arXiv:2303.00856v1 [quant-ph] 1 Mar 2023

单量子比特与多量子比特纠缠态广播：认证、密码学与分布式量子计算

Hiroki Sukeno，[1] Tzu-Chieh Wei，[1] Mark Hillery，[2,3] J´anos A. Bergou，[2,3] Dov Fields，[4] 和 Vladimir S. Malinovsk y[4]

[1] *C. N. Yang Institute for Theoretical Physics and Department of Physics and Astronomy, State University of New York at Stony Brook, NY 11794-3840, USA*[2] *Department of Physics and Astronomy, Hunter College of the CityUniversity of New York, 695 Park Avenue, New York, NY 10065, USA*

[3] *Graduate Center of the City University of New York, 365 Fifth Avenue, New York, NY 10016, USA*

[4] *DEVCOM Army Research Laboratory, Adelphi, MD 20783, USA*

借助测量实现的量子纠缠为网络中的各方提供了多种信息通信途径。在这项工作中，我们推广了此前的一种广播协议，并提出了广播乘积量子态和多体纠缠量子态的方案。在后一种情况下，发送方可以远程添加相位门，也可以中止状态分发。我们首先聚焦于网络中的乘积量子态广播，并将基本协议推广至包含任意基旋转，且允许有多个接收方和发送方。我们展示了如何在网络中添加和删除发送方。这一推广还涵盖了这样一种情况：待施加于广播态的相位事先未知，而是编码在另一个量子态中提供给发送方。乘积态广播的应用包括认证和三态量子密码学。在第二部分，我们研究将一个由多个接收方共享的单个多量子比特态进行分发，该态通过多量子比特相位门与这些接收方纠缠，其中图态便是一例。我们展示了接收方通过与发送方协作，仅凭 Pauli$X$ 基测量，就能协助执行远程分布式测量型量子计算。作为另一项应用，我们讨论了多量子比特格林伯格-霍恩-蔡林格态的分发。

一、引言

在量子网络中，以量子比特或量子位数形式编码的量子信息，可以通过直接发送量子比特，或利用共享纠缠（例如量子隐形传态协议） [1]，在用户之间传送。如果要将相同的信息发送给多个不同用户，则对于一般量子态而言，无克隆定理限制了实现这一目标的能力。尽管如此，人们仍研究了多种广播量子信息的方案，但这些方案通常要求为每个接收方提供每个量子比特一个纠缠比特（ebit） [2–5]。

如果已知要分发的量子态，另一种方法是采用远程态制备的一种形式 [6–10]。对于向单个接收者发送量子态的情况，远程态制备所需的经典通信成本低于量子隐形传态。进一步地，如果限制要发送的量子态集合，则可以将其改用于广播量子信息 [11, 12]。文献 [11] 中的协议利用了暗态，而文献 [12] 中的协议则使用了纠缠的 Dicke 态。

在文献 [12] 中，我们展示了如何将形如 $e^{i\theta}\alpha|0\rangle + e^{-i\theta}\beta|1\rangle$的量子比特态同时发送给多个不同的接收方，其中 α 和 β 是固定的，而 θ 可以由发送方改变。下面我们简要总结这一过程在两个接收方情形下的实现，并将其称为基本广播协议（BBP）。Alice 制备一个由一个三能级量子比特和两个量子比特组成的态，其形式为，

$$|\Psi^{(1,2)}\rangle_{abc} = \alpha^2|0\rangle_a|00\rangle_{bc} + \beta^2|1\rangle_a|11\rangle_{bc} + \alpha\beta|2\rangle_a(|01\rangle_{bc} + |10\rangle_{bc}), \quad (1)$$

并将这两个量子比特分别传输给 Bob 和 Charlie。可以将该态视为由 Alice、Bob 和 Charlie 共享的初始状态。请注意，上标（1、2）表示我们有一个发送方和两个接收方。稍后，当我们考虑 M 个发送方和 N 个接收方的情形时，会将其推广到 $|\Psi^{(M,N)}\rangle$ 。

Alice 随后对她的三能级量子比特施加算符 $U_a(\theta)$，其中 $U_a|0\rangle_a = e^{2i\theta}|0\rangle_a$、$U_a|1\rangle_a = e^{-2i\theta}|1\rangle_a$和$U_a|2\rangle_a = |2\rangle_a$。然后，她在基

$$|u_0\rangle_a = \frac{1}{\sqrt{3}}(|0\rangle_a + |1\rangle_a + |2\rangle_a)$$
$$|u_1\rangle_a = \frac{1}{\sqrt{3}}(e^{2\pi i/3}|0\rangle_a + e^{-2\pi i/3}|1\rangle_a + |2\rangle_a)$$
$$|u_2\rangle_a = \frac{1}{\sqrt{3}}(e^{-2\pi i/3}|0\rangle_a + e^{2\pi i/3}|1\rangle_a + |2\rangle_a), \quad (2)$$

并将测量结果 m_a （可能为 0、1 或 2）发送给 Bob 和 Charlie。他们各自对自己的量子比特施加一个取决于 m_a 的校正算符。具体而言，对于 $m_a = 0$，无需校正。对于 $m_a = 1$，Bob 和 Charlie 各自施加 U_C，其中 $U_C|0\rangle_a = e^{-i\pi/3}|0\rangle_a$、$U_C|1\rangle_a = e^{-i\pi/3}|1\rangle_a$；对于 $m_a = 2$，则改为施加 U_C^{-1} 。Bob 和 Charlie 最终得到的状态与开头所述的量子比特状态相同，即 $e^{i\theta}\alpha|0\rangle + e^{-i\theta}\beta|1\rangle$。

该过程既是远程态制备的限制形式，也是其扩展形式。它是一种限制形式，因为传输状态的集合并非整个量子比特空间，因为 α 和 β 是固定的。它也是一种扩展形式，因为这些状态会发送给多个接收方。在参考文献 [12], 中，我们还展示了如何以概率方式发送一个发送方未知、但编码在量子态中的值 θ 。

发送给多个接收方。在这里，我们希望扩展这些结果并推广我们的 BBP。首先，我们将展示 Alice 如何对远程量子比特施加更一般的一组操作。她可以施加 $e^{i\theta}|s_0\rangle\langle s_0| + e^{-i\theta}|s_1\rangle\langle s_1|$,，而非 $e^{i\theta}|0\rangle\langle 0| + e^{-i\theta}|1\rangle\langle 1|$，其中 $\langle s_0|s_1\rangle = 0$。接下来，我们将展示如何在该过程中纳入多个发送方，以及如何从网络中添加或删除发送方。然后，我们将进一步探讨 Alice 不知道 θ 的情况；她接收到的量子态中编码了该值。存在概率性和近似过程，可使她将一般的未知 θ 转移到 Bob 和 Charlie 持有的量子比特中。此外，我们还将介绍这些协议的另外两种应用：第一种应用能够生成可用于认证的序列，第二种则是一种三态量子密钥分发（QKD）过程。

此外，作为对 BBP 的扩展，我们还考虑在多个接收方之间分发一个共享的多量子比特态，其中包括先前的乘积广播量子比特态，以及通过额外的多量子比特纠缠相位门扩展得到的状态和一般的稳定子态（例如图态 [19]）。我们说明了如何通过两种不同的方式分发其中一些多体纠缠态。结果表明，在这两种方法中，发送方都可以在分发完成后选择相位并将其隐形传态给接收方。尤其是后一种方法，使远程分布式基于测量的量子计算（MBQC） [27, 28], 成为可能：发送方进行测量轴适配，而接收方只需进行 X 基测量。此外，我们还描述了如何分发 GHZ 态[26]。

本文其余部分的结构如下。第 II 节中，我们扩展该协议，并展示 Alice 可以对远程量子比特施加更一般的操作。随后，我们说明如何将该协议推广到多个发送方的情形。第 III 节中，我们讨论 Alice 向接收方发送未知相位这一协议的应用。随后，我们讨论其在认证和三态量子密钥分发中的应用。第 IV 节中，我们说明广播分布式稳定子态的方法。第 V 节中，我们讨论分布式稳定子态的应用。第 VI 节为结论。

II. 单量子比特态广播方案的扩展

在本节中，我们介绍几种推广形式，
我们的 BBP。首先，我们将其扩展到广播态中的基可以是任意基的情形。然后，我们将 BBP 推广到多个发送方和多个接收方。

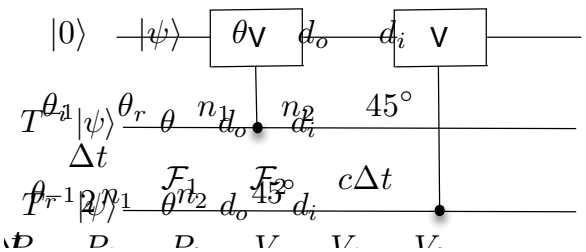

图1. 生成公式（3）中状态的量子电路。顶线表示一个三能级量子比特，初始处于状态 $|0\rangle$，底部两条线表示量子比特。输出端对量子比特施加操作 T。

A. 使用一般单量子比特酉变换扩展 BBP

考虑以下情形。Alice 有两个量子比特，它们都处于状态 $|\psi\rangle$，她可能知道也可能不知道该状态。她想以旋转基 ($e^{-i\theta}|s_1\rangle\langle s_1|$ $|\psi\rangle$ $e^{-i\theta}|s_0\rangle\langle s_0| +$ θ) 将量子比特传送给 Bob 和 Charlie，并可在之后改变相位角。这里，$\{|s_0\rangle,\ |s_1\rangle\}$ 是一个正交归一量子比特基。令 T 为将$\{|0\rangle,$ $|1\rangle\}$ 基映射到 $\{|s_0\rangle,\ |s_1\rangle\}$ 基的幺正算符，即 $T|j\rangle = |s_j\rangle$（$j = 0,\ 1$），并假设 $|\psi\rangle = \mu|s_0\rangle + \nu|s_1\rangle$。Alice 首先对每个量子比特应用 T^{-1}，然后将它们送入图1所示的量子电路。顶线是一个三能级量子比特，底下两条线是两个量子比特。标记为 V 的门是受控移位门，其中 V 是移位算符，控制端是量子比特，目标端是三能级量子比特。如果控制端处于状态 $|0\rangle$，则目标端不发生任何变化；如果控制端处于状态 $|1\rangle$，则对三能级量子比特应用 V，其中 $V|j\rangle = |(j-1)$模$3\rangle$，适用于$j = 0,$ 1，2，减法按模 3 进行。随后，她对量子电路输出端的量子比特应用 $T \otimes T$。所得状态为

$$\mu^2|0\rangle_a|s_0, s_0\rangle_{bc} + \nu^2|1\rangle_a|s_1, s_1\rangle_{bc} + \mu\nu|2\rangle_a(|s_0, s_1\rangle_{bc} + |s_1, s_0\rangle_{bc}). \quad (3)$$

随后将量子比特发送给 Bob 和 Charlie，并且在稍后的时间 $U_a(\theta)$可像原协议中那样作用于三能级量子比特。之后测量该三能级量子比特，Bob 和 Charlie 根据 Alice 的测量结果执行任何必要的纠正过程。

