arXiv:2303.03715v2 [quant-ph] 8 Mar 2023

量子计算的通用资源

Dong-Sheng Wang*中国科学院理论物理重点实验室，中国科学院理论物理研究所，北京 *100190*，中国（日期：2023年3月9日）

揭示量子计算能力的来源一直是量子信息科学领域的重要目标。近年来，量子资源理论（QRT）已建立起来，用于表征各种量子资源，但这些资源在量子计算任务中的作用仍有待研究。所谓的通用量子计算模型（UQCM），例如电路模型，一直是指导量子算法设计、实际量子计算机研制等工作的主要框架。在这项工作中，我们将对 UQCM 的研究与 QRT 结合起来。我们发现，一方面，利用 QRT 可以从资源理论的角度表征 UQCM，揭示不同模型之间的关系并启发新模型；另一方面，利用 UQCM 则可以提供一个应用资源、研究资源之间关系并对其进行分类的框架。

我们在通用量子计算模型（UQCM）的框架下发展了通用资源理论，并发现 UQCM 及其相应通用资源构成了丰富的谱系。根据资源理论的层级结构，我们发现模型可以划分为族。在这项工作中，我们详细研究了 UQCM 的三个自然族：振幅族、准概率族和哈密顿量族。它们包含了一些知名模型，例如基于测量的模型和绝热模型，也启发了新模型，例如我们提出的情境模型。每个族至少包含三个模型，而 UQCM 族这种简洁的结构为研究资源和设计模型提供了统一的图景。它还提供了一个严谨的框架，用于解答诸如纠缠与干涉各自扮演何种角色之类的疑问，并揭示量子算法的资源理论特征。

I. 引言

A. 动机

自量子计算诞生之初，人们就开始尝试找出量子加速的关键资源。随着量子隐形传态等重要发现的出现，人们认识到量子纠缠是一种独特特征。与此同时，通过研究早期量子算法和量子电路模型，人们提出量子干涉是量子计算能力的来源。量子算法通过将许多计算路径叠加起来，再利用干涉快速选出正确路径。

随着纠缠的发展 [8],，人们证明了一个令人惊讶的事实：在基于测量的量子计算 [11]的框架下，纠缠并不足以实现量子加速 [9, 10] 。这一结论后来被推广到电路模型，研究表明，少量纠缠就足以实现通用性 [12]。这在一定程度上促使人们去研究其他资源，例如量子情境性 [13, 14]。事实上，有人提出，基于魔态注入模型 [16], ，量子情境性充当了实现量子加速的魔力 [15]，此后这一范式得到了进一步拓展；例如，参见文献 [17–20]。最近，研究人员已经建立了基于测量的量子计算与对称性保护拓扑序 [21–23]之间的密切联系 [24–28], ，但尚未发展出资源理论。

一般量子资源理论（QRT） [29] 的一个重要先驱是量子相干性的资源理论 [30]。人们从不同角度研究了相干性的度量 [31–36], ，但只有资源理论框架是完备的。如今，可以在 QRT 框架中严格定义量子特征。给定一个集合 $\mathcal{S}$，在其上建立 QRT，就是确定一个子集 $\mathcal{F} \subset \mathcal{S}$ 以及一组操作 $\mathcal{O}$ ，这些操作保留 $\mathcal{F}$，其余部分 $\mathcal{S}$ 则被视为资源。

* wds@itp.ac.cn

随后可以定义一种度量，用于量化资源的数量，并刻画资源之间的转换。

不过，量子资源理论并未提供如何寻找所谓自由集合 $\mathcal{F}$ 和自由操作 $\mathcal{O}$ 的方法。在量子计算中，通用量子计算模型（UQCM）的方法以及算法尤其能弥补这一不足。具体而言，UQCM 考虑各种设定：集合及其上的操作；高效算法能够快速实现集合上的操作，而这些设定则提供了定义自由集合和自由操作的场景。

在这项工作中，我们结合量子资源理论和通用量子计算模型的方法，并取得了富有成果的进展。我们发现，量子资源理论提供了定义和分类通用量子计算模型、识别通用资源的方法；而通用量子计算模型则提供了定义和分类通用资源的场景。由此，我们得以解决一些难题，例如纠缠与干涉之间的张力、相干性与情境性之间的关系；我们还发现了重要的新型通用量子计算模型，例如一种直接基于量子情境性的模型，它与魔态注入属于同一类。下面我们将回顾一些先前工作，然后总结本工作的主要发现。

B. 先前工作

由于该主题内容丰富，存在许多相关的研究方向。这里我们重点介绍与本工作研究最相关的几点。

- 在许多量子资源理论的研究中，资源并不一定具有通用性，也就是说，不必能够实现通用量子计算。例如，热力学的量子资源理论定义了非热性 [29]，但其目标并非实现计算通用性。本文对量子资源理论的研究面向通用量子计算模型。通用量子计算模型是一种实现任意量子算法的框架；如果两个模型中的任务或算法能够高效地相互模拟，那么这两个模型便是等价的。通用性要求考察不同类型的操作任务，而非单个任务，因为有些任务具有特殊性或可以相互替代。因此，我们引入通用资源来表征每种通用量子计算模型。这为量子资源的分类提供了可靠的计算方案。

- 已有研究提出了 UQCM 的一种分类 [37]。该研究基于“四元组模型”，为 UQCM 提出了一张包含两类的表：具有二部输入结构和二部演化结构。见图 1（左）。其中一类用于容错，即基于编码的模型；另一类用于通用性。在本工作中，我们仅研究通用性这一类别，且我们识别出的三个家族都属于该类别。使用量子资源理论改进了四元组模型：二部输入被具体规定为自由态和通用资源，演化门被具体规定为自由操作。此前，测量型量子计算（MBQC）和绝热量子计算（AQC） [38] 被视为基于编码的模型，因为它们可被看作动态编码方法。然而，如果我们仅限于静态编码方法，那么 MBQC 和 AQC 就必须采用其他方法处理。在本工作中，我们发现 MBQC 属于振幅家族，而 AQC 属于哈密顿量家族。本文中的分类是对先前分类的改进。

- 尽管过去并未将测量型量子计算与量子资源理论一同研究，但许多相关研究都为测量型量子计算的资源理论奠定了基础。在量子资源理论兴起之前，人们已广泛研究测量型量子计算的通用性 [39, 40]，例如纠缠宽度的度量。基于测量的量子计算的经典版本也已得到定义 [41]。正如前文所述，高度纠缠态对这一模型大多毫无用处 [9, 10]。相反，近期研究发现，对称性保护拓扑序具有资源价值 [26–28]，这为本文提出的测量型量子计算资源理论奠定了基础。人们也研究了该模型中的量子情境性 [13, 14, 42–44]，但并未宣称它是通用资源 [45, 46]。本文将进一步分析量子情境性的概念，并引入一个直接基于量子情境性的模型。

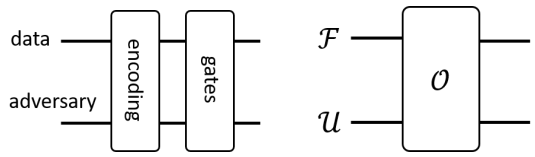

图 1. 用于通用量子计算的“四元组模型” [37]（左）和资源理论模型（右）。

C. 总结

我们研究的基本模型如图 1（右）所示。它包含两个寄存器：数据 $\mathcal{F}$ 和资源 $\mathcal{U}$，而计算由自由操作构成 $\mathcal{O}$。数据的初始态为自由态，因此显然，使用资源 $\mathcal{U}$ 可以通过消耗该资源来实现计算。在资源理论中，自由集合 $\mathcal{F}$ 可以是量子态的集合。如果并非如此，我们可以通过考察量子态上的效应算符，将其转换为量子态集合。

在量子理论中，我们主要研究量子态、演化、可观测量以及通过测量获得的概率。因此，我们可以分别从这四个方面确定通用量子计算模型的四个族。更具体地说，对于可观测量族，我们考虑局域哈密顿量的集合。因此，我们引入通用量子计算模型的振幅（或量子态）族、（准）概率族、哈密顿量族和演化族。后者将单独进行研究。因此，一个通用量子计算模型族由集合 $\mathcal{S}$ 确定。通用量子计算模型可以由一个量子资源理论定义，（$\mathcal{F}$、$\mathcal{O}$、$\mathcal{R}$）。然后，根据资源理论的层级，即少数几个自由集合的子集层级，我们可以定义通用量子计算模型族中的各代。这里，我们为每个族确定三代。必须注意，由于资源理论层级具有灵活性，这些世代既不唯一，也不完备。

下面简要介绍这三类：分别称为*a*类、*p*类和*h* 类。*a*类包含量子电路模型（QCM）、局域量子图灵机（LQTM） [47], 和测量型量子计算（MBQC）。在 QCM 中，对于量子算法加速或量子优势，我们将量子干涉视为资源。对于 LQTM，纠缠比特（或贝尔态）是通用资源，可充当量子存储器，并能够将任意量子态表示为矩阵乘积态（MPS） [48–50]。在 MBQC 中，通过一系列自适应的单点投影测量，对作为资源的 MPS 进行测量。我们指出，与 SPT 序相关的一项特殊性质是其通用资源。

*p*族包含我们所介绍的情境性量子计算（CQC）、魔态注入（MSI），以及受一种非局域隐形传态方案启发的后魔态量子计算（PMQC） [51]。MSI由所谓的魔力驱动，而魔力通常存在于 $|t\rangle = T|+\rangle$ 态中。 不过，魔力比情境性更强，因此可以直接基于情境性构建 UQCM。事实证明，这种CQC模型很有趣，并且能够解释某些量子算法的特征，例如幺正操作的线性组合 [52, 53]。借助更强的非局域盒 [51, 54], , 通信复杂度可以降至最低，从而实现PMQC模型；该模型是盲测量式量子计算的一种变体 [55]。

*h*族包含哈密顿量量子模拟（HQS） [56–59], 哈密顿量量子元胞自动机（HQCA） [60–62], 以及AQC [38]。它依赖于局域哈密顿量相互作用项的集合，以及对这些相互作用项的操控方式。HQS几乎允许任意形式，HQCA允许所谓的并行形式，而AQC只允许对相互作用项进行绝热变化。由此可以有趣地看到，它们确实构成一个族，并且存在一个相互作用效应层级。

从物理角度看，*a*、*p* 和 *h* 这几个族彼此不同，它们的主要物理特征分别可以从量子相干性、关联和相互作用的角度加以理解。它们各自确实都存在资源层级。对于量子态而言，这一层级从相干性到纠缠，再到一种特殊的多体纠缠。对于概率而言，这一层级从少数比特的局域关联到非局域关联。对于哈密顿量而言，这一层级同样是从局域到非局域。通过依据其自由操作所定义的适当操作，可以由较弱的资源制备出更强的资源。资源层级正是由一族资源理论精确刻画的。

为清晰起见，主要发现列举如下：

- 我们将资源理论扩展到普适资源这一情形。这为资源理论找到了应用空间，并建立了量子信息与量子计算之间的联系。

- 我们使用量子资源理论研究通用量子计算模型，并引入通用量子计算模型族，这是一种独特的方

法，可用于统一和分类这些模型、探究其物理性质，并发现新的模型。

• 我们为测量型量子计算定义了一种通用资源理论，并阐明其与情境性的关系。

• 我们介绍 CQC 和 PMQC 模型，将其视为p族中的几种生成形式。

• 我们对基于哈密顿量的模型进行了初步的资源理论研究。

•我们研究量子算法与资源之间的关系。这有助于解开谜题，并为新的量子算法激发灵感。

此外，我们将演化族的研究留待未来开展，因为这方面的研究相对较少。它可能与超信道 [63], 动力学资源理论 [29], 以及量子冯·诺依曼架构 [64]有关。我们还认为，至少应存在一个基于编码的模型族，其中包含基于纠错码的模型 [37]。例如，这将包括拓扑量子计算 [65], 和多粒子量子游走 [66], 。还需注意，我们对通用量子计算模型的分类并非旨在涵盖所有已知的现有模型。相反，它提供了一个资源理论框架，用于研究并拓展这些模型。

本文包含以下几个部分。第二节回顾量子资源理论，随后定义通用资源。接着，我们介绍通用量子计算模型的若干类，并在第三、四、五节分别研究各类的细节。然后，我们在第六节分析几个量子算法。最后，在第七节总结并展望未来的研究方向。为方便起见，本文研究的模型所用的各种缩写汇总于表 I。

QCM	量子电路模型
LQTM	局部量子图灵机
MBQC	基于测量的量子计算
CQC	情境量子计算
MSI	魔态注入
PMQC	后魔态量子计算
HQS	哈密顿量量子模拟
HQCA	哈密顿量量子元胞自动机
AQC	绝热量子计算

表 I. 模型缩写及其全称。

II. 通用资源

A. 资源

我们先简要回顾基于量子态集合的量子资源理论。我们考虑有限维希尔伯特空间。对于希尔伯特空间为 $\mathcal{H}$ 的纯态、密度算符集合为 $\mathcal{D}$的量子系统，资源理论定义为一个元组

$$(\mathcal{F}, \mathcal{O}, \mathcal{R}) \tag{1}$$

其中 $\mathcal{F} \subset \mathcal{D}$ 是自由态的集合， $\mathcal{O}$: $\mathcal{F} \to \mathcal{F}$ 是自由操作的集合，而 $\mathcal{R} := \mathcal{D} \backslash \mathcal{F}$ 是资源态的集合 [29]。为了量化资源，我们要求度量 f 满足以下公理:

i) It is zero for free objects; $f(\rho = 0), \forall \rho \in \mathcal{F}$;

ii) 对于有限维希尔伯特空间，它有正的上界；
iii) 它是渐近连续的；当 $\rho \to \sigma, \forall \rho, \sigma \in \mathcal{D}$ 时，$\mathrm{f}(\rho) \to \mathrm{f}(\sigma)$；iv) 它满足次可加性；$\mathrm{f}(\rho \otimes \sigma) \leq \mathrm{f}(\rho) + \mathrm{f}(\sigma)$, $\forall \rho, \sigma \in \mathcal{D}$；v) 它在自由操作下不增；$\mathrm{f}(\rho) \geq \mathrm{f}(\Phi(\rho))$, $\forall \Phi \in \mathcal{O}$。

