需要在时间窗口内生成状态的量子协议分析工具

BETHANY DAVIES[1,2,3],THOMAS BEAUCHAMP[1,2,3] GAYANE VARDOYAN[1,3], 和 STEPHANIE WEHNER。[1,2,3]

[1] QuTech，代尔夫特理工大学，Lorentzweg 1，2628 CJ 代尔夫特，荷兰 卡夫利纳米科学研究所，代尔夫特理工大学，Lorentzweg 1，
[2] 2628 CJ 代尔夫特，荷兰 量子计算机科学，EEMCS，代尔夫特理工大学，Lorentzweg 1，2628 CJ 代尔夫特，荷兰
[3]

C通讯作者：Bethany Davies（电子邮箱：b.j.davies@tudelft.nl）、Stephanie Wehner（电子邮箱：s.d.c.wehner@tudelft.nl）。

arXiv:2304.12673v1 [quant-ph] 25 Apr 2023

摘要 量子协议通常要求同时具备一定数量的量子资源态。一个重要的例子是量子网络协议，这类协议需要一定数量的纠缠对。在本文中，我们考虑这样一种情形：某个过程以一定概率生成量子资源态 p，并在每个时间步将其存储于受时变噪声影响的量子存储器中。为了维持应用所需的足够质量，每个资源态在存储 w 个时间步后将从存储器中丢弃。设 s 为某协议所需的目标资源态数量。我们刻画了在时间窗口 $X_{(w,s)}$ 内生成 s 个状态后，量子资源态年龄的概率分布 w。结合时变噪声模型，该分布的信息可以用于计算 s 量子资源的保真度统计。我们还给出了等待时间$\tau_{(w,s)}$ 的 s 阶矩和二阶矩的精确解，其中等待时间指在时间窗口 w内生成 $\mathbb{E}$个$\tau_{(w,s)}$资源所需的时间，这为协议速率提供了信息。由于难以获得描述期望等待时间的统计量以及分布的一般闭式表达式，我们提出了两项新结果，以辅助在特定参数范围内进行计算。本文介绍的方法可用于分析和优化量子协议的执行。具体而言，我们以盲量子计算（BQC）协议为例，说明如何利用这些方法推断和，从而优化协议成功执行的速率。

索引词 量子网络、性能分析、扫描统计

I. 引言

I量子计算和量子网络

p协议通常要求同时具备一定数量的高

n 质量量子资源态。在量子网络领域，这类资源态通常是量子比特纠缠对，而协议的执行（例如纠缠蒸馏）以及许多量子网络应用，都要求同时具备多个纠缠对 [1]–[3]。资源态的另一个例子可见于量子计算领域，其中魔态蒸馏依赖于多个初始魔态的存在 [4]。

在这里，我们研究使用概率过程生成资源态的场景。在每个时间步中，该过程以 p 的概率成功生成一个资源态。如果状态准备成功，它会立即存储在受时变噪声影响的量子存储器中。该过程会重复进行，直到协议所需的全部 s 个状态都存储在存储器中。这种场景在量子联网和（光子）量子计算中十分普遍。一个典型例子是预 heralded纠缠生成 [5], [6]，如今量子网络中通常会使用这种方法（例如参见 [7], [8]）。

如果噪声具有时间依赖性，这意味着当一个状态被置于量子存储器中时，其质量会随时间下降。因此在实际应用中，为了传输质量足够高的状态，通常会规定一个包含 w 个时间步的窗口，在此窗口内必须生成所有 s 状态。如果这些状态在所需窗口内生成，则其质量足以使应用成功。否则，这些状态通常会被丢弃（见图1）。在量子中继协议的语境下，这样的窗口大小通常也称为“截止时间”，而对多个节点进行分析通常并非易事 [9]–[14]。如果一个协议

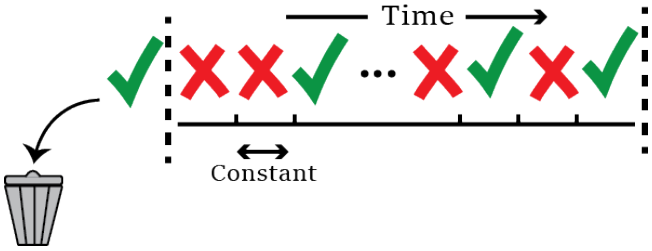

图1. 设置。在每个时间步中，概率过程都会生成一个资源态，其中 p 表示成功概率（勾号），而 $1-p$ 表示失败概率（叉号）。资源态生成后，会立即放入受时变噪声影响的量子存储器中。为确保状态具有足够的质量，能够用于量子协议，超过特定时间窗口 w （即时间步数）年限的状态将被丢弃（箱）。

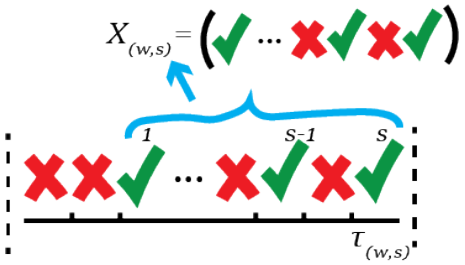

图2。 结束模式。在首次出现 $\tau_{(w,s)}$ 当一个包含 w个时间步的窗口包含 s 次成功时，我们关注每条 s 链路是在多久以前生成的。这使我们能够量化相应资源态的质量。有关这些 s 资源态生成时间的信息包含在结束模式 $X_{(w,s)}$中。

要求 s 量子资源状态同时具有足够高的质量，这就转化为要求在 w 个时间步的窗口内发生 s次成功的生成事件。

在分析依赖于此类资源态生成的协议性能时，我们关注若干性能指标。例如，我们可能会关注执行协议的速率、整个量子协议成功的概率，或者一种综合指标，即单位时间内量子协议成功执行的次数。为了理解并优化这些性能指标，我们需要了解与系统制备协议所需资源态的能力相关的若干量。

首先，可以考虑等待时间 $\tau_{(w,s)}$，即在长度为 w 个时间步的窗口内获得 s 次成功所需的时间。值得注意的是，对于固定参数（w，s，p），这也能提供有关多次执行时协议执行速率的信息。其次，我们考察结束模式 $X_{(w,s)}$（见图2），它包含时间 $\tau_{(w,s)}$ 时 s 个量子资源的年龄。结合退相干模型，可以计算出最后一个状态生成后资源的质量（保真度）；此时即可执行量子协议。

本工作的目标是提供可用于分析给定量子协议在特定 w、s 和 p 取值下性能的工具，并选择这些参数的组合以优化其性能。

A. 结果

我们的主要贡献总结如下 .

- 对于 w、s 和 p 的所有取值，我们给出了 $\tau_{(w,\ s)}$ 的一阶矩和二阶矩公式，以及 $X_{(w,\ s)}$ 的完整分布。对于 $(w,\ s)=(\infty,\ s)$，这些结果具有简单的闭式形式；对于 $(w,\ s)=(w,\ 2)$，情况同样如此。对于 $(w,\ s)$ 的所有其他取值，我们给出一般形式的公式，这些公式构成一个可通过数值方法求解的线性系统。该系统的维数随 w^{s-1} 增长。因此，对于较大的 w 和 s，很难从这些系统中获得闭式形式的表达式。
- 我们提供了一种高效方法，用于确定 w 和 p 的取值范围，使得 $\mathbb{E}(\tau_{(w,s)})$ 和 $X_{(w,s)}$ 可以由 $\mathbb{E}(\tau_{(\infty,s)})$ 和 $X_{(\infty,s)}$ 以任意精度近似。在实际应用中，这使我们能够快速计算窗口大小的阈值，使得进一步增大 w 不会改善协议速率。此外，对于适当的参数范围，这种近似是理想的，因为如上所述，用于求解期望等待时间 $\mathbb{E}(\tau_{(w,s)})$ 和 $X_{(w,s)}$ 的线性系统的维度随 w 和 s 增长。相比之下，在 $w=\infty$ 的情况下，可以为相应的量找到简单的闭式表达式。
- 我们刻画了在成功概率较小的极限下 $\mathbb{E}(\tau_{(w,s)})$和 $X_{(w,s)}$的行为。特别地，我们证明了当 $p\to 0$时，$\mathbb{E}(\tau_{(w,s)})$按 p^{-s}缩放，并且 $X_{(w,s)}$ 的分布趋于均匀。无需进行（可能耗时较长的）数值计算，这一结果也有助于直观理解资源生成成功概率较小时量子应用的性能。
- 我们展示了如何在实践中使用这些方法。我们考虑一个 [15]盲量子计算协议。在我们的模型中，量子比特从客户端设备传输到服务器设备时会消耗纠缠。该模型包含由不完美纠缠链路和存储器退相干引起的噪声。对于涉及四个量子比特计算的设置，我们举例说明如何使用前几节介绍的方法，选择能够优化协议速率的架构参数。

B. 相关工作

为获得我们的结果，我们借鉴了数学文献中称为扫描统计的方法。扫描统计通常关注一系列随机事件中的模式和簇。这一领域融合了数学多个不同分支中的技术。在量子语境下，该问题与其他

领域的问题不同之处在于关注结束模式分布。因此，在本工作中，我们采用鞅方法，因为这使我们能够同时获得 $\mathbb{E}(\tau_{(w,s)})$ 以及 $X_{(w,s)}$ [16] 的分布。利用嵌入式马尔可夫链 [17], 也可以得到相同的量，但我们在此继续采用鞅方法；首先是因为所得公式的维度更小，其次是因为该公式具有规则结构，使我们能够推导出小 p 情况下的渐近结果，而这一参数范围与实验相关。我们注意到，还存在其他方法可以获得 $\mathbb{E}(\tau_{(w,s)})$，原则上也可以获得 $\tau_{(w,s)}$ 的完整分布——例如参见 [18] 或 [19]，其中给出了获得 $\tau_{(w,s)}$ 的概率生成函数的公式。然而，据我们所知，这些方法同样会导致规模较大的方程组，而且无法给出结束模式分布。与 $\tau_{(w,s)}$ 密切相关的其他量已在扫描统计文献中得到深入研究，这些研究也可能与量子领域相关。例如，已有关于 $\mathbb{P}(\tau_{(w,s)} \leq n)$ 的多种界和近似（综述可参见 [20] ），这些结果可能有助于在量子网络调度中为纠缠生成分配时间。相比之下，在本工作中，我们关注 $\mathbb{E}(\tau_{(w,s)})$ 和 $X_{(w,s)}$ 的行为，以及它们对量子协议性能的影响。据我们所知，本工作首次刻画了某些参数范围下结束模式分布的行为，并展示了将扫描统计结果应用于量子协议的一个具体示例。

C. 概述

本文其余部分的组织如下。在第二节中，正式定义 $\tau_{(w,s)}$ 和 $X_{(w,s)}$。在第三节 A 和第三节 B 中，给出$\tau_{(w,s)}$ 的一阶矩和二阶矩以及 $X_{(w,s)}$的分布的公式。在第三节 C 和第三节 D 中，给出有助于理解和近似这些量的结果。在第四节 A 中，概述第三节结果的表现和实际相关性，具体考察 $\mathbb{E}$ （$\tau_{(w,s)}$）。在第四节 B 中，给出一个示例，说明如何利用第三节的结果选择能够优化盲量子计算协议性能的架构参数。最后，在第五节中总结进一步的研究方向。

II. 预备知识

我们将量子资源生成尝试视为一系列独立同分布的伯努利试验（Z_i）$_{i=1}^{\infty}$，成功概率为$p = \mathbb{P}$（$Z_1 = 1$）> 0。因此，如果某个协议要求 $s \leq w$个量子资源同时存在，那么完成该应用所需的时间取决于在大小为 w的窗口内获得 s 次成功所需的等待时间 $\tau_{(w,s)}$。我们还关注结束模式 $X_{(w,s)}$，它使整个过程得以完成，因为它包含了时刻$\tau_{(w,s)}$存在的 s 个量子资源的年龄。我们将可能的结束模式集合记作 $\Omega(w, s)$。该集合包含扫描窗口内 s 次成功的所有可能配置，因此 $X_{(w,s)} \in \Omega(w, s)$。图2直观地展示了某个结束模式如何实现过程的结束。更具体地，我们定义

$$\Omega_l(s) := \{x \in \{0,1\}^l : x_1 = x_l = 1 \wedge \sum_{i=1}^{l} x_i = s\} \quad (1)$$

定义为所有长度为l的二进制字符串 $x =$（x_1，.....，x_l）的集合，其中包含 s 次成功，且其中两次分别出现在字符串的两端。于是，

$$\Omega(w, s) := \bigcup_{l=s}^{w} \Omega_l(s) \quad (2)$$

这是结束模式的集合。集合 Ω（w，s）可以理解为包含所有在不超过 w 个时间步内产生的 s 次成功所形成的簇。注意，可能的结束模式数量为

$$|\Omega(w, s)| = \binom{w-1}{s-1}. \quad (3)$$

为说明这一点，请注意，$\Omega(w, s)$ 中的每个结束模式，都唯一对应于一种结束情景，其中 s 成功次数分布在 w 时间步的窗口内。由于最终的量子资源必须始终在最近的时间步准备完成，因此它是固定的；于是只需将剩余的 $s-1$ 成功次数分布在 $w-1$ 个时间步内，这意味着可能的结束模式数量受限于 (3)。等待时间 $\tau_{(w,s)}$ 随后定义为

$$\tau_{(w,s)} := \min_{x \in \Omega(w,s)} \{\tau_x\}, \quad (4)$$

也就是说，这是我们在伯努利试验序列中看到第一个结束模式之前所经历的时间。在这里，τ_x 是首次看到某个特定结束模式 x 所需的时间，因此对于 $x \in \Omega_l(s) \subset \Omega(w, s)$

$$\tau_x := \min\{t : (Z_{t-l+1}, Z_{t-l+2}, ..., Z_t) = x\}. \quad (5)$$

我们注意到，$\tau_{(w,s)}$ 是定义良好的，因为它的上界是一个几何随机变量（参见附录 B-1）。此外，$\tau_{(w,s)}$ 与 $X_{(w,s)}$ 的分布之间还存在如下关系

$$\mathbb{P}(X_{(w,s)} = x) = \mathbb{P}(\tau_{(w,s)} = \tau_x), \quad (6)$$

回顾一下，$X_{(w,s)}$ 取完成该过程的结束模式的值。由于 $\Omega(w, s)$ 中没有任何元素包含另一个元素，因此没有两个结束模式能同时实现过程的结束，所以 $X_{(w,s)}$ 是定义良好的。

III. 公式与近似

在接下来的两节中，我们给出 $\tau_{(w,s)}$ 的一阶矩和二阶矩的精确解，以及 $X_{(w,s)}$ 的完整分布。对于 w 和 s 的所有可能取值，我们都提供相应公式。在第三节-C中，我们研究当 w 较大时对这些解的近似。在第三节-D中，我们刻画 p 较小时的解的行为。

A. 无限窗口

这里，我们考虑不丢弃任何资源态的情况（或等价地，当 $w = \infty$ 时），并给出 $\tau_{(\infty,s)}$ 的一阶矩和二阶矩以及 $X_{(\infty,s)}$ 的分布。这为问题提供了一个有用的初步研究，有助于理解 w 较大但有限时的情况。