B. 扩展到多个发送方

在本部分中，我们将 BBP 推广到多个发送方和多个接收方的情况。

1. Example: two senders and two receivers

首先，我们研究两个发送方和两个接收方的示例。我们有两位 Alice，即作为发送方的 Alice 1 和 Alice 2，以及作为接收方的 Bob 和 Charlie。Alice 1 和 Alice 2 拥有三能级量子位，而 Bob 和 Charlie 拥有量子比特。我们从纠缠的两个三能级量子位和两个量子比特状态开始

$$\begin{aligned}|\Psi^{(2,2)}\rangle = \alpha^2|0\rangle_{a1}\otimes|0\rangle_{a2}\otimes|00\rangle_{bc}\\ +\alpha\beta|1\rangle_{a1}\otimes|1\rangle_{a2}\otimes(|01\rangle_{bc}+|10\rangle_{bc})\\ +\beta^2|2\rangle_{a1}\otimes|2\rangle_{a2}\otimes|11\rangle_{bc},\end{aligned} \tag{4}$$

该态可在本地制备，例如由 Alice 1 制备，然后将相应的三能级量子比特和量子比特分发给其他人。Alice 1 对她的三能级量子比特施加算符 $U_1(\theta_1)$，其中

$$\begin{aligned}&U_1(\theta_1)|0\rangle_{a1} = e^{i\theta_1}|0\rangle_{a1}, \qquad U_1(\theta_1)|1\rangle_{a1} = |1\rangle_{a1},\\ &U_1(\theta_1)|2\rangle_{a1} = e^{-i\theta_1}|2\rangle_{a1}.\end{aligned} \tag{5}$$

Alice 2 对她的三能级量子比特施加 $U_2(\theta_2)$，其作用与 U_1 相同，只是将 θ_1 替换为 θ_2。我们发现

$$\begin{aligned}&\big(I_{bc}\otimes U_1(\theta_1)\otimes U_2(\theta_2)\big)|\Psi^{(2,2)}\rangle\\ &= \alpha^2 e^{i(\theta_1+\theta_2)}|0\rangle_{a1}\otimes|0\rangle_{a2}\otimes|00\rangle_{bc}\\ &\quad +\alpha\beta|1\rangle_{a1}\otimes|1\rangle_{a2}\otimes(|01\rangle_{bc}+|10\rangle_{bc})\\ &\quad +\beta^2 e^{-i(\theta_1+\theta_2)}|2\rangle_{a1}\otimes|2\rangle_{a2}\otimes|11\rangle_{bc}.\end{aligned} \tag{6}$$

现在，Alice 1 和 Alice 2 都在 $\{|u_j\rangle\,|\,j=0,\ 1,\ 2\}$ 基下测量各自的三能级量子比特，其中

$$|u_j\rangle = \frac{1}{\sqrt{3}}\sum_{l=0}^{2} e^{2\pi i l j/3}|l\rangle. \tag{7}$$

如果 Alice 1 得到 j，而 Alice 2 得到 k，那么 Bob 和 Charlie 的联合态为

$$|\Psi^{(2,2)}\rangle \xrightarrow[\text{measure}]{U_1(\theta_1),U_2(\theta_2)} |\Phi_{(j,k)}\rangle, \tag{8}$$

其中

$$\begin{aligned}|\Phi_{(j,k)}\rangle = &\Big[\alpha e^{i(\theta_1+\theta_2)/2}|0\rangle_b + \beta e^{-2\pi i(j+k)/3}e^{-i(\theta_1+\theta_2)/2}|1\rangle_b\Big]\\ &\otimes\Big[\alpha e^{i(\theta_1+\theta_2)/2}|0\rangle_c + \beta e^{-2\pi i(j+k)/3}e^{-i(\theta_1+\theta_2)/2}|1\rangle_c\Big].\end{aligned} \tag{9}$$

如果 Alice 1 和 Alice 2 告诉 Bob 和 Charlie 他们的测量结果，那么 Bob 和 Charlie 各自都可以对自己的量子比特施加一个幺正算符，以消除相位因子 $e^{-2\pi i(j+k)/3}$。因此，Bob 和 Charlie 各自收到的量子比特都包含来自 Alice 1 和 Alice 2 的贡献。这个过程可以调整为仅由一位 Alice 确定发送的量子比特。例如，如果 Alice 2 不施加 $U_2(\theta_2)$，那么 $\theta_2 = 0$，发送的量子比特就仅由 Alice 1 确定。不过，要将这些量子比特发送给 Bob 和 Charlie，还需要 Alice 2 的合作；她必须测量自己的三能级量子比特，并将结果发送给 Bob 和 Charlie。

2. General case: M senders and N receivers

这个过程可以扩展到有 M 位发送方和 N 位接收方的情形。我们从一个由 M 个具有 $N+1$ 个能级的量子位数和 N 个量子比特组成的状态开始

$$|\Psi^{(M,N)}\rangle = \sum_{k=0}^{N}\alpha^k\beta^{N-k}\binom{N}{k}^{1/2}\left(\prod_{j=1}^{M}|k\rangle_{aj}\right)|k;N{-}k\rangle. \tag{10}$$

这里，$|k\rangle_{aj}$ 是 Alice j的量子位数的状态，且 $|k;\ N{-}k\rangle$ 是一个 N量子比特态，它是归一化完全对称态，其中 k 个量子比特处于状态$|0\rangle$，而 $N-k$ 个处于状态 $|1\rangle$,

$$|k;N-k\rangle \equiv \binom{N}{k}^{-1/2}\text{Symmetrize}\big\{\underbrace{|0\cdots0}_{k}\underbrace{1\cdots1\rangle}_{N-k}\big\}. \tag{11}$$

这些 N 量子比特态也称为 Dicke 态。每位 Alice j 持有一个量子位数，每位接收者持有一个量子比特。Alice j 现在可以通过对她的量子位数施加算符 U_{aj}，选择一个角度 θ_j，其中

$$U_{aj}(\theta_j)|k\rangle_{aj} = e^{i(2k-N)\theta_j}|k\rangle_{aj}. \tag{12}$$

所得状态为

$$\begin{aligned}\prod_{j=1}^{M}U_{aj}|\Psi^{(M,N)}\rangle = &\sum_{k=0}^{N}\Big(\alpha\prod_{j'=1}^{M}e^{i\theta_{j'}}\Big)^k\Big(\beta\prod_{j''=1}^{M}e^{-\theta_{j''}}\Big)^{N-k}\\ &\times\binom{N}{k}^{1/2}\prod_{j_3=1}^{M}|k\rangle_{aj_3}|k;N-k\rangle.\end{aligned} \tag{13}$$

每位 Alice j 现在都在基

$$|u_n\rangle = \frac{1}{\sqrt{N+1}}\sum_{k=0}^{N}e^{2\pi i n k/(N+1)}|k\rangle, \tag{14}$$

其中 $n=0,\ 1,\ \ldots N$。如果 Alice j得到结果 $|u_{n_j}\rangle$，则未归一化的 N 量子比特态为

$$\begin{aligned}&|\Psi^{(M,N)}\rangle \xrightarrow[\text{measure}]{U_j(\theta_j)^{\otimes M}} |\Phi_{\bar{n}}\rangle\ ,\\ &|\Phi_{\bar{n}}\rangle = \prod_{l=1}^{N}\Big(\alpha e^{i\sum_{j=1}^{M}\theta_j}e^{-2\pi i(\sum_{j=1}^{M}n_j)/(N+1)}|0\rangle_l\\ &\qquad +\beta e^{-i\sum_{j=1}^{M}\theta_j}|1\rangle_l\Big),\end{aligned} \tag{15}$$

其中 $\bar{n}=(n_1,\ n_2,\ \ldots n_M)$。随后，每位 Alice 都广播其测量结果，各方将校正算符 $U_{\bar{n}}$ 施加到自己的量子比特上，其中$U_{\bar{n}}|0\rangle = \exp[2\pi i(\sum_{j=1}^{M}n_j)/(N+1)]|0\rangle$ 且 $U_{\bar{n}}|1\rangle = |1\rangle$。这样，每一方都将持有状态 $\alpha e^{i\sum_{j=1}^{M}\theta_j}|0\rangle + \beta e^{-i\sum_{j=1}^{M}\theta_j}|1\rangle$。

如果只有一名发送方需要发送消息，则该发送方执行相应的幺正操作，而

其他发送方不执行任何操作。然而，所有发送方都必须测量其量子dits并广播测量结果，才能完成该过程。

3. *Adding senders to the network: $M \to M+1$*

如果原有发送方中的一位与其他发送方共享一个完全纠缠态，就可以增加发送方。本小节旨在介绍一种从 $|\Psi^{(M,N)}\rangle$ ($M \geq 1$)生成 $|\Psi^{(M+1,N)}\rangle$ 的过程。假设我们从以下状态开始

$$|\Psi^{(M,N)}\rangle \otimes \frac{1}{\sqrt{N+1}} \sum_{\ell=0}^{N} |\ell\rangle_{aM'} |\ell\rangle_{a(M+1)}. \tag{16}$$

量子dits aM和 aM'均由 Alice M持有，而a(M+1)由我们想要添加为额外发送方的人 Alice $M+1$持有。Alice M 让它们通过一个受控移位门（记作 $CX_{c,\,t}$），其中 aM 为控制位， aM' 为目标位。受控移位门的作用是 $|k\rangle_{aM}|\ell\rangle_{aM'} \to |k\rangle_{aM}|\ell+k\rangle_{aM'}$，其中加法按 $N+1$取模。Alice M 现在在计算基下测量 aM'。如果她得到 $|j\rangle_{aM'}$，

$$\begin{aligned} &CX_{aM,aM'}\Big(|\Psi^{(M,N)}\rangle \otimes \frac{1}{\sqrt{N+1}} \sum_{\ell=0}^{N} |\ell\rangle_{aM'} |\ell\rangle_{a(M+1)}\Big) \\ &\xrightarrow{\text{measure}} \sum_{k=0}^{N} \alpha^k \beta^{N-k} \binom{N}{k}^{1/2} \\ &\qquad \times \prod_{j=1}^{M} |k\rangle_{aj} \otimes |j-k\rangle_{a(M+1)} \otimes |k; N-k\rangle. \end{aligned} \tag{17}$$

Alice M 将她的测量结果发送给 Alice$M+1$，后者现在可以应用局域幺正算符来映射 $|j-k\rangle_{a(M+1)} \to |k\rangle_{a(M+1)}$，此时得到的状态为 $|\Psi^{(M+1,N)}\rangle$。

发送方只需测量自己的三能级量子比特即可将自己删除，并将测量结果发送给 Bob_1, Bob_2, ...Bob_N，之后他们各自可以应用酉算符，消除删除方测量所产生的相位因子。