对于我们将在本文中使用的一些资源度量，次可加性条件 iv) 可以加强为可加性。

量化量子态资源量有几种通用方法， $\mathscr{R}(\rho)$，包括基于距离的度量、熵、费 Fisher 信息、见证算子和主序 [29]。例如，对于收缩距离 d，一种基于距离的资源度量为

$$\mathscr{R}_d(\rho) := \min_{\sigma \in \mathcal{F}} d(\rho, \sigma). \tag{2}$$

其中包括资源的迹距离和基于保真度的度量。也可以使用相对 Rényi 熵。对于广泛使用的$S(\rho \| \sigma) \quad = -\mathrm{tr}[\rho (\log \sigma - \log \rho)]$, 资源相对熵为

$$\mathscr{R}_r(\rho) := \min_{\sigma \in \mathcal{F}} S(\rho \| \sigma). \tag{3}$$

研究表明，对于任意资源态 $\rho \in \mathcal{R}$，都存在一种自由参数估计协议，其有效 Fisher 信息为非负值 [67]。

在这项工作中，我们也以更抽象的方式考察量子资源理论。集合 $\mathcal{F}$ 不必是量子态的集合。例如，它可以是厄米算子、幺正算子、量子信道或测量的集合。对于这些情况，我们始终可以通过考察操作对量子态的影响，来使用针对量子态的资源度量。此外，我们不采用蒸馏等资源转换，因为我们的重点是量子计算的通用资源。

B. 通用资源

现在我们来定义通用资源的概念。粗略地说，通用资源就是能够实现通用量子计算的资源。形式上，我们将通用资源理论定义为

$$(\mathcal{F}, \mathcal{O}, \mathcal{R}, \mathcal{U}) \tag{4}$$

与通常的资源理论相比，额外加入了一个集合 $\mathcal{U} \subset \mathcal{R}$ 作为通用资源量子态的集合。通用性意味着 $\mathcal{O}(\mathcal{F} \otimes \mathcal{U})$ 能够高效地模拟任意量子算法。见图 1（右）。这里的高效是指，对于给定算法，其规模增大时，自由操作 $\mathcal{O}$、自由态 $\mathcal{F}$和通用资源 $\mathcal{U}$ 的开销都不会呈指数级增长。

实际上，这种形式体系为定义通用量子计算模型（UQCM）提供了一种独特的方式。在计算机科学中，有一种算法方法：对于一类问题，存在一系列算法以通用方式解决这些问题，并用统一的方法衡量每种算法的复杂度，例如电路成本、预言机调用次数或图灵机的步数。若两个模型中的算法彼此多项式等价，则这两个模型等价。

根据我们的 QRT 形式化框架，我们需要找出 $\mathcal{O}$ 和 $\mathcal{F}$。$\mathcal{F}$ 与信息的表示方式有关。这一点很重要，因为它关系到如何衡量算法的复杂度。在 QRT 中，$\mathcal{O}$ 和 $\mathcal{F}$ 的成本应与$\mathcal{U}$的成本分开计算，后者对于衡量算法的复杂度更为重要。这是对我们之前介绍的四元组模型的改进 [37], 图 1（左）。对手现在充当通用资源，而数据寄存器是自由态。量子门是自由操作 $\mathcal{O}$，这些操作可以是逻辑性的，即编码可能是隐式的。

通用资源是在资源理论中定义的最优资源，旨在促使 $\mathcal{O}$ 实现通用性。其取值为

$$\mathscr{R}(\mathcal{U}) := \max_{\rho \in \mathcal{U}} \mathscr{R}(\rho). \tag{5}$$

由于对于所有 $\rho \in \mathcal{U}$，$\mathscr{R}(\rho)$ 很可能都相同，因此该公式可以放宽为 $\mathscr{R}(\mathcal{U})$ =最大值$_{\rho \in \mathcal{R}} \mathscr{R}(\rho)$。我们看到，通用资源的度量对象不是量子态，而是集合。例如，它可以是集合之间距离的度量

$$\mathscr{R}(\mathcal{U}) = \max_{\rho \in \mathcal{R}} \min_{\sigma \in \mathcal{F}} d(\rho, \sigma). \tag{6}$$

一般而言，最小值和最大值函数不可交换，但对于凸集合和凸度量，冯·诺伊曼-范极小极大定理适用，因此它们可以交换。

此外，还可以引入一种较弱的概念“蒸馏普适性”，用于描述能够高效蒸馏为通用资源的资源。例如，我们发现纠缠比特是一种通用资源，而能够用于高效蒸馏纠缠比特的那些纠缠态，将被视为可蒸馏的通用资源。在大多数量子资源理论中，研究已经表明， [68],渐近地，所有资源态都可以通过对自由态集合不生成资源的操作实现可逆。在量子资源理论中，通过蒸馏或其他方式进行资源转换是重要组成部分。在本文中，我们采用不依赖于资源蒸馏的通用性。

C. 模型族

通过考虑不同类型的集合和操作，我们可以定义不同的通用量子计算模型。对于量子态集合、（准）概率和局域哈密顿量，我们分别引入一系列通用量子计算模型。之所以使用“一系列”一词，是因为每一类中也包含不同的通用量子计算模型。具体而言，对于每一系列，我们确

	QCM		LQTM		MBQC
$\mathcal{F}$	BIT	$\supset$	SEP	$\supset$	PRO
$\mathcal{O}$	CC	$\supset$	随机局域操作与经典通信	$\supset$	1O1C
$\mathcal{U}$	相干性	$\prec$	纠缠比特	$\prec$	通用纠缠

表 II。通用量子计算模型振幅族的三元组。

	CQC		MSI		PMQC
$\mathcal{F}$	BIT	$\supset$	STAB	$\supset$	1STAB
$\mathcal{O}$	CC	$\supset$	CLIF	$\supset$	1CLIF
$\mathcal{U}$	CONT	$\prec$	MAGIC	$\prec$	PMAGIC

表 III。通用量子计算模型概率族的三元组。

	HQS		HQCA		AQC
$\mathcal{F}$	STOQ	$\supset$	BIT	$\supset$	PRO
$\mathcal{O}$	LINEAR	$\supset$	PARALLEL	$\supset$	GAPPED
$\mathcal{U}$	NSTOQ	$\prec$	COH	$\prec$	1DQW

表 IV。通用量子计算模型哈密顿量族的三元组。

定了三个模型，它们构成了通用资源的层级。也就是说，这些通用资源的计算能力存在高低之分。对于两个资源理论，若 $\mathcal{F}_1 \subset \mathcal{F}_2$，则 $\mathcal{O}_1 \subset \mathcal{O}_2$。当总态空间固定时，$\mathcal{R}_1 \supset \mathcal{R}_2$，也就是说，在第一种理论中，更多量子态被视为具有资源性。然而，要实现通用性，第一种理论需要更强的资源能力。我们将其记为

$$\mathcal{U}_1 \succ \mathcal{U}_2, \tag{7}$$

其表述为“通用资源 $\mathcal{U}_1$ 在计算能力上强于通用资源 $\mathcal{U}_2$。”那么，以下两种通用资源之间的转换是可能的

$$(\mathcal{F}_2 \backslash \mathcal{F}_1)|u_2\rangle = |u_1\rangle,\ \mathcal{F}_1|u_1\rangle = |u_2\rangle, \tag{8}$$

对于通用资源态 $|u_{1,2}\rangle \in \mathcal{U}_{1,2}$，模自由态。

现在，我们将说明各个模型族中通用资源之间的转换；各模型的量子资源理论将在以下各节中介绍。表 II、III、IV 概述了相关内容。

a族依赖于量子态集合。信息由纯态的振幅 ψ_i 承载

$$|\psi\rangle = \sum_i \psi_i |i\rangle \tag{9}$$

这些纯态在正交归一基 $\{|i\rangle\}$上展开，而计算就是振幅的运算，即干涉。混态或密度算符 ρ 可以视为纯态 $\rho = \sum_\alpha p_\alpha |\psi_\alpha\rangle\langle\psi_\alpha|$ 的混合，其概率分布为p_α，定义在纯态集合 $\{|\psi_\alpha\rangle\}$上。

我们发现，QCM、LQTM 和测量型量子计算构成了a族中的三代模型。它们的通用资源分别为相干性（COH）、纠缠比特（EBIT）以及称为 UENT 的特殊纠缠。由具有最大相干性的量子位“加”态 $|+\rangle = \frac{1}{\sqrt{d}}\sum_i |i\rangle$，可以生成一个纠缠比特 $|\omega\rangle = \frac{1}{\sqrt{d}}\sum_i |ii\rangle$，如下所示：

$$|\omega\rangle = \mathrm{CX}|+\rangle|0\rangle \tag{10}$$

对于受控非门 CX，它在 QCM 中是免费的，但在 LQTM 中不是。借助纠缠比特，任意量子态都可以表示为 MPS [48–50] 形式

$$|\psi\rangle = (\otimes_n \mathcal{P}_n)|\omega\rangle^{\otimes n} \tag{11}$$

作为在 LQTM 中免费、但在测量型量子计算中不免费的局部算子。这包括二维簇态 [11] 和 AKLT态 [48]，其中包含作为通用资源的通用纠缠。

p族依赖于概率或准概率集合，并与测量效应有关。将量子态表示为

$$\rho = \vec{r} \cdot \vec{\sigma} \tag{12}$$

在厄米算符基 $\vec{\sigma}$中，它被表征为向量 $\vec{r}$。根据 Wootters [69]，，该向量在适当基中满足求和$(\vec{r}) = 1$。如果 $\vec{r} \geq 0$，它可以被视为概率分布；但一般来说会出现负值。因此，量子态被视为准概率，即维格纳函数，而计算就是它的变化。

p 族的灵感来自 MSI 模型 [16]。在该模型中，自由集合由稳定子态（STAB）组成，这些态的维格纳函数均为正值 [70]，，且 Clifford 操作（CLIF）是免费的。该模型选取了魔态

$$|t\rangle = T|+\rangle \tag{13}$$

作为通用资源，用于T，即 T 门。但并非所有维格纳函数为正的量子态

都是稳定子态 [71]。这意味着，在 MSI 之下还存在一种更基本的模型，能够直接刻画维格纳函数的负性。由于维格纳负性等价于量子情境性 [43]，，我们引入情境量子计算（CQC）模型。在该模型中，我们使用量子情境的叠加作为通用资源，这需要诸如 $|t\rangle$、$|+\rangle$ 和纠缠比特 $|\omega\rangle$ 这样的量子态，以及测量反馈（经典通信）。

对于这两种模型，确定性地实现量子门都需要经典通信。这揭示了关联的作用。存在一种更强形式的关联，称为 Popescu-Rohrlich（PR）非局域盒 [54]。研究发现，PR 盒可以在 T 门传态中取代经典通信 [51]。这促使我们定义 PMQC 模型，该模型与测量型量子计算以及瞬时非定域量子计算有关。在 MSI 中，量子传态是免费的；但在 PMQC 中并非如此。

h族以相互作用集合，即哈密顿量项为基础。我们将局域项及其开启和关闭视为操作。算法的初始输入态可以视为某个哈密顿量的本征态

$$H|\psi\rangle = E|\psi\rangle, \tag{14}$$

然后利用哈密顿量算术来改变 H。我们发现，HQS、HQCA 和 AQC 构成了h族中的三代模型，它们具有不同的相互作用项算术自由集合。

尽管它可以追溯到量子计算的起源 [72–75]，，我们发现，HQS 的基础是 H项的通用集合这一概念 [56–58]，，这与通用门集类似。给定一个集合 $\mathcal{S}$，哈密顿量由实权重加权求和构造而成

$$H = \sum_n j_n h_n \tag{15}$$

其中振幅为$j_n \in \mathbb{R}$，每一项为$h_n \in \mathcal{S}$。演化$U = e^{iHt}$ 将通过一系列局域项$e^{it_{n_{jn}h^n}}$ [73]进行 Trotter 分解。众所周知，几乎所有二局域项都是通用的，而随机正定项或经典项则是其特殊形式 [56–58]。我们将随机矩阵哈密顿量定义为自由集合。

HQCA模型作为一类量子元胞自动机，依赖于局域项的并行开关。每一步都有特殊的j_n ，也有t_n。换句话说，HQCA是一种特殊的HQS，就像LQTM和QCM的情况一样。它需要一个局域性更大的特殊局部项才能实现通用性。自由集合是经典元胞自动机，它可以具有经典通用性。最后，AQC使用局域项的绝热求和，且不存在能隙闭合，从而保护编码在基态流形中的信息。自由集合是局域态的乘积，相当于单点哈密顿量；通用资源则等价于一种一维量子游走，它由费曼–Kitaev电路到哈密顿量映射导出 [5]。