当不丢弃任何状态时，看到所有成功次数所需的等待时间简单地变为 s 个参数为 p 的独立同分布几何随机变量之和。这称为负二项分布，其精确分布为

$$\mathbb{P}(\tau_{(\infty,s)} = n) = \binom{n-1}{s-1}(1-p)^{n-s}p^s \tag{7}$$

且期望为

$$\mathbb{E}(\tau_{(\infty,s)}) = \frac{s}{p}. \tag{8}$$

注意，对于 $w' > w$，始终有 $\tau_{(w',s)} \leq \tau_{(w,s)}$，因此

$$\mathbb{E}(\tau_{(w',s)}) \leq \mathbb{E}(\tau_{(w,s)}), \text{ for } w' > w. \tag{9}$$

特别地，有限 w 的等待时间总是大于或等于无限窗口情形。于是，式（8）给出了一个关于 s 和 p 的简单下界

$$\mathbb{E}(\tau_{(w,s)}) \geq \frac{s}{p}. \tag{10}$$

$\tau_{(\infty,s)}$ 的方差为

$$\text{Var}(\tau_{(\infty,s)}) = \frac{s \cdot (1-p)}{p^2}, \tag{11}$$

由此可见，标准差与 p成反比。

还可以推导出 $X_{(\infty,s)}$分布的一个简单表达式。对于一个二进制字符串 $x \in \Omega_l$，它属于（现在是无限的）结束模式集合$\Omega(\infty, s)$,

$$\mathbb{P}(X_{(\infty,s)} = x) = (1-p)^{l-s}p^{s-1}, \tag{12}$$

这一点可以通过考察首次成功生成后生成 B 的其余 $l-1$ 个条目的概率来说明。我们看到，当窗口大小为无限大时，生成长度相同的结束模式的概率是常数。

B. 有限窗口

1) $s = 2$

当 $s = 2$时，可以再次推导出$\tau_{(w,s)}$ 的一阶矩和二阶矩以及 $X_{(w,s)}$的分布的闭式解。下面给出$\mathbb{E}(\tau_{(w,s)})$和结束模式分布的公式。

在这种情况下，结束模式由两个状态之间的时间决定，即 $|\Omega_l(2)| = 1$。我们将资源生成过程分为两部分：第一状态的生成和第二状态的生成。当内存中没有存储状态时，第一条链接的生成就会发生。这不受时间窗口限制，其生成时间服从参数为p的几何分布。要完成该过程，第二状态必须在第一条链接生成后的 $w-1$ 个时间步内生成。当该过程完成时，两个状态之间的时间是在这一事件条件下的几何分布，该事件发生的概率为 $1-(1-p)^{w-1}$。然后，令 $L \in \{1, ..., w-1\}$ 表示在第一状态生成后为生成第二状态所进行的尝试次数，

$$\mathbb{P}(L = n) = \frac{(1-p)^{n-1}p}{1-(1-p)^{w-1}}, \tag{13}$$

这给出了完整的结束模式分布，其中 $L = n$对应于 $X_{(w,s)} \in \Omega_{n+1}(2)$。

现在，令 M 为流程结束前必须生成第一状态的次数。由于这取决于第二状态是否在时间窗口内成功生成，因此有

$$M \sim \text{Geom}\left(1-(1-p)^{w-1}\right). \tag{14}$$

总时间可用 M和 L 表示为

$$\tau_{(w,2)} = \sum_{j=1}^{M} T_j + (M-1)(w-1) + L, \tag{15}$$

其中，随机变量 $T_j \sim \text{Geom}(p)$描述生成第一状态所需的尝试次数。现在，如附录 A 所示，

$$\mathbb{E}\left(\sum_{j=1}^{M} T_j\right) = \mathbb{E}(M)\mathbb{E}(T_1) = \frac{1}{(1-(1-p)^{w-1})} \cdot \frac{1}{p}, \tag{16}$$

and

$$\mathbb{E}(L) = \frac{1-(1-p)^w - wp(1-p)^{w-1}}{p(1-(1-p)^{w-1})}. \tag{17}$$

期望等待时间可计算为

$$\mathbb{E}(\tau_{(w,2)}) = \mathbb{E}(M)\mathbb{E}(T_1) + (\mathbb{E}(M)-1)(w-1) + \mathbb{E}(L), \tag{18}$$

由此可得

$$\mathbb{E}(\tau_{(w,2)}) = \frac{1}{p} + \frac{1}{p(1-(1-p)^{w-1})}. \tag{19}$$

利用式 (15) 也可计算 $\tau_{(w,2)}$ 的方差。计算过程见附录 A。

2) $s > 2$

现在，我们给出一个精确计算有限w的 $\mathbb{E}(\tau_{(w,s)})$ 和完整分布 $\{\mathbb{P}(X_{(w,s)} = x)$ 的公式： $x \in \Omega(w,s)\}$。该公式采用 [16],中的方法推导而来，该方法运用了鞅。为完整起见，我们在附录 B-2 中概述了推导过程，并引入赌博类比以帮助理解。所得公式的形式是一个大小为 $|\Omega(w,s)| + 1$ 的线性方程组，可以精确求解。定义该线性方程组的每个矩阵元素都可以简单而高效地计算。此外，在附录 B-4 中，我们给出了 $\tau_{(w,s)}$ 的二阶矩公式，该公式现在涉及两个大小为

$|\Omega(w,s)|$ 的线性方程组。其推导同样使用了鞅方法，因此我们将其称为 [21]。随后，可以利用 $\tau_{(w,s)}$ 的二阶矩计算 $\tau_{(w,s)}$ 的方差和标准差。

在给出第一个公式之前，我们先介绍一些记号。我们定义一个函数 $*$，将两个二进制字符串 $x = (x_1, ..., x_k)$ 和 $y = (y_1, ..., y_m)$ 映射为一个标量值，其定义为

$$x * y := \sum_{j=1}^{\min(k,m)} \left(\prod_{i=1}^{j} \delta_{(x_i, y_{m-j+i})} \right), \tag{20}$$

其中，对于 $a,\ b \in \{0,1\}$，量 $\delta_{a,\ b}$ 定义为

$$\delta_{(a,b)} = \begin{cases} \frac{1}{p_a} \text{ if } a = b; \\ 0, \text{ otherwise,} \end{cases} \tag{21}$$

其中 $p_1 := p$ 且 $p_0 := 1 - p$。由 (20) 可知，$x * y$ 的值是通过比较 x 和 y 中连续子字符串的重叠情况得到的。如果两个子字符串完全匹配，则将对应项纳入求和，并根据伯努利参数 p 对其加权。通俗地说，$x * y$ 衡量的是 x 和 y 的结构有多相似。下面给出一个简单示例，说明 $*$ 的作用。回顾 (1)，我们考察 $*$ 对两个结束模式的作用。令 $s = 3$ 和 $w \geq 7$，假设 $x = (1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1)$ 且 $y = (1,\ 0,\ 0,\ 0,\ 1,\ 1)$。计算 (20) 得到

$$x * y = \frac{1}{p_1} + 0 + 0 + 0 + \frac{1}{p_1^2} \cdot \frac{1}{p_0^3} + 0 = \frac{1}{p_1} + \frac{1}{p^2 p_0^3}.$$

由于 $\Omega(w,\ s)$ 中的所有元素都以一次成功开始并结束，因此对于任意一对结束模式，都会出现相同的首项 $1/p$。是否存在高阶项取决于连续子字符串的重叠情况。特别是，对于两个结束模式 $x,\ y \in \Omega(w,\ s)$，量 $x * y$ 为 $1/p^s$ 阶，当且仅当 $x = y$。

有了这些定义，我们现在给出期望等待时间和结束模式分布的公式。

定理 1。令 $N := |\Omega(w,s)|$。将结束模式枚举为 $\Omega(w,s) \equiv \{x^{(i)} :\ i = 1, ..., N\}$，令

$$\vec{v} = \begin{pmatrix} \mathbb{E}(\tau_{(w,s)}) \\ \mathbb{P}\left(X = x^{(1)}\right) \\ \mathbb{P}\left(X = x^{(2)}\right) \\ \vdots \\ \vdots \\ \mathbb{P}\left(X = x^{(N)}\right) \end{pmatrix}. \tag{22}$$

Then

$$A\vec{v} = \vec{e_1}, \tag{23}$$

其中 $\vec{e_1} := (1, 0, ..., 0)^T$ 是一个长度为 $N+1$ 的向量，并且

$$A := \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ -1 & x^{(1)} * x^{(1)} & x^{(1)} * x^{(2)} & \cdots & x^{(1)} * x^{(N)} \\ -1 & x^{(2)} * x^{(1)} & x^{(2)} * x^{(1)} & \cdots & x^{(2)} * x^{(N)} \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & \vdots \\ -1 & x^{(N)} * x^{(1)} & \cdots & & x^{(N)} * x^{(N)} \end{pmatrix}. \tag{24}$$

矩阵 A 可逆，因为 $\Omega(w,\ s)$ 中没有任何元素包含另一个 [16]。因此，$\vec{v}$ 的解始终存在且唯一。矩阵 A 完全由成功概率 p 以及参数 w 和 s 确定。如上所述，删除首行和首列后得到的子矩阵中，每个元素都大于或等于 $1/p$。不等于该值的元素含有关于 $1/p$ 的高阶项，这是因为与这些元素的行、列索引相对应的结束模式之间存在更大的重叠。$1/p$ 中最高次幂对应的元素恰好是对角元素，其阶数为 s，因为一个字符串与自身完全重叠，且包含 s 次成功。原则上，可以通过直接求逆 A，将 $\vec{v}$ 的解解析地表示为 p 的函数。注意，系统维数为 $|\Omega(w,\ s)| + 1 = \mathcal{O}(w^{s-1})$，因此当 w 和 s 较大时，实际计算会十分繁重。在接下来的章节中，我们将推导有助于理解和计算相应结果的结论，分别针对两个特征状态：w 较大和 p 较小。

C. 采用无限窗口进行近似

现在，人们可能会问：要使近似 $w = \infty$ 足够准确，窗口大小必须达到多大？由于结果中关于 $\tau_{(\infty,s)}$ 和 $X_{(\infty,s)}$ 的分布具有简单的解析形式（如第三节-A 所示），这是很有意义的。这与第三节-B 中针对有限 w 情况所给出的解形成对比，后者随 w 和 s 变化。当窗口大小已经使该过程达到“饱和”时，近似便成立，此时增大窗口大小不会为速率带来任何显著改善。或者，当 $\mathbb{P}(\tau_{(w,s)} > w)$ 较小时，该近似也会变得准确。以下定理将这一直觉形式化。

定理2。令 $\tau_{(w,s)}$ 表示在 w-窗口中获得 s 成功次数所需的等待时间。令 $X_{(w,s)}$ 表示相应的结束模式。令 p 表示每次试验的成功概率。令 $\epsilon(w、\ s、\ p) := \mathbb{P}(\tau_{(w,s)} > w)$。假设 $0 < p < 1$ 且 $w < \infty$。则

$$\frac{\mathbb{E}(\tau_{(w,s)}) - \mathbb{E}(\tau_{(\infty,s)})}{\mathbb{E}(\tau_{(w,s)})} < \epsilon(w,s,p) \tag{25}$$

and

$$\sum_{x\in\Omega(\infty,s)} |\mathbb{P}(X_{(w,s)}=x) - \mathbb{P}(X_{(\infty,s)}=x)| < 2\epsilon(w,s,p). \tag{26}$$

现在我们来计算 ϵ（w、 s、 p）。回顾关于$\tau_{(\infty,s)}$的分布的恒等式（7），可得

$$\mathbb{P}(\tau_{(w,s)} > w) = \mathbb{P}(\tau_{(\infty,s)} > w) \tag{27}$$

$$= \sum_{n=w+1}^{\infty} \binom{n-1}{s-1}(1-p)^{n-s}p^s. \tag{28}$$

为了计算 (25) 的右侧，将其改写为有限和会比较方便，下面的引理给出了这种改写。证明见附录 C-1。

引理 1. 设 $\tau_{(w,s)}$ 为如 *(4)* 中所定义的、在 w 窗口中获得 s 次成功所需的等待时间。假设 $0 < p < 1$ 且 $w < \infty$。那么

$$\mathbb{P}(\tau_{(w,s)} > w) = \sum_{i=0}^{s-1} \binom{w}{i}(1-p)^{w-i}p^i. \tag{29}$$

当 s 为常数时，这个和易于计算且效率很高，随后可用来找出一段 w 范围，使得两个期望彼此接近。例如，若想计算 $\mathbb{E}(\tau_{(w,s)})$，而事实上 w 足够大，以至于可以合理地用 $\mathbb{E}(\tau_{(\infty,s)}) = s/p$ 近似，那么可用以下方法避免求解大型方程组。给定所需的误差 δ，可以快速计算

$$w^* = \min\{w : \epsilon(w,s,p) < \delta\}. \tag{30}$$

那么，对于所有 $w \geq w^*$，都可以用 $\mathbb{E}(\tau_{(\infty,s)}) = s/p$ 近似 $\mathbb{E}(\tau_{(w,s)})$，精度约为 δ。结束模式分布也可以采用相同的方法：如果想求某个保真度量 $F(X_{(w,s)})$ 的期望，也可以用 $\mathbb{E}(F(X_{(\infty,s)}))$ 以相同精度近似 $\mathbb{E}(F(X_{(w,s)}))$。

D. 期望的渐近行为

由式 (9) 可知，$\mathbb{E}(\tau_{(w,s)})$ 的一个上界为 $\mathbb{E}(\tau_{(s,s)})$，它可以写成简单的解析形式。在 $w = s$ 的情形下，只有一个结束模式 x，对应于连续 s 次成功的情形。因此，由式 (23) 可得

$$\mathbb{E}(\tau_{(s,s)}) = x * x = \sum_{j=1}^{s} \frac{1}{p^j} = \frac{1/p^s - 1}{1-p}, \tag{31}$$

对于较小的 p，满足 $\mathbb{E}(\tau_{(s,s)}) \sim 1/p^s$。相比之下，由(8)可知，$w = \infty$ 的期望的标度与 p成反比。此外，根据(24)中给出的 A 的形式，$\vec{v}$ 的所有元素都将是 $1/p$ 的多项式之比。考察 $\vec{v}$的第一个分量，即等待时间期望，这说明存在某个整数值 $\alpha_s(w)$，它主导了较小 p下的标度，因此

$$\mathbb{E}(\tau_{(w,s)}) \sim \frac{c(w,s)}{p^{\alpha_s(w)}}, \tag{32}$$

其中，$c(w,\ s)$ 是一个常数。现在，回想式 (9) 中 $\mathbb{E}(\tau_{(w,s)})$ 是关于 w 的递减函数，因此我们预计 $\alpha_s(w)$ 也具有同样的性质，它满足 $\alpha_s(s) = s$ 且 $\alpha_s(\infty) =1$。下文将证明，对于 $w < \infty$，$\alpha_s(w)$ 始终等于 s，并推导出标度因子 $c(w,\ s)$。