III. 单量子比特态广播的进一步推广与应用

这里，我们介绍单量子比特态广播的几种应用。第一种是将其扩展到发送编码在量子态中的未知相位。第二种是将我们的广播协议应用于身份认证。最后一种是将其应用于使用三个态的量子密钥分发。

A. 发送未知相位

让我们回到只有一位发送方 Alice 的情况：她想向 Bob 和 Charlie 发送一个带有未知相位的状态。这一问题已在 [12]中得到研究。在那里，Alice 有一个三能级量子比特，它与 Bob 和 Charlie 的量子比特纠缠在一起。该相位编码在三能级量子比特的状态中

$$|\Phi\rangle_d = \frac{1}{\sqrt{3}}(e^{2i\theta}|0\rangle_d + |1\rangle_d + e^{-2i\theta}|2\rangle_d). \tag{18}$$

通过结合幺正操作与测量，Alice 可以将状态 $e^{i\theta}\alpha|0\rangle + e^{-i\theta}\beta|1\rangle$发送给 Bob 和 Charlie，其中，和往常一样， α 和 β 是固定的，成功概率为 $1/3$。这里我们希望进一步拓展这一结果。首先，我们将证明，若 θ 属于集合 $\{\pi k/K \,|\, k = 0, 1, \ldots K-1\}$，并编码在一个 K级系统中，其中 K 固定，则我们可以将状态 $e^{i\theta}\alpha|0\rangle + e^{-i\theta}\beta|1\rangle$ 确定无疑地发送给 Bob 和 Charlie，代价是使用维数更高的编码态。在这种情况下，编码态彼此正交，因此 Alice 只需在适当的基底中对它们进行测量，就能确定它们编码的角度，然后对她的三能级量子比特应用适当的幺正算符。此外，原则上还可以执行逆量子傅里叶变换来估计相位 θ。在$\theta = 2\pi k/K$的情况下，进行相位估计时使用有限个辅助比特即可获得精确相位。不过，下面我们将采用另一种策略，并可将其推广到一般角度的情形。对于一般角度，该协议要么是近似的，要么是概率性的。

1. *Sending unknown restricted angle*

这里我们讨论有两个接收方的情形，并证明 Alice 可以发送一个她并不知晓、但编码在状态（带有标签 d）中的角度。接收方数量为 N 的情形将在附录 A 中给出。

我们从以下状态开始

$$\begin{aligned} &(\alpha^2|0\rangle_a|v_0\rangle_{bc} + \alpha\beta|1\rangle_a|v_1\rangle_{bc} + \beta^2|2\rangle_a|v_2\rangle_{bc}) \\ &\times \frac{1}{\sqrt{K}} \left(\sum_{j=0}^{K-1} e^{2\pi i k j/K}|j\rangle_d\right). \end{aligned} \tag{19}$$

Alice 持有一个三能级量子比特 a，Bob 和 Charlie 分别持有量子比特 b 和c，角度 $2\pi k/K$ 编码在一个 K 维量子位数 d 中，并已发送给 Alice。这里$|v_0\rangle_{bc} = |00\rangle_{bc}$，$|v_1\rangle_{bc} = |01\rangle_{bc} + |10\rangle_{bc}$，以及 $|v_2\rangle_{bc} = |11\rangle$。Alice 不知道这个角度是多少。她对 ad 系统执行受控移位操作，其中 a 为控制端，其作用为 $|j\rangle_a|k\rangle_d \to |j\rangle_a|k+j\rangle_d$，其中加法对 K取模。由此得到以下结果

状态

$$\frac{1}{\sqrt{K}}\left[\alpha^2|0\rangle_a|v_0\rangle_{bc}\left(\sum_{j=0}^{K-1}e^{2\pi ikj/K}|j\rangle_d\right)\right.$$
$$+\alpha\beta|1\rangle_a|v_1\rangle_{bc}\left(\sum_{j=0}^{K-1}e^{2\pi ikj/K}|j+1\rangle_d\right)$$
$$\left.+\beta^2|2\rangle_a|v_2\rangle_{bc}\left(\sum_{j=0}^{K-1}e^{2\pi ikj/K}|j+2\rangle_d\right)\right]. \quad (20)$$

利用恒等式

$$\sum_{j=0}^{K-1}e^{2\pi ikj/K}|j+l\rangle_d=e^{-2\pi ikl/K}\sum_{j=0}^{K-1}e^{2\pi ikj/K}|j\rangle_d, \quad (21)$$

上述状态变为

$$e^{-2\pi ik/K}\left[(\alpha e^{i\pi k/K})^2|0\rangle_a|v_0\rangle_{bc}+\alpha\beta|1\rangle_a|v_1\rangle_{bc}\right.$$
$$\left.+(\beta e^{-i\pi k/K})^2|2\rangle_a|v_2\rangle_{bc}\right]\frac{1}{\sqrt{K}}\left(\sum_{j=0}^{K-1}e^{2\pi ikj/K}|j\rangle_d\right) \quad (22)$$

如果 Alice 现在执行向 Bob 和 Charlie 发送量子比特态的步骤，他们都会收到 $\alpha e^{i\pi k/K}|0\rangle+\beta e^{-i\pi k/K}|1\rangle$。请注意，编码角度的状态不受此过程影响，因此可以将其发送给另一位 Alice，由她将编码角度传输给另外一位 Bob 和 Charlie。

2. Sending unknown general angle

现在让我们考虑一般角度 θ。我们从状态开始

$$(\alpha^2|0\rangle_a|v_0\rangle_{bc}+\alpha\beta|1\rangle_a|v_1\rangle_{bc}+\beta^2|2\rangle_a|v_2\rangle_{bc})$$
$$\times\frac{1}{\sqrt{K}}\left(\sum_{k=0}^{K-1}e^{ik\theta}|k\rangle_d\right). \quad (23)$$

现在，Alice 像之前一样执行受控移位操作。假设她在 $\{|u_j\rangle\,|\,j=0$、1、$2\}$ 基上测量她的三能级量子比特（见式 (2)），并得到 $|u_0\rangle$（如果她得到另外两个基矢中的任意一个，Bob 和 Charlie 会执行校正操作，以消除不需要的相位因子）。所得 bcd 状态为

$$|w_0\rangle_{bc}|0\rangle_d+|w_1\rangle_{bc}|1\rangle_d+|w_2\rangle_{bc}\times\frac{1}{\sqrt{K}}\Big(\sum_{k=2}^{K-1}e^{ik\theta}|k\rangle_d\Big). \quad (24)$$

这里，我们有

$$|w_0\rangle_{bc}=\alpha^2|v_0\rangle_{bc}+\alpha\beta e^{i(K-1)\theta}|v_1\rangle_{bc}$$
$$+\beta^2e^{i(K-2)\theta}|v_2\rangle_{bc} \quad (25)$$
$$|w_1\rangle_{bc}=\alpha^2e^{i\theta}|v_0\rangle_{bc}+\alpha\beta|v_1\rangle_{bc}$$
$$+\beta^2e^{i(K-1)\theta}|v_2\rangle_{bc} \quad (26)$$
$$|w_2\rangle_{bc}=\alpha^2|v_0\rangle_{bc}+\alpha\beta e^{-i\theta}|v_1\rangle_{bc}$$
$$+\beta^2e^{-2i\theta}|v_2\rangle_{bc} \quad (27)$$
$$=(\alpha|0\rangle_b+\beta e^{-i\theta}|1\rangle_b)\otimes(\alpha|0\rangle_c+\beta e^{-i\theta}|1\rangle_c).$$

此时，如果 Alice 想采用概率性协议，她最显而易见的做法是以基 $\{|k\rangle_d\,|\,k=0,\ 1,\ \ldots K-1\}$测量 d系统。如果她得到 $k=0$ 或 1，$|w_0\rangle$ 和 $|w_1\rangle$ 便会在 Bob 与 Charlie 之间纠缠，无法通过局部操作将其纠正为所需的广播态。反之，如果她得到除 $k=0,\ 1$ 以外的任何结果，协议便成功了，也就是说，Bob 和 Charlie 得到状态 $|w_2\rangle_{bc}$，成功概率为 $(K-2)/K$，且与 θ无关。然而，此过程会破坏 d 状态中残留的所有相位信息。我们将在附录 A 中讨论一些改进方法，这些方法能够在一定程度上重复使用编码态。

B. 认证

每个位置都不一致的符号序列可用于认证协议 [14]。Alice 可以向 Bob 提供她序列中的元素来证明自己的身份，而 Bob 可以检查 Alice 发来的内容是否在每个位置都与他的序列不一致。对于未发送元素的检验序列，也就是发送的状态序列与测量结果序列不一致的情况，已被用于数字签名方案 [15]。如果参与方多于两方，不一致序列便可用于匿名发送消息或认证选票。假设有三方：Alice、Bob 和 Charlie，他们各自持有由四个符号组成、且所有位置彼此均不一致的序列。Bob 想给 Alice 发送一条消息，但不希望她知道消息来自谁。他将自己序列的一部分附在消息上，然后发给 Alice。Alice 随后可以验证消息来自 Bob 或 Charlie，但无法判断究竟来自哪一方。在投票场景中，每位选民都有一个序列，负责计票的计票机构也有一个序列。每位选民在提交选票时附上自己的序列。计票机构可以检查每个序列是否在所有位置都与自己的序列不一致，从而认证选票，但它无法知道哪个序列来自哪位选民。例如，Cabello 曾提出一种利用超单态量子态生成此类序列的量子方法 [16]。

这里我们将展示如何生成由三个符号组成的三条随机序列。这些序列具有这样的性质：Bob 和 Charlie 持有的序列在每个位置上都与 Alice 持有的序列不同，

但他们彼此持有的序列不一定不同。此外，Bob 不知道 Charlie 的序列，反之亦然。该过程以量子比特的三元态和反三元态为基础。将量子比特的三元态定义为

$$
\begin{aligned}
|\psi_0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
|\psi_1\rangle &= \frac{1}{\sqrt{2}}(e^{2\pi i/3}|0\rangle + e^{-2\pi i/3}|1\rangle) \\
|\psi_2\rangle &= \frac{1}{\sqrt{2}}(e^{-2\pi i/3}|0\rangle + e^{2\pi i/3}|1\rangle),
\end{aligned} \tag{28}
$$

类似地，反三元态为

$$
\begin{aligned}
|\bar{\psi}_0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
|\bar{\psi}_1\rangle &= \frac{1}{\sqrt{2}}(e^{2\pi i/3}|0\rangle - e^{-2\pi i/3}|1\rangle) \\
|\bar{\psi}_2\rangle &= \frac{1}{\sqrt{2}}(e^{-2\pi i/3}|0\rangle - e^{2\pi i/3}|1\rangle).
\end{aligned} \tag{29}
$$

这是通常三元态和反三元态的一个旋转版本，但在我们一直讨论的这类过程中，这些态最为有用。注意，

$$\langle\psi_j|\psi_k\rangle = \langle\bar{\psi}_j|\bar{\psi}_k\rangle = -\frac{1}{2} \quad (j \neq k), \tag{30}$$

$$\langle\bar{\psi}_j|\psi_j\rangle = 0. \tag{31}$$

现在考虑基于反三元态的 POVM，其测量算符为

$$A_j = \sqrt{\frac{2}{3}}|\bar{\psi}_j\rangle\langle\bar{\psi}_j|, \quad \sum_{j=0}^{2} A_j^\dagger A_j = I, \tag{32}$$