III. 《a》-族

A. 量子电路模型

本节回顾量子电路模型（QCM），并阐述其与相干性和干涉的联系。为简单起见，我们聚焦于量子比特情形，扩展到量子位情形则很直接。它包含三个基本阶段：

i) Initialize at the all-zero state $|00\cdots0\rangle$ of qubits;

ii) 施加一系列幺正门；

iii) 在 Pauli Z基中进行测量以读取结果。

QCM 中的量子算法通常描述为一系列量子门，可能还包括额外的经典预处理和后处理。一个核心结果是存在通用门集，可由此高效构造群$SU(2^n)$ 中的任意幺正演化 [6]。两个著名的门集是 {H、T、受控-X门} 和{ H、受控受控-X门}，其中 H 表示 Hadamard门，T 表示

$$\mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \mathrm{T} = \begin{pmatrix}\tau & 0\\ 0 & \tau^*\end{pmatrix}, \tag{16}$$

以及受控非门 CX、Toffoli门 CCX，适用于$\tau \equiv e^{i\pi/8}$。Toffoli门本身对经典计算具有通用性，这启发了我们为 QCM 建立资源理论。

现在我们介绍 QCM 的量子资源理论。自由态集合 $\mathcal{F}$ 是所有可由经典算法高效表示的量子态构成的集合。自由操作集合 $\mathcal{O}$ 是所有高效经典算法。也就是说，自由态

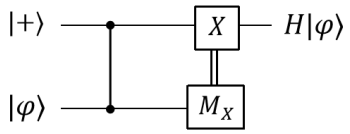

图2. H门的量子隐形传态。

和自由操作构成了通常的经典计算，可解决复杂度类有界错误概率多项式时间（BPP）中的问题。为方便起见，我们将它们分别记为 BIT 和 CC（见表 II）。通用资源 $\mathcal{U}$ 可将有界错误概率多项式时间（BPP）提升至有界错误量子多项式时间（BQP），从而实现通用量子计算，并成为实现量子加速的必要且充分资源。

通用资源 $\mathcal{U}$ 包含加态

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{17}$$

以及任意有限的张量积 $|+\rangle^{\otimes n}$，连同它们在自由操作下的所有等价态，例如“减态” $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$。加态 $|+\rangle$是 H门的魔态,因为给定 $|+\rangle$，就可以通过量子隐形传态实现 H，而量子隐形传态属于自由操作。参见图2。一个耐人寻味的事实是，测量必须在 X基上进行，而不是在 Z基上。从另一个角度来看，我们将在下一节展示，这与所研究的情境性的资源理论有关。

显然，含有 Toffoli门的经典电路只能在基态之间进行转换，而 H 门可以对振幅进行运算，这就是干涉。所有不会产生叠加的门也都是经典的，例如受控-X门、相位门S和 T门。自由测量不仅包括 Z基测量，也包括泡利测量。经典测量结果可以用作条件经典门的经典控制，而这些门也构成自由操作。

在 QCM 中，量子电路通常不表示为加态的注入。相反，它往往是一系列幺正门。为了衡量量子电路的能力，可以应用相干性的量子资源理论（COH），但该理论是针对量子态定义的。我们为门引入一种新的干涉（INT）能力度量，将其作为门的相干性度量。

给定量子态 ρ，相干性的 ℓ_1-范数度量为

$$C(\rho) = \sum_{i \neq j} |\rho_{ij}|. \tag{18}$$

不过，它并非可加的。可以将其转换为可加度量

$$Q(\rho) = \log_2(C(\rho) + 1), \tag{19}$$

以及$C(\rho) + 1$ 是 ρ的 ℓ_1-范数。我们将Q 称为对数相干性，简称“对数相干性”。显然,

$$Q(\rho_1 \otimes \rho_2) = Q(\rho_1) + Q(\rho_2). \tag{20}$$

其最大值为 $\log d$，其中d 为维数；这与相干性的相对熵的最大值相符

$$C_r(\rho) = S(\Delta(\rho)) - S(\rho) = \min_{\sigma \in \mathcal{F}} S(\rho \| \sigma), \tag{21}$$

它是可加的： [76], 对于S ，即冯·诺依曼熵，Δ 作为完全退相干信道。量子态ρ的本征值p_i 为$S(\rho)$ 香农熵 $H(p_i)$，对应的概率分布为p_i。

要量化干涉，我们需要一种动态相干性度量。根据信道-态对偶， [77, 78],一个过程 $\mathcal{E}$ 会映射为一个 Choi 态

$$\mathcal{E} \mapsto \omega_{\mathcal{E}} := \mathbb{1} \otimes \mathcal{E}(\omega) = \frac{1}{d} \sum_{ij} |i\rangle\langle j| \otimes \mathcal{E}(|i\rangle\langle j|), \tag{22}$$

对于纠缠比特 $\omega = |\omega\rangle\langle\omega|$。为方便起见，注意我们将信道作用于纠缠比特的第二部分。于是，该量子态的相干性可以视为量子门的干涉功率。然而，这种做法并不奏效。例如，泡利门 X、Y、Z 分别映射为具有非零相干性的贝尔态，但我们预期泡利门的干涉功率应为零。通过基于以下观察修改对偶性，可以解决这一困难：此类度量的定义域是自由集合，而不是整个态空间。我们介绍如下的经典信道-态对偶。

定义 1（经典信道-态对偶）。 对于一个

量子信道 $\mathcal{E}$ 的经典对偶态定义为

$$\mathcal{E} \mapsto m_{\mathcal{E}} := \mathbb{1} \otimes \mathcal{E} \circ \Delta(\omega) = \frac{1}{d} \sum_i P_i \otimes \mathcal{E}(P_i), \quad (23)$$

对于投影算符 $P_i = |i\rangle\langle i|$, Δ ，作为完全退相干信道。

退相干贝尔态 $\mathbb{1} \otimes \Delta$（$\omega$）具有最大经典相关性。该量子态的相干性 $m_{\mathcal{E}}$ 为

$$C(m_{\mathcal{E}}) = \frac{1}{d} \sum_i C(\mathcal{E}(P_i)), \quad (24)$$

并且对数相干性具有可加性

$$Q(m_{\mathcal{E}_1 \otimes \mathcal{E}_2}) = Q(m_{\mathcal{E}_1} \otimes m_{\mathcal{E}_2}) = Q(m_{\mathcal{E}_1}) + Q(m_{\mathcal{E}_2}). \quad (25)$$

相干性的相对熵为

$$C_r(m_{\mathcal{E}}) = \frac{1}{d} \sum_i C_r(\mathcal{E}(P_i)), \quad (26)$$

并且它确实具有可加性。根据相对熵和 ℓ_1-范数，量子门 $\mathcal{E}$ 的干涉功率可以看作由自由态 P_i分别生成的输出量子态 （P_i）的相干性的平均值。现在，我们可以应用这一度量来验证直觉：泡利门的干涉功率为零，而Hadamard门在一个量子比特上的干涉功率最大。我们将在第六节应用这一点研究量子算法。

B. 局域量子图灵机

现在我们考虑一种计算模型，其中自由态集合小于经典态集合。纠缠资源理论（ENT）很适合这一情形。对于双体情形，如果一个量子态可以写成以下形式，则称其为可分态:

$$\rho = \sum_i p_i \rho_i^A \otimes \rho_i^B \quad (27)$$

对于系统的双体划分 $A|B$ 。我们还要求局部维数为常数。自由操作 $\mathcal{O}$ 是随机局域操作与经典通信（ SLOCC），它只能保持或降低纠缠。对于双部设置 $\mathcal{H}_d \otimes \mathcal{H}_d$，量子态

$= \frac{1}{\sqrt{d}} \sum_i e^{i\theta_i} |ii\rangle$ 是最大纠缠态，其纠缠量为 $\log d$，包括贝尔态。

我们发现，以 ENT 作为资源的计算模型是 LQTM [47], ，它是对原始模型 [79–81] 的简化。在该模型中，计算需要两个寄存器：一个用于数据，另一个作为对手或“机器”。机器依次与数据寄存器中的每个量子比特相互作用，从而制备矩阵乘积态

$$|\psi\rangle = \sum_{i_1,\ldots,i_N} \mathrm{tr}(B A^{i_N} \cdots A^{i_1}) |i_1 \ldots i_N\rangle, \quad (28)$$

对于边界算符 B，其作用已在文献 [47] 中得到详细分析。数据量子比特彼此之间不直接相互作用，这是一种自然的局域性约束，也表明 ENT 是 LQTM 的资源。

每个局域位置 $n \in \{1, 2, \ldots\ldots N\}$ 上的矩阵集合 $\{A^{i_n}\}$ 构成一个作用于对手空间的信道 $\mathcal{E}_n$；在其他上下文中，该空间也称为虚拟空间、键空间、边缘空间或关联器。对手空间的维数决定了整个系统所含 ENT 的量。由于每个 $\mathcal{E}_n$ 都可以扩张为酉算符U_n，因此可以通过顺序电路制备矩阵乘积态。

表示 MPS 的另一种方式——实际上也是最初的方式——是价键固体方法 [48]。请注意，MPS 一词通常用于纠缠较弱的一维系统，而张量网络态（TNS）或 PEPS 则用于更高维系统；但从数学上讲，它们都是 MPS [82]。给定一组纠缠比特，通过将算符 $\mathcal{P}_n$ 作为随机局域操作与经典通信来应用，即可制备 MPS，见公式（11）。这明确体现了纠缠比特作为通用资源 $\mathcal{U}$ 的作用。非最大纠缠态需要蒸馏方案 [8], ，因此弱于纠缠比特。没有纠缠比特时，随机局域操作与经典通信作为自由操作 $\mathcal{O}$，只能生成可分态（SEP），它们构成自由集合 $\mathcal{F}$。

尽管可分态也具有局域相干性，但它们可以通过经典方法高效模拟，也就是说，分别以恒定的局部维数实现混合和局域态。总希尔伯特空间的维数实际上不会随系统大小呈指数增长。随机局域操作与经典通信下的局域相干性无法产生纠缠或大量的 INT。

ENT 与 COH 之间的关系已得到充分研究，例如参考文献 [83, 84]。给定一个双部设置$\mathcal{H}_A \otimes \mathcal{H}_B$ 以及正交归一乘积基 $\{|a,b\rangle\}$,

作为极端非相干态的集合，一个量子态的 ENT 不超过其 COH

$$E(\rho) \leq \min_{U} C(U\rho U^{\dagger}) \tag{29}$$

将$U = U_A \otimes U_B$ 表示为乘积酉算符。这意味着我们可以根据量子门的非相干功率研究其纠缠功率。反过来，COH 也可以用 ENT 量化为

$$C(\rho) = \lim_{d_a \to \infty} \sup_{\Lambda} E(\Lambda(\rho \otimes |0\rangle\langle 0|)) \tag{30}$$

将d_a 作为辅助系统维数，将 Λ 作为双部非相干操作 [83]。利用相对熵，存在一个 Λ （广义 CNOT 门），使$d_a \geq d$达到上确界。ENT 本身也是最终态的 COH。

从物理上看，ENT 和 COH 并不相同。COH 描述的是系统的整体特征。ENT 是一种特殊的 COH，以共享或分布的形式存在，用于表征系统各部分之间的量子关联。这种量子关联可以理解为量子存储器。在另一项研究中，由矩阵乘积态导出的信道被称为带记忆信道 [85]。对于 LQTM，将控制机器视为“记忆”确实很直观。在量子通信中，建立一个远程纠缠比特可以将量子信息从一方传送给另一方 [1]。近期研究表明，基于信道-态对偶，纠缠比特是量子存储器的基本单元 [64] 。存储量子程序是由纠缠比特构成的 Choi 态，对其进行局域测量即可执行读写操作。

C. 基于测量的量子计算

现在我们来研究一种模型，它将特殊的纠缠态视为通用资源，因此自由态和自由操作受到更多限制。例如，贝尔态测量 [6]将不再是自由操作。这就是测量型量子计算（MBQC），通常包含两个部分：

i) 一个通用资源态；

ii) 一系列格点自适应测量。

需要对测量结果进行经典后处理。众所周知，最初的量子态是二维簇态 [11] ，其量子门执行的底层机制被确定为门隐形传态 [86]。后来，通过将资源态表示为矩阵乘积态（MPS），该方法得到了扩展

$$|\psi(\ell)\rangle = \sum_{i_1,\ldots,i_N} A^{i_N} \cdots A^{i_1} |\ell\rangle |i_1 \ldots i_N\rangle, \tag{31}$$

其中数据 $|\ell\rangle$ 由边缘空间承载，并通过在体区上进行一系列格点自适应局域投影测量（LPM），在其上实现通用性 [87]。LPM 也可以扩展为局域 POVM [88]。最近，这也被理解为边缘码上的单向码切换 [37]。通过码串接和纠错，可以实现容错切换。

没有资源态时，格点自适应测量只能生成乘积态。因此，我们将自由态集合 $\mathcal{F}$ 定义为乘积态（PRO），它是可分态（SEP）的子集。自由操作 $\mathcal{O}$ 是单格点操作（1O）和单向经典通信（1C），记为单向局域操作与单向经典通信（1O1C）。单向局域操作与单向经典通信作用于乘积态时不会生成可分态，尤其不会生成全局共享的概率比特。这类概率比特应由单向局域操作与单向经典通信作用于资源态来生成。

近年来，研究表明 MBQC 与 SPT order 之间存在密切联系 [26–28]。SPT ground states 是 injective 的，并且具有良定义的 locality。具体而言，其 local sites 的定义满足局域张量 A 是 injective 的。injectivity 意味着，通过作用于 physical spins，我们可以在 edge space 上实现任意操作 [23, 89]。通常还具有 translational invariance。通过对少数几个位点进行 blocking，可以得到一个 injective 张量。但这会违反 1O1C condition。对于 MBQC，还需要更严格的逐位点 injectivity，而这可以由 SPT order 提供。

