

量子纠错码进展简介

高攀¹ 张江¹ 龙桂鲁^{1,2}

(1. 北京量子信息科学研究院 100193; 2. 清华大学 100084)

量子计算机作为量子力学发展的重大成果之一,已然成为全球各强国竞相争夺的战略高地。然而,在量子器件执行信息处理任务的过程中,不可避免地会受到噪声和退相干的干扰。若不有效处理,将导致错误结果,使大规模量子计算的实现面临严峻挑战。发展量子纠错,实现容错量子计算是当前量子计算机研究的最重要的任务之一。

当前量子错误处理技术主要涵盖错误抑制、错误缓解和量子纠错三大类别^[1]。错误抑制通过精心设计和优化量子比特的操控技术,有效降低原始错误率,然而该方法通常仅适用于低频非马尔科夫噪声,且容易导致错误随时间累积,从而使计算结果偏离真实值。错误缓解作为近期量子计算领域的一种过渡性方案,在一定程度上能够减轻错误对统计测量结果的影响,但其后处理过程较为复杂,扩展性欠佳。相较之下,量子纠错通过将逻辑量子信息编码至多个物理量子比特之中,提供了一种从根本上解决噪声问题的技术途径。尤其是表面码(Surface code)、颜色码(Color code)等拓扑纠错方案,展现出对各类噪声的极高容忍度^[2]。

量子纠错为容错量子计算的实现提供了至关重要的基础架构。通过将单个逻辑量子比特巧妙地编码至多个物理量子比特中,量子纠错不仅能主动检测并纠正错误,还能在逻辑操作过程中有效控制错误的传播。当物理量子比特的错误率降至特定阈值以下时,量子纠错可通过级联机制无限抑制错误的发生。

量子纠错是诸多量子应用算法走向现实的理论基石,如Shor算法等密码分析算法、量子化学模拟算法等。此外,量子纠错不仅适用于基于量子比

特的量子计算系统,在基于连续变量的高斯量子计算中,通过GKP编码同样能实现错误校正和通用量子计算^[3]。这些跨领域应用展示了量子纠错技术在未来量子技术生态系统中的核心价值。

近年来(约2022~2025年)量子纠错研究在理论、实验与工程实现层面均取得了一系列阶段性突破。一方面,随着超导量子器件实验技术在量子比特寿命、扩展性、操控精度等方面的不断提高,基于量子拓扑编码的表面码、颜色码等方案得以在多个平台实现了码距从3到5甚至7的实验演示,证实了逻辑错误率随码距增加而降低,即量子纠错“越纠越对”的理论基础。这推动了量子计算研究跨上了容错量子计算研究的新台阶。另一方面,从面向量子存储器的静态纠错解码转至面向量子计算机的动态实时解码成为当下量子纠错研究的重要趋势,发展“纠得准、解得快”的实时编解码方案成为量子计算机通向实用化面临的紧迫现实问题。

在这一背景下,有必要在统一视角下系统总结量子纠错码,特别是表面码与颜色码,在编码结构、容错逻辑操作、实验实现及解码算法等方面的最新进展。本文正是基于这一动机,力图整合近年来分散于不同研究方向的成果,为理解量子纠错从理论构想走向可扩展实现的整体脉络提供一份阶段性综述。

一、量子错误理论与处理方法

1.1 量子错误的物理起源与数学模型

量子信息处理过程中的错误主要来源于环境退相干、量子门操作错误和制备与测量误差三大

类。退相干过程源于量子系统与环境间不可避免的相互作用,导致量子信息的丢失,具体包括能量弛豫和退相位两类主要过程^[4]。在能量弛豫过程中量子系统自发地从高能态跃迁到低能态导致能级占据情况的改变;在退相位过程中量子系统能级间的相对相位发生随机漂移导致量子干涉性受到破坏。量子门操作错误则来自操控过程中不精确的控制脉冲,包括转角偏差、频率偏差及比特间串扰效应等。制备与测量误差表现为量子态制备过程中0/1状态的翻转及读取误判概率。这些噪声过程可建模为量子通道:

$$N(\rho) = \sum_k E_k \rho E_k^\dagger, \quad \sum_k E_k^\dagger E_k = I \quad (1)$$

1.2 量子错误抑制与错误缓解

错误抑制技术如动力学解耦和脉冲整形等虽能降低等效噪声强度,但存在根本性局限,如对高频噪声效果下降等,且无法应对算法执行过程中错误的累积效应。硬件层面的改进(如提高超导量子比特相干时间)虽能延缓错误积累,但无法改变错误率随操作次数增加而放大的本质特征。

作为容错量子计算实现前的过渡方案,错误缓解技术展现出一定实用价值。零噪声外推法通过不同噪声强度下的测量结果外推至零噪声极限,而概率误差消除则利用噪声特征的先验知识进行后处理校正^[5]。然而理论分析表明,随着问题规模的增大,误差缓解所需的线路采样测量次数将急剧增加(超过多项式形式),严重制约其可扩展性^[6]。

1.3 量子纠错编码

量子纠错码将一个逻辑量子比特编码到多个物理量子比特的纠缠态中,通过冗余信息检测并纠正错误,同时避免直接测量破坏量子叠加态。早期方案如Shor码(9比特)和Steane码(7比特)仅能纠正单比特错误,且缺乏扩展性。