在状态 ρ 中获得结果 j 的概率为 $\mathrm{Tr}(\rho A_j^\dagger A_j)$。Bob 和 Charlie 将使用此 POVM 测量他们的量子比特，并利用测量结果生成各自的序列。

为生成序列，Alice 按照原始广播过程向 Bob 和 Charlie 发送一个处于某个三态之一的量子比特。Bob 和 Charlie 使用反三元态 POVM 测量各自的量子比特，并将测量结果作为序列中的元素。Bob 和 Charlie 得到的结果都不同于 Alice 发送的状态。例如，如果 Alice 发送了 $|\psi_0\rangle$，那么 Bob 可以得到 1 或 2，Charlie 也可以得到 1 或 2。Bob 不知道 Charlie 的结果，Charlie 也不知道 Bob 的结果，而且他们的结果可能相同，也可能不同。（结果相同的概率会随着序列长度的增加而呈指数级下降。）不过，他们的结果都会不同于 Alice 发送的状态。因此，Bob 和 Charlie 可以分别建立一个可用于与 Alice 进行认证的序列。我们在表 I 中给出一个示例。

如果有两位 Alice（如第 II B 1 节所示），Bob 和 Charlie 接收到的量子比特将取决于他们各自选择的角度。具体而言，该角度将是

Slot	1	2	3	4	5	6
状态 Alice 广播 $\|\psi_1\rangle$	$\|\psi_2\rangle$	$\|\psi_1\rangle$	$\|\psi_0\rangle$	$\|\psi_1\rangle$	$\|\psi_2\rangle$	
Bob 的结果	$\|\bar{\psi}_2\rangle$	$\|\bar{\psi}_1\rangle$	$\|\bar{\psi}_0\rangle$	$\|\bar{\psi}_2\rangle$	$\|\bar{\psi}_2\rangle$	$\|\bar{\psi}_0\rangle$
Charlie 的结果	$\|\bar{\psi}_0\rangle$	$\|\bar{\psi}_1\rangle$	$\|\bar{\psi}_2\rangle$	$\|\bar{\psi}_2\rangle$	$\|\bar{\psi}_0\rangle$	$\|\bar{\psi}_0\rangle$

表 I. 如何从广播态生成用于认证的密钥示例。

Alice 1 和 Alice 2 所选角度之和。为了对 Bob 或 Charlie 进行身份验证，两位 Alice 必须合作。

我们注意到，在有两个接收方和一个发送方的情况下，Alice 只需在 BBP 中设置 $\alpha = \beta = 1/\sqrt{2}$ 和 $\theta = 0$，然后便可通过来自她测量的随机相位生成其中一种三态。还可以考虑将三态直接广播给 N 个接收方，此时 Alice 会使用 α、β 和 $U(\theta)$，并将她的测量结果告知接收方，以便他们校正不需要的相位。

C. 三态量子密钥分发

Phoenix、Barnett 和 Chefles (PBC) [17] 利用方程 (28) 中的三个态提出了一种三态量子密钥分发协议。发送方 Alice 会随机选择三个态之一发送给接收者 Bob，而 Bob 随后会随机选择三个测量基

$$\{|\psi_j\rangle, |\bar{\psi}_j\rangle\} \quad (j = 0, 1, 2) \tag{33}$$

来测量收到的量子比特。我们先介绍他们的协议（Alice 和一位 Bob），随后便可清楚看出，我们的广播协议允许 Alice 分别与两位 Bob 建立密钥。

首先，如果 Bob 的测量结果对应于 $|\psi_j\rangle$，他就宣布本轮失败。否则，Alice 会宣布方程 (28) 中她未发送的一个态。假设 Bob 在标记为 $j = 1$ 的基下测量，而 Alice 宣布她没有发送 $j = 1$，那么 Bob 无法推断出任何信息，因为他的测量结果 $|\bar{\psi}_1\rangle$ 基本上印证了这一点。只有在 Alice 宣布的态与 Bob 的测量基标签不同时，这种情形才有用。例如，如果她宣布自己没有发送 $j = 0$，那么 Bob 可以推断她一定发送了 $|\psi_{j=2}\rangle$，我们将此事件标记为（发送标签，未发送态）=(2,0)。接着，根据如下规则：从第一个索引到第二个索引，如果相差 $+1$ 跳（模 3），就将其赋值为 0。另一方面，如果 Alice 宣布她没有发送 $j = 2$，那么 Bob 可以推断 Alice 所发送态的标签为 $j = 0$，该事件便标记为 (0,2)，从 0 到 2（模 3）需要 $+2$，因此对应于 1。我们在图2中说明了将结果赋值为 0 或 1 的约定。表II给出了 PBC 协议的一个示例。

对很长的序列 k 重复上述步骤后，就可以建立一个预期长度为

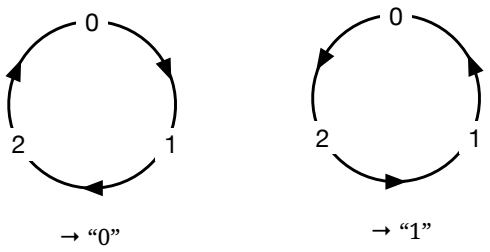

图2. PBC量子密钥分发中的秘密密钥编码。每个圆圈内的数字表示三态 j 的标签 $|\psi_j\rangle$ （式（28））。读取这对标签 j：已发送状态的标签（Alice知道该标签，或Bob根据测量推断出该标签），以及未发送状态的标签（由Alice公布），然后查看箭头“$j \to k$”是逆时针还是顺时针流动，分别编码“0”和“1”。

Time	1	2	3	4	5	6	7	8	9	10
Alice广播的状态： $\|\psi_j\rangle$	$\|\psi_1\rangle$	$\|\psi_2\rangle$	$\|\psi_1\rangle$	$\|\psi_0\rangle$	$\|\psi_1\rangle$	$\|\psi_2\rangle$	$\|\psi_0\rangle$	$\|\psi_0\rangle$	$\|\psi_2\rangle$	$\|\psi_1\rangle$
Bob的测量 $\{\|\psi_\ell\rangle,\ \|\ \ \bar{\psi}_\ell\rangle\}$	1	1	0	2	1	1	1	2	0	1
结果	$\|\psi_1\rangle$	$\|\bar{\psi}_1\rangle$	$\|\psi_0\rangle$	$\|\bar{\psi}_2\rangle$	$\|\psi_1\rangle$	$\|\bar{\psi}_1\rangle$	$\|\psi_1\rangle$	$\|\bar{\psi}_2\rangle$	$\|\bar{\psi}_0\rangle$	$\|\psi_1\rangle$
Alice宣布不是（k）		0		1		1		2	1	
Bob成功推断出 $\|\psi_j\rangle$		✓		✓		No		No	✓	
$j \to k$		$2 \to 0$		$0 \to 1$					$2 \to 1$	
共享比特		0		0					1	

表II. PBC三态量子密钥分发协议的一个示例。在原始设计中， [17], Bob执行随机选择的二结果投影测量；这可以替换为由反三元态定义的POVM。

$k/3$ 的密钥。注意，Bob 可以使用由 $\{\frac{2}{3}|\bar{\psi}_j\rangle\langle\bar{\psi}_j|, j = 0,1,2\}$ 定义的 POVM，这样可获得 3/2 倍的提升，预期密钥长度为 $k/2$。在我们的协议中，*Alice* 可以随机地向两个 *Bob* 广播相同的状态。也就是说，我们使用广播态 $|\Psi^{(1,2)}\rangle$ ，其中 $\alpha = \beta = \frac{1}{\sqrt{2}}$ 和 $\theta = 0$，于是两个 Bob 都会得到三元态之一。然而，两个 Bob 可能选择不同的投影测量基；若采用 POVM，他们也可能得到不同的正值算符值测度结果。显然，根据 PBC 协议，Alice 与每个 Bob 分别共享不同的密钥。（两个 Bob 也可能共享密钥中一个较小的子集。）

显然，接收方可以多于两个，在这种情况下，我们使用 $|\Psi^{(1,N)}\rangle$ 将同一状态分发给 N 个接收方。Alice可以不采用由测量产生的随机相位，而是使用 U（θ）或预设参数 α，β 来选择要发送的三态，并让接收方校正测量 $e^{2\pi nj/(N+1)}$ （$n = 0$，..，N）产生的不需要的相位。

IV. 广播分布式稳定子态

本节将讨论广播分布式稳定子态 $|\psi\rangle$ $S|\psi\rangle = $ 的不同方 $|\psi\rangle$ S 式，其中任意 G 都是由泡利算符构成、且不包含 $-I$的群的乘积。发送方可以选择分发该状态，也可以中止任务。我们将主要以图态为例，簇态是图态的特例。此外，所有稳定子态在局域等价意义下都等价于图态 [20]。图态定义于一个图之上，该图由一组顶点 V 和一组边 E 组成，其稳定子具有 $K_v = X_v \bigotimes_{\langle u,v\rangle \in E} Z_u$ 的形式，其中 $v \in V$。（注意，我们使用符号 K 表示图态稳定子，而不是S，这是文献中的惯例。）由于$K_v = (\prod_{\langle u,v\rangle \in E} CZ_{v,\ u})^{\dagger} X_v (\prod_{\langle u,v\rangle \in E} CZ_{v,\ u})$，图态 $|\psi_G\rangle$ 由下式给出

$$|\psi_G\rangle = U_{CZ}|+\rangle^{\otimes |V|}, \quad U_{CZ} = \prod_{\langle u,v\rangle \in E} CZ_{u,v}. \qquad (34)$$

我们讨论的方法之一可用于非稳定子态。

A. 图态的分发（I）

本节介绍的方法适用于图态及其他非稳定子态，例如超图态，以及关键纠缠部分仅由相位构成的其他状态。

首先考虑分发图态的最简单示例，这是对引言中所述设置的扩展。具体而言，参与者包括 Alice（发送方）和两个 Bobs（接收方）；最终，两个接收方将共享两个量子比特，它们构成一个双量子比特图态（$V = \{v_1, v_2\}$）。我们认为，该状态由这三位

参与者共享，其正比于

$$|0\rangle_a|0,0\rangle_{b_1,b_2}+|1\rangle_a(|0,1\rangle+|1,0\rangle)_{b_1,b_2}+|2\rangle_a|1,1\rangle_{b_1,b_2}\ . \tag{35}$$

该状态是一种特殊的广播态，具有 $\alpha=\beta=\frac{1}{\sqrt{2}}$，且可由 Alice 在本地制备。对于图态分发，Alice 施加一个相位门，使该状态现在正比于

$$|0\rangle_a|0,0\rangle_{b_1,b_2}+|1\rangle_a(|0,1\rangle+|1,0\rangle)_{b_1,b_2}-|2\rangle_a|1,1\rangle_{b_1,b_2}. \tag{36}$$