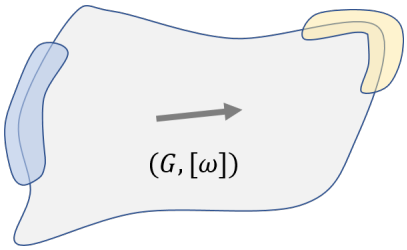

图3. 测量型量子计算中，由 $(G, [\omega])$ 标记的计算从输入（蓝色区域）到输出（黄色区域）的信息流（箭头）示意图。

这种逐位点 injectivity 可以由 SPT order 提供。

目前已知有三类SPT序具有通用性。其中包括一些具有弱SPT序的二维AKLT相 [88,90] 、具有1-形式SPT序的二维簇相 [28] ，以及一些具有强SPT序的超图态 [91, 92]。与此同时，已知一些图态也具有通用性，其纠缠由纠缠宽度度量 [40]刻画，显然不一定需要是SPT相。

不难证明，单射矩阵乘积态（或高维情况下的张量网络态）可以通过自由操作驱动到SPT相，尽管这种驱动方式并不唯一。给定一个量子态$|\psi\rangle$，确定输入、输出和体区所在的区域，以及信息流的方向。示意见图 3。一对

$$(G, [\omega]) \tag{32}$$

对称性（通常由群G指定）以及由群上同调群中的一个元素 $[\omega]$ 标记的SPT类需要预先选定，从而确定其局域张量A。 $|\psi\rangle$ 的每个局域张量都可以通过自由局部操作变换为张量A。换句话说，单射张量网络态可以视为一种带有无序和晶格缺陷的SPT态（例如，可能缺少少数几个格点）。例如，通用图态和加权图态可以视为二维簇态的变体。此外，利用类似蒸馏的技术 [27], ，SPT相中的量子态可以通过局域操作与经典通信驱动至其固定点。

因此，我们将二维 SPT 对称保护拓扑序的固定点视为通用资源。更准确地说，任何在单向一比特通信自由操作下等价于二维簇态的二维 SPT 对称保护拓扑序固定点都是如此。SPT 纠缠的概念已在 [93]一维阿贝尔情形中得到研究，也可以扩展到更高维。纠缠宽度 [40]表明，通用资源的纠缠应随逻辑系统尺寸线性增长。因此，我们使用“通用纠缠”（UENT）一词来指代测量型量子计算通用资源中的纠缠。

从矩阵乘积态形式可以很容易看出，二维簇态（及其等价态）是通过对纠缠比特施加非单向一比特通信的局域操作与经典通信来制备的。矩阵乘积态中的局部操作 (11) 正是此类操作。

已有证明表明，具有较大 ENT 的随机态对测量型量子计算并无用处 [9, 10]。事实上，这些高度

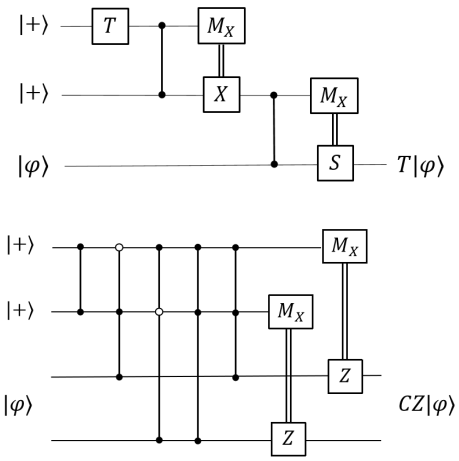

图4. 用于实现 T 门和受控 Z 门的量子电路。

纠缠态在测量型量子计算下的行为大多类似于局部概率比特。因此，并不存在全局共享的 p 比特。这意味着，通用性需要资源态具备某些全局特征，而这与对称性有关；对称性确实是量子系统的全局特征。要实现通用性，我们既需要广延的 ENT，也需要现场单射性；前者由二维系统的能隙特征提供，后者则由对称保护拓扑序的特征提供。我们还应注意，这并不意味着高度纠缠的随机态在其他模型中毫无用处。

IV. p 族

A. 情境量子计算

本节将介绍情境量子计算（CQC）模型。我们从情境性的物理基础谈起，它源于隐变量理论 [13]。量子情境是一种量子操作，例如态制备、演化或测量 [42]。两个操作若彼此对易，则它们相容，因此可以同时存在。相容设置不具有情境性，这意味着算子可以化为数值。量子情境性指不相容量子情境同时存在。经典情境性可定义为不相容量子情境的混合。随后，我们将量子情境性（CONT）刻画为量子情境的叠加——

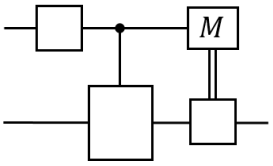

图5. 情境量子电路示意图。

——这正是 CQC 模型的出发点。

用泡利基表示后，我们得到图4中的 T 门和受控 Z 门电路；H 门电路另见图2。若将泡利算符视为基本量子情境，则每个量子门都体现了量子情境性。这些情境电路是通用的，因为 H 门、T 门和受控 Z 门构成一个通用门集。

现在，我们给出情境量子电路的一般定义，并在图5中加以示意。

定义 2 (情境量子电路)。 情境量子电路包含两个寄存器：一个用作控制寄存器，另一个用作数据寄存器，并实现如下形式的过程

$$\mathrm{tr}_c \circ (CV(U_2 \otimes \mathbb{1})CU(U_1 \otimes \mathbb{1})) \tag{33}$$

其结构为夹心式：控制寄存器的特殊初态由 U_1，制备；控制寄存器上的特殊测量由 U_2 制备，并通过 CV 将反馈传递至数据寄存器，同时对控制寄存器取迹；中间则是以数据寄存器为目标的量子受控门 CU。这两个受控门也称为多路复用器，其形式为

$$CU = \sum_i P_i \otimes U_i, \tag{34}$$

控制端的投影算符 $P_i = |i\rangle\langle i|$ ，以及数据端的幺正算子 U_i 。

通过将其表示为门的线性组合，它可以确定性地实现一个门 U 。量子控制寄存器是必需的，因为没有它，直接应用的门只会产生态的叠加。情境混合则通过经典控制实现。

现在，我们可以通过在中间使用更一般的门，对定义进行略微扩展；这些门会在控制端引入反馈操作。这里不再对此进行详细讨论。

在这个模型中，测量非常重要。量子测量由正算子值测度描述。正算子值测度是一个集合 $\{E_i\}$ ，其中包含效应算符 $E_i \geq 0$ 和 $\sum_i E_i = \mathbb{1}$。一次测量——作用于量子态 ρ 会产生三方面的信息：测量结果 i、测量结果的概率 $p_i = \mathrm{tr}(E_i\rho)$，以及每个 i 对应的最终态 ρ_i 。如果索引 i 是明确已知的，则该测量是选择性的；如果可以获得 ρ_i ，则该测量是非破坏性的。如果它是混合态，那么它实际上就是一个量子信道。

在测量控制操作中，引入经典测量结果i 至关重要：根据i的不同，还可以进一步应用不同的算子。这对于量子隐形传态以及 MBQC 同样至关重要：泡利副产物校正需要根据先前的测量结果进行条件控制。实际上，情境电路可以被视为量子隐形传态的扩展。

现在，我们可以定义 CQC 的 QRT。自由集合包括 BIT 和 CC，与 QCM 类似：算法的输入可以是比特或概率比特，计算电路由 S门、T 门、受控-X门、受控 Z 门、受控受控-X门以及任意对角门构成，但读出测量只能在 Z基中进行，同时还包括 Z测量控制电路。此类电路永远无法生成态的叠加。

不难看出，通用资源是泡利测量M_X。选择性M_X 不仅能制备初始资源态 $|+\rangle$，还会导致 CONT。借助自由的受控 Z 门和 T 门，它还会生成 $|\omega\rangle$ 和 $|t\rangle$。

因此，在我们的框架中，CONT 等价于 INT。对于 QCM，我们将 $|+\rangle$ 视为资源，而将 M_X 视为自由操作。不过，严格来说，M_X 能够制备 $|+\rangle$ ，因此更适合将其视为 Hadamard门的资源等价物。我们可以直接使用 COH 和 INT 作为量子态和量子门 CONT 的度量。例如， $|t\rangle = T|+\rangle$的 CONT 为 1，即 $|+\rangle$的 COH 值。我们将在第六节进一步研究 CONT 与 INT 之间的关系。

尽管上述研究远未完善，但它为 CQC 奠定了基础。此时，将其与其他模型联系起来颇有意义。首先，与 QCM 相比，CQC 中量子控制的作用是显式的。一个通用的情境电路可以拥有多个控制寄存器。一个潜在应用是模块化计算场景，在这种场景中，需要将未知操作作为黑盒或预言机进行控制 [94–97]。例如，Kitaev 的量子相位估计算法 [5], 可以估计未知U 的相位因子 θ ，前提是已知它的本征态$|\psi\rangle$ ，其中$U|\psi\rangle = e^{i\theta}|\psi\rangle$。

对偶量子计算模型中研究了算符干涉的概念 [53, 98], , 由此发展出了酉算符线性组合（LCU）算法。LCU 已用于哈密顿量演化模拟等领域，但通常需要对控制寄存器进行后选择 [52, 99, 100], , 因此具有概率性。对于某些特殊的 LCU 情形，后续采用测量控制操作即可避免这一点。要在 CQC 中模拟量子门U ，首先可以将其分解为由 H 门、T 门和受控 Z 门组成的序列，然后通过情境电路确定性地实现其中的每个量子门。

最后，由于测量起着至关重要的作用，MBQC 中的 CONT 已得到研究 [45, 46],。从 MBQC 的隐形传态图景来看 [26], , 量子门通过门隐形传态来模拟。我们可以将辅助量子比特以及 $|+\rangle$或纠缠比特 $|\omega\rangle$ 量子态和 M_X 视为隐形传态的资源。基于二维簇态的 MBQC 是通用的，因此必然具有上下文性，并且需要进行偏离 Z 基的测量。然而，隐形传态图景会将 MBQC 过程拆分成若干部分，从而失去其整体特征。相比之下，我们发现，第三节 C 中的 MBQC 量子资源理论更适用于通用纠缠；通用纠缠首先作为通用资源给出，然后通过免费的局域自适应正交投影值测量加以消耗。相反，在 CQC 中，上下文的作用是明确的，而且无需一开始就制备高度纠缠的量子态。

B. 魔态注入

MSI 的资源理论已经得到了充分发展 [101]。这里我们简要介绍一下，以求完整。该模型适用于采用稳定子码的容错量子计算，这类编码通常允许横向克利福德逻辑门。在该模型中，自由集合 $\mathcal{F}$ 由具有正维格纳函数的稳定子态（STAB） [102], 构成，而克利福德操作（CLIF）是自由的 [70], $\mathcal{O}$。这使魔态 $|t\rangle = T|+\rangle$ 成为通用资源，其中T 称为 T 门。

一种重要的可加度量称为“魔力” [101]。对于奇数维量子位态 [69, 70],，采用标准维格纳函数$W\rho$时，魔力为

$$M(\rho) = \log(2N(\rho) + 1), \tag{35}$$

对于总负性$N(\rho) = \sum'_u |W\rho(u)|$ 对于$W\rho(u) <$

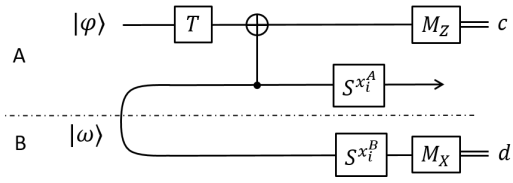

图6. Broadbent 的非信号 T 门隐形传态。曲线表示纠缠比特 $|\omega\rangle$。带箭头的中间线路承载输出。

0. 为了说明与相干性的联系，显然$N(\rho) \leq C(\rho)$，因为前者衡量到 STAB 的距离，而后者衡量到非相干集合的距离，非相干集合是 STAB 的一个子集 [103]。这与这样一个事实类似：对于一个量子态 [83]，纠缠小于相干性。

C. 后魔态量子计算

对于哪一种 UQCM，其通用资源会比 MAGIC 更强？我们需要确定 STAB 的一个子集。然而，这并不是唯一的。在此，我们研究一种依赖于比 MAGIC 更强的 CONT 形式的模型；CONT 是一种瞬时非定域量子计算（INQC），并且与测量型量子计算（MBQC）有着密切联系。

我们已经看到，测量反馈是有用的。相反，也存在一些不允许测量反馈或对其有严格限制的情形。一个极端例子是 INQC：它不允许经典通信，而只允许广播局部结果。这类操作被称为基于广播的局部操作和经典通信（LOBC） [104], , 是 LOCC 的一个子集。一种主要场景是双参与方的非局域任务：A 和 B 各自获得一个输入 x、y，然后使用 LOBC 操作输出 a、b，再利用它们计算结果 $f(x$、$y)$。安全性是一个自然要求；在此，我们考虑所谓的单边安全性 [105], , 即其中一方可以知晓计算结果。

一种经典的加密方案是使用泡利算符 X^aZ^b 进行编码，并以 a、$b \in \{0,1\}$ 作为密钥 [106]。Broadbent [51] 发现，T 门隐形传态中的测量反馈可以由波佩斯库-罗里希（PR）盒 [54], 取代，该盒