随着理论发展,拓扑码成为主流方案,其中表面码因高容错阈值和局部连接特性脱颖而出。表面码通过周期性测量“稳定子”(如X/Z泡利算符)提

取错误信息,逻辑错误率随码距(d)增大呈指数下降,但需消耗约 d^2 个物理比特。

颜色码作为另一类拓扑码,虽需更复杂的稳定子测量,但支持高效的横向逻辑门操作(如所有Clifford门),且比特利用率更高。

二、稳定子码

稳定子码是经典线性码在量子纠错编码领域的自然推广^[2],其通过在Pauli群中定义具有高度对称性的编码子空间来提升逻辑量子比特的噪声鲁棒性。

稳定子码理论中的几个基本概念:

a) Pauli群: n -比特Pauli群是由单比特Pauli算符张量积而来的离散群 $P_n = (\pm 1, \pm i) \{ I, X, Y, Z \}^{\otimes n}$ 。

b) 稳定子群: 稳定子群 S 是 n 量子比特Pauli群 P_n 的不含 $-I$ 的阿贝尔子群,群 S 作用不变的子空间 $|\psi\rangle = s|\psi\rangle, \forall s \in S$ 即该稳定子码的编码子空间,群元 s 称为稳定子。

c) 中心子: 稳定子群 S 在Pauli群 P_n 中的中心子定义为 P_n 中与 S 所有群元均对易的元素的集合,即 $C_p(S) = \{ g \in P, gs = sg, \forall s \in S \}$ 。

d) 正规子: 稳定子群 S 在Pauli群 P_n 中的正规子定义为 P_n 中保持 S 不变的所有的元素的集合,即 $N_p(S) = \{ g \in P, gSg^\dagger = S \}$ 。由于Pauli群中所有元素要么与稳定子 s 对易,要么反对易,因此稳定子群 S 在Pauli群 P_n 中的中心子与正规子实际上是等价的,即 $C_p(S) = N_p(S)$ 。但在更一般意义下,如稳定子群在Clifford群下的中心子与正规子,两者截然不同。

e) 逻辑Pauli群: 定义为正规子与稳定子群的商群 $L = N_p(S)/S$,其生成元即逻辑量子门。群 L 中非平庸元素的最小Hamming权重衡量了稳定子码 S 的抗噪声能力,称为编码距离 d 。

以编码1个逻辑量子比特的稳定子码为例,图1示意了Pauli群、稳定子群、正规子与逻辑门操作间的集合关系。

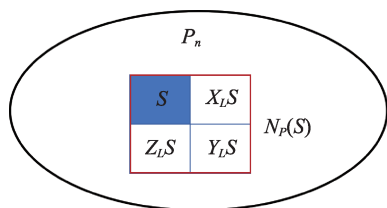


图1 多比特 Pauli 群、稳定子群、正规子与逻辑量子门操作间的集合关系示意。其中 P_n 表示 n 量子比特 Pauli 群, S 表示某特定的稳定子群, $N_f(S)$ 表示稳定子群在 Pauli 群中的正规子

在噪声环境下的信息处理过程中,通过测量稳定子群生成元 s ,并结合合适的解码算法即可推断出物理比特上发生的错误类型,从而实现错误纠正。我们熟知的可抵抗单比特翻转噪声的3比特重复码和9比特 Shor 码都属于稳定子码。

在 n 个物理比特上编码了 k 个逻辑量子比特,可以抵抗 Hamming 权重小于 d 的任意量子噪声的编码方案记为 $[n, k, d]$ 编码。显然在理论上 k/n 越大、 d 越大,编码效率越高。若考虑到在真实物理器件上实现的技术难度,那么稳定子生成元 s 越局域、编码方案越好,逻辑门操作实现越简单(越具有“横向”特性)、编码方案越好。这里,逻辑门实现的“横向”性是指在物理量子比特上并行地施加一些局域地、甚至是单比特上的量子操作即可等价地实现逻辑量子比特上的逻辑量子门操作。“横向”不仅意味着物理实现的简单,也保证了物理比特上的错误不会向远处扩散,从而保证纠错的可行性。

CSS 码是一种特殊的稳定子码,其稳定子分为仅含 Pauli- X 的 S_x 和仅含 Pauli- Z 的 S_z 两个独立组。与经典线性码类似,这两组稳定子分别定义了两个不同的校验矩阵 H_x 和 H_z 。由于稳定子群 S 的阿贝尔特性总有 $H_x H_z^T = 0$ 。

拓扑码是一类特殊的具有 CSS 结构的稳定子码,其稳定子具有空间上的局域性质,逻辑编码空间的维度仅与物理比特所处空间的整体拓扑性质有关。二维的表面码和颜色码是两种最主要的拓扑编码方案。特别地,在颜色码方案中,校验矩阵 $H_x = H_z$ 。我们熟知的具有 $[7, 1, 3]$ 结构的 Steane 码即为结构最简单的颜色码。

三、表面码理论与实验进展

3.1 从 Toric code 到旋转 planar code 的理论演化

1997 年 Kitaev 在二维轮胎面上定义了一种称为 Toric code 的具有拓扑性质的纠错码方案^[7]。在如图 2 具有周期性结构的二维方格子中,记面元为 f ,十字格点为 v ,边段为 e 。在每段边 e 上均放置了一个物理量子比特,定义稳定子

$$Z_v = \prod_{e \in \partial v} Z_e, \tag{2.a}$$

$$X_f = \prod_{e \in \partial f} X_e. \tag{2.b}$$

由于 $\prod_v Z_v = \prod_f X_f = I$, 稳定子群独立生成元的数量总是比物理比特数量少两个。即在 $d \times d$ 的周期边界方格子上定义了 $[2d^2, 2, d]$ 码,其中原格子和对偶格子(将原格子的所有边段旋转 90 度得到的格子)上具有非平庸拓扑的弦算符定义了相应的逻辑量子门。

事实上方格子系统中物理比特数目和独立稳定子生成元数量的关系(即编码逻辑量子比特数 k)是由系统所处的空间拓扑性质决定的,有 $k = |e| - (|v| + |f| - 2) = 2 - \chi = 2g$ 。其中 $| \cdot |$ 表示对应元素的数量, χ 为系统所处拓扑空间的欧拉示性数, g 为拓扑空间的亏格数。

