见度控制》，《物理评论快报》**95**, 060501（2005）。[2] M. Weilenmann、E. A. Aguilar 和 M. Navascu´es，《基于制备博弈框架的量子自适应测量协议分析与优化》，

Nature Communications 12, 10.1038/s41467-021-24658- 9 (2021). [3] S. Geller, D. C. Cole, S. Glancy 和 E. Knill, 《利用自适应序贯观测改进量子态探测》（2022）。[4] M. Navascu´es、S. Pironio 和 A. Ac´ın, 《量子关联集合的界定》, Phys. Rev. Lett. 98, 010401 (2007)。[5] M. Navascu´es、S. Pironio 和 A. Ac´ın, 《表征量子关联集合的半定规划收敛层级》, 《新物理学杂志》10, 073013 (2008)。[6] T. Moroder、J.-D. Bancal、Y.-C. Liang、M. Hofmann 和 O. G¨uhne, 《设备无关的纠缠量化及相关应用》, 《物理评论快报》111, 030501 2013( )。[7] V. Saggio、A. Dimi´c、C. Greganti、L. A. Rozema、P. Walther 和 B. Daki´c, 《实验检测少拷贝多体纠缠》, Nature physics 15, 935 (2019)。[8] A. Paz, *Introduction to probabilistic automata*（学术出版社，1971）。[9] M. O. Rabin, 《概率自动机》, 《信息与控制》6, 230 (1963)。[10] M. Kleinmann、O. G¨uhne、J. R. Portillo、J. rAke Larsson 和 A. Cabello, 《量子情境性的记忆成本》, 《新物理学杂志》13, 113011 (2011)。[11] G. Fagundes 和 M. Kleinmann, 《模拟 Peres–Mermin 情境中的所有量子关联所需的记忆成本》, 《物理学杂志A》50, 325302 (2017)。[12] C. Budroni、G. Fagundes 和 M. Kleinmann, 《时间关联的记忆成本》, 《新物理学杂志》21, 093018 (2019)。[13] C. Budroni、A. Cabello、O. G¨uhne、M. Kleinmann 和 J.-A. Larsson, 《Kochen-Specker 情境性》, 《现代物理评论》94, 045007 (2022)。[14] A. J. P. Garner、Q. Liu、J. Thompson、V. Vedral 和 M. Gu, 《利用量子力学进行随机模拟时可证明的无界记忆优势》, 《新物理学杂志》19, 103009 (2017)。[15] T. J. Elliott 和 M. Gu, 《量子设备在连续时间随机过程模拟中的卓越记忆效率》, 《npj量子信息》4, 1 (2018)。[16] T. J. Elliott、C. Yang、F. C. Binder、A. J. P. Garner、J. Thompson 和 M. Gu, 《利用量子建模实现极端维数缩减》, 《物理评论快报》125, 260501 2020( )。[17] C. Spee, 《利用时间关联认证量子态的纯度》, Phys. Rev. A 102, 012420 (2020)。[18] J. Hoffmann、C. Spee、O. G¨uhne 和 C. Budroni, 《量子比特时间关联的结构》, 《新物理学杂志》20, 102001 (2018)。[19] C. Spee、H. Siebeneich、T. F. Gloger、P. Kaufmann、M. Johanning、M. Kleinmann、C. Wunderlich 和 O. G¨uhne, 《真正的时间关联能够认证量子维数》, 《新物理学杂志》22, 023028 (2020)。[20] C. Spee、C. Budroni 和 O. G¨uhne, 《模拟极端时间关联》, 《新物理学杂志》22, 103037 (2020)。[21] P. Erker、M. T. Mitchison、R. Silva、M. P. Woods、N. Brunner 和 M. Huber, 《自主量子时钟：热力学是否限制了我们的时间测量能力？》, Phys. Rev. X 7 ’ 031022（2017）。