定理3。设 $\tau_{(w,s)}$ 为式 *(4)* 中定义的、在 w 窗口内获得 s 次成功所需的等待时间。设 $X_{(w,s)}$ 为相应的结束模式。设 p 为该过程的成功概率。那么，在极限 $p \to 0$ 下，

$$\mathbb{E}\left(\tau_{(w,s)}\right) \sim \frac{1}{|\Omega(w,s)|p^s}, \tag{33}$$

以及对于所有 $x \in \Omega(w,s)$

$$\mathbb{P}(X_{(w,s)} = x) \to \frac{1}{|\Omega(w,s)|} \tag{34}$$

其中 $|\Omega(w,s)| = \binom{w-1}{s-1}$ 是可能的结束模式数量。

定理3的证明见附录C-2。量化式（33）和（34）的收敛速度是一个有趣的未来研究方向。

作为对（34）的直观理解，请注意，当 p非常小时，在结束模式之前出现 w 次失败的概率很高。在这种情况下，结束模式分布等价于给定我们在 w次尝试中成功时的结束模式分布；当 p趋近于零时，该分布收敛于均匀分布。

定理2和定理3所描述的行为，可以分别看作该问题在 p较小和较大情形下的两种极限行为。特别是，我们预计定理1给出的公式在这两种情形下都不适用，即当 p 既不够小、也不够大，无法应用任一近似时。此外，需要注意的是，这种情形将取决于 w 和 s的选择。

IV. 图示与应用

我们预计，上述各节所介绍的方法将有助于为量子协议选择最优的窗口大小。为此，我们首先对 $\mathbb{E}(\tau_{(w,s)})$ 的行为进行更为详细的分析。随后，我们将演示如何利用这些方法优化盲量子计算协议的性能。

A. 图示

我们以 $s = 4$ 为例，展示期望等待时间的特征性行为。根据我们的研究，对于 s 的其他取值，所得解呈现出相同的定性行为。$s = 4$ 的值足够小，因此

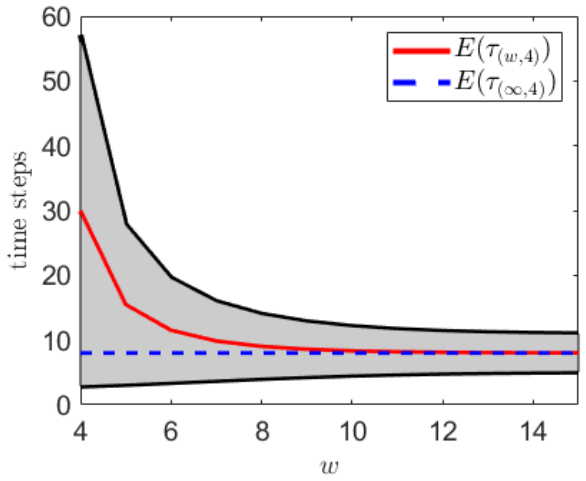

图3。 如何 $\mathbb{E}(\tau_{(w,4)})$ 随 w变化。我们看到， $\mathbb{E}(\tau_{(w,4)})$ （红线）收敛至下界 $\mathbb{E}(\tau_{(\infty,4)}) = 4/p$ （蓝线），当 w 变大时。灰色区域表示$\tau_{(w,4)}$ 高于和低于其期望值一个标准差的范围（当 $w < \infty$时）。所有量的计算均采用成功概率 $p = 0.5$。

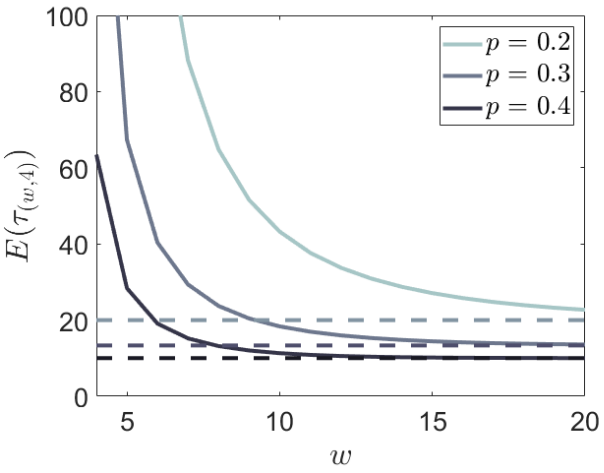

图4。 如何 $\mathbb{E}(\tau_{(w,4)})$ 随 w 和 p变化。我们看到，对于较大的 p， $\mathbb{E}(\tau_{(w,4)})$ （实线）以更高的速率趋近下界 $\mathbb{E}(\tau_{(\infty,4)}) = 4/p$ （虚线）。

该问题的复杂度不会大到无法在笔记本电脑上求解。

在图3中， $\mathbb{E}(\tau_{(w,4)})$ 绘制为关于 w 的函数，成功概率设为 $p = 0.5$。我们注意到其收敛至 $w = \infty$ 下界。灰色区域表示高于和低于期望值一个标准差的范围。还需注意，标准差也预期会收敛至 $\tau_{(\infty,4)}$ 的标准差，其闭式形式由式（11）给出。

在图4中， $\mathbb{E}(\tau_{(w,4)})$再次绘制为关于 w的函数，但这次取成功概率的三个不同值。每种情况下，解都再次趋近于相应的$w = \infty$ 下界。每条曲线都从 $\mathbb{E}(\tau_{(4,4)}) = (1/p^s - 1)/(1-p)$开始，对应于 $w = s$，并收敛

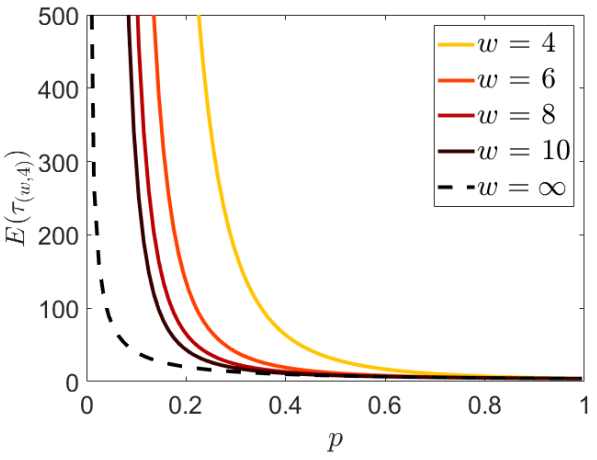

图 5。 我们考察 $\mathbb{E}(\tau_{(w,4)})$ 随 p的变化。可以看到， $\mathbb{E}(\tau_{(w,4)})$ （实线）展示了倒数缩放关系，即当 $p \to 0$时，如定理3所概括。这一结果收敛于 $\mathbb{E}(\tau_{(w,4)})$ （虚线）。该图通过将 p 离散化为 100 个点，并在范围 (0,1)内均匀间隔取点得到。

到 $w = \infty$ 极限。这种收敛是一个重要特征，因为当 w 增加到一定程度后，协议速率便不会显著提升。正如直觉所料， p越大，收敛就越快，因为增大窗口大小能够更轻易地使问题趋于饱和。为量化这一点，我们可以采用III-C节中的论证。例如，将期望的误差范围设为2%，定义

$$w^* = \min\{w : \epsilon(w,s,p) < 0.02\}, \tag{35}$$

其中， $\epsilon(w,s,p)$ 由式（29）给出。根据定理2和引理 1，对于所有 $w > w^*$，近似 $\mathbb{E}(\tau_{(w,s)}) \approx \mathbb{E}(\tau_{(\infty,s)})$ 均可在相同的误差范围内成立。比较这一结果与能够作出相同近似的最小窗口大小 w^*_{true} 很有意义；该窗口大小的形式化定义如下：

$$w^*_{\text{true}} = \min\left\{w : \frac{\mathbb{E}(\tau_{(w,s)}) - \mathbb{E}(\tau_{(\infty,s)})}{\mathbb{E}(\tau_{(w,s)})} < 0.02\right\}. \tag{36}$$

w^* 的值是 w^*_{true}的上界。例如，令 $p = 0.5$ 和 $s = 4$，可得 $w^* = 15$；与精确解进行核对后得到 $w^*_{\text{true}} = 12$。图 6 展示了更多 p 取值下的结果。从图中可以看到，随着 p 增大，该上界似乎变得更加紧。由于 w^*_{true} 的计算是计算密集型的，因此只针对 p 的少数几个选定取值进行了绘制。

在图 5 中， $\mathbb{E}(\tau_{(w,4)})$ 针对窗口大小的五个不同取值绘制为 p 的函数。可以看出， $\mathbb{E}(\tau_{(w,4)})$ 的标度在较大的 w 下变化得更慢。这表明了式 (33) 所给出的倒数行为，其中 $\mathbb{E}(\tau_{(w,4)}) \sim 1/|w\ 4\ |p^4$) Ω(,);

而在取值较大时，常数Ω(w, 4)| 会抑制标度。随着 $p \to 1$ 的增大，所有曲线都简单地收敛到 $s = 4$，因为在这种情况下该过程是确定性的。此外，我们再次看到期望收敛到无限窗口极限。如果 p 变大，

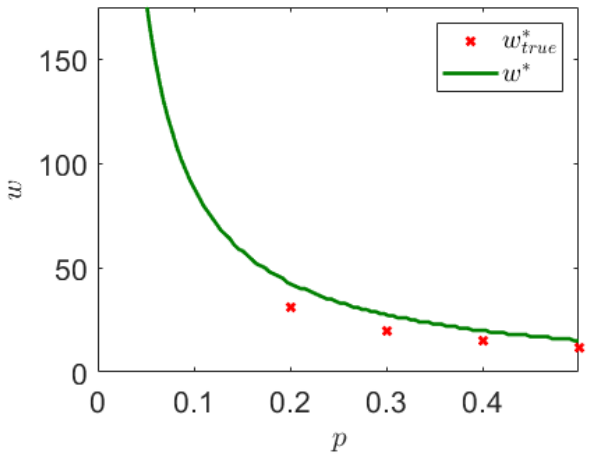

图 6。 在 w 的无限窗口近似下的阈值比较。可以使用 w^* （绿色线）作为阈值，其计算比 w^* 真实值（红色叉号）更容易。参见（35）和（36）以了解这些量的定义。这里假设所需误差为 2%。

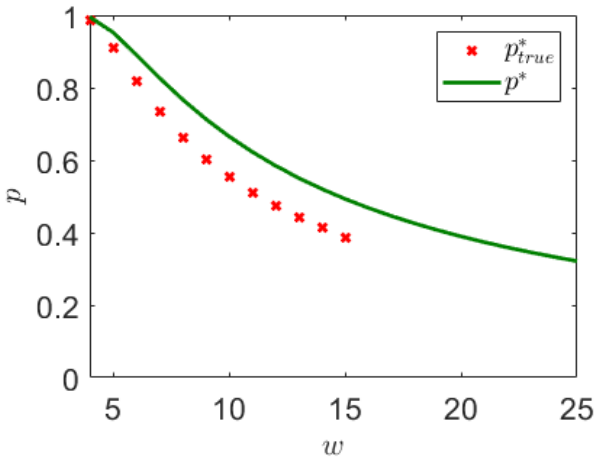

图7. 关于 p 无限窗口近似的阈值比较。可以使用 p^* （绿色线）作为阈值，因为它比p^* 真实值（红色叉号）更容易计算。这些量的定义见（37）和（38）。这里假设期望误差为2%。

我们预计问题会以与之前相同的意义“饱和”，从而使得 $\mathbb{E}(\tau_{(w,s)}) \approx \mathbb{E}(\tau_{(\infty,s)})$。利用第三节-C的结果，我们还可以量化这种收敛的速率。要求误差同样为 2%，我们取满足以下条件的p^*

$$p^* = \inf\{p : \epsilon(w,s,p) < 0.02\}, \tag{37}$$

或者等价地， p^* 是满足$\epsilon(w、 s、 p^*) = 0.02$的 p 的唯一值。值 p^* 是真实阈值 p^*_{true}的上界，

$$p^*_{\text{true}} := \inf\left\{p : \left(\frac{\mathbb{E}(\tau_{(w,s)}) - \mathbb{E}(\tau_{(\infty,s)})}{\mathbb{E}(\tau_{(w,s)})}\right)\Bigg|_p < 0.02\right\}. \tag{38}$$

其中我们现在纳入了期望对成功概率 p的依赖关系。在图7中，将 p^* 和 p^*_{true} 相对于 w作图。对于较大的 w 值，寻找值 p^*_{true} 的计算密集程度较高，因此仅针对选定的较小 w值绘制了该值。然而，上界 p^*的计算效率较高。我们观察到，对于较小的 w，该上界似乎更紧。

B. 应用于盲量子计算协议

下面我们举例说明如何将第三节的结果用于量子网络应用的性能分析。我们考虑一个可验证盲量子计算（BQC）协议 [15]。该协议涉及一个客户端，客户端借助功能更强大的服务器设备来执行有界误差量子多项式时间（BQP）计算[22], ，该计算在基于测量的形式体系[23]中指定。在这一形式体系中，计算是相对于一个图 $G = (V, E)$定义的，其中 V是顶点集合， E 是边集合。计算首先创建与 G对应的图态，然后对一组量子比特依次执行一系列测量（“测量流程”），即其中的一个子集。BQC协议经过专门设计，使服务器始终无法获知客户端所需执行的计算（盲性）。此外，即使存在一定程度的噪声或恶意服务器，该协议也能确保客户端验证计算结果是否正确（可验证性）。这些性质通过协议 [24]的可组合安全性质进行了精确定义。关于该协议的完整细节，请参阅 [15]。这里我们简要概述BQC协议及其执行方式的一个简单模型。随后，我们应用第三节的结果来研究该协议的性能。

1）协议可行性

BQC协议包含一系列轮次。在每一轮中，客户端向服务器发送 $|V|$ 量子比特，同时发送一份说明，告知服务器应执行的测量流程。如果服务器是诚实的，那么它将通过施加与 E中的边相对应的纠缠门来创建图态，执行相应的测量流程，并将测量结果发送回客户端。

该协议交错进行两类轮次：计算轮次和测试轮次。计算轮次用于执行客户端所需的运算。在这些轮次中，计算测量流程经过加密，以维持盲性。测试轮次的作用是检查是否偏离客户端指定的运算。偏差可能由噪声或服务器的恶意行为导致。每个测试轮次的结果要么通过，要么失败；如果失败测试轮次的比例超过某个阈值，协议就会中止。

假设测试轮次的结果是独立同分布的，我们将考虑的可验证性充分条件为

$$p_{\text{av}} < \frac{2\gamma - 1}{k(2\gamma - 2)}, \tag{39}$$

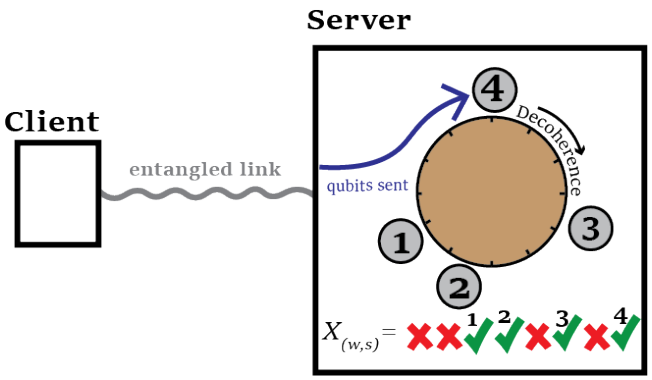

图8。 BQC模型所考虑的场景。纠缠链路的生成按顺序进行尝试，成功概率为 p。成功后，纠缠链路会立即用于将量子比特从客户端传输至服务器。在服务器中，量子比特（编号为灰色圆圈）会发生退相干（棕色时钟）。量子比特在服务器中存在 w 个时间步后将被丢弃。