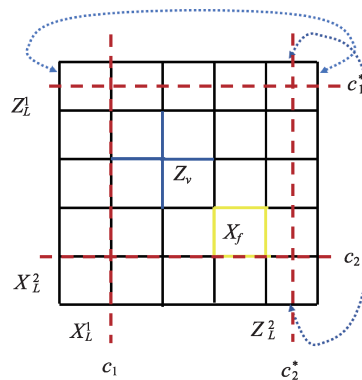


图2 5×5 Toric code 示意。其中 X_f 和 Z_v 分别为定义在面元和十字格点上的局域稳定子, c_1 和 c_2 为原格子上的两条不等价的拓扑非平庸的弦, c_1^* 和 c_2^* 为对偶格子上的两条不等价的拓扑非平庸的弦。在这四条弦上可以分别定义分属于两个逻辑量子比特的 X 和 Z 型逻辑 Pauli 门

考虑到周期性边界条件在物理系统中的实现难度,通过“挖洞”的形式在二维拓扑平庸的球面结构中引入不平庸的拓扑结构,可以给出一种更具有实验友好性的 planar code。在 planar code 中,我们在球面上的方格子中移除 2 个 X_v 和 1 个 Z_v , 可以将其等价地铺平成一个如图 3 具有开边界的二维平面。图 3 的 7×7 方格子上定义的 planar code 具有上下和左右两组不同性质的开放边界,其中上下被形象地称为“光滑”边界,左右则称为“粗糙”边界。连接两个不同光滑边界的对偶 Pauli-Z 弦算符 $\prod_{e \in c_i} Z_e$ 扮演了逻辑 Z 门的角色,连接两个粗糙边界的原格子上的 Pauli-X 弦算符 $\prod_{e \in c_i} X_e$ 则扮演了逻辑 X 门的角色。

可以证明在具有开边界的二维 $m \times n$ 格子中,物理比特数量为 $2mn - m - n + 1$, 而独立的稳定子数量为 $2mn - m - n$, 即该结构总是编码了 1 个逻辑量子比特,与 m 和 n 的具体数值无关。显然 planar code 的编码密度相较于 Toric code 几乎小了一半。

为了提高表面码的编码密度, Bombin 和 Martin-Delgado 在 2007 年给出了一种“旋转” planar code^[8]。如图 3 中虚线框中的结构即定义了一个同样具有距离 $d = 7$ 的 $[[d^2, 1, d]]$ 纠错编码方案,其中连

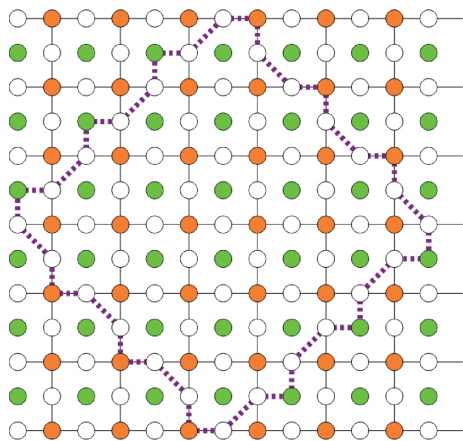


图3 planar code 和旋转 planar code(摘自参考文献[4])。其中整个格点系统即为原始的 planar code。上下两个边界构成光滑边界,左右两个边界构成粗糙边界。白色圆圈表示物理比特,绿色圆圈表示 X_v 相应的测量比特,橙色圆圈表示 Z_v 相应的测量比特。虚线包括的范围即与整个 planar code 具有相同码距的旋转 planar code

接上下两个顶点处物理比特的对偶 Pauli-Z 弦算符定义了该编码下的逻辑 Z 门,连接左右两个顶点处物理比特的原始 Pauli-X 弦算符定义了相应的逻辑 X 门。旋转 planar code 具有和 Toric code 一样的编码密度。

值得一提的是,通过在拓扑平庸的二维球面上“挖出”更多的孔洞,即增大拓扑空间的亏格数,可以在相同数量的物理比特中编码更多的逻辑量子比特(代价是码距的减小)。同样的,我们可以将这种带有许多孔洞的球面等价地平铺成一个具有多个开放边界的二维平面结构。如图 4 是一个编码了 3 个逻辑比特的具有开放边界的二维平面,其中 v_i 是粗糙边界, v_i^* 是光滑边界。连接粗糙边界 v_i 和 v_{i+1} 的直接弦 c_i 上的 Pauli-X 弦算符构成了第 i 个逻辑量子比特上的逻辑 X_i 门,仅与 c_i 有奇数次相交而与其他 $c_{j \neq i}$ 有偶数次相交的对偶弦 c_i^* 上的 Pauli-Z 弦算符构成了第 i 个逻辑量子比特上的逻辑 Z_i 门。

3.2 表面码的实验研究进展

由于表面码具有较高的噪声阈值、高度局域化的稳定子、易于实现的逻辑门(X、Z 和 CNOT)等优势,近年来国际上多个团队相继在不同的物理体系中开展了表面码的实验实现研究。

早在 2017 年, Wootton 等人即在理论上提出了一个最小化的表面码实验方案^[10], 利用 17 个物理量

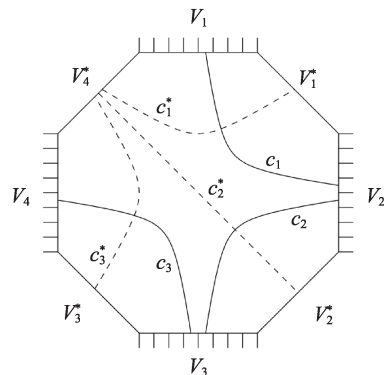


图4 具有多个开放边界的二维平面格子可以编码更多的逻辑量子比特(摘自参考文献[9])。其中 v_i 是粗糙边界, v_i^* 是光滑边界。 c_1, c_2, c_3 为原格子上的弦,可在其上定义相应的逻辑 X 门。 c_1^*, c_2^*, c_3^* 为对偶格子上的弦,可在其上定义相应的逻辑 Z 门