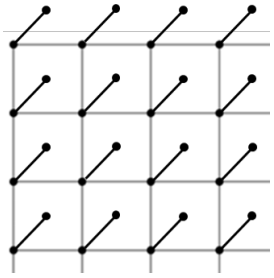

图7. 带尾簇态的示意图 $|\Phi\rangle$。

输入 x、y 后，将输出 a、b，且满足

$$a \oplus b = x \cdot y, \tag{36}$$

由此实现了对 CHSH 不等式的最大违背 [107]，其值大于量子理论所允许的值。Broadbent 的非局域T门隐形传态（BTT）如图6所示，是我们 PMQC 模型的起点。在通常的 T 门隐形传态中，需要校正相位门 S，这是因为

$$TX^aZ^b = X^aZ^{a\oplus b}S^aT. \tag{37}$$

这也意味着，T 门会破坏密钥的更新规则。通过使用一个纠缠比特和一个 PR盒，可以避免使用相位门。PR盒用于将$(x_i^A \oplus c)x_i^B$线性化为$z^A \oplus z^B$，而纠缠比特则用于稍后注入值x_i^A、x_i^B，以抵消 S 门。

现在我们介绍 PMQC 模型。更准确地说，它是对采用二维簇态的测量型量子计算的扩展。不同于通常的簇态，现在每个量子比特都有一个“尾巴”（或称伙伴），如图7所示，而带尾簇态

$$|\Phi\rangle = \left(\bigotimes_e CZ_e\right)|\omega\rangle_{AB}^{\otimes n} \tag{38}$$

制备方式如下：将纠缠比特集合中的所有“头部”（“尾部”）分别标记为参与方A（B）。以纠缠比特$|\omega\rangle^{\otimes n}{}_{AB}$作为初始态，对于正方晶格的每条边$e$，在参与方A中相邻的量子比特之间施加一个$CZ^e$ 门。这样的电路是带尾量子电路 [64]的一个示例。

二维簇态的通用性体现在它能够模拟 CZ 门和任意量子比特旋转，其中每一行都对应一个量子比特的逻辑演化方向。我们不需要任意量子比特旋转，只需 H 门和 T 门，它们对于 SU(2) 是通用的 [6]。H 门通过 M_X(a) 实现，得到 HZ^a；T 门则通过 M_X(b)TM_X(a) 实现，得到 $HZ^bHZ^aT = X^bZ^aT$。若要在 PMQC 模型中对加密态依次实施 H 门和 T 门（见簇态的顶行），则通过测量最左侧的尾部量子比特，将输入加密态 $X^aZ^b|\psi\rangle$ 注入其中。借助 BTT，可将类似 $HX^aZ^bTHX^cZ^dHT\cdots$ 这样的序列中的泡利副产物移至末尾（图6）。具体来说，对于参与方A的每个量子比特，都要消耗一个纠缠比特和一个 PR盒。CZ 门的实现方式与原始测量型量子计算相同。因此，我们证明，PMQC 模型能够对由客户端参与方B提供给服务器参与方A的加密数据实现通用门集 {H,T, CZ}；参与方A并不知道数据的输入和输出，且参与方A与参与方B之间只需进行最后一轮广播通信。

为了构建PMQC的量子资源理论，首先注意到，所有T 门都可以在测量之前先施加。也就是说，为了模拟由H、T、受控 Z 门组成的电路，可以将每个待模拟的门“印刻”到子晶格 A 的某个格点或边界上，并且将与受控 Z 门对易的T 门施加到适当的 A 格点上，从而得到电路特定的簇态。这样，只需进行泡利基测量即可模拟该电路。因此，我们将单量子比特克利福德操作的张量积和广播通信确定为自由操作集合 $\mathcal{O}$，记为1CLIF。自由态集合 $\mathcal{F}$（1STAB）包含作为极值点的泡利本征态的张量积。它们比MBQC以及MSI中的自由设置更小。由此，电路特定的带尾簇态和PR盒共同构成通用资源，其中PR盒发挥核心作用。目前，我们将“后魔法”（PMAGIC）这一术语定义为PMQC模型中的通用资源。

PR盒的提出源于对量子非定域性（NONL）的研究，而如今量子非定域性通常被视为 CONT 的一种特殊类型 [44]。与一般的 CONT 情形不同，NONL 不允许条件操作和非定域操作。有人提出使用局域操作与共享随机性（预共享随机性）作为定义 NONL 的自由操作 [108]。以局域态作为滤波器时，可以看出纠缠等价于非定域性。至此，将非定域性与 MAGIC 进行比较或许会有所启发。我们确立了纠缠，因此很可能

NONL 是 LQTM 的资源，位于 QCM 与测量型量子计算之间。Magic 是 MSI 的资源，位于 CQC 与 PMQC 之间。NONL 与 MAGIC 不可比较，因为 MAGIC 依赖条件操作，而 NONL 不依赖。MAGIC 还取决于 Clifford 层级 [109]。我们看到，PMQC 是 MAGIC 与 NONL 的结合。

令人颇感意外的是，实现通用性竟需要 PR盒，因为它的关联超出了量子理论。此外，PR盒不必完美：只需略微超出量子理论的关联，就能使通信复杂度变得平凡 [110]。它能够实现时间上“平坦”的通用盲测量式量子计算 [55]。如果用纠缠比特取代 PR盒，那么要在没有通信的情况下实现量子隐形传态，就需要指数数量的纠缠比特 [111]。不过，允许的经典通信量也可以是有限的，而不必达到最小值。是否存在一种量子通用资源，其能力强于 MAGIC、弱于 PMAGIC，仍有待探究。

V. h族

A. 哈密顿量量子模拟

本节研究一种基于哈密顿量演化的基本模型。具体而言，我们依靠哈密顿量相互作用项的通用集合理论 $\mathcal{S}$ – 59], , 这与通用门集类似。首先，若能用一个 H' 模拟 H，那么在局部编码 $\mathcal{E}$ 下，当能量低于 Δ 时，若

$$\|H'_{\leq\Delta} - \mathcal{E}(H)\| \leq \epsilon \tag{39}$$

对于$H'_{\leq\Delta}$ ，将其视为H' 在能量 Δ以内的限制。更精确的定义见 [56–58]。模拟成本是H的系统大小和相互作用能量的函数。给定 ϵ，时间演化$U = e^{iHt}$ 可在误差不超过 ϵt的情况下进行模拟。

哈密顿量量子模拟过程由一系列局部演化 $e^{it_n j_n h^n}$ 构成，其中局部项为 h_n，相互作用强度参数为 j_n，时间参数为 t_n。它可以被视为一个 Lie-Trotter 序列。每个局部项都可以从集合 $\mathcal{S}$ 中选取，并通过实数加权的 sum

$$H = \sum_n j_n h_n \tag{40}$$

振幅 $j_n \in \mathbb{R}$ 和每个项 $h_n \in \mathcal{S}$ 构造出模拟哈密顿量。

最近已有证明表明，存在通用哈密顿量集合 [56–59], , 例如二局域海森堡相互作用和 XY交换相互作用。给定目标H，该模拟方案首先将其映射为量子相位估计（QPE）电路U [59], , 然后使用Feynman-Kitaev电路到哈密顿量映射得到哈密顿量H_{FK} [5]，再依靠微扰构造 [112]，用一个 $\mathcal{S}$-哈密顿量H' 对其进行模拟。为确保模拟的效率，该方法不会直接模拟H ；例如，相互作用振幅仅随系统大小呈多项式增长。

一类特殊的哈密顿量被称为随机正定，其所有非对角元均为实数且非正。已有研究表明，随机矩阵哈密顿量比经典计算更强大 [112, 113]。这促使我们为 HQS 构建量子资源理论。自由集合 $\mathcal{F}$ 是随机矩阵哈密顿量的集合，记为 STOQ；自由操作 $\mathcal{O}$ 是保持随机正定性的任意线性组合，记为 LINEAR。例如，双量子比特随机正定相互作用的形式为 $\alpha ZZ + A\mathbb{1} + \mathbb{1}B$ ，其中 $\alpha \in \mathbb{R}$ 在适当基 [112, 113], 下，而经典相互作用是对角的 [114]。可以通过距离或基于熵的测度，或通过将其转换为对量子态的效应算符，来定义非随机正定性的度量。不过，本文不对此进行探讨，仅介绍普适资源的特定形式。

此外，将其与其他研究联系起来并辨析其差异也很有价值。哈密顿量演化的量子模拟旨在通过将给定的演化$U = e^{iHt}$ （或时变演化）分解为一系列局部么正项，例如使用李-特罗特公式，在 QCM 中对其进行模拟，但不涉及通用哈密顿量集合 [73,115]。HQS 可视为模拟量子模拟（专用特定用途）的扩展 [116],，其对局部项可控性的要求较低。例如，模拟器可能具有特殊形式的局域相互作用项，而这些项可能无法在局部开启和关闭，

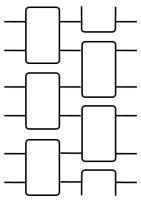

图 8. 量子元胞自动机砖墙电路示意图。

其开关可能无法在局部实现。相反，HQS 演化在本质上是数字式的，因为h_n 的集合是有限的，时间参数也可以数字化，即划分为可控的时间段。对时间依赖性和经典控制的要求，也使其有别于某些基于哈密顿量的自主量子计算模型 [66, 117–122]，例如连续时间量子行走 [66]。这表明h 族的主要特点是探索子系统之间的相互作用，将其视为资源。自动化等其他要求是否会催生其他模型族，还有待进一步研究。

B. 哈密顿量量子元胞自动机

对哈密顿量项的运算施加限制后，会产生新的模型。本节定义一种基于哈密顿量的量子元胞自动机模型，称为 HQCA。

对于经典计算，元胞自动机是一种通用模型。已知存在二维通用元胞自动机，而一维元胞自动机无法实现通用性 [45, 123]。它将比特排列在具有明确定义邻域的晶格上，并通过并行局部动力学来规定演化；例如，每个比特在之后某一时刻的取值由其当前邻居决定。元胞自动机可以通过经典电路模拟。局部规则被映射为一个置换 P。但在此之前，我们需要对每个比特执行一个复制步骤。模拟电路呈砖墙形式，见图 8，其中一层是复制操作，一层是 P，如此交替进行。

人们已经开发出多种量子元胞自动机（QCA）模型 [60–62]。其中有基于电路的模型，也有基于哈密顿量的模型；本文采用后者。与经典情形不同，一维哈密顿量量子元胞自动机可以通过两体局域量子位相互作用项实现通用性。我们先概述一个半经典模型，说明其工作原理，然后将介绍作为该模型变体的我们的模型。在 Nagaj-Wocjan 模型中 [124]，，一个包含$d = 10$ 个局域位置的系统由若干带构成，分别用于数据量子比特、程序和控制器。一维链被划分为许多区域，每个区域对应模拟电路中的一个步骤。所有数据量子比特都位于某个特定区域。模型通过设计平移不变的相互作用来模拟电路。对于一个含N 个量子比特、包含M 个步骤的电路，HQCA 系统大小为MN，运行时间为多项式级。直观地说，该模型的工作方式类似打字机：数据量子比特保持不动，而程序则通过移动程序的量子态、使其经过数据来执行。该模型是自主的，因此在演化e^{iHt}下，只有有限概率能实现所需的最终量子态 $|\psi_f\rangle$ 。通过重复运行算法或修改模型本身，可以提高成功概率。

对于 HQS 模型，我们允许经典控制。这里借鉴经典控制量子元胞自动机的思路，定义一种经典控制 HQCA [125]。经典控制量子元胞自动机通常由一系列不同的量子元胞自动机组成，每个量子元胞自动机都由经典方式控制，即开启或关闭。我们的模型定义如下：对于一维数据量子比特阵列，在每对数据量子比特之间添加一个辅助量子比特和一个程序三能级量子比特。局部维数为十二。局部相互作用为

$$H = |0\rangle\langle 1| \otimes U + |1\rangle\langle 0| \otimes U^{\dagger}, \tag{41}$$

第一部分作为辅助量子比特，并且

$$U = P_0 \otimes \mathbb{1} + P_1 \otimes W + P_2 \otimes \Pi, \tag{42}$$

第一部分作为程序三能级量子比特，用于

$$W = P_0 \otimes \mathbb{1} + P_1 \otimes HZ, \tag{43}$$

第一部分作为数据量子位， Π 作为作用于两个数据量子比特的 SWAP门。量子门W 已知是通用的—

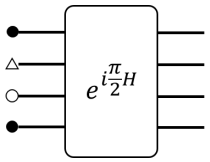

图9。HQCA模型中的一个局部项。黑点表示数据量子比特，圆圈表示辅助量子比特，三角形表示程序三能级量子比特。

如果它可以应用于任意一对量子比特 [125]。注意，在 HZ 中，它是 Hadamard门H。

现在，给定一个由最近邻W 门和 SWAP 门组成的电路，首先将其排列成一系列横向步骤。每个步骤都是 W 门和 SWAP 门的张量积。程序三能级量子比特 $|p\rangle$ 对作用于两个数据量子比特的量子门类型进行编码，$G \in \{\mathbb{1}, W, \Pi\}$。辅助量子比特初始化为 $|1\rangle$。局部演化的作用为

$$e^{i\frac{\pi}{2}H}|1\rangle|p\rangle|\psi\rangle = |0\rangle|p\rangle G|\psi\rangle, \tag{44}$$

它不会改变程序三能级量子比特，但会翻转辅助量子比特。进入下一步之前，必须重置程序三能级量子比特和辅助量子比特。时间 $\frac{\pi}{2}$ 是常数，因此可以视为快速淬火；整个 HQCA 则被视为构成砖墙结构的 Trotter化步骤。