如 [25] 所示。这里， p_{av} 是测试轮次失败的平均概率， γ 是 BQP 计算固有的错误概率。数值 k 是一个整数，对应于客户端选择的 k 颜色。该颜色划分将顶点集合划分为 k 个子集，称为颜色，并且同一颜色的两个顶点之间不存在边。有关其对盲量子计算协议的意义，请参见附录E-1，其中介绍了测试轮次。对于确定性的计算（$\gamma = 0$），(39) 简化为

$$p_{\text{av}} < \frac{1}{2k}. \tag{40}$$

当服务器是诚实时， p_{av} 的数值由噪声的大小决定。例如，噪声可能源于不完善的局部操作和测量，或服务器中不完善的存储器。此外，在客户端和服务器相距较远的联网场景中，客户端可以利用已在双方之间建立的纠缠，将其量子比特发送至服务器。通过这种方式，协议的性能直接取决于连接客户端和服务器的量子网络架构的属性。然而，在此类架构中，速率和质量通常存在权衡。对于这一BQC协议，要求满足条件（39）实际上会对协议速率施加一个上界。下文中，我们将考虑网络和设备架构的一个简单模型，并演示如何使用第三节中介绍的方法，在给定约束条件（39）的情况下，寻找能够最大化协议速率的架构参数。

2) 量子网络架构模型

我们对执行 BQC协议所基于的量子网络架构模型概述如下。图8给出了示意图。

- 服务器是诚实的，这意味着它会执行客户端指定的所有任务。BQC协议能够防范恶意服务器活动，并且对噪声具有鲁棒性。在此，我们仅旨在量化噪声对协议的影响。
- 客户端与服务器之间的纠缠生成通过依次尝试的方式进行。每次尝试成功的概率为 p。
- 纠缠成功后，会进行量子比特传输过程。我们假设，每个量子比特在相应时间步结束时进入服务器存储器。
- 传输完成后，每个量子比特立即以保真度 $F_{\text{est}}(p)$ 建立，其中 $F_{\text{est}}: [0,1] \to [0,1]$为递减函数。通过这种方式，我们纳入了客户端与服务器之间发生的纠缠生成过程中固有的速率与保真度之间的权衡。下文中，我们选择令其为$F_{\text{est}}(p) = 1 - \lambda p$。附录 D中给出了选择 F_{est} 的动机。
- 量子比特存储在服务器中时，会受到记忆寿命为 T 时间步的退极化噪声影响。对于 d维密度矩阵 $\rho \in \mathcal{D}(\mathcal{H}_d)$，其作用为

$$\rho \to e^{-\frac{t}{T}}\rho + \left(1 - e^{-\frac{t}{T}}\right)\frac{\mathbb{I}_d}{d}, \tag{41}$$

其中， $\mathbb{I}_d$ 是 d维单位矩阵， t 是 ρ 在服务器中存在的时间步数。对于量子比特的情况，即 $d = 2$，保真度随后衰减为

$$F_{\text{est}} \to \left(F_{\text{est}} - \frac{1}{2}\right)e^{-\frac{t}{T}} + \frac{1}{2}. \tag{42}$$

- 为减少退相干，服务器会在量子比特存储 w 时间步后将其丢弃。
- 客户端和服务器设备执行的所有局部操作和测量都是完美且瞬时完成的。特别是，一旦轮次所需的全部量子比特都已到达服务器，服务器就会立即且完美地应用客户端指定的测量流程。
- 在每轮开始前，客户端从 V中均匀随机选择一个元素。对应的量子比特是第一个发送的量子比特。随后，客户端按照预先定义的顺序，依次发送从 V 开始的量子比特。加入这种随机性后，量子比特年龄的排列将呈现出完全随机的特征。我们继续采用这一假设，因为它简化了 p_{av} 的计算，消除了量子比特年龄对最近 w 时间步之前发生的事件的任何依赖。有关协议测试轮次的更多详细信息见附录 E。

因此，在我们的模型中，服务器中量子比特的保真度仅取决于其在服务器中存储的时长，以及纠缠生成成功概率 p。请注意，我们的设置包括依次尝试在服务器中建立量子比特，并在这些量子比特存在达到预先设定的时间步数后将其丢弃。于是，我们面对的情形与本文第一部分所讨论的情形类似，其中量子比特充当

相应的量子资源。随后可以应用第三节中给出的方法来研究这一情形：完成一轮所需的时间为$\tau_{(w,s)}$ 个时间步，其中$s = |V|$ 是生成图态所需的量子比特数，而$\tau_{(w,s)}$ 是第二节中定义的等待时间。此外，服务器应用纠缠门和测量时的量子比特保真度由结束该过程的结束模式 $X_{(w,s)}$ 决定。更具体地说，可以利用结束模式分布精确计算 p_{av}。下面简要介绍这一点。

假设在某一特定测试轮次中，当服务器将执行其局部操作和测量时，服务器量子比特的保真度为 $\vec{F} = (F_1, F_2, \ldots\ldots F_{|V|})$。那么，根据上一节所述的模型，可以找到一个函数，用于表示测试轮次的错误概率 $P_G(\vec{F})$。这是关于数值 F_i 的多项式，其形式取决于图 G 以及所选择的 k-着色。附录 E 给出了如何获得该函数的具体细节。于是，测试轮次的平均错误概率的表达式为

$$p_{\text{av}} = \sum_{\vec{F}} \mathbb{P}(\vec{F}) P_G(\vec{F}), \tag{43}$$

其中，$\mathbb{P}(\vec{F})$ 是获得特定保真度向量 F 的概率。注意，在上一节引入的模型中，量子比特的保真度 F 由量子比特存储在服务器中的时间长短决定。此外，请回想一下，链路的年龄恰好包含在结束模式 $X_{(w,s)}$ 中。将这种依赖关系写作

$$\vec{F} = \vec{F}(X_{(w,s)}), \tag{44}$$

然后，我们改写（43），得到测试轮次失败的平均概率表达式，

$$p_{\text{av}} = \sum_{x \in \Omega(w,s)} \mathbb{P}(X_{(w,s)} = x) P_G\left(\vec{F}(x)\right). \tag{45}$$

这是一个现在可以使用第三节所介绍的方法进行评估的量。通过这种方式，第三节中的工具将BQC协议的可行性（由 p_{av}确定）与其速率直接联系起来。由于上述 p_{av} 公式取决于图结构和 k着色，某些参数范围可能足以进行某些计算，但不适用于其他计算。例如，对于需要更大 k的复杂图，条件（39）更加严格。此外，如果在计算中选择不同的图或 k着色，多项式 P_G 可能会有所不同。

3）数值评估

现在，我们旨在为协议的一轮找到架构参数 p 和 w 的最优值。这里的<贪?>还需要对更多协议参数进行进一步优化（例如计算轮次与测试轮次的比例），这不在本文的讨论范围内。

在我们的情形中，速率与保真度之间存在多重权衡：首先是由于成功概率的变化，其次是由于窗口大小的变化。 p 的增加会提高生成成功链路的速率，但会使服务器中量子比特的初始保真度降低，降低幅度由 $F_{\text{est}}(p)$ 确定。因此，我们预计需要更小的 w 值，以最大限度地减少服务器处的退相干，从而确保满足条件（39）。这反过来会增加在时间窗口内生成所有必要纠缠链路所需的期望时间。更正式地说，在给定固定 p的情况下，我们可以通过以下步骤求得一轮的最小期望时间。

1) 求出 w 的最大值，使得对于 p 的该取值，协议仍然可行，

$$w_{\max}(p) \coloneqq \max\left\{ w : p_{\text{av}} < \frac{2\gamma - 1}{k(2\gamma - 2)} \right\}. \tag{46}$$

2) 计算 $\mathbb{E}\left(\tau_{(w_{\max}(p),\ s)}\right)\big|_p$。这是一轮的最小预期时间。

作为这一方法付诸实践的一个例子，我们考虑客户端希望在一个方形图上执行 BQP 计算的情况，因此 $|V| = 4$。这要求在时间窗口内生成 $s = 4$ 个纠缠对。为简单起见，我们将考虑确定性计算，因此对错误概率的要求为 $p_{\text{av}} < 1/2k$。在这种情况下，可以将 k 选为 2（有关方形图的二着色示例，请参见附录 E），充分条件变为 $p_{\text{av}} < 1/4$。

在图9中，我们绘制了在 $F_0(p) = 1 - \lambda p$时，针对 T的三种不同取值，完成一轮所需的最小期望时间随 p 的变化关系。鉴于我们的计算资源，我们选择 $\lambda = \frac{1}{2}$，以便最佳地展示该解的行为。具体而言，我们所绘制的 p 范围经过选择，以清晰展示两种权衡的最优组合所在区域。对于较小的 p，由于纠缠生成概率较低，期望等待时间较长。对于较大的 p，由于F_{est}降低而必须采用较小的窗口大小，期望等待时间同样较长。因此，我们在图的中部看到一个区域，其中平均等待时间最小，或者等价地说，能够执行轮次的速率最大。对于较大的 T，存储器中量子比特的退相干程度降低，因此可以使用更大的窗口大小，而不会破坏关于 p_{av}的条件。由此可见，一轮的期望时间随 T增加而降低。此外，对于每个 T，图中都存在尖锐的峰值，这是由于 w的离散性质所导致的。其原因如下：在两个峰值之间，可以增大 p 的值而不破坏条件（39）。然而，当达到某一点时，该条件实际上会变为等式，此时必须减小窗口截断。这会导致期望时间离散地跃升至更高的数值。

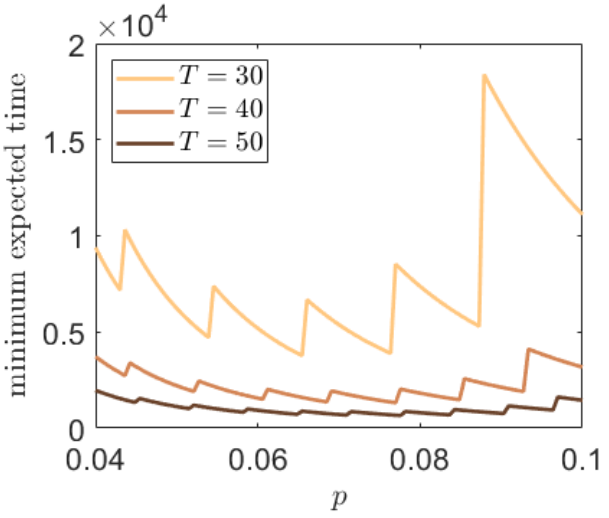

图9。 盲量子计算一轮计算的最小期望时间与纠缠生成成功概率的关系。对于给定的 p，我们求出最大窗口大小（46），然后利用该值计算最小期望等待时间。此处，将 p 离散为 p 个值，这些值在范围 $[0.04, 0.1]$内均匀分布。我们假设计算在方形图上进行，这需要在一个时间窗口内生成四条纠缠链路。

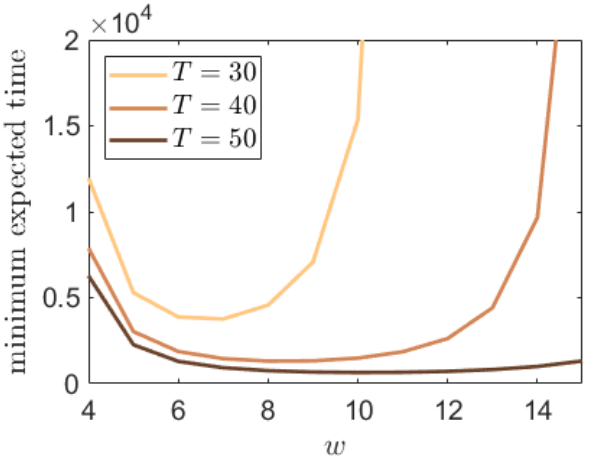

图10。 盲量子计算一轮计算的最小期望时间与窗口大小的关系。对于每个窗口大小 $4 \leq w \leq 15$，我们求出最大成功概率（47），然后利用该值计算期望等待时间。我们假设计算在方形图上进行，这需要在一个时间窗口内生成四条纠缠链路。

改变窗口大小时，也可以采取类似的方法。给定固定的 w，我们通过以下步骤求得一轮的最小期望时间。

1) 求出使协议仍然可行的 p 的最大值，

$$p_{\max}(w) := \sup\left\{p : p_{\text{av}} < \frac{2\gamma - 1}{k(2\gamma - 2)}\right\}. \tag{47}$$

2) 计算 $\mathbb{E}\left(\tau_{(w,s)}\right)\big|_{p_{\max}(w)}$。

In Fig. 10, we illustrate the minimum expected time for one round as a function of the window size in the same square-grid setting.

图10 绘制了在相同方形图的情形下，对应存储器寿命参数 T 的三个相同取值。我们观察到的趋势与改变成功概率时类似：较小的 w 会导致更长的期望时间。当 s 较大时，量子比特会受到更多退相干的影响；为了满足条件 (39)，必须降低成功概率。这会使 w 较大时的等待时间更长。因此，我们再次观察到 w 的一个最优范围，在该范围内，执行一轮协议的期望时间最短。

最后，我们指出，在实践中，为了优化完整的盲量子计算协议，还需要考虑硬件、架构和协议等设置的其他方面如何影响性能。本文选择的简单情形旨在突出第三节结果的应用。从图 9 和图 10 可以看出，对于这样的 T 和 s取值，第三节中的方法能够帮助人们谨慎选择 $(w,\ p)$，与同样足以保证协议可行性的其他非最优选择 $(w,\ p)$ 相比，这可以将协议的轮次速率提高两到三倍。

V. 进一步研究方向

借助本文所提出的方法，我们重点计算 $\tau_{(w,s)}$的一阶矩和二阶矩，以及 $X_{(w,s)}$的完整分布。我们已经看到，对于 w 有限且$s > 2$的情况，本文给出的用于计算 $\mathbb{E}(\tau_{(w,s)})$ 及 $X_{(w,s)}$ 分布的公式表现为线性方程组，其标度为 $|\Omega(w,\ s)| + 1$。如果希望计算完整的结束模式分布，那么这种标度似乎是合适的，因为结果由 $|\Omega(w,\ s)|$ 个概率组成。然而，例如，如果只关注$\mathbb{E}(\tau_{(w,s)})$（例如用于计算协议速率），那么对于 w 和 p 的某些取值范围，考虑连续近似可能会有所帮助，其中两次成功的资源生成尝试之间的时间服从指数分布。扫描统计文献中经常研究这种情况（例如，参见 [20]）。不过，连续情形下结束模式的计算并不明确。

我们还注意到，一个有用的近似工具是进一步理解定理3所强调的渐近标度。更具体地说，值得确切了解式（33）和（34）的趋近速度，即其关于s 和 w的变化。

在该问题的设置中，还可以考虑一种更现实的量子网络架构模型。例如，可能存在参数漂移，即由于噪声增加，成功概率会随时间降低。此外，在更一般的情况下，连续尝试不一定相互独立，而是马尔可夫的，此时也可以再次将与本文所采用的方法类似的方法应用于该问题——例如参见 [19], 。

致谢

作者感谢 Francisco Ferreira da Silva、Janice van Dam 和 Álvaro G. Iñesta 对稿件提出的批评性意见。BD 感谢荷兰皇家艺术与科学学院Am-

modo奖项（SW）的支持。BD、TB 和 SW 感谢量子互联网联盟（欧盟地平线欧洲计划资助协议编号：101102140）的支持。GV 还获得了 NWO ZK QSC AdaLovelace奖学金的部分资助。

.