子比特(其中9个为物理比特,8个为辅助比特)构建码距为3的编码,以实现物理比特上 X 和 Z 型错误的完整检测与纠正,这一工作为表面码实验奠定了理论基石。

在经历数年的硬件与算法准备后,2022年中科大Zhao等人在“祖冲之2.1”超导量子处理器上实现了真正可运行的表面码纠错实验,该实验使用与最小方案一致的17比特码距3编码^[11]。他们通过优化的电路设计与动态耦合技术有效抑制了频率拥挤问题,并在多轮纠错周期中观测到逻辑错误率降低了约26%,逻辑比特寿命得到有效延长。这一实验展示了表面码的重复纠错能力,意味着表面码不再停留于理论框架,而真正进入了实验验证阶段。

在随后的2023年,Google Quantum AI团队实现了更大规模的实验,在72比特超导处理器上演示了码距为5的表面码编码^[12]。与此前的码距3相比,更大的编码规模使逻辑错误率进一步下降,从而以实验方式确认了增大码距能够抑制逻辑错误这一关键理论预言。同时,该研究揭示了空间相关错误的重要性,包括泄漏与串扰等非理想效应,这些误差超出了传统Pauli模型的描述范围。研究人员还发现高能宇宙射线事件能够导致罕见但显著的逻辑错误,这提示未来系统必须考虑环境因素的屏蔽与缓解。这一阶段的工作标志着表面码研究从“能否实现”转向“如何在真实噪声下扩展规模”。

2024年至2025年,Google团队进一步在Willow架构的105比特超导处理器上实现了码距7的表面码^[13]。在这一实验中,逻辑错误率随着码距增大实现了指数级抑制,表现出错误抑制因子大于2的特征,符合理论上关于阈值条件的预测。逻辑比特寿命已超过最佳物理比特寿命的两倍,这标志着量子比特在逻辑层面超越了物理层面的性能瓶颈。同时,研究团队通过低延迟硬件与Sparse Blossom解码算法的结合,对码距为5的方案实现了百万次循环水平的实时解码操作,并利用DQLR技术有效抑制了超导体特有的量子比特泄漏。这些进展清晰地表明,表面码在超导平台上已经跨越了“阈

值”这一关键门槛,向真正可扩展的容错计算迈出坚实一步。

总体而言,从2017年的17比特方案,到2022年的首例可重复纠错实现,再到2023年的规模扩展以及2025年的实时解码与阈值突破,表面码实验已展现出逻辑错误率随码距扩大而呈指数级下降的趋势。这一进程清晰地描绘了容错量子计算的技术路线:在硬件层面持续提升比特保真度与相干性,在系统层面实现更大规模与实时控制,并逐步跨平台探索不同物理体系的实现可能。未来,随着误差来源的进一步识别与抑制,以及更高阈值码种与优化解码方案的结合,表面码有望成为实现大规模容错量子计算的核心支撑。

四、颜色码及其优势

4.1 颜色码基本理论

量子颜色码是继表面码外另一类具有拓扑性质的CSS纠错码,由Bombín与Martín-Delgado于2007年提出,其独特的三色(一般记为红、绿、蓝)结构和高编码率使其成为实现容错量子计算的重要候选方案之一^[14]。相较于表面码,颜色码在逻辑门实现、资源开销和结构对称性方面展现出显著优势。特别地,在二维表面码中可以“横向”地实现 X 、 Z 和CNOT门,而在二维颜色码中除此之外还可以“横向”地实现相位门 S 和Hadamard门 H (但不能“横向”地实现 T 门),在三维颜色码上则可以“横向”地实现 T 门(但仍然不能“横向”地实现普适量子门)。Eastin-Knill定理告诉我们,天下没有免费的午餐,即不存在常数深度下可以“横向”实现普适量子门集的纠错编码方案^[15]。

不同于表面码定义在方格子系统上,颜色码定义在可以进行三着色的格点系统上,即:(i)每个格点连接三条边;(ii)对每个面着色后,相同颜色的面不相邻。物理量子比特位于格子的顶点上,每个面上都同时定义了 X 和 Z 型稳定子,即

$$X_f = \prod_{v \in f} X_v, Z_f = \prod_{v \in f} Z_v. \quad (3)$$

显然在封闭的几何体中,当把所有相同颜色面上的稳定子乘起来时,他们总满足

$$\prod_{f \in r} X_f = \prod_{f \in g} X_f = \prod_{f \in b} X_f, \quad (4.a)$$

$$\prod_{f \in r} Z_f = \prod_{f \in g} Z_f = \prod_{f \in b} Z_f, \quad (4.b)$$

其中 r, g, b 分别表示红色、绿色和蓝色的面元。式(4)意味着独立稳定子的数量为 $2(|r| + |g| + |b|) - 4$ 个。

颜色码理论中的几个重要概念:

a) 收缩格子(Shrunk lattice): 红、绿、蓝每种颜色都可以构造一个相应颜色的收缩格子。以红色面为例,假设每个红色面都收缩为一个点,那么连接这些红色点的边段(同样着色为红色)即构成一个红色收缩格子。收缩格子上每个边段上则等价地存在着两个物理比特。

在收缩格子下,我们可以很清晰地看到颜色码的拓扑性质。记原格子的点、边和面的数量分别为 $|v|, |e|$ 和 $|f| = |r| + |g| + |b|$, 那么红色收缩格子的点、边和面的数量应分别为 $|r|, |v|/2$ 和 $|g| + |b|$ 。编码的逻辑量子比特数量 $k = |v| - 2(|r| + |g| + |b|) + 4 = 4 - 2(|r| + |g| + |b| - |v|/2) = 2(2 - \chi^r) = 4g$, 即逻辑量子比特的数量与欧拉示性数(等价地,亏格数)相关。以二维轮胎面 $g=1$ 为例,其编码了4个逻辑量子比特,是表面码的两倍。

b) 弦算符: 某颜色 c 的收缩格子上的闭弦 γ 上可以定义两个 c 颜色的 Pauli- X 和 Pauli- Z 弦算符 $S_\gamma^{c,\sigma} = \prod_{v \in \gamma} \sigma_v$, 其中 $\sigma = X$ 或 Y 。由于三着色格子中每个格点都精确地有三个不同颜色的临面,拓扑等价弦上的三种不同颜色、相同 Pauli 类型的弦算符总是满足 $S_\mu^{r,\sigma} \cdot S_\mu^{g,\sigma} \cdot S_\mu^{b,\sigma} = I$, 这里 μ 表示拓扑等价类。即一种颜色的弦算符等价于另两种颜色的拓扑等价弦算符的组合,如图5。