注意，如果使用上面的U (42)代替H (41)，就不需要辅助量子比特了。这基本上简化为一个经典控制量子元胞自动机模型 [125]。如果将程序三能级量子比特的值移出，这将进一步简化为电路本身。相反，HQCA模型的主要特点是并行性。只需确保相互作用具有平移不变性。此外，与自主模型 [124, 126]，相比，使用经典控制可以确保所需最终态的确定性制备。

对于HQCA模型的量子资源理论，将经典元胞自动机视为自由集合 $\mathcal{F}$是自然的。自由操作 $\mathcal{O}$ 是局部相互作用的并行控制，记为PARALLEL。然而，量子门W 显然不会约化为经典情形。基于类似的思想，我们可以选取Toffoli门和Hadamard门构成的门集合，并将受控Toffoli门和受控Hadamard门视为横向步骤，尽管这会增大相互作用的局域性和局部维数。由于Toffoli门在经典情况下是通用的，因此显然量子资源源于Hadamard门，即相干性。因此，我们将COH确定为该模型的通用资源。通过观察局部四体项H (41)显然是非随机矩阵的，可以看出COH与NSTOQ之间的关系。项H 可以在HQS中通过通用哈密顿量集合中的二体项加权求和进行模拟。

C. 绝热量子计算

本节将介绍AQC模型 [38]。众所周知，我们仅说明它如何属于h族。在该模型中，通常首先以易于制备的 H_0 的基态 $|\psi_0\rangle$ 作为初始量子态，然后使用绝热路径

$$H(t) = tH_0 + (1-t)H_1,\ t \in [0,1] \tag{45}$$

对于时间参数t ，基态 $|\psi_1\rangle$ 的H_1 编码了最终输出。绝热条件要求在演化$e^{i\int_0^1 H(\tau)d\tau}$过程中不存在能隙闭合，该演化会使 $|\psi_0\rangle$ 经过基态流形 $|\psi_t\rangle$。通常，我们还可以将一系列绝热路径依次连接起来。

证明 AQC 通用性的标准方法是 Feynman-Kitaev 历史态方法。给定一个电路$U = U_1 U_2 \cdots U_L$，可将其映射为一个五体局域但非几何局域的哈密顿量H_{FK} ，其基态为历史态

$$|\Phi\rangle = \frac{1}{\sqrt{L+1}} \sum_{\ell=0}^{L} |\gamma_\ell\rangle \tag{46}$$

对于 $|\gamma_\ell\rangle = |\psi_\ell\rangle|\ell\rangle$，并以 $|\psi_\ell\rangle = U'_\ell|\psi_0\rangle$、$U'_\ell = UUU_\ell$、$|\psi_0\rangle$ 作为初始数据态，以及 $|\ell\rangle$ 作为时钟寄存器的量子态。随后设计一条绝热路径$H(t)$ ，使 $|\gamma_0\rangle$ 成为$H(0)$的基态，并使 $|\Phi\rangle$ 成为$H(1)$的基态。历史态得到输出的概率仅为 $1/(L+1)$。通过用一系列恒等门填充电路来放大这一概率；这样会使用更多时钟量子比特和相互作用项，使成功概率接近 1。

现在，我们定义属于h族的 AQC 的 QRT。我们将位点项作为自由集合 $\mathcal{F}$，对应于自由乘积态 PRO，它们通常被设为算法的初始量子态 $|\psi_0\rangle$ 。自由操作 $\mathcal{O}$ 记为 GAPPED，即绝热开启与关闭位点项；该操作不得导致任何位点项发生能隙闭合。事实上，绝热位点切换是一种特殊的并行或横向切换。通用资源则是能够实现通用量子计算的项。对于H_{FK} 模型，限制在历史流形 $\mathrm{span}\{|\gamma_\ell\rangle = |\psi_\ell\rangle|\ell\rangle\}$ 上时，最终哈密顿量为

form

$$H_w = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & & & \\ -\frac{1}{2} & 1 & -\frac{1}{2} & & \\ & -\frac{1}{2} & 1 & -\frac{1}{2} & \\ & & \ddots & \ddots & \ddots \end{pmatrix}, \tag{47}$$

这是一个一维量子游走模型。请注意，它仅在这个特殊的历史态基下是随机矩阵的。而在标准计算基下，随机矩阵哈密顿量无法实现通用计算。因此，我们将一维量子游走视为 AQC 的通用资源。显然，在可控性受到更多限制时，所需的相互作用会变为非局域。这与我们已建立的相干性和关联资源理论相呼应。对于资源转换，很明显，量子漫步H_w 可以通过量子元胞自动机实现或模拟。从 $\{|\ell\rangle\}$ 到 $\{|\gamma_\ell\rangle\}$ 的基变换也可以通过量子元胞自动机模拟。

VI. 量子算法与资源

本节将对一些著名的量子算法进行初步的资源理论研究。我们主要关注依赖量子电路的算法。具体而言，我们研究相干性、干涉、纠缠与情境性之间的相互作用。

对于量子电路，我们可以计算干涉量。我们用 I 表示干涉。我们采用相干性的相对熵。一般而言，对于两个量子多能级门 V、W $\in$ U(d)，I(V)、I(W) 与 I(VW) 之间不存在确定的关系。若 V 是非相干的，则 I(VW) $=$ I(WV) $=$ I(W)。若非相干的 V 也是非幺正的，则 I(VW) $\leq$ I(W)，I(WV) $\leq$ I(W)，且 I(V_2 WV_1) $\leq$ I(W)，其中 V_1 和 V_2 均为非相干的。一种重要的电路形式是夹心式结构，如图10所示，其中受控-U 门

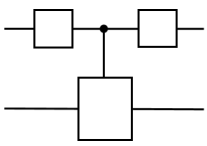

图10. 夹层电路的示意图，它是图5中电路的一种特殊情况。

作为由方程 (34) 定义的多路复用器。控制寄存器和数据寄存器的维数可以不同，d_1 和d_2。CU 的干涉量为平均值 $\frac{1}{d_1}\sum_i I(U_i)$。对于$(V\otimes\mathbb{1})CU(W\otimes\mathbb{1})$，相对熵为平均值

$$\frac{1}{d_1 d_2}\sum_{b,\nu} H(p_{a,\mu}) \tag{48}$$

对于 $p_{a,\mu} = |\sum_i v_{ai} w_{ib} U_{i,\mu\nu}|^2$。对 i 求和对应一种干涉。一个简单的特例是，当CU 为经典时，它就简化为 $I(VW)$。我们还发现了加法关系

$$I(CU(V\otimes\mathbb{1})) = I((V\otimes\mathbb{1})CU) = I(V) + I(CU). \tag{49}$$

例如，$I(CX) = 0, I(CX(U\otimes\mathbb{1})) = I(CU(H\otimes\mathbb{1}))$，$= 1 + I(CU)$。这印证了我们的直觉。许多算法都具有夹心形式的电路，例如确定性量子计算_1和SWAP测试 [127, 128]。我们的研究表明，干涉是它们计算能力的来源。

1. Van den Nest 模型

在电路模型中，一个作用于n 个量子比特的算法从 $|0\rangle^{\otimes n}$ 开始，经过电路U演化，并通过在计算基中测量第一个量子比特获得输出，其中p_0 为成功概率。在此基础上，Van den Nest 模型可转换为一个额外增加一个量子比特的电路，测量前的最终态形式为

$$|\psi\rangle = \sqrt{1-\epsilon}|0\rangle|0\rangle^{\otimes n} + \sqrt{\epsilon}|1\rangle U|0\rangle^{\otimes n}, \tag{50}$$

对于 $\epsilon \sim 1/\mathrm{poly}(n)$，误差参数足够小，从而可以高效地提升成功概率。已有研究表明，纠缠在多项式意义下很小，而该模型是通用的。

我们将证明，该模型中的干涉并不小。令$V_\epsilon = \begin{pmatrix} \sqrt{1-\epsilon} & -\sqrt{\epsilon} \\ \sqrt{\epsilon} & \sqrt{1-\epsilon} \end{pmatrix}$。Van den Nest 电路的干涉为

$$I(CU(V_\epsilon\otimes\mathbb{1})) = I(V_\epsilon) + \frac{1}{2}I(U) \tag{51}$$

对于 $I(V_\epsilon)$ 作为 $Cr(V_\epsilon) = h(\epsilon)$ 或 $C(V_\epsilon) = 2\sqrt{\epsilon(1-\epsilon)}$，它们都接近于零。主要贡献来自

电路本身 $I(U)$，这意味着电路用于解决问题的特征得以保留。

因此，通过从U 到 Van den Nest 电路的映射可以看出，纠缠可能发生显著变化，而干涉则不会。这解释了该模型为何有效。然而，有人认为，纠缠既不是实现量子加速的必要条件，也不是充分条件。我们的资源理论研究否定了这一观点，并指出，必须在通用量子计算模型中定义通用资源。我们证明，纠缠或纠缠比特（EBIT）是 LQTM 的通用资源，而 LQTM 与张量网络态密切相关。正如第 III B 节所分析的，纠缠主要指不同部分之间的量子关联，而相干性和干涉则指振幅的动态变化。换言之，我们可以将纠缠和干涉视为坐标系中的两条正交轴：纠缠描述量子态的静态特征，干涉则描述量子态如何演化。不过，纠缠和相干性也密切相关。一个关键事实是，在 Van den Nest 模型中，纠缠仅以多项式幅度减小，因此可以通过高效方法增强；而指数级减小的纠缠则无法如此增强。这意味着纠缠确实仍然存在，而用干涉来描述其特征更为方便。

2. 幺正算子的线性组合算法

近年来，幺正算子的线性组合算法得到了发展 [52, 53, 98–100]。最初，幺正算子的线性组合算法的灵感来源于多缝干涉实验：一个具有两个自由度的粒子，即路径 $\mathcal{H}_p$和自旋 $\mathcal{H}_s$，会遵循在特殊屏幕上观察到的干涉图样。干涉作用于整个粒子。在幺正算子的线性组合任务中

$$U = \sum_i c_i U_i, \tag{52}$$

其中，c_i 来自路径，而U_i 作用于自旋。其主要组成部分也采用电路的夹心形式，可能还会进行后选择。

需要注意的是，这里的干涉并非针对量子态的振幅，而是针对幺正算子。实际上，我们在 IV A 节论证过，这与情境性有关。形式 $\sum_i c_i U_i$ 是上下文的量子叠加——其中每个上下文都由U_i定义。这或许是理解 LCU 及夹层电路算法的更好视角。事实上，夹层电路并不是整个空间 $\mathcal{H}_p \otimes \mathcal{H}_s$中干涉量最大的电路。整个空间上的哈密顿量演化$e^{itH}$ 或傅里叶变换可以产生更强的干涉，也能展现量子加速，例如特殊图上的量子漫步 [129]。因此，我们发现，尽管情境性和相干性是等价的通用资源，但它们在算法中的用法可能有所不同。这为在不同设置下设计算法提供了灵活性。

3. Shor、*Grover*、等 算法

Shor因式分解算法是量子计算领域最重要的进展之一 [4]。它与 Deustch-Jozsa、Simons 的算法以及 Kitaev 的量子相位估计算法密切相关，并解决隐藏子群 [6]类中的问题。除了一些经典的后处理之外，其主要量子电路采用夹心形式，是定义 2 中的情境电路。因此，该资源可归因于干涉或情境性。事实上，情境性比干涉更加明显：控制寄存器的干涉使情境性成为可能，因而更为关键。模幂运算中的黑箱酉算子表现得像经典算子。量子傅里叶变换应用于控制寄存器，而其中的干涉达到最大。

Deustch-Jozsa 算法中的干涉程度并不显著，因此相较于随机算法，它并没有实现指数级加速。对于 Simons 和 Shor 算法，最终态处于叠加态，且干涉显著。纠缠程度也很高。

从这些算法中可以清楚地看到干涉如何作为振幅的算术运作。“振幅算术”是超越经典算法的额外量子部分。具体而言，振幅可以为负，因此能够产生相消干涉。当基于振幅算术的干涉提升成功概率时，就会出现量子加速。

Grover搜索算法 [130] 展示了另一类量子算法的威力。尽管它采用预言机设置，但更适合将其描述为在某个合适的基下进行的量子比特旋转。旋转角度随迭代次数线性增加。对于量子比特演化 [31, 36]，干涉的程度似乎并不显著。然而，我们必须考虑所采用的基，而它通常并非计算基。由于相干性是相对于计算基定义的，Grover算法中可能存在大量干涉。

Grover 算法可以视为一种量子态制备算法。例如，对于制备满足 $|\psi\rangle$ which satisfies $|\psi\rangle = U|0\rangle$ 的问题，U 的干涉由 $|\psi\rangle$ 的相干性所刻画。对于一般的量子态 $|\psi\rangle$，可以利用不确定性原理导出的量子速度极限，为制备该量子态所需的时间给出下界 [131]。这也为大小为 N 的无结构数据库搜索问题给出了下界 $\Omega(\sqrt{N})$，并证明了 Grover 算法的最优性 [132]。

最近，Grover 算法通过“量子比特化”和量子奇异值变换（QSVT） [133, 134]得到了推广。这里不展开细节：幺正算子U 被视为一组量子比特旋转U_i 的直和，其中每个旋转对应特殊基中的一个奇异值 s_i 。Grover 算法是只有一个奇异值的情形。因此，U 的干涉为平均值 $\sum_i I(U_i)/d$，因而并非广延量。不过，还需考虑该特殊基下的相干性。这使得通过 QSVT 算法实现广延干涉以及量子加速成为可能。

VII. 结论

在这项工作中，我们使用量子资源理论（QRT）研究了通用量子计算模型（UQCM）的若干族。我们证明，QRT 提供了一个严谨的框架，可用于刻画 UQCM，甚至对其进行分类；而 UQCM 则提供了广泛的场景，可供利用资源并探索量子优越性。对于每一族，我们都确定了三种模型。这种划分并非唯一，而且很可能是最小的代际集合。