她分别将相应的量子比特分发给两个 Bobs。然后，Alice 在基$\tilde{}\{|j\rangle\}$中测量她的三能级量子比特，

$$|\tilde{j}\rangle=\frac{1}{\sqrt{3}}\sum_{k=0,1,2}e^{2\pi ijk/3}|k\rangle\quad(j=0,1,2)\ . \tag{37}$$

两个接收方得到的状态为

$$\begin{aligned}&\Big(|0,0\rangle+e^{-2\pi ij/3}(|0,1\rangle+|1,0\rangle)-e^{-4\pi ij/3}|1,1\rangle\Big)_{b_1,b_2}\\&=CZ_{b_1,b_2}\left(|0\rangle+e^{-2\pi ij/3}|1\rangle\right)_{b_1}\left(|0\rangle+e^{-2\pi ij/3}|1\rangle\right)_{b_2}\ .\end{aligned} \tag{38}$$

我们注意到，额外的相位 $e^{-2\pi ij/3}$ 与CZ 算符对易，因此，如果 Alice 将 j的测量结果告知每位接收者，他们便可在本地进行纠正，就像前一种广播情形一样。

如果 Alice 决定中止协议，则应将测量基改为 $\{|0\rangle,\ |1\rangle,\ \ |2\rangle\}$。这可能会留下一个由 Bobs 共享的纠缠态。

推广到含有 N 个顶点的图是直截了当的。为了分发具有一般图连通性的图态，Alice 应在分发物理量子比特之前，在本地施加 CZ 门。

在这种情形下，我们制备

$$|\Psi_{CZ}^{(1,N)}\rangle=\sum_{k=0}^{N}\begin{pmatrix}N\\k\end{pmatrix}^{1/2}|k\rangle_a U_{CZ}|k;N-k\rangle, \tag{39}$$

其中， U_{CZ} 是生成具有所需连接关系的图态的 CZ 门的乘积。Alice 测量后（假设结果为 j），接收方 Bobs 得到状态

$$\begin{aligned}|\Psi_{CZ}^{(1,N)}\rangle\xrightarrow{\text{measure}}&\sum_{k=0}^{N}\begin{pmatrix}N\\k\end{pmatrix}^{1/2}e^{-2\pi ijk/N}U_{CZ}|k;N-k\rangle\\&=U_{CZ}\left(|0\rangle+e^{-2\pi ij/N}|1\rangle\right)^{\otimes N}.\end{aligned} \tag{40}$$

所得状态是图态（34），只差一个可校正的相位 $e^{-2\pi ij/N}$。

一般而言，任何能通过在乘积态上施加多量子比特相位门（例如，由 CZ 门或 CCZ 门构成的乘积）生成的状态，都可以采用这一策略进行分发。这类量子态包括图态 [19], 、超图态 [21], ，以及其他短程纠缠态，其中包括对称性保护拓扑（SPT）有序态 [22, 23], ；在最后一种情况下，相位来自与对称相相关联的余循环。

我们可以推广式（15）的结果，使多个发送方能够在分发后添加相位。将多量子比特相位门写作 U_{phase}，则利用

$$\begin{aligned}&|\Psi_{\text{phase}}^{(M,N)}\rangle\\&=\sum_{k=0}^{N}\alpha^k\beta^{N-k}\begin{pmatrix}N\\k\end{pmatrix}^{1/2}\prod_{j=1}^{M}|k\rangle_{aj}U_{\text{phase}}|k;N-k\rangle\end{aligned} \tag{41}$$

并让多个 Alice 施加额外的相位门后，以下纠缠态便被分发给多个接收方:

$$|\Psi_{\text{phase}}^{(M,N)}\rangle\xrightarrow[\text{measure}]{U_j(\theta_j)^{\otimes M}}U_{\text{phase}}\prod_{l=1}^{N}\left(\alpha e^{i\sum_{j=1}^{M}\theta_j}e^{-2\pi i(\sum_{j=1}^{M}n_j)/(N+1)}|0\rangle_l+\beta e^{-i\sum_{j=1}^{M}\theta_j}|1\rangle_l\right) \tag{42}$$

$$\xrightarrow{\text{correct}}U_{\text{phase}}\prod_{l=1}^{N}\left(\alpha e^{i\sum_{j=1}^{M}\theta_j}|0\rangle_l+\beta e^{-i\sum_{j=1}^{M}\theta_j}|1\rangle_l\right). \tag{43}$$

B. 广播一个稳定子态

这里我们介绍另一种协议，用于将单个稳定子态“广播”并分发给多个接收方。为简单起见，我们考虑一个 N 量子比特稳定子态，它有 N 个独立的稳定子生成元 $\{S_k\}$。（可以考虑使用较少的稳定子生成元来编码分布式逻辑状态。）在这种情况下，Alice 需要 $2N$ 个量子比特，其中前 N 个量子比特均初始化为 $|+\rangle$，作为控制集，用于将控制-S_k作用于第二组中对应的量子比特。第二组中的量子比特可方便地初始化

为 $|+\rangle$ 。鉴于每个 S_k 都是单个泡利算符的乘积，控制-S_k 门可分解为双量子比特受控泡利门的乘积。随后，Alice 将第二组中的量子比特发送给目标接收者 Bobs。

Alice 进行任何测量之前，所得状态可以改写为

$$|\psi\rangle = \prod_{k=1}^{N} \frac{1}{\sqrt{2}}\big(|0\rangle_k \otimes I + |1\rangle_k \otimes S_{k'}\big) \prod_{k'=1}^{N} |+\rangle_{k'}. \quad (44)$$

如果 Alice 打算分发稳定子态，那么她会在剩余的 N 个量子比特上按 X 基进行测量。测量结果表示执行了操作 $(I \pm S_k)/2$ ，或者等价地，表示稳定子算符 $S_k = \pm 1$ 的取值。她可以找出需要校正的泡利乘积，并通知相应各方执行校正操作。

另一方面，如果她打算中止任务，只需在她所有的量子比特上按 Z 基进行测量。测量结果表明是否应用了相应的 S_k 算符；无论测量结果如何，所有 Bobs 随后都会共享一个乘积态。

1. *Distribution of graph states (II)*

本节余下部分将重点讨论图态，这是一般稳定子态的一种特殊情况。我们考虑初始化为 $|+\rangle$ 的 $2|V|$乘积态的量子比特，即，$\prod_{v\in V}|+\rangle_v \prod_{v'\in V}|+\rangle_{v'}$，其中量子比特 v 将与稳定子算符$K_{v'} = X_{v'}\prod_{\langle u',v'\rangle\in E} Z_{u'}$ 相关联，而符号 $'$ 表示将分发给 Bobs 的量子比特。应用所有受控-$K_{v'}$ 门（这些门可分解为 CX 门和 CZ 门的乘积）之后，

$$|\psi\rangle = \prod_{v\in V} \frac{1}{\sqrt{2}}\Big(|0\rangle_v \otimes I + |1\rangle_v \otimes X_{v'} \prod_{\langle u',v'\rangle\in E} Z_{u'}\Big) \times \prod_{w'\in V} |+\rangle_{w'} \ . \quad (45)$$

记 Alice 的 Pauli-X 测量中，作用于 v量子比特的结果为 $s(v) \in \{0,1\}$，则测量后的状态为

$$\prod_{v\in V} \frac{1}{2}\Big(1 + (-1)^{s(v)} X_{v'} \prod_{\langle u',v'\rangle\in E} Z_{u'}\Big) \prod_{w'\in V} |+\rangle_{w'}, \quad (46)$$

并且该状态是由 Bobs 共享的图态，至多相差一些副产物算符，

$$\Big(\prod_{v\in V} Z_v^{s(v)}\Big)|\psi_G\rangle_B, \quad (47)$$

其中，$|\psi_G\rangle_B$ 表示具有 $s\,(v)\ = 0$的图态。注意，作用于公式（46）中乘积态的算符是一个投影算符。如果测量结果是理想的（即，$s\,(v)\ = 0$ 对所有 $v \in V$均成立），Bobs 获得投影到目标子空间的状态，其中对所有 $v \in V$均有 $K_v = 1$ ，该状态就是图态 $|\psi_G\rangle$。如果出现 $s\,(v)\ = 1$的结果，则可以在相应的 v' 处施加 Pauli-Z 算符，以校正稳定子的本征值。在图3中，我们给出了一个图态示例，其图由三个顶点组成。

2. *Rotated graph states*

前面对发送相位的讨论促使我们设计一种在图态设置中传送相位门的方法。如果希望对 Bob 持有的顶点 v 施加相位 θ，例如，我们可以在用上述过程制备的图态上增加一次门隐形传态。假设 Alice 想要将相位门 $e^{i\theta Z}$ 发送到顶点 $u \in V$。那么 Alice 会在 $|+\rangle_{u_A}$中制备另一个辅助量子比特，并通过$CZ_{u_A,\ u_B}$将其与 u_B 耦合。在分发完所有 Bobs 的量子比特后，Alice 使用以下基测量她的辅助量子比特

$$\mathcal{M}_\theta = \left\{e^{-i\theta X}|s\rangle \ \middle|\ s = 0,1\right\} \ . \quad (48)$$

随后，凭借门隐形传态，酉门 $(Z)^s e^{i\theta Z}$ 会在 u_B处生成，并作用于图态。很容易将这一过程推广到每个顶点使用不同相位门的情形。最终，分发的状态如下：

$$\left(\prod_{v\in V} e^{i\theta_v Z_v}\right)|\psi_G\rangle, \quad (49)$$

至多相差取决于 Alice 的测量结果的 Z 副产物算符。我们在附录 D 中进一步详细阐述了该方案。

V. 分布式稳定子态的应用

A. GHZ态的分发

分布式 GHZ 态可用于量子秘密共享等应用 [25]。GHZ 态可由星形图态获得：对除星形中心处的量子比特外的所有量子比特施加哈达玛门 [19]。例如，可以让 Alice 持有中心量子比特，而其他量子比特由 Bobs 持有。之后，所有 Bob 都施加哈达玛门，于是 Bobs 和 Alice 共享一个 GHZ 态。附录 C 中介绍了另一种分发 GHZ 态的方法。