弦算符的等价性直接意味着,对于闭弦而言:(i) 相同 Pauli 类型的任意弦算符对易,(ii) 拓扑等价弦上的任意弦算符对易,(iii) 相同颜色的任意弦算符对易。这构成了颜色码上逻辑门的实现理论基础。以图6二维轮胎面上的蜂窝状六角格子为例,

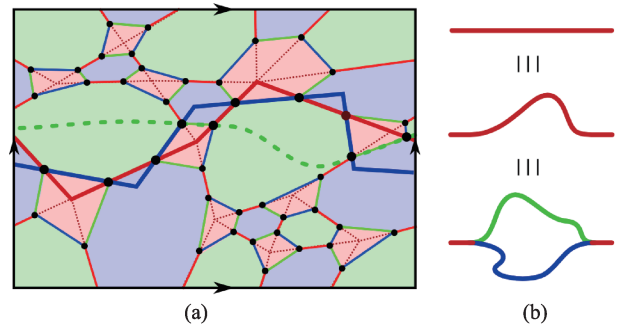


图5 (a)颜色码示意(摘自参考文献[14]),其中红色虚线构成的格子即红色收缩格子;红色和蓝色的粗实线表示相应颜色的弦算符,绿色点线则是红蓝弦算符乘积而来的等价绿色弦算符;(b)拓扑等价弦上相同颜色的弦算符等价(相差稳定子),一种颜色弦算符与另两种颜色拓扑等价弦算符的乘积等价

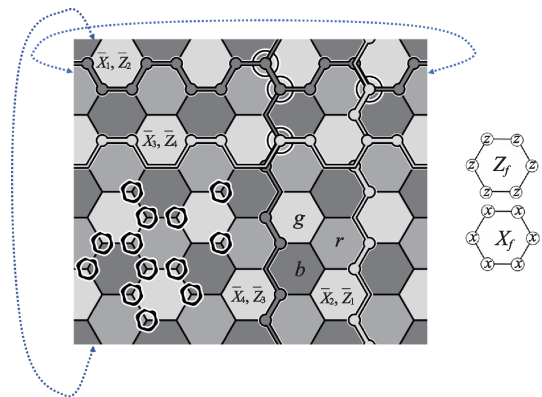


图6 二维轮胎面上的蜂窝状六角格子色码(摘自参考文献[2])。其中蜂窝格子的节点上放置物理量子比特,各不同颜色(r, g, b)的六角形面元上则均定义了 X 和 Z 两种局域稳定子。两条拓扑等价的蓝色(b)和绿色(g)横向闭弦(γ_1)和两条拓扑等价的蓝色(b)和绿色(g)纵向闭弦(γ_2)上各自定义了两种不同类型的 Pauli 弦算符,作为4个逻辑比特的逻辑量子门。左下角的标记节点表示该编码下的局域算符(如局域错误等)

其有两个拓扑不等价的非平庸闭弦 γ_1 (横向)和 γ_2 (纵向),可以选取

$$\{ S_{\gamma_1}^{b,X}, S_{\gamma_1}^{b,Z}, S_{\gamma_1}^{g,X}, S_{\gamma_1}^{g,Z}, S_{\gamma_2}^{b,X}, S_{\gamma_2}^{b,Z}, S_{\gamma_2}^{g,X}, S_{\gamma_2}^{g,Z} \}$$

作为4个逻辑比特相应的逻辑 Pauli 门。

类似于表面码,在拓扑平庸的球面上“挖洞”可以引入非平庸的拓扑性,进一步地,将这种带有孔洞的平面剪开,可以等价地铺展成具有开边界的二维平面,这种二维平面上同样可以定义具有拓扑性

质的颜色码。以最简单的蜂窝状六角格子系统为例,在拓扑平庸球面上的蜂窝格子中挖去一个节点及其三个邻边,然后将其平铺在二维面上,即可得到如图7所示的具有三条开放边界的编码了1个逻辑量子比特的颜色码。由于蜂窝状格子中红绿蓝三色稳定子都是正六边形(包含6个物理比特),这种颜色码被称为[6,6,6]颜色码。

在具有开放边界的二维颜色码中,每一条边界上都可以定义两个弦算符: $\prod_{v \in \text{boundary}} X_v$ 和 $\prod_{v \in \text{boundary}} Z_v$, 他们扮演着逻辑量子门的角色。考虑到给逻辑量子门乘上任意的局域稳定子仍然得到一个相同作用效果的逻辑量子门(即弦算符的等价性质),边界上的逻辑门弦算符等价于一种具有“T”形结构的弦网算符,如图8,其三条弦各着一种颜色。若给图7中所示三角形的三条边按照如下规则也着上颜色:与两种不同颜色面相邻的边界着上第三种颜色。那么这种“T”形弦网的三条弦各自与相

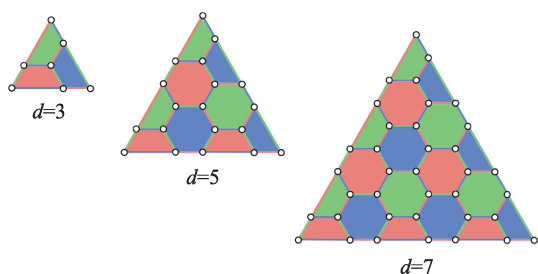


图7 不同码距的[6,6,6]颜色码(摘自参考文献[16])。其中白色圆点处放置物理量子比特,三种不同颜色的面元上定义了相应的X和Z型局域稳定子,任一边界上的弦算符都可以定义彼此等价的逻辑Pauli门