量子电路模型（QCM）确实简- 单且易于使用。它处于振幅族的最低层级。然而，人们常常发现 QCM 不足以满足更现实或理论性的需求，例如安全性、可编程性、模块化、可控- 性、能效和并行性等。这就要- 求对量子资源和通用量子计算模型进行多样化探索。为进一步研究，我们想指出几点。

我们发现，许多模型都可以通过某种特定形式的电路来识别。在这项工作中，我们分析了横向电路、顺序电路、砖墙电路、夹心电路、情境电路、尾随电路和稳定子电路。这些电路的设计受到量子资源理论相关场景的启发，每种电路都可能适用于满足特定需求。它们也可用于其他目的，例如实现量子加速 [135] 以及对纠缠态进行分类。

在我们研究的九种通用量子计算模型中，情境量子计算（CQC）和后魔态量子计算（PMQC）相对较新。CQC 模型依赖于我们对情境性的定义。然而，情境性的图景错综复杂 [14]。还有一些利用情境性的方案或模型，因此仍有待研究这些情境方案之间的关系，以及能否将它们统一起来，形成一致的情境性概念。PMQC 模型是唯一一个因非局域盒 [54]而略微超出量子理论的模型。一方面，目前尚不清楚是否存在比 PMQC 更弱的模型；另一方面，我们对非定域世界本身的理解 [136] 也尚不完整。

我们对哈密顿量族的研究相对不够深入。我们没有研究资源度量和算法。然而，这意味着该族与其他族同样强大，因此值得研究基于哈密顿量的资源、容错方案等。此外，该族不需要自动化，即一种在中间不进行控制的自由演化 e^{iHt} 。研究也表明，这类自主哈密顿量模型具有强大能力 [66, 117–122],，因此可以进一步研究。

我们提到，除了研究过的三个族之外，还应存在其他族，例如演化族、基于编码的族，甚至是面向通信、计量学等受限用途的非通用族 [137]。具体而言，演化族依赖于量子信道的集合；对这些量子信道进行运算所得的结构称为梳或超信道——

道 [138]。最近提出的量子冯·诺依曼架构 [64] 依赖于此，并能够执行量子超算法，从而实现由一个量子算法自动设计另一个量子算法。我们将把这部分留待未来工作。

致谢

本研究得到中国国家自然科学基金资助，项目编号为 12047503 和 12105343。

[1]C. H. Bennett、G. Brassard、C. Cr´epeau、R. Jozsa、A. Peres 和 W. K. Wootters，“通过双重经典与爱因斯坦-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 1895–1899 页，1993 年 3 月。[2] R. Jozsa 和 N. Linden，“纠缠在量子计算加速中的作用”，*Proc. R. Soc. (London),Ser. A*，第 459 卷，第 2011 页，2003 年。[3] A. M. Steane，“量子计算机只需要一个宇宙”，《现代物理学史与哲学研究》，第 34 卷，第 3 期，第 469–478 页，2003 年。[4]P. W. Shor，“量子计算算法：离散对数与因数分解”，载于第 *35* 届计算机科学基础年度研讨会论文集，第 124–134 页，IEEE，1994 年。[5] A. Kitaev、A. H. Shen 和 M. N. Vyalyi，《经典与量子计算》，数学研究生教材丛书第 47 卷。普罗维登斯：美国数学学会，2002 年。[6] M. A. Nielsen 和 I. L. Chuang，《量子计算与量子信息》。英国剑桥：剑桥大学出版社，2000 年。[7] R. Cleve、A. Ekert、C. Macchiavello 和 M. Mosca，“重新审视量子算法”，*Proc. R. Soc. (London), Ser. A*，第 454 卷，第 339 页，1998 年。[8] R. Horodecki、P. Horodecki、M. Horodecki 和 K. Horodecki，“量子纠缠”，《现代物理评论》，第 81 卷，第 865–942 页，2009 年 6 月。[9] D. Gross、S. T. Flammia 和 J. Eisert，“大多数量子态的纠缠程度过高，无法用作计算资源”，《物理评论快报》，第 102 卷，第 190501 页，2009 年 5 月。[10] M. J. Bremner、C. Mora 和 A. Winter，“ 随机纯态对量子计算有用吗？ ”，《物理评论快报》，第 102 卷，第 190502 页，2009 年 5 月。[11] R. Raussendorf 和 H. J. Briegel，“单向量子计算机”，《物理评论快报》，第 86 卷，第 5188–5191 页，2001 年 5 月。[12]M. Van den Nest，“以少量纠缠实现通用量子计算”，《物理评论快报》，第 110 卷，第 060504 页，2013 年 2 月。[13] N. D. Mermin，“隐变量与 John Bell 的两个定理”，《现代物理评论》，第 65 卷，第 803–815 页，1993 年 7 月。[14] C. Budroni、A. Cabello、O. G¨uhne、M. Kleinmann 和 J. Larsson，“量子情境性”，2021年。arXiv预印本 arXiv:2102.13036。[15]M. Howard、J. Wallman、V. Veitch 和 J. Emerson，“情境性为量子计算提供了‘魔力’”，《自然》，第 510 卷，第 351 页，2014 年。[16] S. Bravyi 和 A. Kitaev，《使用理想 Clifford 门和含噪辅助量子比特进行通用量子计算》，《物理评论*A*》，第 71 卷，页码 022316，2005年2月。[17] H. Pashayan、J. J. Wallman 和 S. D. Bartlett，《使用准概率估算量子电路的测量结果概率》，《物理评论快报》，第 115 卷，页码 070501，2015年8月。[18] R. Raussendorf、D. E. Browne、N. Delfosse、C. Okay 和 J. Bermejo-Vega，《量子比特量子计算中的情境性与 Wigner 函数负性》，《物理评论*A*》，第 95 卷，页码 052334，2017年5月。[19] S. Bravyi、D. Browne、P. Calpin、E. Campbell、D. Gosset 和 M. Howard，《通过低秩稳定子分解模拟量子电路》，《*Quantum*》，第 3 卷，页码 181，2019年9月。[20] J. R. Seddon、B. Regula、H. Pashayan、Y. Ouyang 和 E. T. Campbell，《量化量子加速：通过更紧的魔态单调量改进经典模拟》，《*PRX Quantum*》，第 2 卷，页码 010345，2021年3月。[21]Z.-C. Gu 和 X.-G. Wen，《张量纠缠滤波重整化方法与对称性保护拓扑序》，《物理评论*B*》，第 80 卷，页码 155131，2009年10月。[22] X. Chen、Z.-C. Gu 和 X.-G. Wen，《一维自旋系统中有能隙对称相的分类》，《物理评论*B*》，第 83 卷，页码 035107，2011年1月。[23] N. Schuch、D. P´erez-Garc´ıa 和 I. Cirac，《利用矩阵乘积态和投影纠缠对态对量子相进行分类》，《物理评论*B*》，第 84 卷，页码 165139，2011 年 10 月。[24] A. Miyake，《对称性保护拓扑序边界上的量子计算》，《物理评论快报》，第 105 卷，页码 040501，2010年7月。[25] D. V. Else、I. Schwarz、S. D. Bartlett 和 A. C. Do-herty，《基于测量的量子计算中的对称性保护相》，《物理评论快报》，第 108 卷，页码 240505，2012年6月。[26] D.-S. Wang、D. T. Stephen 和 R. Raussendorf，《具有全局对称性的矩阵乘积态上的量子位量子计算》，《物理评论*A*》，第 95 卷，页码 032312，2017年3月。[27] D. T. Stephen、D.-S. Wang、A. Prakash、T.-C. Wei 和 R. Raussendorf，《对称性保护拓扑相的计算能力》，《物理评论快报》，第 119 卷，页码 010504，2017年7月。[28] R. Raussendorf、C. Okay、D.-S. Wang、D. T. Stephen 和 H. P. Nautrup，《量子物质的计算通用相》，《物理评论快报》，第 122 卷，页码 090501，2019年3月。[29] E. Chitambar 和 G. Gour，《量子资源理论

》，《现代物理评论》，第 91 卷，页码 025001，2019年4月。[30] A. Streltsov、G. Adesso 和 M. B. Plenio，《专题综述：量子相干性作为一种资源》，《现代物理评论》，第 89 卷，页码 041003，2017年10月。[31] D. Braun 和 B. Georgeot，《干涉的定量度量》，《物理评论A》，第 73 卷，页码 022314，2006年2月。[32] J. ˚Aberg，《量化叠加》，2006年。arXiv预印本 arXiv:0612146。[33] K. Niu、K. Xue、Q. Zhao 和 M.-L. Ge，《l1 范数在量子信息理论中的作用及两类杨–巴克斯特方程》，《物理学杂志 A：数学与理论》，第 44 卷，页码 265304，2011年6月。[34] D.-S. Wang，《量子范围中的叠加与纠缠》，2012年。arXiv预印本 arXiv:1101.5002。[35]D.-S. Wang，《量子细粒度熵》，2012年。arXiv预印本 arXiv:1205.1235。[36] D. Stahlke，《量子干涉作为量子加速的资源》，《物理评论A》，第 90 卷，页码 022302，2014年8月。[37] D.-S. Wang，《通用量子计算模型比较研究：迈向物理统一》，《量子工程》，第 2 卷，页码 85，2021年。[38] T. Albash 和 D. A. Lidar，《绝热量子计算》，《现代物理评论》，第 90 卷，页码 015002，2018年1月。[39] M. Van den Nest、W. D¨ur、G. Vidal 和 H. J. Briegel，《基于测量的量子计算中的经典模拟与通用性》，《物理评论A》，第 75 卷，页码 012337，2007年1月。[40] M. Van den Nest、W. D¨ur、A. Miyake 和 H. J. Briegel，《单向量子计算通用性的基础》，《新物理学杂志》，第 9 卷，页码 204，2007年。[41]M. J. Hoban、J. J. Wallman、H. Anwar、N. Usher、R. Raussendorf 和 D. E. Browne，《基于测量的经典计算》，《物理评论快报》，第 112 卷，页码 140505，2014年4月。[42] R. W. Spekkens，《制备、变换与非锐测量的情境性》，《物理评论A》，第 71 卷，页码 052108，2005年5月。[43] R. W. Spekkens，《负性与情境性是非经典性的等价概念》，《物理评论快报》，第 101 卷，页码 020401，2008年7月。[44]S. Abramsky 和 A. Brandenburger，《非定域性与情境性的层论结构》，《新物理学杂志》，第 13 卷，页码 113036，2011年。[45] J. Anders 和 D. E. Browne，《关联的计算能力》，《物理评论快报》，第 102 卷，页码 050502，2009年2月。[46] R. Raussendorf，《基于测量的量子计算中的情境性》，《物理评论A》，第 88 卷，页码 022322，2013年8月。[47] D.-S. Wang，《量子图灵机的局域模型》，《量子信息与计算》，第 20 卷，第 3 期，页码 0213–0229，2020年。[48] I. Affleck、T. Kennedy、E. H. Lieb 和 H. Tasaki，《反铁磁体中价键基态的严格结果》，《物理评论快报》，第 59 卷，页码 799–802，1987年8月。[49] M. Fannes、B. Nachtergaele 和 R. F. Werner，《量子自旋链上的有限关联态》，《数学物理通讯》，第 144 卷，第 3 期，页码 443–490，1992年。

[50] D. Perez-Garcia、F. Verstraete、M. Wolf 和 J. Cirac，“矩阵乘积态表示”，《量子信息与计算》，第7卷，第5期，第401–430页，2007年。[51] A. Broadbent，“Popescu-Rohrlich 关联意味着高效的瞬时非定域量子计算”，《物理评论A》，第94卷，文章号022318，2016年8月。[52] A. M. Childs 和 N. Wiebe，“利用酉操作的线性组合进行哈密顿量模拟”，《量子信息与计算》，第12卷，第901页，2012年。[53] G. L. Long，“对偶量子计算与对偶量子信息处理”，《国际理论物理学杂志》，第50卷，第1305页，2011年。[54] S. Popescu 和 D. Rohrlich，“作为公理的量子非定域性”，《基础物理学》，第24卷，第379页，1994年。[55] A. Broadbent、J. Fitzsimons 和 E. Kashefi，“通用盲量子计算”，载于《第50届计算机科学基础年会论文集》（IEEE计算机学会，加利福尼亚州洛斯阿拉米托斯，2009年），第517–527页，2009年。[56] T. S. Cubitt、A. Montanaro 和 S. Piddock，“通用量子哈密顿量”，《美国国家科学院院刊》，第115卷，第38期，第9497–9502页，2018年。[57]T. Kohler、S. Piddock、J. Bausch 和 T. Cubitt，“一维平移不变通用量子哈密顿量”，《亨利·庞加莱年鉴》，第23卷，第223–254页，2021年。[58] T. Kohler、S. Piddock、J. Bausch 和 T. Cubitt，“量子哈密顿量通用性的一般条件”，《PRX Quantum》，第3卷，文章号010308，2022年1月。[59] L. Zhou 和 D. Aharonov，“强通用哈密顿量模拟器”，2021年。arXiv：quant-ph/2102.02991。[60]P. Arrighi，“量子元胞自动机概述”，《自然计算》，第18卷，第885–899页，2019年。[61] T. Farrelly，“量子元胞自动机综述”，《Quantum》，第4卷，文章号368，2020年11月。[62] K. Wiesner，“量子元胞自动机”，2008年。arXiv预印本 arXiv:0808.0679。[63] G. Chiribella、G. M. D’Ariano 和 P. Perinotti，“变换量子操作：量子超映射”，《欧洲物理快报》，第83卷，文章号30004，2008年。[64] D.-S. Wang，“量子冯·诺依曼架构原型”，《理论物理通讯》，第74卷，文章号095103，2022年。[65] C. Nayak、S. H. Simon、A. Stern、M. Freedman 和 S. D. Sarma，“非阿贝尔任意子与拓扑量子计算”，《现代物理评论》，第80卷，第3期，第1083页，2008年。[66]A. M. Childs、D. Gosset 和 Z. Webb，“通过多粒子量子游走实现通用计算”，《科学》，第339卷，第791页，2013年。[67] K. C. Tan、V. Narasimhachar 和 B. Regula，“费 Fisher 信息普遍地识别量子资源”，《物理评论快报》，第127卷，文章号200402，2021年11月。[68] F. G. S. L. Brand˜ao 和 G. Gour，“量子资源理论的可逆框架”，《物理评论快报》，第115卷，文章号070503，2015年8月。[69] W. K. Wootters，“有限态量子力学的维格纳函数表述”，《物理年鉴》，第176卷，第1页，1987年。[70]D. Gross，“有限维量子系统的Hudson定理