B. 接收者仅使用 X 的分布式基于测量的量子计算

下面，我们描述 Alice 传送的相位旋转门如何被 Bob 用来执行

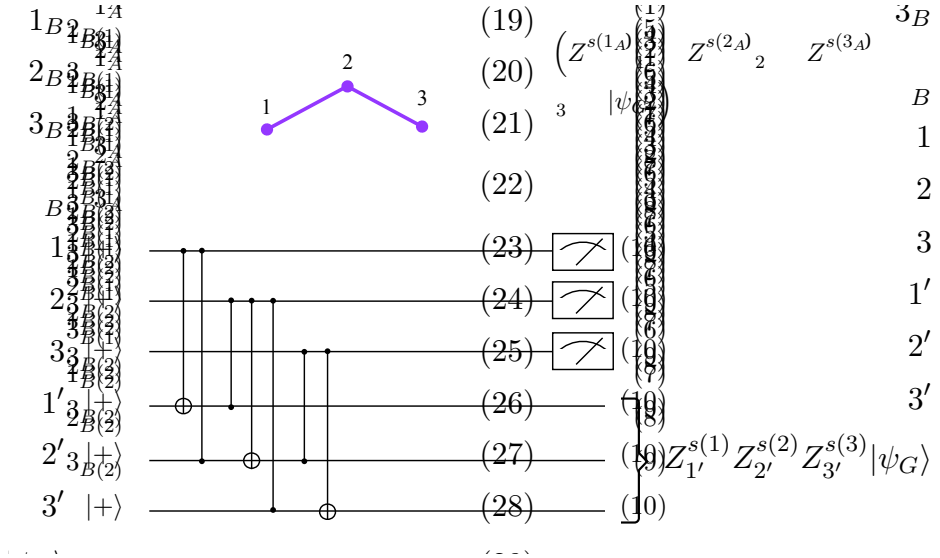

图3. 图态分发的一个示例。此示例中的图由三个顶点 $v \in \{1,2,3\}$ 构成，图态已完成分发。图态 $|\psi_G\rangle$ 由 $X_1 Z_2$、$Z_1 X_2 Z_3$ 和 $Z_2 X_3$ 稳定。

基于测量的量子计算（MBQC）[27,28]。借助发送相位旋转门的能力，Alice 和 Bob 可以协作执行通用的基于测量的量子计算；其中，Alice 通过旋转控制测量轴的适应，而 Bob 始终在相同的测量基中进行测量，X。这样便可以实现一个通用门集。我们还在附录 B 中指出，Alice 可以通过适当选择测量基，从 Bob 所拥有的图中移除一个顶点。

通用的基于测量的量子计算可以在适当的图态——砖墙态——上实现，并通过旋转基进行测量，$B = \{e^{i\theta Z}|+\rangle, e^{i\theta Z}|-\rangle\}$[27, 29, 30]。也就是说，在基 B 中适当选择角度 θ，即可实现单量子比特 $SU(2)$ 旋转门和受控非门。见图4。正如我们在第IV节所述，Alice 可以向 Bob 的量子比特施加相位门 $e^{i\theta_v Z_v}$，因此 Bob 仅通过基 X 测量，就能在 Bob 的图态上执行通用的基于测量的量子计算。Bob 需要将测量结果告知 Alice，这样她就能知道先前测量作用于其图态所产生的副产物算符，并判断是否需要对 $e^{i\theta_v Z_v}$ 或 $e^{-i\theta_v Z_v}$ 进行量子隐形传态，以实现所需的旋转。见图5。技术细节见附录 D。

第VI节：结论

我们将关于向多个接收方广播量子状态的研究结果扩展到了包括多个发送方的可能性。可以从网络中添加和删除发送方，我们也讨论了执行这些操作的过程。此外，我们还进一步研究了发送具有未知相位的状态。在这种情况下，相位以编码在量子态中的形式提供给发送方。我们展示了如何重复使用编码态，并说明了对于一般相位，每次使用都会使其中包含的信息减少。随后，我们给出了广播协议的两种应用，包括身份验证和三态量子密码学。

我们以两种不同的方式研究了图态的分发。第一种方法推广了最初用于广播乘积态的状态，并通过补充多量子比特相位门使乘积态彼此纠缠。这种方法不仅适用于图态，也适用于超图态以及非平凡的定点对称性保护拓扑序态。广播图态的另一种方法是实施由发送方控制的投影。发送方 Alice 可以通过恰当选择测量基来决定图的结构，也可以发送作用于图态的额外相位门。我们还讨论了图态分发的应用：GHZ态的分发，以及远程分布式通用量子计算。后者由分布式接收方仅通过 X 基测量，并由发送方控制（自适应）旋转来完成。后者与盲量子计算恰好相反：服务器将计算任务外包给第三方，却不让他们有机会了解计算内容。

致谢

作者谨此感谢 Himanshu Gupta 提出的宝贵意见。MH、JB、HS 和 T-CW 的研究得到了美国国家科学基金会项目 FET-2106447 的资助。MH 和 JB 的研究还得到了 DEV-

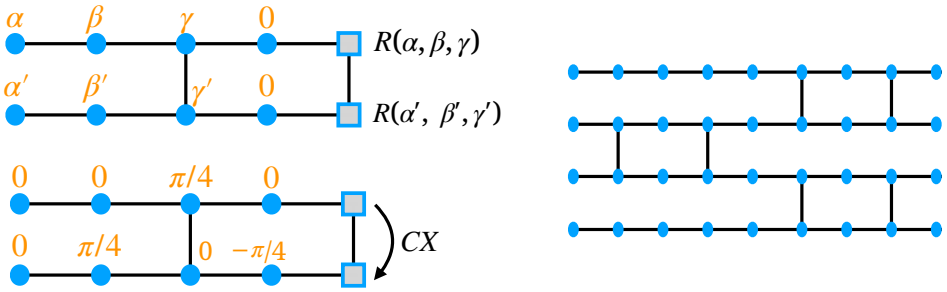

图4。（左上）实现单量子比特 $SU(2)$ 旋转门的测量模式。 $R(\alpha,\ \beta,\ \gamma)$ 表示欧拉旋转。（左下）实现受控非门的测量模式。我们按顺序测量量子比特时，信息从左向右流动。每个球上方的数字表示测量基 $\{e^{i\theta Z}|+\rangle,\ e^{i\theta Z}|-\rangle\}$ 中的角度 θ。（右）砖墙态。将左侧所示的模块向上平铺，即可依次串接酉变换。详情参见文献 [29, 30]。

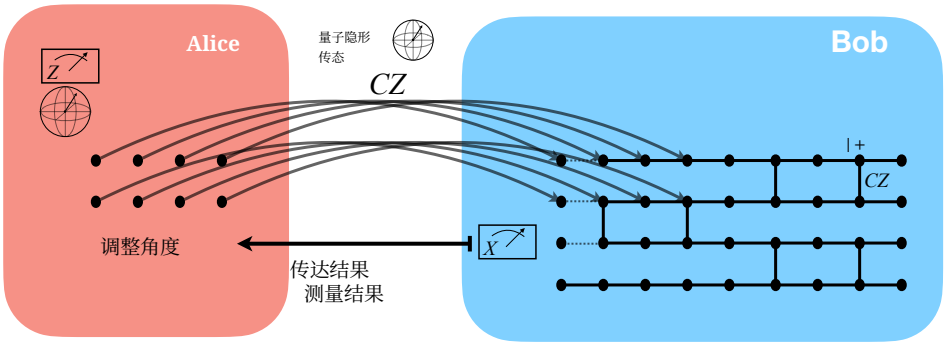

图5。在完成向接收者分发砖墙态的阶段后，Alice 和 Bob 可以协作执行通用的基于测量的量子计算。

COM 陆军研究实验室的资助，并在合作协议编号 W911NF-20-2-0097。此外，T-CW 和 HS 谨此感谢石溪大学教务长办公室提供的教务长风险基金支持。

[1] H. J. Kimble，《量子互联网》，《自然》**453**，1023-1030（2008）。[2] Yan Yu、Xin Wei Zha 和 Wei Li，《基于四量子比特簇态的量子广播方案和多输出量子隐形传态》，《量子信息处理》**16**，41（2017）。[3] Yan Yu 和 Nan Zhao，《基于纠缠的一般量子广播与多播通信》，《光学快报》**26**，29296（2018）。[4] Y. J. Zhou 和 Y. H. Tao，《基于四量子比特簇态的多方概率远程态制备广播方案》，《国际理论物理杂志》**57**，549（2018）。[5]Nan Zhao、Wandou Li 和 Yan Yu，《基于部分纠缠信道的量子广播与多播方案》，《IEEE Access》**8**，29658（2020）。[6] Hoi-Kwong Lo，《分布式量子信息处理中的经典通信成本：量子通信复杂度的推广》，《物理评论A》**62**，012313（2000）。

[7] C. H. Bennett、D. P. DiVincenzo、P. W. Shor、J. A. Smolin、B. M. Terhal 和 W. K. Wootters，远程态制备，《物理评论快报》**87**，077902（2001）。[8] D. W. Leung 和 P. W. Shor，无知远程态制备，《物理评论快报》**90**，127905（2003）。[9] C. H. Bennett、P. Hayden、D. W. Leung、P. W. Shor 和 A. Winter，量子态的远程制备，《IEEE信息论汇刊》**51**，56（2005）。[10] M. Radmark、M. Wiesniak、M. Zukowski 和 M. Bourennane，实验性多地点远程态制备，《物理评论A》**88**，032304（2013）。[11] P. Agrawal、P. Parashar 和 A. K. Pati，利用暗态为多方实现精确远程态制备，《国际量子信息杂志》1，301（2003）。[12]Mark Hillery、J´anos A. Bergou、Tzu-Chieh Wei、Sid- dhartha Santra 和 Vladimir Malinovsky，受限量子比特与量子三能级态集合的广播，《物理评论A》**105**，042611（2002）。

[13] J. Vaccaro、S. Croke 和 S. M. Barnett，相干性是否具有催化作用，J. Phys. A **51**，414008（2018）。[14] A. Dutta 和 A. Pathak，量子身份认证协议简述：Bob 如何知道自己正在与 Alice 通话，arXiv:2112.04234。[15] P. Walden 、 V. Dunjko、A. Kent 和 E. Andersson，采用量子密钥分发组件的量子数字签名，《物理评论A》**91**，042304（2015）。[16] A. Cabello，超单态，J. Mod. Opt. **50**，10049（2003）。[17] S. J. D. Phoenix、S. M. Barnett、A. Chefles，三态量子密码学，J. Mod. Opt. **47**，507-516（1999）。[18] T.C. Wei，基于测量的量子计算的量子自旋模型，Advances in Physics: X, **3**，1461026 2018( )。[19] Hein, M. 和 D¨ur, W. 和 Eisert, J. 和 Raussendorf, R. 和 Nest, M. Van den 和 Briegel, H. -J. 图态中的纠缠及其应用，https://arxiv.org/abs/quant-ph/0602096 [20] M. Van den Nest、J. Dehaene 和 B. De Moor，稳定子态的局域幺正等价与局域克利福德等价，《物理评论A》**71**，062323（2005）。[21] Rossi, M., Huber, M., Bruß, D. 和 Macchiavello, C.，量子超图态，New Journal of Physics **15**，113022 2013( )。[22] Chen, X., Gu, Z.C., Liu, Z.X. 和 Wen, X.G.，相互作用玻色子系统中的对称性保护拓扑序，Science **338**，1604（2012）。[23] B. Yoshida，具有广义全局对称性的拓扑相。Physical Review B **93**，155131（2016）。[24]Tantivasadakarn, Nathanan、Ryan Thorngren、Ashvin Vishwanath 和 Ruben Verresen，通过测量对称性保护拓扑相产生长程纠缠，arXiv:2112.01519。[25] Hillery, Mark、Vladim´ır Bu˘zek 和 Andr´e Berthiaume，量子秘密共享，Physical Review A **59**，1829（1999）。[26] Greenberger, Daniel M.、Michael A. Horne 和 Anton Zeilinger，超越贝尔定理，载于《贝尔定理、量子理论与宇宙观》，第69-72页。Springer, Dordrecht，1989。[27] Robert Raussendorf 和 Hans J. Briegel，单向量子计算机，《物理评论快报》**86**，5188（2001）。[28] Robert Raussendorf、Daniel E. Browne 和 Hans J. Briegel，簇态上的基于测量的量子计算，《物理评论A》**68**，022312（2003）。[29] A. Broadbent、J. Fitzsimons 和 E. Kashefi，“通用盲量子计算”，2009年第50届IEEE计算机科学基础研讨会，2009年，第 517 526 页。[30] J. F. Fitzsimons，私有量子计算：盲量子计算及相关协议导论。NPJ Quantum Inf **3**，23（2017）。