附录 A（两个资源态情形下的恒等式）

1）计算 $\mathbb{E}\left(\tau_{(w,2)}\right)$ 计算 $\mathbb{E}(L)$。回顾式（13）中L的分布，我们有

$$\begin{aligned}\mathbb{E}(L) &= \sum_{n=1}^{w-1} \frac{n(1-p)^{n-1}p}{1-(1-p)^{w-1}} \\ &= \frac{p}{1-(1-p)^{w-1}} \sum_{n=1}^{w-1} n(1-p)^{n-1} \\ &= \frac{p}{1-(1-p)^{w-1}} \cdot -\frac{\mathrm{d}}{\mathrm{d}p} \sum_{n=1}^{w-1} (1-p)^n \\ &= \frac{p}{1-(1-p)^{w-1}} \cdot -\frac{\mathrm{d}}{\mathrm{d}p} \frac{1-(1-p)^w}{1-p} \\ &= \frac{p}{1-(1-p)^{w-1}} \cdot \frac{1-(1-p)^w - wp(1-p)^{w-1}}{p^2} \\ &= \frac{1-(1-p)^w - wp(1-p)^{w-1}}{p(1-(1-p)^{w-1})},\end{aligned}$$

在计算该求和时，我们使用了几何级数的恒等式。

□

证明 $\mathbb{E}\left(\sum_{j=1}^{M} T_j\right) = \mathbb{E}(M)\mathbb{E}(T_1)$。这用于计算期望 $\mathbb{E}(\tau_{(w,2)})$。随机变量 M和 $\{T_j\}$ 相互独立，并且由于 $\{T_j\}$ 同分布，

$$\begin{aligned}\mathbb{E}\left(\sum_{j=1}^{M} T_j\right) &= \sum_{m=1}^{\infty} \mathbb{E}\left(\sum_{j=1}^{m} T_j\right) \mathbb{P}(M=m) \\ &= \sum_{m=1}^{\infty} \mathbb{E}(T_1) \cdot m\mathbb{P}(M=m) \\ &= \mathbb{E}(T_1)\mathbb{E}(M).\end{aligned}$$

□

2）计算 $\mathrm{Var}(\tau_{(w,2)})$

回顾第三节-B1中给出的 M、T_j 和 L。这些变量相互独立，M 和 T 的分布分别为 $M \sim \mathrm{Geom}(1-(1-p)^{w-1})$ 和 $T_j \sim \mathrm{Geom}(p)$，而 L 的分布如（13）式所示。由（15）式可得

$$\mathrm{Var}(\tau_{(w,2)}) = \mathrm{Var}\left(\sum_{j=1}^{M} T_j + (M-1)(w-1)\right) + \mathrm{Var}(L), \quad (48)$$

因为 L 与 M 和 T_j 相互独立。现在，令 $\mathrm{Cov}(X,Y) = \mathbb{E}(XY) - \mathbb{E}(X)\mathbb{E}(Y)$ 表示协方差，

$$\begin{aligned}&\mathrm{Var}\left(\sum_{j=1}^{M} T_j + (M-1)(w-1)\right) \\ &\quad = \mathrm{Var}\left(\sum_{j=1}^{M} T_j\right) + \mathrm{Var}\left((M-1)(w-1)\right) + \\ &\qquad 2 \cdot \mathrm{Cov}\left(\sum_{j=1}^{M} T_j, (M-1)(w-1)\right), \quad (49)\end{aligned}$$

其中我们使用了恒等式 $\mathrm{Var}(X+Y) = \mathrm{Var}(X) + \mathrm{Var}(Y) + 2\cdot\mathrm{Cov}(X, Y)$。现在我们逐项计算式（49）。首先，

$$\begin{aligned}\mathbb{E}\left(\left(\sum_{j=1}^{M} T_j\right)^2\right) &= \sum_m \mathbb{E}\left(\left(\sum_{j=1}^{m} T_j\right)^2\right) \mathbb{P}(M=m) \\ &= \sum_m \mathbb{E}\left(\sum_{j=1}^{m} T_j^2 + \sum_{i\neq j} T_i T_j\right) \mathbb{P}(M=m) \\ &= \sum_m \left(m\mathbb{E}(T_1^2) + m(m-1)\mathbb{E}(T_1)^2\right) \mathbb{P}(M=m) \\ &= \mathbb{E}(M)\mathbb{E}(T_1^2) + \left(\mathbb{E}(M^2) - \mathbb{E}(M)\right)\mathbb{E}(T_1)^2.\end{aligned}$$

减去 $\mathbb{E}\left(\sum_{j=1}^{M} T_j\right)^2 = \mathbb{E}(M)^2\mathbb{E}(T_1)^2$ 后得到

$$\mathrm{Var}\left(\sum_{j=1}^{M} T_j\right) = \mathbb{E}(M)\mathrm{Var}(T_1) + \mathrm{Var}(M)\mathbb{E}(T_1)^2. \quad (50)$$

其次，

$$\mathrm{Var}\left((M-1)(w-1)\right) = (w-1)^2\mathrm{Var}(M). \quad (51)$$

第三，

$$\begin{aligned}&\mathrm{Cov}\left(\sum_{j=1}^{M} T_j, (M-1)(w-1)\right) \quad (52)\\ &\qquad = (w-1)\mathrm{Cov}\left(\sum_{j=1}^{M} T_j, M\right) \quad (53)\\ &= (w-1)\left(\sum_m m^2\mathbb{E}(T_1)\mathbb{P}(M=m) - \mathbb{E}(M)^2\mathbb{E}(T_1)\right) \quad (54)\\ &\qquad = (w-1)\mathrm{Var}(M)\mathbb{E}(T_1). \quad (55)\end{aligned}$$

现在还需要计算 $\mathrm{Var}(L)$。我们首先计算

$$\begin{aligned}\mathbb{E}(L^2) &= \sum_{n=1}^{w-1} \frac{n^2(1-p)^{n-1}p}{1-(1-p)^{w-1}} \quad (56)\\ &= \mathbb{E}(L) + \frac{p}{1-(1-p)^{w-1}} \sum_{n=1}^{w-1} n(n-1)(1-p)^{n-1}. \quad (57)\end{aligned}$$

Now,

$$\sum_{n=1}^{w-1} n(n-1)(1-p)^{n-1} = (1-p)\frac{\mathrm{d}^2}{\mathrm{d}p^2}\sum_{n=0}^{w-1}(1-p)^n = (1-p)\frac{\mathrm{d}^2}{\mathrm{d}p^2}\left(\frac{1-(1-p)^w}{p}\right),$$

so

$$\mathrm{Var}(L) = \frac{p(1-p)}{1-(1-p)^{w-1}}\frac{\mathrm{d}^2}{\mathrm{d}p^2}\left(\frac{1-(1-p)^w}{p}\right) + \mathbb{E}(L) - \mathbb{E}(L)^2. \quad (58)$$

现在我们可以计算$\tau_{(w,2)}$的完整方差,

$$\mathrm{Var}(\tau_{(w,2)}) = \mathbb{E}(M)\mathrm{Var}(T_1) + \mathrm{Var}(M)\mathbb{E}(T_1)^2 + 2(w-1)\mathrm{Var}(M)\mathbb{E}(T_1) + (w-1)^2\mathrm{Var}(M) + \mathrm{Var}(L), \quad (59)$$

其中，将几何随机变量的标准恒等式代入后，即可得到一个闭式表达式，这些恒等式为

$$\mathbb{E}(T_1) = \frac{1}{p} \quad (60)$$

$$\mathrm{Var}(T_1) = \frac{1-p}{p^2} \quad (61)$$

$$\mathbb{E}(M) = \frac{1}{1-(1-p)^{w-1}} \quad (62)$$

$$\mathrm{Var}(M) = \frac{(1-p)^{w-1}}{(1-(1-p)^{w-1})^2}. \quad (63)$$

附录 B（有限窗口大小情况下的结束模式分布与等待时间矩）

1) 等待时间定义良好

我们在此证明， τ_x 可以由一个服从几何分布的随机变量从上界进行界定。使用记号$p_1 = p$、 $p_0 = 1-p$ 表示结束模式 $x \in \Omega_l(s)$，该确切序列将在任意给定的 l 个连续试验Z_{i-l+1}，……， Z_i 中以概率 $\gamma_x := p_{x_1}...p_{x_l}$ 出现。定义一个新的随机变量序列 $(Y_n)_{n=1}^{\infty}$,

$$Y_n = \begin{cases} 1 \text{ if } Z_i = x_i \text{ for all } (n-1)l < i \le nl; \\ 0, \text{ otherwise.} \end{cases} \quad (64)$$

每个 Y_n 均为参数为 γ_x的伯努利随机变量。当 $n$th段 l 试验恰好与x匹配时，它取值 1。于是存在一个相应的等待时间随机变量$\tilde{\tau}_x$ ，其服从参数为 γ_x的几何分布，

$$\tilde{\tau}_x := \min\{n : Y_n = 1\}. \quad (65)$$

此外，等待看到 x 所需的等待时间满足 $\tau_x \le \tilde{\tau}_x \cdot l$。取期望可得

$$\mathbb{E}(\tau_{(w,s)}) \le \mathbb{E}(\tau_x) \le \mathbb{E}(\tilde{\tau}_x \cdot l) = \frac{l}{\gamma_x} < \infty, \quad (66)$$

这就完成了我们的证明。我们注意到，同样的方法可以用来证明$\tau_{(w,s)}$ 的所有矩都是有限的。

2）简单模式的期望等待时间

利用鞅理论以及有助于理解的赌博类比，我们现在推导出一种数值计算结束模式分布 $\{\mathbb{P}(x) : x \in \Omega(w,s)\}$以及等待时间 $\tau_{(w,s)}$的一阶矩和二阶矩的方法，该方法适用于有限窗口大小的情况。其结果就是正文中的定理 1。该方法首次在 [26],中提出，文中考虑的是由一般离散独立同分布随机变量组成的一般序列，以及一般的结束模式集合。在这里，鉴于其与正文主题的相关性，我们继续讨论独立同分布的伯努利试验情形。

首先考虑这样一种情况会很有帮助：我们等待单个模式 $x = (x_1、……、x_l) \in \{0,1\}^l$ 的某次出现，而不是等待集合 $\Omega(w、s)$ 中任一模式的出现。前一种情况称为简单模式，后一种情况称为复合模式。本节将求出 $\mathbb{E}(\tau_x)$ 的精确表达式。这里， τ_x 指的是直到看到模式 x之前的等待时间，其定义见（5）。

为了帮助理解，我们引入以下赌场中赌徒的情景。假设在第一次试验进行之前，一名赌徒（以下简称赌徒 1）下注 $\in 1$，赌结果为 $\{Z_1 = x_1\}$。我们还假设赔率是公平的，因此如果结果如此，她将赢得 $\in \frac{1}{p_{x_1}}$[1]。此外，如果她获胜，她会立即将全部赢款下注在结果 $\{Z_2 = x_2\}$ 上。如果没有获胜，赌场会收走她的 $\in 1$，她也不再下注。对于一般的 n，赌徒1随后会以类似的方式参与第 n 次试验：如果她尚未输掉，她会将全部赢款下注在结果 $\{Z_n = x_n\}$上；否则，她不会下注。此外，在每次试验中，我们都会引入一名行为完全相同的新赌徒。因此，赌徒2下注 $\in 1$，赌结果为 $\{Z_2 = x_1\}$，并继续将全部赢款下注在后续轮次中结果等于 x 的情形上，直到输掉一轮为止。赌徒 j 下注 $\in 1$，赌结果为 $\{Z_j = x_1\}$，并继续采用完全相同的策略。当序列 x 首次出现时，游戏停止；根据定义，这发生在第 τ_x次试验。

现在，我们的目标是写出一个表达式，表示在第 n 次试验后，赌徒们的合计净赢款，其中 n 为一般情况。为简洁起见，我们回顾一下量 $\delta_{(a,b)}$ 的定义（21）。给定前 n 次试验的一个实现值 $C_n := (c_1, ..., c_n)$，那么赌徒 j 在第 n 轮后的赢款可写为

$$W^{(j)}(C_n) = \begin{cases} \delta_{(x_1,c_j)}\delta_{(x_2,c_{j+1})}...\delta_{(x_{n-j+1},c_n)} \\ \text{for } n-l+1 \le j \le n; \\ 0, \text{ otherwise.} \end{cases} \quad (67)$$

这里我们看到，函数 $\delta_{(a,b)}$ 使我们能够优雅地写出一名赌徒的赢款。有鉴于此，

[1]即赌徒的预期净收益为零⎓将其记为 G，我们可以通过明确写出 $\mathbb{E}(G) = 0$. $(1/p_{\lambda_1} - 1)\cdot p_{\lambda_1} + (-1)\cdot(1-p_{\lambda_1})$ 来加以验证

合计 赌徒在第 n次试验后的赢款为

$$W(C_n) := \sum_{j=1}^{n} W^{(j)}(C_n) = \sum_{j=n-l+1}^{n} W_n^{(j)} \equiv x*C_n, \quad (68)$$