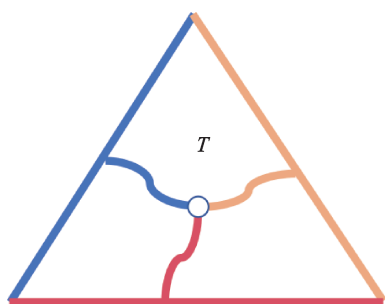


图8 二维开边界色码上的逻辑门由边界上弦算符或其等价的“T”弦网算符构成。“T”形弦网算符通过红绿蓝三种不同的弦与相应颜色的边界连接,其上定义了逻辑X和Z门

同颜色的边界相连。

4.2 颜色码的理论优势

能否以更简单的方式实现更多类型的逻辑量子操作是衡量纠错编码理论性能的一个重要参考。所有CSS类型的纠错码天然都具有“横向”的CNOT门。在此基础上,表面码上可以“横向”地实现逻辑Pauli门,但不能“横向”实现逻辑Hadamard门H和相位门 $S = \text{diag}(1, i)$ 。而颜色码上却可以横向的实现逻辑Hadamard门H和相位门S,即可以横向实现完整的Clifford门。

由于 $HXH=Z$, $HZH=X$,在颜色码中对所有物理比特施加H仅仅调换 X_i 和 Z_i 的角色而保持稳定子群不变,同时将逻辑 X_L 与逻辑 Z_L 调换。换句话说,在所有物理比特上同时施加H的操作等效于逻辑Hadamard门 H_L ,此即颜色码上逻辑 H_L 的“横向”实现方法。

我们知道 $SZS^\dagger = Z$, $SXS^\dagger = iXZ$ 及 $S^\dagger XS = -iXZ$,当对所有物理比特施加相位门S(或 S^\dagger)时 Z_j 稳定子不变,但 X_j 稳定子变成 $i^{\sum_{v \in j} \text{sgn}(v)} X_j Z_j$,这里 $\text{sgn}(v) = 1$ 表示在物理比特v上施加的是S, $\text{sgn}(v) = -1$ 表示在物理比特v上施加的是 S^\dagger 。若要 $i^{\sum_{v \in j} \text{sgn}(v)} X_j Z_j$ 仍是一个稳定子,必然要求 $i^{\sum_{v \in j} \text{sgn}(v)} = 1$ 。两种情况可以满足该要求:(i)所有面元上物理比特(即格点)的数量都是4的整数倍;(ii)所有面元上物理比特(即格点)的数量都是偶数,对于非4倍数的面,其中一半物理比特施加S,另一半施加 S^\dagger 。

由于二维开放边界格子上颜色码中逻辑Pauli门弦(或弦网)算符总是包含奇数个物理比特,无论在条件(i)还是(ii)下,都有 $Z_L \rightarrow Z_L$, $X_L \rightarrow iX_L Z_L$ 或 $X_L \rightarrow -iX_L Z_L$,即总是横向地实现了逻辑相位门 S_L 或其逆 S_L^\dagger 。也就是说,颜色码允许“横向”实现完整的Clifford操作。

事实上,结合Clifford门的“横向”性和二维平面的阿基米德镶嵌,二维颜色码的可能构型只有如下图9所示的三种,

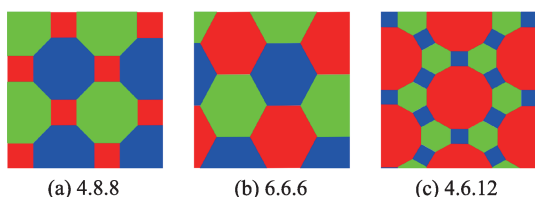


图9 二维颜色码的可能构型(摘自参考文献[17])。其中格子节点上放置物理量子比特,各面元上定义了相应颜色的局域稳定子

4.3 颜色码的实验研究进展

2024年 Google Quantum AI 团队在 72-qubit Willow 超导处理器上实现三角颜色码的实验演示^[18]。他们提出了一种“超密集颜色码”方案用来在方格子系统等价实现六角稳定子的测量。实验演示了 X/Z 基态保存,证实当编码距离从 3 扩展至 5 时,逻辑错误率抑制因子 $A_{3/5} = 1.56(4)$ 。他们还通过逻辑随机基准测试证实该系统上横向 Clifford 门的平均错误率近似为 0.002 7(3),魔态注入的保真度则超过 99%。除此之外,他们还演示了基于晶格手术进行逻辑态传送的实验,单比特传送态的平均保真度大于 84.7(1)%。该工作表明了颜色码对于在超导量子处理器上实现容错量子计算有重要价值。

五、纠错码的解码算法

拓扑码(表面码和颜色码)作为当前最具实验可行性和容错潜力的量子纠错码,其核心任务在于根据奇偶校验测量(综合征)准确推断出潜在的物理错误,从而恢复逻辑量子态。由于量子系统的退相干时间尺度很短,解码算法必须在极短时间内完成高精度的推断。同时,“简并性”使得多个不同的错误模式可能导致相同的综合征测量结果,解码器不仅要找到单一错误路径,更需识别在稳定子群意义下等价的错误类,这一过程在计算复杂性上属于 #P-完全问题。因此解码的挑战不仅在于结果的准确性,也在于解码算法的运行速度。为此,研究者们围绕“如何高效、准确地重建最可能错误类”提出了多种算法思路。