附录 A：关于发送未知相位的补充内容

1. 向 N 个接收方发送未知受限角度

我们从这个状态开始

$$|\Psi^{(1,N)}\rangle \otimes \frac{1}{\sqrt{K}}\Big(\sum_{j=0}^{K-1} e^{2\pi ikj/K}|j\rangle_d\Big). \tag{A1}$$

与正文中讨论的 $N=2$ (Bob, Charlie) 情形一样，Alice 应用受控移位门 $CX_{a,\ d}$，得到

$$\sum_{\ell=0}^{N}\alpha^{\ell}\beta^{N-\ell}\begin{pmatrix}N\\ \ell\end{pmatrix}^{1/2}|\ell\rangle_a|\ell;N-\ell\rangle \times\frac{1}{\sqrt{K}}\sum_{j=0}^{K-1}e^{2\pi ijk/K}|j+\ell\rangle_d. \tag{A2}$$

将求和指标 j 移位 ℓ后，我们得到

$$\sum_{\ell=0}^{N}\left(e^{-2\pi ik/K}\alpha\right)^{\ell}\beta^{N-\ell}\begin{pmatrix}N\\ \ell\end{pmatrix}^{1/2}|\ell\rangle_a|\ell;N-\ell\rangle \otimes\Big(\frac{1}{\sqrt{K}}\sum_{j=0}^{K-1}e^{2\pi ijk/K}|j\rangle_d\Big) \tag{A3}$$

Alice 在傅里叶基下测量其量子位数，随后每位接收方在对 Alice 测量所引入的相位进行校正后，得到以下状态：

$$e^{-2\pi ik/K}\alpha|0\rangle+\beta|1\rangle\ . \tag{A4}$$

2. 以一般角度重复使用编码态

正文中，我们讨论了将编码在状态 d 中的未知角度 θ 发送给 Bob 和 Charlie 的方法。对于一般角度，我们证明 Alice 可以在计算基下测量编码态 d，且该过程以概率 $(K-2)/K$ 成功，但编码态会被破坏。本节将讨论其他方法，以便重复使用编码态。

更好的过程如下。定义

$$Q_2=\sum_{k=2}^{K-1}|k\rangle_d\langle k|. \tag{A5}$$

Alice 在 d 系统上测量 Q_2，其特征值为 0 和 1；如果她测得 1（其概率为 $(K-2)/K$），则过程成功，得到的 d 状态为 $(1/\sqrt{K-2})\sum_{k=2}^{K-1}e^{ik\theta}|k\rangle_d$。该状态包含的相位信息不如原始状态多，但仍然包含相当多的信息。它可以传递给第二位爱丽丝，后者可以在同一协议中将其用于另一组 Bob 和 Charlie。随后成功概率将降低至 $(K-4)/(K-2)$，对应于特征值 1 的

$$Q_4=\sum_{k=4}^{K-1}|k\rangle_d\langle k|. \tag{A6}$$

另一种选择是让Alice不测量 d 系统，这样Bob和Charlie将获得近似的

目标状态。在这种情况下，d 状态可以重复使用，不过经过第一次使用后会发生一些改变。为了查看Bob和Charlie获得了什么，我们可以根据式（24）中的状态构造一个密度矩阵，并对 c 和 d 进行偏迹，得到Bob的状态（Charlie的状态与之相同）。结果为

$$\begin{aligned}\rho_b = \frac{K-2}{K}(\alpha e^{i\theta/2}|0\rangle + \beta e^{-i\theta/2}|1\rangle)\\ (\alpha^* e^{-i\theta/2}\langle 0| + \beta^* e^{i\theta/2}\langle 1|)\\ +\frac{1}{K}\left[2|\alpha|^2|0\rangle\langle 0| + 2|\beta|^2|1\rangle\langle 1|\right.\\ +\alpha\beta^* e^{i\theta}(1+e^{-iK\theta})|0\rangle\langle 1|\\ \left.+\alpha^*\beta e^{-i\theta}(1+e^{iK\theta})|1\rangle\langle 0|\right] \qquad \text{(A7)}\end{aligned}$$

请注意，误差的量级为 $1/K$。

如前所述，编码相位的状态可以重复使用。为了了解使用一次后它改变了多少，我们可以计算一次使用后 d 系统的约化密度矩阵 ρ_d 与原始编码态 $|\Phi(\theta,\ K)\rangle = (1/\sqrt{K})\sum_{k=0}^{K-1} e^{ik\theta}|k\rangle_d$ 的保真度； ρ_d 可通过对式 (24) 中的 b 和 c 求迹得到。我们发现

$$\begin{aligned}F &= \langle\Phi(\theta,K)|\rho_d|\Phi(\theta,K)\rangle\\ &= 1-4|\beta|^2(1-\cos K\theta)\frac{1}{K^2}(K-2+|\alpha|^2), \qquad \text{(A8)}\end{aligned}$$

因此，首次使用引入的误差量级为 $1/K$。如果现在将 d 状态发送给一位新的 Alice，我们称她为 Alice′，随后她用该状态将角度发送给 Bob′ 和 Charlie′，那么得到的 $bcb'c'$ 密度矩阵形式为

$$\rho_{bcb'c'} = \frac{K-4}{K}\rho_{prod} + \rho_{noise}, \qquad \text{(A9)}$$

其中， ρ_{prod} 是与乘积态（ $e^{i\theta/2}\alpha|0\rangle_{bc} + e^{-i\theta/2}\beta|1\rangle_{bc}\quad e^{i\theta/2}\alpha|0\rangle_{b'c'} +$)( ) $e^{-i\theta/2}\beta|1\rangle_{b'c'}$ ρ_{noise} 对应的密度矩阵，它是四个状态的非相干叠加，其大小（算子范数）为 $1/K$量级。如果 $\exp(iK\theta) = 1$，那么 $\rho_{noise} = (4/K)\rho_{prod}$。当 K 较大时，这一过程将使 Bob 和 Charlie 双方都能很好地近似所需状态。进一步使用会使编码态进一步退化，并为传输的状态增加更多噪声。 [13]对量子态中存储的相位信息随使用而退化的情况进行了更全面的分析。

附录 B：通过 Z 测量约化图

即使在向 Bob 分发量子比特之后，Alice 仍可决定将顶点从图中断开。（我们改用 $|+\rangle^{\otimes|V|}$ 表示 Alice， $|0\rangle^{\otimes|V|}$ 表示 Bob。）假设原始图由顶点 $v \in V$ 和边 $e \in E$ 组成，但 Alice 希望将其简化为由顶点 $V^R \subset V$ 和边 $E^R \subset E$ 组成的图。我们记作 $\bar{V} = V\backslash V^R$ 和 $\bar{E} = E\backslash E^R$。参见图 6。

Alice 用 X 基测量与 V^R 对应的量子比特，用 Z 基测量与 V 对应的量子比特。那么 Bob 得到

$$\begin{aligned}&\left(\prod_{v\in V^R}\frac{1+(-1)^{s(v)}K_v}{2}\prod_{u\in\bar{V}}K_u^{s(u)}\right)\prod_{v\in V^R}|0\rangle_v\prod_{u\in\bar{V}}|0\rangle_u\\ &=\left(\prod_{v\in V^R}\frac{1+(-1)^{s(v)}K_v}{2}\right)\prod_{v\in V^R}|0\rangle_v\prod_{u\in\bar{V}}|s(u)\rangle_u\ ,\end{aligned} \qquad \text{(B1)}$$

其中 $K_v = X_v\prod_{\langle u,v\rangle} Z_u$ 是图态稳定子算符 S_v。现在将约化图的稳定子写为

$$K_v^R = X_v\prod_{\langle w,v\rangle\in E^R} Z_w \quad (v\in V^R)\ . \qquad \text{(B2)}$$

然后定义

$$\prod_{\langle u,v\rangle\in\bar{E}}(-1)^{s(u)} \equiv (-1)^{t(v)} \qquad \text{(B3)}$$

当 $t(v) = 0,1$ 时，所得状态为

$$\left(\prod_{v\in V^R}\frac{1+(-1)^{s(v)+t(v)}K_v^R}{2}\right)\prod_{v\in V^R}|0\rangle_v\prod_{u\in\bar{V}}|s(u)\rangle_u\ . \qquad \text{(B4)}$$

这是一个图态，其图为（V^R, E^R），其余量子比特处于乘积态。

附录 C：分发 GHZ 的另一种方式

这里我们考虑分发一个 N 量子比特的格林伯格-霍恩-蔡林格（GHZ）类状态。我们考虑一个由顶点 $V = \{1,2,...,2N\}$ 和边 $E = \{\langle 1,2\rangle,\langle 2,3\rangle,...,\langle 2N-1,2N\rangle,\langle 2N,1\rangle\}$ 给出的图态。也就是说，这是一个用整数标记的一维周期链。我们使用第 IV B 节中描述的量子电路来生成广播态方程（45）。然而这一次，不同之处在于，在目标量子比特中，奇数部分 $V_o = \{1,3,...,2N-1\}$ 分发给接收方，而偶数部分 $V_e = \{2,4,...,2N\}$ 由 Alice 保留。注意，Alice 还保留了控制作用于 Bobs 量子比特的稳定子算符的量子比特，因此她拥有 $|V| + |V_e| (= |V| + |V|/2)$ 个量子比特。在 Alice 对其控制量子比特执行测量后，由于投影，Alice 和 Bobs 共享由以下稳定子稳定的图态

$$Z_{2n-1}X_{2n}Z_{2n+1}|\psi_G\rangle = |\psi_G\rangle \qquad \text{(C1)}$$
$$Z_{2n}X_{2n+1}Z_{2n+2}|\psi_G\rangle = |\psi_G\rangle \qquad \text{(C2)}$$

最多相差 ± 1 符号。现在，Alice 使用 X 基测量偶数部分 V_e。由于式（C1）中的新稳定子条件变为，

$$Z_{2n-1}X_{2n}Z_{2n+1} = (-1)^{s_{2n}}Z_{2n-1}Z_{2n+1} = 1 \qquad \text{(C3)}$$