其中，我们引入了函数 $*$，它在式 (20) 中定义，将两个二进制字符串映射为一个标量值。由式 (67) 可知，第 j 位赌徒在第 n 个时间步后的净收益为

$$G^{(j)}(C_n) := W^{(j)}(C_n) - 1, \quad (69)$$

类似地，经过第 n 次试验后，赌徒的总净收益为

$$G(C_n) := \sum_{j=1}^{n} G^{(j)}(C_n) = x * C_n - n. \quad (70)$$

现在，我们可以定义一个随机变量序列 $(G_n)_{n\geq 0}$,

$$G_n := G(C_n) \quad (71)$$

该序列的取值为每轮结束后赌徒的总净收益。特别是，游戏结束后，总净收益为

$$G_{\tau_x} = x * x - \tau_x. \quad (72)$$

注意， $x * x$ 仅取决于模式 x。由于游戏被定义为每轮都是公平的，因此直观上，游戏结束时总净收益的期望值应为零，即

$$\mathbb{E}(G_{\tau_x}) = 0, \quad (73)$$

利用期望的线性性质，可以得到序列 B 的期望等待时间的一个简洁表达式，

$$\mathbb{E}(\tau_x) = x * x. \quad (74)$$

为证明 (73)，我们利用这样一个事实：$(G_n)_{n\geq 0}$ 是一个鞅，因此必须满足以下性质：

(i) $\mathbb{E}(|G_n|) < \infty$.
(ii) $\mathbb{E}(G_{n+1}|G_n, ..., G_1) = G_n$

为证明 (i)，我们使用定义 (72)，并可得

$$\mathbb{E}(|G_n|) \leq x * C_n + \mathbb{E}(\tau_x) < \infty, \quad (75)$$

由于等待时间 τ_x 定义良好，且 $x * C_n$ 有界。为证明条件 (ii)，我们利用这样一个事实：该游戏在每一轮次中都是公平的。假设我们掌握了关于前 n 次试验所发生情况的最大量信息，即我们知道它们所取的值为 (c_1，……， c_n)。那么， G_{n+1}的条件期望满足

$$\begin{aligned}
&\mathbb{E}(G_{n+1}|Z_1 = c_1, ..., Z_n = c_n) \\
&= \sum_{c_{n+1}\in\{0,1\}} G\left(C_n, c_{n+1}\right) \mathbb{P}(Z_{n+1} = c_{n+1}) \\
&= \sum_{j=1}^{n+1} \sum_{c_{n+1}\in\{0,1\}} G^{(j)}\left(C_n, c_{n+1}\right) p_{c_{n+1}} \\
&= \sum_{j=1}^{n+1} G^{(j)}(C_n) = G_n,
\end{aligned}$$

其中，为了得到最后一行，我们用到了 $G^{(j)}$ 的定义。由于 ($Z_1, ..., Z_n$) 的实现值完全决定了 $G_1, ..., G_n$ 的取值，这也证明了 (ii)。

现在我们知道 $(G_n)_{n\geq 0}$ 是一个鞅。然而，这还不足以证明 (73)，而证明 (73) 正是得到 $\mathbb{E}(\tau_x)$ 最终简洁形式所必需的。具体而言，我们还需要引入一些额外工具，即 Doob 的可选停止定理；其证明可见 [27]。下面陈述该定理的一个版本。

定理 4 (可选停止)。 设 G_n 是一个鞅，τ 是一个停止时间。假设存在一个常数 K，使得对所有 n，都有 $|G_n - G_{n-1}| < K$ 。此外，假设 τ 几乎处处有限。则 $\mathbb{E}(G_\tau) = \mathbb{E}(G_1)$。

剩下要做的就是证明，式 (72) 中定义的鞅满足定理 4 所要求的性质。首先，我们有

$$|G_n - G_{n-1}| < x * C_n + x * C_{n-1} + 1 \leq K, \quad (76)$$

其中

$$K = 2 \cdot \max_{C\in\{0,1\}^l}\{x * C\} + 1. \quad (77)$$

其次，由于 τ_x 被一个几何随机变量从上方所界，因此它几乎必然有限。这就得到了式 (73)。

3）从另一种模式开始

现在，我们调整上述结果，以求出已从某个模式y开始时，看到 x所需的期望时间。为了说明这一概念，我们扩展赌博类比，并假设我们想计算在已实现若干轮次 m（例如）之后，直到看到 y 所需的期望时间。具体而言，在第 m 轮之后，我们知道独立同分布伯努利序列的前 m 个实现值，并将它们记为 $y =$(y_1，……， y_m)。此时，赌徒的净收益为 $G_m = x * y - m$。我们将评估在这 n 次试验中的每一˜轮结束后，赌徒相较于此时的净收益；对于 $n \geq m$ ，我们将其记为 G_n。这只需写作

$$\begin{aligned}
\tilde{G}_n = G_n - G_m &= (x * C_n - n) - (x * y - m) \quad (78)\\
&= x * C_n - x * y - (n - m), \quad (79)
\end{aligned}$$

其中 C_n 不再完全一般，因为其前 m项必须对应于 y。运用与

˜之前相同的推理，可以证明 $(G_n)_{n\geq 0}$ 是一个鞅。然后，将 τ_{xy} 定义为在已看到模式 y的条件下，等待看到 x 给定 所需的时间，再次可以利用定理 4证明

$$0 = \mathbb{E}(\tilde{G}_{\tau_{xy}}) = \mathbb{E}(x * x - x * y - \tau_{yx}),$$

因此，根据期望的线性性，

$$\mathbb{E}(\tau_{xy}) = x * x - x * y. \tag{80}$$

现在我们可以利用上述推导出的结果，得出 $\mathbb{E}(\tau_{(w,s)})$ 的公式以及 $X_{(w,s)}$ 的分布。给定 $x \in \Omega(w,\ s)$，我们写作

$$\begin{aligned}
&\mathbb{E}(\tau_x) = \mathbb{E}(\tau_{(w,s)}) + \mathbb{E}(\tau_x - \tau_{(w,s)}) \\
&= \mathbb{E}(\tau_{(w,s)}) + \sum_{y\in\Omega(w,s)} \mathbb{P}(X_{(w,s)} = y)\mathbb{E}(\tau_x - \tau_{(w,s)}|X_{(w,s)} = y) \\
&= \mathbb{E}(\tau_{(w,s)}) + \sum_{y\in\Omega(w,s)} \mathbb{P}(X_{(w,s)} = y)(x * x - x * y),
\end{aligned}$$

其中我们注意到 $\mathbb{E}(\tau_x - \tau_{(w,s)}|X_{(w,s)} = y) = \mathbb{E}(\tau_{xy})$。应用定理 4，并施加结束模式概率之和必须为一这一条件，即可得到公式 (23)。

4）等待时间二阶矩的公式

可以利用上述赌博类比的扩展，推导等待时间二阶矩的公式，相关内容参见 [19]。这里我们只给出公式。首先定义一个新的运算 †，它将两个元素 $x,\ y \in \Omega(w,\ s)$ 映射为一个实数。若 $x = (x_1,\ \ldots\ldots,\ x_k)$ 且 $y = (y_1,\ \ldots\ldots,\ y_m)$，

$$x \dagger y := \sum_{j=1}^{\min(k,m)} (1-j) \prod_{i=1}^{j} \delta_{(x_i, y_{m-j+i})}. \tag{81}$$

令 $\Omega \equiv \Omega(w,\ s)$，通过求解以下方程组即可得到 $\tau_{(w,s)}$ 的二阶矩

定理5。令 $\{u_j\}_{1\leq j\leq|\Omega|}$ 和 $\{v_j\}_{1\leq j\leq|\Omega|}$ 分别求解线性方程组

$$\sum_{j=1}^{|\Omega|} W_{ij}u_j = 1,\ for\ 1 \leq i \leq |\Omega|, \tag{82}$$

$$\sum_{j=1}^{|\Omega|} (N_{ij}u_j + W_{ij}v_j) = 1,\ for\ 1 \leq i \leq |\Omega| \tag{83}$$

其中 $W_{ij} := x^{(i)} * x^{(j)}$，以及 $N_{ij} := x^{(i)} \dagger x^{(j)}$。于是，

$$\mathbb{E}\left(\tau^2_{(w,s)}\right) = \frac{1 + \left(1 - \sum_j v_j - \sum_j u_j/2\right) \cdot \mathbb{E}(\tau_{(w,s)})}{\sum_j u_j/2}. \tag{84}$$

使用此公式计算 $\mathbb{E}\left(\tau^2_{(w,s)}\right)$ 的代码见 [28]。

附录C（近似）

1）无限窗口大小近似

定理2的证明。令 $\epsilon \equiv \epsilon\ (w,\ s,\ p) = \mathbb{P}\ (\tau_{(w,s)} > w)$，则 $\tau_{(w,s)}$ 的期望可改写为

$$\begin{aligned}
\mathbb{E}(\tau_{(w,s)}) = (1-\epsilon)\mathbb{E}\left(\tau_{(w,s)}|\tau_{(w,s)} \leq w\right) + \\
\epsilon\mathbb{E}\left(\tau_{(w,s)}|\tau_{(w,s)} > w\right).
\end{aligned} \tag{85}$$

现在注意，对于 $n \leq w$

$$\mathbb{P}(\tau_{(w,s)} = n) = \mathbb{P}(\tau_{(\infty,s)} = n),$$

即，对于 n 的这一范围，$\tau_{(w,s)}$ 和 $\tau_{(\infty,s)}$ 的分布完全一致。因此，我们可以将（85）改写为

$$\begin{aligned}
&(1-\epsilon)\mathbb{E}\left(\tau_{(\infty,s)}|\tau_{(\infty,s)} \leq w\right) + \epsilon\mathbb{E}\left(\tau_{(w,s)}|\tau_{(w,s)} > w\right) \\
&= \mathbb{E}(\tau_{(\infty,s)}) - \epsilon\mathbb{E}\left(\tau_{(\infty,s)}|\tau_{(\infty,s)} > w\right) + \\
&\qquad \epsilon\mathbb{E}\left(\tau_{(w,s)}|\tau_{(w,s)} > w\right),
\end{aligned}$$

其中，为得到最后一个等式，我们以与（85）相同的方式展开了 $\mathbb{E}(\tau_{(\infty,s)})$。现在，如果考虑在经过最初的 w 个时间步后重新开始整个过程，我们看到$\mathbb{E}\left(\tau_{(w,s)}|\tau_{(w,s)} > w\right) \leq w + \mathbb{E}(\tau_{(w,s)})$。结合 $\mathbb{E}(\tau_{(\infty,s)}|\tau_{(\infty,s)} > w) > w$这一事实，我们得到

$$\mathbb{E}(\tau_{(w,s)}) - \mathbb{E}(\tau_{(\infty,s)}) \leq \epsilon \cdot \left(w + \mathbb{E}(\tau_{(w,s)}) - w\right), \tag{86}$$

由此可得（25）。

我们进一步界定结束模式分布之间的距离。利用

$$\begin{aligned}
\mathbb{P}(X_{(w,s)} = x) = \mathbb{P}(X_{(w,s)} = x|\tau_{(w,s)} \leq w)(1-\epsilon) \\
+ \mathbb{P}(X_{(w,s)} = x|\tau_{(w,s)} > w)\epsilon,
\end{aligned}$$

我们有

$$\begin{aligned}
&\mathbb{P}(X_{(w,s)} = x) - \mathbb{P}(X_{(\infty,s)} = x) \\
&= \left(\mathbb{P}(X_{(w,s)} = x|\tau_{(w,s)} > w) - \mathbb{P}(X_{(\infty,s)} = x|\tau_{(w,s)} > w)\right)\epsilon,
\end{aligned}$$

因此，令 $\Omega \equiv \Omega(\infty,\ s)$

$$\begin{aligned}
&\sum_{x\in\Omega} |\mathbb{P}(X_{(w,s)} = x) - \mathbb{P}(X_{(\infty,s)} = x)| < \\
&\sum_{x\in\Omega} \left(\mathbb{P}(X_{(w,s)} = x|\tau_{(w,s)} > w) + \mathbb{P}(X_{(\infty,s)} = x|\tau_{(w,s)} > w)\right)\epsilon \\
&\qquad = 2\epsilon(w,s,p).
\end{aligned}$$

□

引理*1*的证明。 这里，我们证明恒等式 (29) 对于$\epsilon(w,\ s,\ p)$成立。令 $q=1-p$，则有

$$\begin{aligned}\epsilon(w,s,p) &= \sum_{n=w+1}^{\infty}\binom{n-1}{s-1}q^{n-s}p^s \\ &= \frac{p^s}{(s-1)!}\sum_{n=w+1}^{\infty}\frac{(n-1)!}{(n-s)!}q^{n-s} \\ &= \frac{p^s}{(s-1)!}\sum_{n=w+1}^{\infty}\frac{\mathrm{d}^{s-1}}{\mathrm{d}q^{s-1}}\left(q^{n-1}\right) \\ &= \frac{p^s}{(s-1)!}\frac{\mathrm{d}^{s-1}}{\mathrm{d}q^{s-1}}\left(\sum_{n=w+1}^{\infty}q^{n-1}\right) \\ &= \frac{p^s}{(s-1)!}\frac{\mathrm{d}^{s-1}}{\mathrm{d}q^{s-1}}\left(\frac{q^w}{1-q}\right) \\ = \frac{p^s}{(s-1)!}\sum_{i=1}^{s-1}\binom{s-1}{i}\frac{\mathrm{d}^i}{\mathrm{d}q^i}\left(q^w\right)\frac{\mathrm{d}^{s-1-i}}{\mathrm{d}q^{s-1-k}}\left((1-q)^{-1}\right) \\ = \frac{p^s}{(s-1)!}\sum_{i=1}^{s-1}\frac{(s-1)!}{i!(s-i-1)!}\frac{w!}{(w-i)!}q^{w-i}\frac{(s-i-1)!}{(1-q)^{s-i}} \\ &= \sum_{i=1}^{s-1}\binom{w}{i}q^{w-i}p^i.\end{aligned}$$

□

2) 期望等待时间和结束模式的渐近行为

定理*3*的证明。 为简洁起见，这里取 Ω ≡Ω(w,s)。 A 的逆可用其伴随矩阵 adj A [29]表示，

$$[\mathrm{adj}\,A]_{ij} := (-1)^{(i+j)}\det M_{ji}. \tag{87}$$

其中， M_{ij} 是从 A中删除第i 行和第 j 列后得到的 $|\Omega|\times|\Omega|$ 矩阵。由于 A 可逆，其逆为

$$A^{-1} = \frac{\mathrm{adj}\,A}{\det A}, \tag{88}$$

现在考虑系统（23）。如果我们通过乘以 A^{-1}来求解 $\vec{v}$，可以看到其第一个元素为

$$\mathbb{E}(\tau_{(w,s)}) = \frac{\det B}{\det A}, \tag{89}$$

其中， B 是从 A中删除第一行和第一列后得到的 $|\Omega|\times|\Omega|$ 矩阵，因此 $B_{ij}=x^i*x^j$。由于 A 的所有元素都是关于 $1/p$ 和 $1/q$的多项式，因此 det B和 det A也都是多项式。

为了继续证明 (33)，我们刻画小 p时 det B 和 det A 的标度。由于小 p时 $q=1-p$ 接近 1，因此分析当 $p\to 0$ 时的渐近标度，只需考虑 $1/p$ 的幂（回顾星积的定义 (20)）。我们首先考虑 det B。注意到，$1/p$ 中的高阶项由对角线上的星积给出，而且这些项的首项均为 $1/p^s$。因此，其形式 det B是一个最高次数为 $1/p^{s|\Omega}$的多项式。事实上，其次数恰好为此值。通过考虑最高次幂对应的矩阵 B，即可计算这一˜贡献：˜令 $r\equiv 1/p^s$，有 det $B\sim$ det B，其中

$$\tilde{B} = \begin{pmatrix} r & 0 & \dots & 0 \\ 0 & r & \dots & 0 \\ \vdots & & \ddots & 0 \\ 0 & 0 & \dots & r \end{pmatrix}, \tag{90}$$