5.1 几种主要解码算法

最早期且最具代表性的算法是最小权重完美匹配(Minimum-Weight Perfect Matching, MWPM)解码器。该方法通过将综合征映射为图结构,将非平庸的测量输出点视作图的节点,以路径长度为边权重,进而利用图论中的 Blossom 等算法求解最小权重完美匹配,得到最可能的错误组合。在最差情况下该算法的复杂度关于问题规模(综合征测量数量 N)成三次多项式关系 $O(N^3 \log(N))$,在码距较大时解码耗时较长。此外该算法假设各物理比特上的错误服从独立同分布,在实际硬件存在噪声非均匀性时性能下降。

为进一步降低计算复杂度,人们提出了联合查找(Union-Find, UF)解码器,其解码过程分为“簇生长”和“剥离”两个阶段。该方法以非平庸综合征点为种子,逐步扩张并合并相邻节点形成簇,当簇满足偶宇称或触及边界时冻结。随后,剥离阶段通过叶节点回溯,消除偶宇称簇,得到最终的错误链。该方法的复杂度接近线性 $O(Na(N))$,这里 a 是 Ackerman 函数的逆函数,在实际应用中一般有 $a(N) \leq 3$ 。UF 计算效率显著优于 MWPM,且天然兼容擦除错误(如量子比特泄漏)。然而,当物理错误率较高时,簇的过度合并会引入虚假相关,导致逻辑错误率迅速上升。

另一类方法基于信念传播(Belief Propagation, BP)。传统 BP 算法通过消息传递估计后验概率,实现最大似然解码,BP 过程的计算复杂度为 $O(N)$ 。然而,量子简并性导致其难以收敛,使得单纯的 BP 方法不适用于拓扑码的解码过程。为此,研究者提出了 BP-OSD(Ordered Statistics Decoding)增强方案:先由 BP 生成软判决概率,再选取高置信度变量构建简化线性系统,通过有序统计方法求解最优简并错误类,这一方法可近似实现简并量子最大似然解码(DQMLD)。由于 OSD 过程涉及到矩阵求逆计算,其计算复杂度在 $O(N^3)$ (OSD-0)或更高(OSD-w)。

张量网络(Tensor Network, TN)解码器是一种

基于张量网络收缩方法实现 DQMLD 的数值工具。该方法将二维拓扑码的联合错误概率分布表示为矩阵乘积态,并通过张量收缩计算后验概率。其创新在于将表面码的拓扑边界条件映射为矩阵乘积态形式的边界向量,并利用纠缠熵面积律对收缩过程进行截断近似来压缩计算复杂度,使之降至 $O(N\chi^3)$ 。TN 解码在低密度噪声下能接近理论最优阈值,其中 χ 表示张量网络结构的虚拟维度(即收缩阶段维度)。

5.2 新兴方法与未来趋势

近年来,面向实际硬件的高效解码需求推动了多种新兴算法的出现。其中,元胞自动机(Cellular Automaton, CA)解码器以局部规则迭代传播信息,仅需邻域通信,计算成本极低,适合硬件集成实现实时响应,但解码精度有限,主要用于低码距($d \leq 7$)场景。

更具潜力的方向是深度学习解码器,如基于 Transformer 架构^[19]及混合生成对抗学习^[20]的解码方法。以谷歌的 AlphaQubit 为例,其采用两阶段训练机制:首先使用合成噪声数据进行预训练,再在真实量子处理器(如 Sycamore)的实验数据上进行微调。其循环 Transformer 结构能有效处理“软测量”信息,从而在非理想测量条件下保持高精度解码。此外,图神经网络(GNN)被用于表面码的图结构建模,通过图卷积机制聚合邻域信息,在存在空间关联噪声时展现出比传统算法更强的鲁棒性。

不同解码器在复杂度、容错阈值与适用场景方面各具优势。MWPM 算法成熟稳定,在独立同分布噪声下阈值接近理论上界,但在 Z 偏置噪声下性能下降。Union-Find 以近线性复杂度和擦除容错性著称,却在高错误率下失效。BP-OSD 兼具高精度与较低复杂度,适合中等规模量子芯片。张量网络解码器虽能逼近理论最优,但资源消耗较大;深度学习解码展现出对真实硬件噪声的强适应性,是未来的重要发展方向。

展望未来,拓扑码解码仍面临几项关键挑战:

其一,实时性突破——当前在码距 $d > 15$ 时,解码延迟普遍严重,亟需借助 FPGA 等专用硬件实现亚微秒级解码;其二,噪声自适应性——量子硬件的噪声特性随时间和操作而漂移,要求解码算法具备在线噪声图谱建模能力;其三,量子-经典协同解码——探索将部分计算任务卸载至辅助量子处理器,以缓解经典计算瓶颈;其四,标准化工具生态——推动如 PyMatching、Fusion Blossom 等开源库的硬件加速化与跨平台标准接口建设。

总体来看,拓扑码解码正经历从启发式图搜索(MWPM、UF)向概率推理(BP-OSD)与智能化学习(深度学习)的范式转变。随着谷歌 AlphaQubit 等深度学习解码器的实验成功,未来的量子容错体系将更加依赖于自适应、硬件协同的智能解码架构。算法效率与硬件可实现性的协同优化,仍是迈向实用化容错量子计算的关键技术路径。

六、总结与展望

量子纠错技术为 Shor 大数分解算法等关键量子算法提供了抗噪声保护机制。2019 年 Gidney 和 Ekerå 基于二维表面码分析认为在当前技术条件下要基于 Shor 算法实现 2048 位 RSA 分解大约需要 2000 万个物理量子比特,运行时间大约 8 个小时^[21]。2021 年 Gouzien 和 Sangouard 基于三维规范颜色码和多模式量子存储器给出了一种可在 13 436 个物理比特上在 177 天实现 2028 位 RSA 分解的方法,但同时要求量子存储器可以储存 2000 万个空间模式和 45 个时间模式,且存储时间应达到 2 小时^[22]。换句话说,基于纠错码方案实现容错量子计算是 Shor 算法大规模运行的技术基础,当前技术条件距离这一目标仍然有不小距离。为此,2022 年清华大学龙桂鲁等人基于经典 Shnorr 方法提出了一种有望在当前真实物理器件上实现较大规模 RSA 分解的“量子+经典”混合算法^[23],引起了广泛关注^[24,25]。