[22] M. P. Woods, R. Silva, G. P¨utz, S. Stupar 和 R. Renner, 《量子时钟比经典时钟更准确》, PRX Quantum 3, 010319 (2022). [23] C. Budroni、G. Vitagliano 和 M. P. Woods, 《非经典时间相关性提升滴答时钟的性能》, Phys. Rev. Research 3, 033051 (2021). [24] L. B. Vieira 和 C. Budroni, 《最简单测量序列中的时间相关性》, Quantum 6, 623 (2022). [25] M. Zurel、C. Okay 和 R. Raussendorf, 《基于量子比特魔态实现通用量子计算的隐变量模型》, 《物理评论快报》125, 260404 (2020). [26] G. Vitagliano 和 C. Budroni, 《Leggett-Garg 宏观实在论与时间相关性》, Phys. Rev. A 107, 040101 (2023). [27] F. G. Brandao、A. W. Harrow、J. R. Lee 和 Y. Peres, 《对抗性假设检验与受限测量的量子 Stein 引理》, 载于 *Proceedings of the 5th conference on Innovations in theoretical computer science* 2014 183 194 ( ) pp. – . [28] Y. Li、V. Y. Tan 和 M. Tomamichel, 《序贯量子假设检验的最优自适应策略》, Communications in Mathematical Physics 392, 993 (2022). [29] H. Gimbert 和 Y. Oualhadj, 《有限词上的概率自动机：可判定与不可判定问题》, 载于 *International Colloquium on Automata Languages and Programming* 2010 527 538 (Springer,) pp. – . [30] D. Elkouss 和 D. P´erez-Garc´ıa, 《记忆效应可能使通信信道的传输能力变得不可计算》, Nature Communications 9, 1 (2018). [31] M. P. Woods、R. Silva 和 J. Oppenheim, 《自主量子机器与有限尺寸时钟》, Annales Henri Poincar´e 20, 125 (2019). [32] Y. Yang、L. Baumg¨artner、R. Silva 和 R. Renner, 《提升量子时钟精度的协议》, arXiv, arXiv:1905.09707 (2019), arXiv:1905.09707. [33] Y. Yang 和 R. Renner, 《时间信号生成的极限》, arXiv, arXiv:2004.07857 (2020), arXiv:2004.07857.[34] E. Schwarzhans、M. P. E. Lock、P. Erker、N. Friis 和 M. Huber, 《自主时间概率集中：时钟装置与热力学第二定律》, Phys. Rev. X 11, 011046 (2021). [35] F. Meier、E. Schwarzhans、P. Erker 和 M. Huber, 《计时装置的基本精度—分辨率权衡》, 《物理评论快报》131, 220201 (2023). [36] R. Silva、N. Nurgalieva 和 H. Wilming, 《量子理论中的滴答时钟》, arXiv, arXiv:2306.01829 (2023), arXiv:2306.01829.[37] A. N. Pearson、Y. Guryanova、P. Erker、E. A. Laird、G. A. D. Briggs、M. Huber 和 N. Ares, 《测量计时的热力学成本》, Phys. Rev. X 11, 021029 2021( ).[38] 选择哪个初始状态并不重要，因为这些选择只相差一个重新标记。[39] S. Gharibian, 《量子可分性问题的强 NP 困难性》, Quantum Information & Computation 10, 343 (2010). [40] I. P. McCulloch, 《无限尺寸密度矩阵重整化群：再探》(2008). [41] M. L. Puterman, *Markov decision processes: discrete stochastic dynamic programming* (John Wiley & Sons ’

2014). [42] J. B. Lasserre、D. Henrion、C. Prieur 和 E. Tr´elat，《通过占据测度和 LMI 松弛实现非线性最优控制》，SIAM 控制与优化杂志 47, 1643 (2008). [43] J. L. Krivine，《有序环》，Journal d'Analyse Math´ematique 12, 307 (1964). [44] J. L. Krivine，《半代数几何中的零点定理与正值定理》，数学年刊 207, 87 (1974). [45] K. Schm¨udgen，《紧半代数集合上的 k-矩问题》，数学年刊 289, 203 (1991). [46] M. Putinar，《紧半代数集合上的正多项式》，印第安纳大学数学杂志 42, 969 (1993). [47] J. B. Lasserre，《多项式全局优化与矩问题》，SIAM 优化杂志 11, 796 (2001). [48] P. Parrilo，《半代数问题的半定规划松弛》，数学规划，B辑 96 (2003). [49] R. Murray、V. Chandrasekaran 和 A. Wierman，《牛顿多胞体与相对熵优化》，Foundations of Computational Mathematics 21, 1703 (2021). [50] M. Dressler 和 R. Murray，《符号项优化的代数视角》(2021). [51] M. ApS, *The MOSEK optimization toolbox for MATLAB manual. Version 9.0.* 2019 ( ).