因此，det $B\sim r^{|\Omega|}=1/p^{s|\Omega|}$。然后我们对 A进行同样的˜。在这种情况下，det $A\sim$ det A，其中

$$\tilde{A} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ -1 & r & 0 & \dots & 0 \\ -1 & 0 & r & \dots & 0 \\ \vdots & \vdots & & \ddots & 0 \\ -1 & 0 & 0 & \dots & r \end{pmatrix}, \tag{91}$$

此时，左上角出现 0，˜使得无法像上文那样沿˜对角线相乘来计算行列式 A 。接下来，我们通过按 A顶行展开来计算行列式，

$$\det\tilde{A} = \sum_{k=1}^{|\Omega|}(-1)^k\det\tilde{A}_k, \tag{92}$$

˜其中 A_k $|\Omega|\times|\Omega|$ 矩阵是从 A中删去第一˜行和第 k列后得到的，

$$\tilde{A}_k = \begin{pmatrix} -1 & r & 0 & & \dots & & 0 \\ \vdots & 0 & \ddots & & & & \vdots \\ & & & r & 0 & & \\ & & & 0 & 0 & & \\ & & & 0 & r & & \\ \vdots & & & & & \ddots & 0 \\ -1 & 0 & \dots & & \dots & 0 & r \end{pmatrix}. \tag{93}$$

˜在 A_k中， r位于第 1, ..., k –1 行的对角线上方，并位于第 $k+1$, ..., |Ω|行的对角线上。矩阵 A_1 的行列式˜可通过将对角元素相乘直接求得，结果为

$$\det\tilde{A}_1 = -r^{|\Omega|-1}. \tag{94}$$

˜ ˜接下来我们注意到，任何 A_k 都可以通过将第 k行移到顶行而变换为 A_1 。如果通过依次与其上方的行交换来移动该行，则可通过进行 $k-1$ 次行变换实现 $k-1$ 。然后，由于每次行变换都会引入一个$(-1)^k$因子，

$$\det\tilde{A}_k = (-1)^{k-1}\det\tilde{A}_1 = (-1)^k r^{|\Omega|-1}. \tag{95}$$

结合（92），我们可以看出

$$\det\tilde{A} = |\Omega| r^{|\Omega|-1}, \tag{96}$$

因此行列式 $A \sim |\Omega|/p^{s(|\Omega|-1)}$。代入（89），可得

$$\mathbb{E}(\tau_{(w,s)}) \sim \frac{p^{s(|\Omega|-1)}}{|\Omega|p^{s|\Omega|}} = \frac{1}{|\Omega|p^s}. \tag{97}$$

为证明（34），我们采用类似的方法。由（88）可得

$$\mathbb{P}(X_{(w,s)} = x^{(k)}) = (-1)^{1+k}\frac{\det M_{k0}}{\det A} \tag{98}$$

$$\sim (-1)^{1+k}\frac{\det C_k}{\det X}, \tag{99}$$

其中，C_k 由从 A中删除第一列和第 k行得到，

$$C_k = \begin{pmatrix} 1 & \dots & & & \dots & 1 \\ r & 0 & \dots & & \dots & 0 \\ 0 & \ddots & & & & \vdots \\ \vdots & & r & 0 & 0 & \\ & & 0 & 0 & r & \vdots \\ \vdots & & & & \ddots & 0 \\ 0 & \dots & & \dots & 0 & r \end{pmatrix}, \tag{100}$$

其中，在 C_k 中，x项位于第 1，...，$k-1$列的对角线下方，以及第$k+1$，...，$|\Omega|$列的对角线上。注意到，C_k 是 B_k的转置矩阵，其第一列乘以标度因子 -1。因此，$\det C_k = -\det B_k = (-1)^{k+1}r^{|\Omega|-1}$，再次利用（96）可得，

$$\mathbb{P}(X_{(w,s)} = x^{(k)}) \sim \frac{r^{|\Omega|-1}}{|\Omega|r^{|\Omega|-1}}, \tag{101}$$

由此即可得到结果。 □

附录 D（由纠缠生成方案产生的权衡函数）

在本附录中，我们说明 BQC 分析中所使用的线性权衡函数 $F_{\text{est}} = 1 - \lambda p$ 的依据；该函数描述了量子比特传输后立即在服务器中的保真度。

令 σ 表示客户端与服务器之间在尝试成功时生成的含噪双量子比特纠缠态。成功后，客户端和服务器会执行某种量子比特传输过程 Λ_σ，例如量子隐形传态或远程态制备协议。我们假设该协议能使服务器中的所有量子比特具有相同的保真度 F_{est}。例如，当含噪纠缠态是退极化的

$$\sigma = \frac{4F_0 - 1}{3}|\Phi^+\rangle\langle\Phi^+| + \frac{1 - F_0}{3}\mathbb{I}_4, \tag{102}$$

并应用 [30]中的标准量子隐形传态协议。此处，$F_0 = \langle\Phi^+|\,\sigma\,|\Phi^+\rangle$ 是 σ 与目标状态之间的保真度。这涉及在贝尔基$\{|\Phi_{ij}\rangle\}$ 中执行完整测量，并应用相应的泡利校正。如果 $|\psi\rangle$ 是要进行量子隐形传态的量子比特状态，其作用表示为Λ^{st}，

$$\Lambda^{\text{st}}_\sigma(|\psi\rangle\langle\psi|) := \sum_{i,j} X^i Z^j \langle\Phi_{ij}|(|\psi\rangle\langle\psi| \otimes \sigma)|\Phi_{ij}\rangle Z^j X^i \tag{103}$$

其中，贝尔测量作用于包含量子比特状态 $|\psi\rangle$ 的寄存器以及 σ 的第一个量子比特。假设纠缠态和量子比特传输过程分别由 (102) 和 (103) 给出。那么，传输任意量子比特 $|\psi\rangle$ 后，所得保真度为 [31]

$$F_{\text{est}} = \frac{2F_0 + 1}{3}. \tag{104}$$

现在，可以通过指定 F_{est} 是 p 的递减函数，将纠缠生成协议固有的一般速率-保真度权衡纳入考量。特别地，我们在此借鉴一个单光子纠缠生成方案的示例。采用单光子方案 [6], 时，生成状态的保真度为

$$F_0(p_{\text{suc}}) = 1 - \frac{p_{\text{suc}}}{2p_{\text{det}}}, \tag{105}$$

其中，p_{suc} 是物理纠缠尝试的成功概率，p_{det} 是检测到发射光子的概率。当 p_{suc}非常小时，可以考虑以批次的方式进行纠缠尝试，从而尽量减少与软件栈上层通信所产生的开销（当尝试成功或失败时，都必须通知上层）。该方案已在金刚石中的NV中心上实现，其中通常有 $p_{\text{suc}} \ll 1$ [32]。在这种情况下，选择一个时间步对应于一批 $M \ll 1/(p_{\text{suc}})^2$ 次尝试，则一个时间步内至少生成一条纠缠链路的概率为

$$p = 1 - (1 - p_{\text{suc}})^M \approx Mp_{\text{suc}}. \tag{106}$$

将其代入(104)和(105)，可得到如下权衡函数:

$$F_{\text{est}}(p) = \frac{2\left(1 - \frac{p}{2Mp_{\text{det}}}\right) + 1}{3} = 1 - \lambda p, \tag{107}$$

其中，$\lambda := 1/(3Mp_{\text{det}})$。由于 M 是一个可自由调节的参数，因此 λ也是如此。简单关系式(107)也是关于 p 的递减函数的一般一阶行为，其中 $F_{\text{est}}(0) = 1$，这证明了该选择可能适用于其他硬件和纠缠生成协议。

附录 E（计算 BQC 测试轮次的错误概率）

1）测试轮次

如前所述，该协议会随机交错进行测试轮次和计算轮次。测试轮次使协议具备可验证性，因为它们允许客户端检查是否偏离理想测量结果。回想一下，BQC协议中客户端的目标是执行一个BQP 计算，它

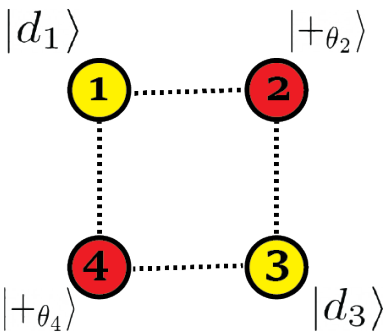

图 11. BQC协议中的测试轮次。 这里选择一个在方形图上执行运算的示例。客户端选择一种 k-着色：这里 $k=2$，两个集合分别着为黄色和红色。在这种情况下，红色顶点对应陷阱量子比特，黄色顶点对应哑量子比特。

是在基于测量的形式体系中针对图 $G=(V,\ E)$ 定义的。在协议的一轮中，客户端向服务器发送 $|V|$ 量子比特；如果服务器诚实，它会按照边集 E 中的定义，对成对的量子比特施加 CZ门，从而创建一个图态。在执行协议之前，客户端会选择一种 k着色 $\{V_j:\ j=1,\ \ldots\ldots,\ k\}$，它将顶点集 V 划分为不同的子集，称为颜色，并确保同一颜色的任意两个顶点之间都没有边。因此，这个 k 对应于可行性条件（39）中的 k。

在每次测试轮次之前，客户端 V_j均匀随机地选择一种颜色作为陷阱颜色。与该集合中的顶点相对应的量子比特随后被称为陷阱量子比特。任何其他量子比特都被称为哑量子比特。每个陷阱量子比特 $v\in V_j$ 将$|+_{\theta_v}\rangle:=(|0\rangle+e^{i\theta_v}|1\rangle)/\sqrt{2}$，其中角度 θ_v 从$\Theta=\{\frac{k\pi}{4}$ 中均匀随机选择$:=\ k=0,\ 1,\ \ldots\ldots,\ 7\}$。每个哑量子比特 $v\in V\setminus V_j$将 $|d_v\rangle$，其中 $d_v\in\{0,1\}$ 均匀随机选择。随后，服务器应用其纠缠门的效果是：将每个陷阱量子比特翻转到正交基向量，其翻转次数对应于相邻哑量子比特之和（模2）。这是客户端可以计算的量。在构造图态后，服务器测量其量子比特，并将结果发送给客户端。对于每个陷阱 $v\in V_j$，客户端指定的陷阱量子比特测量基为 $\{|\pm_{\delta_v}\rangle\}$，其中 $\delta_v=\theta_v+r_v\pi$，并且 $r_v\in\{0,1\}$ 均匀随机选择。客户端将陷阱量子比特的测量结果与所有状态和局部操作均完美时的预期结果进行比较；如果至少有一次陷阱测量不正确，则宣布测试轮次失败。图11给出了方形图情况下的图态、一种 k-着色以及一次测试轮次中量子比特选择的示意图。

2) 一般图的错误概率

我们假设客户端希望知道某次 BQP 计算的结果，该计算对应的图为 $G=(V,\ E)$，并且客户端选择了一个 k-着色 $\{V_j\}_{j=1}^{k}$。那么，鉴于服务器执行其运算时的保真度向量为 $\vec{F}=(F_1,\ \ldots\ldots\ F_{|V|})$，我们可以得到测试轮次错误概率的一般形式，即 $P_G(\vec{F})$。这是对 [25], 中结果的推广，其中讨论了使用两个量子比特的盲量子计算。

我们首先求出错误概率，给定 客户端选择了陷阱颜色 V_j。将其记为 P_{V_j}。因此，客户端选择发送陷阱量子比特 $v\in V_j$，其状态为 $|+_{\theta_v}\rangle$。然后，在进行测试轮次时，与顶点 $v\in V_j$ 对应的陷阱量子比特分别处于状态 ρ_v，其中

$$\rho_v=F_v|+_{\theta_v}\rangle\langle+_{\theta_v}|+(1-F_v)|-_{\theta_v}\rangle\langle-_{\theta_v}|+(\text{o.d.1}),\quad(108)$$

其中，我们使用 (o.d.1) 来表示（相对于基 $\{|+_{\theta_v}\rangle$、$|-_{\theta_v}\rangle\}$ 而言的）非对角元。我们不将它们完整写出，因为正如稍后将看到的，它们最终不会对 $P_{V_j}(\vec{F})$ 产生任何贡献。同样，哑量子比特$v\in V\setminus V_j$ 将处于以下状态

$$\rho_v=F_v|d_v\rangle\langle d_v|+(1-F_v)|d_v\oplus1\rangle\langle d_v\oplus1|+(\text{o.d.2}),\quad(109)$$

其中，这里我们使用 (o.d.2) 来表示非对角元，这次是相对于计算基而言的。于是，服务器的状态由所有这些状态的张量积给出

$$\rho_{\text{server}}=\bigotimes_{v\in V_j}\rho_v\bigotimes_{w\in W_j}\rho_w\bigotimes_{u\in V\setminus(V_j\cup W_j)}\rho_u,\quad(110)$$

其中，我们将 $W_j\subset V\setminus V_j$ 定义为与陷阱量子比特共享一条边的所有顶点的集合。随后，服务器继续执行 BQC 协议 的下一步，并对对应于 E 中各条边的所有量子比特对应用 CZ 个门，从而得到状态

$$\rho'_{\text{server}}=U\rho_{\text{server}}U^{\dagger},\quad(111)$$

其中 $U:=\prod_{(w,\ v)\in E}CZ_{(w,v)}$。回想一下，我们关注的是 $P_{V_j}(\vec{F})$，即该过程导致误差的概率。事实上，求出成功概率 $Q_{V_j}(\vec{F})=1-P_{V_j}(\vec{F})$ 的形式会更简单。当至少有一个陷阱量子比特的测量结果与所有状态均为完美状态时应得到的结果不匹配时，就会发生误差。具体而言，如果一切均为完美状态，则客户端预期与陷阱量子比特 v 对应的测量结果为 $r_v\oplus D_v$，其中

$$D_v=\bigoplus_{w\in W_j:(v,w)\in E}d_w,\quad(112)$$

即陷阱量子比特周围所有哑变量 d_v 的和（模 2）。因此，成功概率为

$$Q_{V_j}(\vec{F})=\text{Tr}_V\left(\left(\bigotimes_{v\in V_j}|(-1)^{r_v\oplus D_v}_{\delta_v}\rangle\langle(-1)^{r_v\oplus D_v}_{\delta_v}|\right)\rho'_{\text{server}}\right),\quad(113)$$

为方便起见，我们采用记号 $|+1_{\theta}\rangle\equiv|+_{\theta}\rangle$ 和 $|-1_{\theta}\rangle\equiv|-_{\theta}\rangle$。重写 $|-1^{D_v}_{\theta_v}\rangle=|^{r_v+D_v}_{\delta_v}\rangle$，并考察方程 (110) 和 (111) 后，

我们看到，与顶点$v \in V \setminus (V_j \cup W_j)$对应的量子比特寄存器将不会对该量作出贡献，因此

$$Q_{V_j}(\vec{F}) = \mathrm{Tr}_{V_j}\mathrm{Tr}_{W_j}\left(\left(\bigotimes_{v\in V_j}|(-1)^{D_v}_{\theta_v}\rangle\langle(-1)^{D_v}_{\theta_v}|\right)\sigma'_{\text{server}}\right), \tag{114}$$

with

$$\sigma'_{\text{server}} := \tilde{U}\sigma_{\text{server}}\tilde{U}^\dagger, \tag{115}$$