除 Shor 算法等密码分析应用外,量子纠错技术的意义已远超单一算法层面。它构成了实现通用容错量子计算的根基,也是量子通信、量子模拟乃

至量子计量等方向的基础支撑。从理论角度看,稳定子码体系已构成较为完备的编码框架,为逻辑门集的容错实现和多维拓扑结构的编码设计提供了系统化的理论工具。从实验角度看,近年来超导、离子阱及光学平台均相继实现了小规模的面码与颜色码逻辑比特,逻辑寿命已首次超越物理寿命,标志着量子纠错从概念验证迈入了可扩展实现阶段。

展望未来,量子纠错的研究将主要聚焦于三个方向:其一,高阈值编码与多维拓扑结构——通过引入低密度奇偶校验(LDPC)码、三维颜色码及自纠错拓扑相等新型结构,提高编码率与误差容忍度;其二,高效实时解码与智能化协同——结合张量网络、深度学习与硬件加速,实现低延迟、可自适应的解码体系;其三,跨层协同的容错体系工程——在硬件、编译与算法层面建立端到端的容错架构,优化量子资源开销与逻辑门保真度。随着量子比特相干性与制造工艺的持续进步,量子纠错的理论实验体系正逐步融合,未来十年有望实现“后阈值时代”的中等规模容错量子计算机,为量子算法的实用化奠定坚实基础。

参考文献

- [1] Matthias Steffen, What's the difference between error suppression, error mitigation, and error correction? <https://www.ibm.com/quantum/blog/quantum-error-suppression-mitigation-correction>
- [2] Bombín H. An introduction to topological quantum codes[J]. arXiv preprint arXiv:1311.0277, 2013.
- [3] Grimsmo A L, Puri S. Quantum error correction with the Gottesman-Kitaev-Preskill code[J]. PRX Quantum, 2021, 2(2): 020101.
- [4] deMartini O, Fuentes P, Orús R, et al. Decoding algorithms for surface codes[J]. Quantum, 2024, 8: 1498.
- [5] Cai Z, Babbush R, Benjamin S C, et al. Quantum error mitigation [J]. Reviews of Modern Physics, 2023, 95(4): 045005.
- [6] Quek Y, Stilck França D, Khatri S, et al. Exponentially tighter bounds on limitations of quantum error mitigation[J]. Nature Physics, 2024, 20(10): 1648-1658.
- [7] Kitaev A Y. Fault-tolerant quantum computation by anyons[J]. Annals of Physics, 2003, 303(1): 2-30.
- [8] Bombín H, Martin-Delgado M A. Optimal resources for topological two-dimensional stabilizer codes: Comparative study[J]. Physical Review A—Atomic, Molecular, and Optical Physics, 2007, 76(1): 012305.
- [9] Bravyi S B, Kitaev A Y. Quantum codes on a lattice with boundary [J]. arXiv preprint quant-ph/9811052, 1998.
- [10] Wootton J R, Peter A, Winkler J R, et al. Proposal for a minimal surface code experiment[J]. Physical Review A, 2017, 96(3): 032338.
- [11] Zhao Y, Ye Y, Huang H L, et al. Realization of an error-correcting surface code with superconducting qubits[J]. Physical Review Letters, 2022, 129(3): 030501.
- [12] Suppressing quantum errors by scaling a surface code logical qubit [J]. Nature, 2023, 614(7949): 676-681.
- [13] Quantum error correction below the surface code threshold[J]. Nature, 2025, 638(8052): 920-926.
- [14] Bombin H, Martin-Delgado M A. Topological quantum distillation[J]. Physical Review Letters, 2006, 97(18): 180501.
- [15] Eastin B, Knill E. Restrictions on transversal encoded quantum gate sets[J]. Physical Review Letters, 2009, 102(11): 110502.
- [16] Takada Y, Fujii K. Improving threshold for fault-tolerant color-code quantum computing by flagged weight optimization[J]. PRX Quantum, 2024, 5(3): 030352.
- [17] Landahl A J, Anderson J T, Rice P R. Fault-tolerant quantum computing with color codes[J]. arXiv preprint arXiv:1108.5738, 2011.
- [18] Lacroix N, Bourassa A, Heras F J H, et al. Scaling and logic in the color code on a superconducting quantum processor[J]. Nature, 2025: 1-3.
- [19] Li A Q, Tian C W, Xu X X, et al. Global receptive field transformer decoder method on quantum surface code data and syndrome error correction[J]. Chinese Physics B, 2025, 34(3): 030306.
- [20] Tian C, Fan Z, Guo X, et al. Transformer-based quantum error decoding enhanced by QGANs: towards scalable surface code correction algorithms[J]. EPJ Quantum Technology, 2025, 12(1): 76.
- [21] Gidney C, Ekerå M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits[J]. Quantum, 2021, 5: 433.
- [22] Gouzien É, Sangouard N. Factoring 2048-bit rsa integers in 177 days with 13 436 qubits and a multimode memory[J]. Physical Review Letters, 2021, 127(14): 140503.
- [23] Yan B, Tan Z, Wei S, et al. Factoring integers with sublinear resources on a superconducting quantum processor[J]. arXiv preprint arXiv:2212.12372, 2022.
- [24] 王潮, 王启迪等. 基于 d-wave advantage 的量子退火公钥密码攻击算法研究[J]. 计算机学报, 2024, 47(5): 1030-1044.
- [25] Tesoro M, Siloi I, Jaschke D, et al. Quantum inspired factorization up to 100-bit RSA number in polynomial time[J]. arXiv preprint arXiv:2410.16355, 2024.