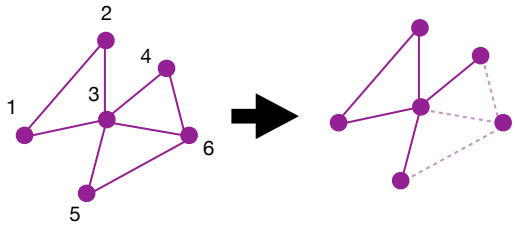

图 6。图的约简示例。 $V = \{1,2,3,4,5,6\}$、 $E = \{12,13,23,34,35,36,46,56\}$、 $V^R = \{1,2,3,4,5\}$、 $E^R = \{12,13,23,34,35\}$ $\bar{V} = \{6\}$ $\bar{E} = \{36,56,46\}$ 、 、 。

并且由式（C2）中的条件 $X_1 ... X_{2n+1} ... X_{2N+1} = 1$ 推导出的全局对称性仍然成立，此时接收方共享的状态是一个 GHZ 型态 [26] ，最多相差相位翻转。例如，文献 [24] 给出了这种技术。

附录 D：分布式远程 MBQC 的一些技术细节

本节旨在向读者介绍分布式远程 MBQC 的一些细节。我们将重点解释我们的方法，并在此过程中介绍 MBQC 领域中通常已知的基本要素。最初提出将砖墙态用于盲通用量子计算的想法来自文献 [29]。读者可以参阅文献 [18, 30]，其中对砖墙态上的 MBQC 作了便于教学理解的介绍。

1. 旋转图态与测量

考虑图4（左）所示的图态。我们从左上、右上、左下到右下，按顺序用集合 $V = \{1,2,3,4,5,6,7,8,9,10\}$ 标记这 10 个量子比特。量子比特对 (1,2) (2,3) (3,4) (4,5) (6,7) (7,8) (8,9) (9,10) 在水平方向上通过 CZ 门纠缠。量子比特对 (3,8) 和 (5,10) 在垂直方向上也通过 CZ 门纠缠。我们将这些边的集合记为 E_{bw}。初始信息编码在 (1,6) 这对量子比特（最左侧的一对）上，记为 $|\psi\rangle_{1,6}$。此设置下的砖墙态写作

$$|\psi_{bw}\rangle := \prod_{\langle u,v\rangle \in E_{bw}} CZ_{u,v}\Big(|\psi\rangle_{1,6} \otimes |+\rangle^{\otimes V\setminus\{1,6\}}\Big). \quad \text{(D1)}$$

Alice 拥有一份 10 个量子比特的副本，用于量子隐形传态 XY- 平面旋转。我们用下标 A 标记它们，而 Bob 拥有的砖墙态中的量子比特将用下标 B标记。考虑如下状态（该状态是在我们的广播协议中，Bob 根据稳定子进行投影并执行校正后得到的状态），

$$|\Psi\rangle_{AB} = \prod_{v\in V} CZ_{v_A,v_B}\Big(|\psi_{bw}\rangle_B \otimes |+\rangle_A^{\otimes V}\Big). \quad \text{(D2)}$$

现在考虑 Alice 使用基$\{e^{-i\theta X}|0\rangle, e^{-i\theta X}|1\rangle\}$进行的测量。将 v 处的测量结果记为 $s_v \in \{0,1\}$ ，并将角度记为 θ_v，测量后的状态为

$$\begin{aligned}&\Big(\bigotimes_{v\in V}\langle s_v|e^{i\theta_v X_v}\Big)_A |\Psi\rangle_{AB}\\ &\propto \Big(\prod_{v\in V} Z_v^{s_v} e^{i\theta_v Z_v}\Big)|\psi_{bw}\rangle_B =: |\psi_{bw}(\boldsymbol{\theta};\boldsymbol{s})\rangle \end{aligned} \quad \text{(D3)}$$

差一个归一化常数。

现在我们继续考虑 Bob 在基 $\{|\tilde{t}\rangle|t=0,1\}$ 下的测量，其中 $|\tilde{0}\rangle = |+\rangle$ 且 $|\tilde{1}\rangle = |-\rangle$。作为基于测量的量子计算的构建模块，我们注意到，对于一对通过 CZ纠缠的状态，

$${}_1\langle\tilde{t}|Z_1^s e^{i\theta Z_1} CZ_{1,2}|\psi\rangle_1 \otimes |+\rangle_2 = \frac{1}{\sqrt{2}}\Big(He^{i\theta Z}Z^{t+s}\Big)_2|\psi\rangle_2. \quad \text{(D4)}$$

这涉及一次量子隐形传态和一个旋转门。泡利 Z^{t+s} 取决于测量结果，是副产物算符的一个例子。通过将此公式依次应用于旋转后的砖墙态 $|\psi_{bw}(\boldsymbol{\theta};\boldsymbol{s})\rangle$，即可得到基于测量的量子计算的酉门集合。对于 $v \in V$，定义 $w_v = t_v \oplus s_v \in \{0,1\}$ ($\oplus$: $\mathbb{Z}_2$ sum) 很方便。

2. 受控非门

我们来看受控非门的测量模式。我们测量 V 除 5 和 10 以外的量子比特，因为输出态将在这两个位置定义。（表达式 $|\psi_{bw}(\boldsymbol{\theta};\boldsymbol{s})\rangle$ 包含作用于 5 和 10 的量子隐形传态相位门。在基于测量的量子计算的后续步骤中会用到这些门，此时 5 和 10 处诱导出的输出态将被视为新的输入态。在当前分析中，我们推导酉变换时只需忽略它们。）我们设

$$\begin{aligned}&\theta_i = 0 \quad (i = 1,2,4,6,8),\\ &\theta_9 = \alpha,\ \theta_3 = \beta,\ \theta_7 = \gamma. \end{aligned} \quad \text{(D5)}$$

利用该公式，我们得到作用于$|\psi\rangle_{5,\ 10}$上的以下酉算符：

$$CZ\,(HZ^{w_4}\otimes He^{i\alpha Z}Z^{w_9})(He^{i\beta Z}Z^{w_3}\otimes HZ^{w_8})$$
$$CZ\,(HZ^{w_2}\otimes He^{i\gamma Z}Z^{w_7})(HZ^{w_1}\otimes HZ^{w_6}). \tag{D6}$$

这里，在$(\mathcal{P}\otimes\mathcal{Q})$中，$\mathcal{P}$作用于量子比特 5，$\mathcal{Q}$作用于量子比特 10。它等于

$$\pm\Big(X^{w_2+w_4}Z^{w_1+w_3+w_9}\otimes X^{w_7+w_9}Z^{w_4+w_6+w_8}\Big)$$
$$\times\exp[i(-1)^{w_2}\beta Z\otimes I]\exp[i(-1)^{w_2+w_6+w_8}\alpha Z\otimes X]$$
$$\times\exp[i(-1)^{w_6}\gamma I\otimes X]. \tag{D7}$$

旋转门前的泡利算符集合是基于测量的量子计算中副产物算符的一个例子。它总是被传播到我们希望模拟的酉变换之前，而参数集合（例如$(\alpha,\ \beta,\ \gamma)$）则根据先前的测量结果选取。

更准确地说，如果我们将 10 量子比特的砖块态视为基于测量的量子计算中间的一个区块，那么“初始”态$|\psi\rangle_{1,\ 6}$也携带了先前基于测量的量子计算步骤产生的副产物算符。因此，我们将定义在 1，6 处的状态写作$|\psi\rangle_{1,\ 6}=(X^{x_1}Z^{z_1}\otimes X^{x_6}Z^{z_6})|\psi'\rangle_{1,\ 6}$。那么，经过这组测量后的状态将是

$$\pm\Big(X^{w_2+w_4+x_1}Z^{w_1+w_3+w_9+z_1}$$
$$\otimes X^{w_7+w_9+x_6}Z^{w_4+w_6+w_8+z_6}\Big)$$
$$\times\exp[i(-1)^{w_2+x_1}\beta Z\otimes I]$$
$$\times\exp[i(-1)^{w_2+w_6+w_8+x_1+z_6}\alpha Z\otimes X]$$
$$\times\exp[i(-1)^{w_6+z_6}\gamma I\otimes X]|\psi'\rangle_{5,10}. \tag{D8}$$

现在，我们将参数选择如下：

$$\alpha=(-1)^{w_2+w_6+w_8+x_1+z_6}\times\frac{-\pi}{4},$$
$$\beta=(-1)^{w_2+x_1}\times\frac{\pi}{4},$$
$$\gamma=(-1)^{w_6+z_6}\times\frac{\pi}{4}. \tag{D9}$$

然后我们得到酉算符

$$\exp[-\frac{\pi i}{4}(I-Z_5)(I-X_{10})]=CX_{5,10} \tag{D10}$$

前面带有副产物算符和一个常数相位。

我们注意到，参数始终可以按照（D9）进行设置，因为所有测量结果w_i（以及$x_i,\ z_i$）都在实施参数化旋转之前获得。例如，我们在$\{1,2,3,6,7,8\}$处进行测量、在 9 处使用α进行测量之前，已经获得了测量结果$t_v,\ s_v$（以及$x_i,\ z_i$）。显然，为了让 Alice 正确选择要发送的θ_i，她需要知道 Bobs 之前的测量结果，我们将其记为t_v，这样她就可以构造出与她的s_v相结合的$w_v=s_v\oplus t_v$。

3. 单量子比特旋转门

对于包含$\theta_4=\theta_9=0$的测量模式，我们得到如下酉算符：

$$\pm\Big(X^{w_2+w_4+x_1}Z^{w_1+w_3+w_9+z_1}$$
$$\otimes X^{w_7+w_9+x_6}Z^{w_4+w_6+w_8+z_6}\Big)$$
$$\times\Big(\exp[i(-1)^{x_1}\theta_3 Z]\exp[i(-1)^{w_1+z_1}\theta_2 X]$$
$$\times\exp[i(-1)^{x_1}\theta_1 Z]$$
$$\otimes\exp[i(-1)^{x_6}\theta_8 Z]\exp[i(-1)^{w_6+z_6}\theta_7 X]$$
$$\times\exp[i(-1)^{x_6}\theta_6 Z]\Big). \tag{D11}$$

将参数选择为

$$\theta_1=(-1)^{x_1}\alpha,\quad \theta_2=(-1)^{w_1+z_1}\beta,\quad \theta_3=(-1)^{x_1}\gamma \tag{D12}$$
$$\theta_6=(-1)^{x_6}\gamma',\quad \theta_7=(-1)^{w_6+z_6}\beta',\quad \theta_8=(-1)^{x_6}\alpha', \tag{D13}$$

我们得到单量子比特旋转门

$$R(\alpha,\beta,\gamma)=e^{i\gamma Z}e^{i\beta X}e^{i\alpha Z} \tag{D14}$$

acting on 5 and 10 as $R(\alpha,\beta,\gamma)\otimes R(\alpha',\beta',\gamma')$.