量子系统理论杂志》，" 第 47 卷，第 122107 页，2006 年。[71] V. Veitch、C. Ferrie、D. Gross 和 J. Emerson，“负准概率作为量子计算的资源”，《新物理学杂志》，第 14 卷，第 113011 页，2012 年。[72] R. P. Feynman，“用计算机模拟物理”，《国际理论物理学杂志》，第 21 卷，第 6/7 期，第 467–488 页，1982 年。[73]S. Lloyd，“通用量子模拟器”，《科学》，第 273 卷，第 1073–1078 页，1996 年 8 月。[74] P. Wocjan、M. Roetteler、D. Janzing 和 T. Beth，“使用有限组控制操作对哈密顿量进行通用模拟”，《量子信息与计算》，第 2 卷，第 2 期，第 133 页，2002 年。[75] J. L. Dodd、M. A. Nielsen、M. J. Bremner 和 R. T. Thew，“利用任意纠缠哈密顿量和局域酉变换实现通用量子计算与模拟”，《物理评论*A*》，第 65 卷，第 040301 页，2002 年 4 月。[76] A. Winter 和 D. Yang，“相干性的操作性资源理论”，《物理评论快报》，第 116 卷，第 120404 页，2016 年 3 月。[77] A. Jamiołkowski，“保持算子迹和半正定性的线性变换”，*Rep. Math. Phys.*，第 3 卷，第 275 页，1972 年。[78] M.-D. Choi，“复矩阵上的正线性映射”，*Linear Algebra Appl.*，第 290 卷，第 10 期，第 285–290 页，1975 年。[79] E. Bernstein 和 U. Vazirani，“量子复杂性理论”，*SIAMJournalonComputing*，第 26 卷，第 5 期，第 1411–1473 页，1997 年。[80] A. C.-C. Yao，“量子电路复杂性”，载于计算机科学基础，*1993* 年。第 *34* 届年度研讨会论文集，第 352–361 页，IEEE，1993 年。[81] A. Molina 和 J. Watrous，“重新审视用量子电路模拟量子图灵机”，*Proc. Royal Soc. A*，第 475 卷，第 2226 期，第 20180767 页，2019 年。[82]U. Schollw¨ock，“矩阵乘积态时代的密度矩阵重整化群”，《物理学年鉴》，第 326 卷，第 1 期，第 96–192 页，2011 年。[83]A. Streltsov、U. Singh、H. S. Dhar、M. N. Bera 和 G. Adesso，“利用纠缠测量量子相干性”，《物理评论快报》，第 115 卷，第 020403 页，2015 年 7 月。[84] H. Zhu、Z. Ma、Z. Cao、S.-M. Fei 和 V. Vedral，“相干性与纠缠度量之间的操作性一一映射”，《物理评论*A*》，第 96 卷，第 032316 页，2017 年 9 月。[85] F. Caruso、V. Giovannetti、C. Lupo 和 S. Mancini，“量子信道与记忆效应”，《现代物理评论》，第 86 卷，第 1203–1259 页，2014 年 12 月。[86] A. M. Childs、D. W. Leung 和 M. A. Nielsen，“基于测量的量子计算方案的统一推导”，《物理评论*A*》，第 71 卷，第 032318 页，2005 年 3 月。[87] D. Gross 和 J. Eisert，“基于测量的量子计算新方案”，《物理评论快报》，第 98 卷，第 220503 页，2007 年 5 月。[88]T.-C. Wei 、 I. Affleck 和 R. Raussendorf，“ 蜂窝晶格上的 Affleck-Kennedy-Lieb-Tasaki 态是一种通用量子计算资源”，《物理评论快报》，第 106 卷，第 070501 页，2011 年 2 月。[89] N. Schuch、J. I. Cirac 和 D. Perez-Garcia，“投影纠缠对态作为基态：简并与拓扑”，《物理年鉴》，第325卷，第2153页，2010年。[90] A. Miyake，“二维价键固体相的量子计算能力”，《物理学年鉴》，第326卷，第7期，第1656–1671页，2011年。2011年7月特刊。[91] J. Miller和A. Miyake，“二维测量式量子计算中普适纠缠的层级”，npj《量子信息》，第2卷，第16036页，2016年。[92] M. Gachechiladze、O. G¨uhne和A. Miyake，“利用超图态改变测量式量子计算的电路深度复杂度”，《物理评论A》，第99卷，第052304页，2019年5月。[93] I. Marvian，“对称性保护拓扑纠缠”，《物理评论B》，第95卷，第045111页，2017年1月。[94] M. Araujo、A. Feix、F. Costa和C. Brukner，“量子电路无法控制未知操作”，《新物理学杂志》，第16卷，第093026页，2014年。[95] J. Thompson、K. Modi、V. Vedral和M. Gu，“量子即插即用：量子领域中的模块化计算”，《新物理学杂志》，第20卷，第013004页，2018年。[96] Z. Gavorova、M. Seidel和Y. Touati，“实现受控未知酉算符的拓扑障碍”，2020年。arXiv预印本 arXiv:2011.10031。[97] A. Vanrietvelde和G. Chiribella，“利用保持扇区的信道实现对量子过程的普适控制”，《量子信息与计算》，第21卷，第15–16期，第1320–1352页，2021年。[98] G. L. Long，“一般量子干涉原理与对偶计算机”，《理论物理通讯》，第45卷，第825–844页，2006年。[99] D. W. Berry、A. M. Childs、R. Cleve、R. Kothari和R. D. Somma，“利用截断泰勒级数模拟哈密顿量动力学”，《物理评论快报》，第114卷，第090502页，2015年3月。[100] S. Wei和G. L. Long，“对偶量子计算机与高效量子模拟”，《量子信息处理》，第15卷，第1189–1212页，2016年。[101]V. Veitch、S. A. H. Mousavian、D. Gottesman和J. Emerson，“稳定子量子计算的资源理论”，《新物理学杂志》，第16卷，第013009页，2014年1月。[102] D. Gottesman，“容错量子计算理论”，《物理评论A》，第57卷，第127–137页，1998年1月。[103] C. Mukhopadhyay、S. Sazim和A. K. Pati，“相干性使量子系统变得‘神奇’”，《物理学杂志A：数学与理论》，第51卷，第414006页，2018年。[104] A. Gonzales和E. Chitambar，“瞬时非局域量子计算的界”，《IEEE信息论汇刊》，第66卷，第2951页，2020年。[105] R. Colbeck，“安全双方经典计算的不可能性”，《物理评论A》，第76卷，第062308页，2007年12月。[106] A. Ambainis、M. Mosca、A. Tapp和R. d. Wolf，“私有量子信道”，载于FOCS 2000，第547–553页，IEEE，2000年。[107] J. F. Clauser、M. A. Horne、A. Shimony和R. A. Holt，“检验局域隐变量理论的拟议实验”，《物理评论快报》，第23卷，第880–884页，1969年10月。[108] F. Buscemi，“所有纠缠量子态都是非局域的”，《物理评论快报》，第108卷，第200401页，2012年5月。[109]D. Gottesman和I. L. Chuang，“利用量子隐形传态和单量子比特操作展示通用量子计算的可行性”，《自然》，

第402卷，第6760期，第390–393页，1999年。[110] G. Brassard、H. Buhrman、N. Linden、A. A. M´ethot、A. Tapp和F. Unger，“在通信复杂性并非平凡的任何世界中，非定域性的限制”，《物理评论快报》，第96卷，第250401页，2006年6月。[111] L. Vaidman，“非定域变量的瞬时测量”，《物理评论快报》，第90卷，第010402页，2003年1月。[112] S. Bravyi和M. Hastings，“量子伊辛模型的复杂性”，《数学物理通讯》，第349卷，第1–45页，2017年。[113]C. T.和A. Montanaro，“局域哈密顿量问题的复杂性分类”，《*SIAM*计算杂志》，第45卷（第2期），第268–316页，2016年。[114]G. De las Cuevas和T. S. Cubitt，“简单的普适模型能够涵盖所有经典自旋物理”，《科学》，第351卷，第1180–1183页，2016年。[115] D. W. Berry、G. Ahokas、R. Cleve和B. C. Sanders，“用于模拟稀疏哈密顿量的高效量子算法”，《数学物理通讯》，第270卷，第2期，第359–371页，2007年。[116] J. I. Cirac和P. Zoller，“量子模拟的目标与机遇”，《自然物理学》，第8卷，第4期，第264–266页，2012年。[117]D. Janzing，“在具有最近邻相互作用的二维晶格上运动的自旋1/2粒子能够实现自主量子计算机”，《物理评论*A*》，第75卷，第012307页，2007年1月。[118] D. Nagaj，“利用铁路道岔局域哈密顿量实现快速通用量子计算”，《数学物理杂志》，第51卷，第062201页，2010年。[119] D. Nagaj，“通用二体哈密顿量量子计算”，《物理评论*A*》，第85卷，第032330页，2012年3月。[120] N. Bao、P. Hayden、G. Salton和N. Thomas，“通过费米–哈伯德模型中的散射实现通用量子计算”，《新物理学杂志》，第17卷，第093028页，2015年9月。[121] S. Lloyd和B. Terhal，“利用简单的双量子比特相互作用在二维晶格上进行绝热计算与哈密顿量计算”，《新物理学杂志》，第18卷，第023042页，2016年2月。[122] K. F. Thompson、C. Gokler、S. Lloyd和P. W. Shor，“利用自旋链实现时间无关的通用计算：量子弹珠机”，《新物理学杂志》，第18卷，第073044页，2016年7月。[123] T. Toffoli和N. Margolus，《元胞自动机机器：用于建模的新环境》。麻省理工学院出版社，1987年。[124] D. Nagaj和P. Wocjan，“一维哈密顿量量子元胞自动机”，《物理评论*A*》，第78卷，第032311页，2008年9月。[125]D. J. Shepherd、T. Franz 和 R. F. Werner，《通用可编程量子元胞自动机》，《物理评论快报》，第97卷，第020502页，2006年7月。[126] K. G. H. Vollbrecht 和 J. I. Cirac，《量子模拟器、连续时间自动机与平移不变系统》，《物理评论快报》，第100卷，第010501页，2008年1月。[127] E. Knill 和 R. Laflamme，《一比特量子信息的力量》，《物理评论快报》，第81卷，第5672–5675页，1998年12月。[128]H. Buhrman、R. Cleve、J. Watrous 和 R. de Wolf，《量子指纹识别》，《物理评论快报》，第87卷，第167902页，2001年9月。[129] A. M. Childs、R. Cleve、E. Deotto、E. Farhi、S. Gutmann 和 D. Spielman，《通过量子漫步实现指数级算法加速》，载于第*35*届*ACM*计算理论研讨会论文集，第35卷，（纽约），第59–68页，圣迭戈，ACM，纽约，2003年。[130] L. K. Grover，《用于数据库搜索的快速量子力学算法》，载于第二十八届*ACM*计算理论研讨会年度论文集，1996年。[131] L. B. Levitin 和 T. Toffoli，《量子动力学速率的基本极限：统一界是紧的》，《物理评论快报》，第103卷，第160502页，2009年10月。[132] E. Farhi 和 S. Gutmann，《数字量子计算的模拟类比》，《物理评论*A*》，第57卷，第2403–2406页，1998年4月。[133] A. Gilyen、Y. Su、G. H. Low 和 N. Wiebe，《量子奇异值变换及其扩展：量子矩阵运算的指数级改进》，载于第*51*届*ACM SIGACT*理论计算研讨会论文集，2019年。[134]J. M. Martyn、Z. M. Rossi、A. K. Tan 和 I. L. Chuang，《量子算法的大统一》，《*PRX Quantum*》，第2卷，第040203页，2021年12月。[135] S. Bravyi、D. Gosset 和 R. Konig，《浅层电路的量子优势》，《科学》，第362卷，第308–311页，2018年。[136] F. Dupuis、N. Gisin、A. Hassidim、A. A. M´ethot 和 H. Pilpel，《不存在通用的非定域盒》，《数学物理杂志》，第48卷，第082107页，2007年。[137] H. Kristj´ansson、G. Chiribella、S. Salek、D. Ebler 和 M. Wilson，《通信资源理论》，《新物理学杂志》，第22卷，第073014页，2020年。[138] G. Chiribella、G. M. D’Ariano 和 P. Perinotti，《量子信道判别中的记忆效应》，《物理评论快报》，第101卷，第180501页，2008年10月。