其中我们定义 $\sigma_{\text{server}} := \bigotimes_{v\in V_j}\rho_v \bigotimes_{w\in W_j}\rho_w$ 和 $\tilde{U} = \prod_{w\,v\,\in E_j} CZ_{(w,v)}$ $E_j = \{v\ w \in E \quad v \in V_j\}$ 并将 $:(,):$ 定义为任意一个元素与任意其他顶点之间所有边的集合。回顾式 (108) 和 (109) 中给出的量子比特状态，并定义 $F^{(0)} := F, F^{(1)} := 1 - F$，以便更简洁地写出部分项，于是可以写成

$$\begin{aligned}\sigma_{\text{server}} &= \bigotimes_{v\in V_j}\left(\sum_{x_v\in\{0,1\}} F_v^{(x_v)}|(-1)^{x_v}_{\theta_v}\rangle\langle(-1)^{x_v}_{\theta_v}|\right)\cdot \\ &\quad \bigotimes_{w\in W_j}\left(\sum_{y_w\in\{0,1\}} F_w^{(y_w)}|d_w + y_w\rangle\langle d_w + y_w|\right) \\ &= \bigotimes_{v\in V_j}\left(\sum_{x_v\in\{0,1\}} F_v^{(x_v)}|(-1)^{x_v}_{\theta_v}\rangle\langle(-1)^{x_v}_{\theta_v}|\right)\cdot \\ &\quad \bigotimes\left(\sum_{\vec{y}\in\{0,1\}^{|W_j|}}\prod_{w\in W_j} F_w^{(y_w)}|\vec{d}+\vec{y}\rangle\langle\vec{d}+\vec{y}|\right),\end{aligned} \tag{116}$$

其中在式 (116) 中，我们将求和重写为对所有长度为 $|W_j|$ 的二进制字符串 $\vec{y} \equiv (y_w)_{w\in W_j} \in \{0,1\}^{|W_j|}$ 求和。$\vec{}$我们还将哑变量存储在向量 d 中，因此 $(\vec{d}+\vec{y})_w = d_w + y_w$。同样地，我们没有写出非对角项，因为在取迹时这些项都会消失，因此不会对最终的 $\tilde{}$ 表达式作出贡献。应用酉算符 U 后得到

$$\sigma'_{\text{server}} = \sum_{\vec{y}\in\{0,1\}^{|W_j|}}\prod_{w\in W_j} F_w^{(y_w)}|\vec{d}+\vec{y}\rangle\langle\vec{d}+\vec{y}|\cdot$$

$$\bigotimes_{v\in V_j}\left(\sum_{x_v\in\{0,1\}} F_v^{(x_v)}|(-1)^{x_v+s_v(\vec{y})+D_v}_{\theta_v}\rangle\langle(-1)^{x_v+s_v(\vec{y})+D_v}_{\theta_v}|\right)$$

其中，对于陷阱 $v \in V_j$，我们定义

$$s_v(\vec{y}) := \sum_{w\in W_j:(w,v)\in E_j} y_w, \tag{117}$$

即对所有与 v 相邻的顶点上的二进制变量 y_w 求和。现在，我们可以开始对寄存器进行迹运算，以便找到用量子比特保真度表示的 $Q_{V_j}(\vec{F})$ 的最终表达式。对所有陷阱量子比特 $v \in V_j$ 取内积 $\langle(-1)^{D_v}_{\delta_v}|...|(-1)^{D_v}_{\delta_v}\rangle$ 并对 W_j 求迹，得到我们的成功概率的最终表达式，如公式 (113) 所引入的那样，

$$Q_{V_j}(\vec{F}) = \sum_{\vec{y}\in\{0,1\}^{|W_j|}}\prod_{w\in W_j} F_w^{(y_w)}\prod_{v\in V_j} F_v^{(s_v(\vec{y}))}, \tag{118}$$

这是关于保真度 $\vec{F} = (F_1, ..., F_{|V|})$ 的多项式，其形式完全由图结构和陷阱颜色 V_j 的选择决定。因此，错误概率 $P_{V_j}(\vec{F})$ 也具有相同的性质。在第四节 B2 中给出的模型里，还需要考虑这样一个事实：发送的第一个量子比特是随机选择的。因此，错误概率实际上要对 $|V|$ 个可能的起始量子比特按以下方式进行对称化。不失一般性地，令量子比特按字典序发送，则错误概率为

$$P_{V_j}(\vec{F}) \to \tilde{P}_{V_j}(\vec{F}) := \frac{1}{|V|}\sum_j P_{V_j}(\sigma^j\vec{F}), \tag{119}$$

其中，σ 是将向量元素向左移动一位的置换，即 $\sigma(F_1, ..., F_{|V|}) = (F_2, ..., F_{|V|}, F_1)$。要得到最终的错误概率，还需对陷阱颜色的选择取平均，并注意到陷阱颜色是均匀随机选取的。由此得到 $P_G(\vec{F})$ 的最终表达式，

$$P_G(\vec{F}) = \frac{1}{k}\sum_{j=1}^{k}\tilde{P}_{V_j}(\vec{F}). \tag{120}$$

3) 方形图的错误概率

方形图情况下，这样一个多项式的示例如下。考虑图 11 所示的 k 着色，并选择红色作为陷阱颜色。假设服务器应用其门和测量时，量子比特的保真度为 $\vec{F} = (F_1, F_2, F_3, F_4)$。那么，根据 (118)，成功概率为

$$\begin{aligned}Q_{\text{red}}(\vec{F}) &= F_1F_2F_3F_4 + F_1(1-F_2)(1-F_3)(1-F_4) \\ &+(1-F_1)(1-F_2)F_3(1-F_4) + (1-F_1)F_2(1-F_3)F_4,\end{aligned}$$

因此，错误概率为

$$P_{\text{red}}(\vec{F}) = 1 - Q_{\text{red}}(\vec{F}). \tag{121}$$

根据方形图的对称性，错误概率 $P_{\text{yellow}}(\vec{F})$ 可通过在 (121) 中交换索引 $1 \leftrightarrow 2$，$3 \leftrightarrow 4$ 得到。对于方形图，对称化将 $P_{\text{red}}(\vec{F})$ 映射为 $\to \tilde{P}_{\text{red}}(\vec{F})$，其中

$$\begin{aligned}\tilde{P}_{\text{red}}(\vec{F}) = &\frac{1}{4}\big[P_{\text{red}}(F_1,F_2,F_3,F_4) + P_{\text{red}}(F_2,F_3,F_4,F_1) \\ &+ P_{\text{red}}(F_3,F_4,F_1,F_2) + P_{\text{red}}(F_4,F_1,F_2,F_3)\big].\end{aligned}$$

注意，错误函数 P_{red} 和 P_{yellow} 的对称性反映了图的对称性，也就是说，它们在交换 $1 \leftrightarrow 3$ 或 $2 \leftrightarrow 4$ 时保持对称。然后，

$$\tilde{P}_{\text{red}}(\vec{F}) = \frac{1}{2}\left(P_{\text{red}}(\vec{F}) + P_{\text{yellow}}(\vec{F})\right) \tag{122}$$

另一个错误函数 P_{yellow} 经对称化（119）后映射为相同的函数，即 $\tilde{P}_{\text{yellow}}(\vec{F}) = \tilde{P}_{\text{red}}(\vec{F})$。因此，误差概率为

$$P_{\text{square}}(\vec{F}) = \frac{1}{2}\left(\tilde{P}_{\text{yellow}}(\vec{F}) + \tilde{P}_{\text{red}}(\vec{F})\right) \tag{123}$$

$$= \frac{1}{2}\left(P_{\text{red}}(\vec{F}) + P_{\text{yellow}}(\vec{F})\right). \tag{124}$$

这是我们结合（45）使用的函数，用于计算模型的 p_{av}，并在第 IV-B3 节中计算一个方形图示例的结果。

参考文献

[1] C. H. Bennett、G. Brassard、S. Popescu、B. Schumacher、J. A. Smolin 和 W. K. Wootters，《噪声信道中的噪声纠缠纯化与忠实传态》，《物理评论快报》，第 76 卷，第 5 期，第 722 页，1996 年。[2] D. Deutsch、A. Ekert、R. Jozsa、C. Macchiavello、S. Popescu 和 A. Sanpera，《量子隐私放大与噪声信道上量子密码学的安全性》，《物理评论快报》，第 77 卷，第 13 期，第 2818 页，1996 年。[3] S. Wehner、D. Elkouss 和 R. Hanson，《量子互联网：未来发展愿景》，《科学》，第 362 卷，第 6412 期，第 eaam9288 页，2018 年。[4] 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》，《物理评论 A》，第 71 卷，第 2 期，第 022316 页，2005 年。[5] S. D. Barrett 和 P. Kok，《使用物质量子比特和线性光学实现高效高保真度量子计算》，《物理评论 A》，第 71 卷，第 6 期，第 060310 页，2005 年。[6] C. Cabrillo、J. I. Cirac、P. Garcia-Fernandez 和 P. Zoller，《通过干涉创建远距离原子的纠缠态》，《物理评论 A》，第 59 卷，第 2 期，第 1025 页，1999 年。[7] S. Baier、M. Pompili、S. L. Hermans、H. K. Beukers、P. C. Humphreys、R. N. Schouten、R. F. Vermeulen、M. J. Tiggelman、L. dos Santos Martins、B. Dirkse 等，《远程固态量子比特多节点量子网络的实现》，载于《量子信息与测量》。Optica 出版集团，2021 年，第 M2A–2 页。[8] M. Pompili、C. D. Donne、I. t. Raa、B. van der Vecht、M. Skrzypczyk、G. Ferreira、L. de Kluijver、A. J. Stolk、S. L. Hermans、P. Pawełczak 等，《使用量子网络协议栈实现纠缠分发的实验演示》，arXiv 预印本 arXiv:2111.11332，2021 年。[9] B. Li、T. Coopmans 和 D. Elkouss，《量子中继器链中截止时间的高效优化》，载于《2020 IEEE量子计算与工程国际会议（QCE）》。IEEE，2020 年，第 158–168 页。[10] S. Khatri，《量子网络中基本链路的策略》，《Quantum》，第 5 卷，第 537 页，2021 年 9 月。 [在线]。可访问：https: //doi.org/ 10 22331 2021 09 07 537 . /q- - - - L. Praxmeyer，[11]《概率性不完美存储器中的重新定位时间》，arXiv 预印本 arXiv:1309.3407，2013 年。[12] E. Shchukin、F. Schmidt 和 P. van Loock，《具有概率性纠缠交换的量子中继器中的等待时间》，《物理评论 A》，第 100 卷，第 3 期，第 032322 页，2019 年。[13] A. G. Iñesta、G. Vardoyan、L. Scavuzzo 和 S. Wehner，《具有截止时间的均匀中继器链中的最优纠缠分发策略》，arXiv 预印本 arXiv:2207.06533，2022 年。[14] F. Rozp.edek、K. Goodenough、J. Ribeiro、N. Kalb、V. C. Vivoli、A. Reis- erer、R. Hanson、S. Wehner 和 D. Elkouss，《单个顺序量子中继器的参数范围》，《量子科学与技术》，第 3 卷，第 3 期，第 034002 页，2018 年。[15] D. Leichtle、L. Music、E. Kashefi 和 H. Ollivier，《在噪声设备上以最小开销验证 BQP 量子计算》，《PRX Quantum》，第 2 卷，第 4 期，第 040302 页，2021 年。[16] S.-Y. R. Li，《重复实验中序列模式出现的鞅方法》，《概率年刊》，第 8 卷，第 6 期，第 1171–1176 页，1980 年。[在线]。可访问：https://www.jstor.org/stable/ 2245018 [17] J. C. Fu 和 W. W. Lou，《游程与模式的分布理论及其应用：有限马尔可夫链嵌入方法》。世界科技出版公司，2003 年。[18] M. Ebneshahrashoob、T. Gao 和 M. Sobel，《序贯窗口问题》，《序贯分析》，第 24 卷，第 2 期，第 159–175 页，2005 年。[19] J. Glaz、V. Pozdnyakov 和 S. Wallenstein，《扫描统计：方法与应用》。Birkhäuser，2009 年。[20] J. Glaz、J. I. Naus 和 S. Wallenstein，《扫描统计》。Springer，2001 年。[21] V. Pozdnyakov 和 J. M. Steele，《模式与扫描统计的鞅方法》，载于《扫描统计：方法与应用》。马萨诸塞州波士顿：Birkhäuser，2009 年，第 289–317 页。 [在线]。可访问：https://doi.org/ 10 1007 978 0 8176 4749 0_14 . / - - - - [22] M. A. Nielsen 和 I. Chuang，《量子计算与量子信息》，2002 年。[23] R. Raussendorf 和 H. J. Briegel，《单向量子计算机》，《物理评论快报》，第 86 卷，第 22 期，第 5188 页，2001 年。[24] V. Dunjko、J. F. Fitzsimons、C. Portmann 和 R. Renner，《委托量子计算的可组合安全》，载于《密码学进展——ASIACRYPT 2014：密码学与信息安全理论及应用第 20 届国际会议，2014 年 12 月 7–11 日，中国台湾高雄，会议录，第二部分 20》。Springer，2014 年，第 406–425 页。[25] G. Avis、F. F. da Silva、T. Coopmans、A. Dahlberg、H. Jirovská、D. Maier、J. Rabbie、A. Torres-Knoop 和 S. Wehner，《现实世界光纤网格中处理节点量子中继器的要求》，arXiv 预印本 arXiv:2207.10579，2022 年。[26] S.-Y. R. Li，《重复实验中序列模式出现的鞅方法》，《概率年刊》，第 8 卷，第 6 期，第 1171–1176 页，1980 年。[27] D. Williams，《鞅与概率》。剑桥大学出版社，1991 年 2 月。[28] 待提供的 Github 仓库。[29] R. A. Horn 和 C. R. Johnson，《矩阵分析》。剑桥大学出版社，1985 年。[30] C. H. Bennett、G. Brassard、C. Crépeau、R. Jozsa、A. Peres 和 W. K. Wootters，《通过经典信道和爱因斯坦-波多尔斯基-罗森信道传送未知量子态》，《物理评论快报》，第 70 卷，第 13 期，第 1895–1899 页，1993 年 3 月，出版者：美国物理学会。 [在线]。可访问：https://link.aps.org/doi/10.1103/PhysRevLett. 70 1895 。M. Horodecki、P. Horodecki 和 R. Horodecki，[31]《一般隐形传态信道、单态分数与准蒸馏》，《物理评论 A》，第 60 卷，第 3 期，第 1888–1898 页，1999 年 9 月，出版者：美国物理学会。[在线]。可访问：https://link.aps.org/doi/10.1103/PhysRevA. 60.1888[32] S. L. N. Hermans、M. Pompili、L. D. S. Martins、A. R.-P. Montblanch、H. K. C. Beukers、S. Baier、J. Borregaard 和 R. Hanson，《使用单光子协议纠缠远程量子比特：深入的理论与实验研究》，2022 年 8 月，arXiv:2208.07449 [quant-ph]。