[52] S. Diamond 和 S. Boyd，《CVXPY：嵌入 Python 的凸优化建模语言》，机器学习研究杂志 17, 1 (2016). [53] B. O'Donoghue、E. Chu、N. Parikh 和 S. Boyd，《SCS：分裂锥求解器，版本 3.2.2》，https://github. com/cvxgrp/scs (2022).[54] 请注意，多项式优化中的变量是多项式的系数 V_k，而不是序贯模型的变量 s_k。[55] J. L¨ofberg，《Yalmip：用于 MATLAB 建模与优化的工具箱》，载于 *Proceedings of the CACSD Conference* 2004 (台北，台湾，).[56] 请注意，SOLVEMOMENT 有时允许直接提取问题的最优解，例如下文的例子。这并不奇怪，因为当 Lasserre 层级在某个有限层级收敛时，可以从矩矩阵中找到多项式变量的最优值。[57]若进一步要求 $P(b = 1|0) = 0$，则可直接解析推导这个上界；加入这一条件不会改变我们的上界。在这种情况下，多项式会简化，检查梯度即可立即得到这些界。[58] 请注意，此处我们将值函数的记号从 $\{V_k\}_k$ 改为 $\{W_k\}_k$，以便与 $L = 3$ 情形区分。[59] 证明 $W_2(s_2, \lambda)$是奖励的上界，与上文 $L = 3$ 情形中的论证类似。[60] 此外，若假设 $P(b = 1|0) = 0$，解析验证这一点会更加直接。[61] K. X. Wei、I. Lauer、S. Srinivasan、N. Sundaresan、D. T. McClure、D. Toyli、D. C. McKay、J. M. Gambetta 和 S. Sheldon，《通过多量子相干验证多体纠缠的 Greenberger-Horne-Zeilinger 态》，Phys. Rev. A 101, 032343 (2020). [62] C. Song、K. Xu、H. Li、Y.-R. Zhang、X. Zhang、W. Liu, Q. Guo, Z. Wang, W. Ren, J. Hao, H. Feng, H. Fan, D. Zheng, D.-W. Wang, H. Wang, 和 S.-Y. Zhu，《生成多达 20 个量子比特的多组分原子薛定谔猫态》，《科学》365, 574 (2019)。[63] A. Omran, H. Levine, A. Keesling, G. Semeghini, T. T. Wang, S. Ebadi, H. Bernien, A. S. Zibrov, H. Pichler, S. Choi, J. Cui, M. Rossignolo, P. Rembold, S. Montangero, T. Calarco, M. Endres, M. Greiner, V. Vuleti´c, 和 M. D. Lukin，《里德伯原子阵列中薛定谔猫态的生成与操控》，《科学》365, 570 (2019)。[64] H.-Y. Huang, R. Kueng, 和 J. Preskill，《仅凭极少测量预测量子系统的诸多性质》，《自然·物理》16, 1050 (2020)。[65] O. G¨uhne 和 G. T´oth，《纠缠检测》，Physics Reports 474, 1 (2009)。[66] N. D. Mermin，《宏观上不同的态叠加中的极端量子纠缠》，《物理评论快报》65, 1838 (1990)。[67] M. Boyer，《经典获胜概率趋于 0 的扩展 GHZ 多玩家博弈》(2004), arXiv:quant-ph/0408090 [quant-ph].[68] 由于实验轮次数量较少，我们使用均值而非 [64] 中推荐的"均值的中位数"来估计影子协议中的 GHZ 保真度。[69] S. T. Flammia 和 Y.-K. Liu，《通过少量泡利测量直接估计保真度》，Phys. Rev. Lett. 106, 230501 2011( )。[70] [30]中的陈述更为一般，因为该引理是在额外要求自动机可重置的情况下证明的。然而，我们的应用并不需要这一性质，因此在下文的陈述中将其省略。[71] 请注意，这项限制并非必要。具体而言，只要我们能用相应有界变量 α 的多项式来表述类似的约束，也可以使用类似方法处理 f_k、r_k 依赖于 k的情形。[72] 出于数值稳定性的考虑，建议同时限制 A、B、C 等可能取值的范围。[73] 为了进一步支持这样的猜想：MOSEK 报告的值接近半定规划的实际解，我们考察了求解器输出的值函数 $\{W_{-j}\}_{j=0}^{3}$、W^1、W^2，然后使用 Lasserre 层级验证关系式 (52) 成立。我们只在最后两个递推关系中发现了极小的正性违反（量级为 -10^{-5}）。[74] D. P. Kingma 和 J. Ba，《Adam：一种随机优化方法》(2017), arXiv:1412.6980 [cs.LG]。[75] S. Bravyi 和 A. Kitaev，《使用理想 Clifford 门和噪声辅助量子比特进行通用量子计算》，Phys. Rev. A 71, 022316 (2005)。[76] V. Veitch, S. A. H. Mousavian, D. Gottesman, 和 J. Emerson，《稳定子量子计算的资源理论》，New Journal of Physics 16, 013009 (2014)。[77] 式 (13) 的对偶问题似乎没有唯一解，因为我们发现使用式 (72) 会导致半定规划不可行。[78] S. Aaronson，《量子态的影子层析》，载于 *Proceedings of the 50th Annual ACM SIGACT symposium on theory of computing* 2018 325 338 ( ) 第 – 页。[79] 更准确地说，正多项式 $p(z)$ 存在平方和分解的一个充分条件是

对于某个 $K > 0$，多项式 $K - \sum_i z_i^2$ 存在平方和分解。反过来，这意味着 Z 有界。[80]这种对更常见的 Lasserre-Parrilo 层级的改造依赖于 Schmuedgen 正定性定理 [45]

相反，这里采用该方法，以便在后续讨论的问题中获得更好的数值性能。[81] 为方便起见，我们在此选择第一项和第三项，因为我们进行的是泡利测量，因此可以更直接地建立运动方程。