通用量子计算机和容错量子计算*
——概念、现状和展望*

李 颖[1] 孙昌璞[1,2,†]
(1 中国工程物理研究院研究生院 北京 100193)
(2 北京计算科学研究中心 北京 100193)

2019－07－17收到
† email:suncp@gscaep.ac.cn
DOI:10.7693/wl20190801

Universal quantum computer and fault-tolerant quantum computation
——concepts, status and prospects

LI Ying[1] SUN Chang-Pu[1,2,†]
(1 Graduate School of China Academy of Engineering Physics, Beijing 100193, China)
(2 Beijing Computational Science Research Center, Beijing 100193, China)

摘 要 量子计算技术近年来快速发展并受到广泛关注。文章将介绍一些量子计算的基本概念、现状以及远期和近期的主要挑战，使读者可以更准确地理解一些新近的进展，避免误解。通用量子计算机的主要应用之一是破解RSA密码。没有量子纠错，我们很难实现密码破解规模的量子计算。因此，量子计算技术的一大挑战是如何实现有量子纠错保护的量子计算，也就是容错量子计算。通过介绍现有的实验技术，将发现目前已经可以在实验中实现错误率低于容错阈值的量子门，但容错量子计算离实际应用还有距离。主要的困难在于，量子容错需要数量巨大的低错误率的量子比特，超出了现有技术能达到的水平，需要进一步的发展。有噪声中等规模量子计算有可能在近期内成为现实，目前仍有一些理论和技术方面的瓶颈问题需要深入研究。在看到量子计算技术巨大潜在价值和长足进步的同时，有必要了解有哪些亟需解决的问题，直面关键、攻坚克难。

关键词 通用量子计算机，容错量子计算，有噪声中等规模量子计算

Abstract Quantum computing technology has developed rapidly in recent years and received wide attention. In this article, we review some basic concepts, current status, long-term and near-term challenges of quantum computing, so that readers can more accurately understand some recent progress and avoid misunderstanding. One of the main applications of universal quantum computers is to break RSA cryptographic systems. Without quantum error correction, it is difficult to achieve quantum computing in the scale of code breaking. Therefore, a primary challenge of quantum computing technology is to implement quantum computing protected by the quantum error correction, i.e. fault-tolerant quantum computation. By looking at the existing experimental technologies, we will find that quantum gates with error rates lower than the fault-tolerance threshold have been realised in experiments, but fault-tolerant quantum computation is still far from practical applications. The main difficulty is that quantum fault tolerance requires an enormous number of qubits with low error rates, beyond what can be achieved by

* 国家自然科学基金委员会—中国工程物理研究院联合基金(批准号：U1730449)、国家自然科学基金(批准号：11534002、11875050)资助项目

state-of-the-art technologies; therefore, further development is needed. Noisy intermediate-scale quantum computation is likely to be realised in the near future, and there are still some theoretical and technical bottlenecks that need to be addressed. While we can see the huge potential value of quantum computing and recent significant progress, it is important to acknowledge the challenges, face the key problems, and overcome difficulties.

Keywords universal quantum computer, fault-tolerant quantum computation, noisy intermediate-scale quantum computation

1 引言

计算机技术已经引起了经济和社会的巨大改变，其发展得益于传统量子物理的研究。晶体管是计算机的主要元件，有了量子力学理论我们才能够理解这种半导体器件的基本原理。在过去的四五十年当中，集成电路中的晶体管数量大概每一年半增长一倍，被称为摩尔(Moore)定律。然而，目前这个趋势正在放缓。在这个时候，量子物理研究有可能再一次从根本上突破瓶颈并促进计算机技术的大规模发展。

与今天广为使用的计算机(我们称之为经典计算机)相比，量子计算机通过一种完全不同的方式进行计算，因此给计算技术带来了全新的可能性。量子力学理论创立于20世纪初，经由大量的物理实验验证，业已成为半导体和现代化学的理论基础。在量子力学中，物理系统的状态需要用波函数来描述，存在不是非黑即白的状态，被称为量子叠加态。同时，量子力学预言了波函数的相干、纠缠等经典物理理论中没有的现象。虽然我们很难在日常生活中直接看到这些现象，但它们都能在实验室中被观测到。量子计算机的“量子”指的就是在计算中利用量子相干、纠缠等效应，进而能够用比经典计算机更短的时间完成某些特殊计算。这正是我们研发量子计算机的最主要原因。除此以外，量子计算技术还促进了基础研究和其他量子技术，例如量子通讯和量子传感等。

虽然经历了近年来的快速发展，与成熟的经典计算机技术相比，量子计算机技术仍处于初级阶段。量子计算机的概念在20世纪80年代被提出[1, 2]，此后在很长的时期内属于基础研究的范畴。目前，量子计算刚刚由基础研究转向工程实现和应用研究。我们还没有发现任何基本问题可能导致最终无法实现有应用价值的量子计算机；与此同时，也很难预测这一转变的最终完成需要多长时间[3]。

下面，我们将具体介绍量子计算机的概念、优势以及实现方法。除此以外，还会介绍一些典型的量子计算物理系统，以及探讨在近期内实现量子计算技术实际应用的可能性。希望通过这些介绍，使专家和领域外的人士对量子计算的概念和发展态势有一个科学的理解。

2 通用量子计算机

从算法的角度来说，量子计算机具有比经典计算机更强大的计算能力。这个想法最初是由费曼(R. Feynman)和马宁(Y. Manin)在20世纪80年代初提出[1, 2]。自20世纪40年代美国核武器研究起，数值计算被广泛应用于物理学以及其他学科的研究中。其中重要的一项应用是对物理系统的数值模拟。自然界的物理系统均为量子系统。然而，由于记录和处理量子态需要很大的信息存储空间，利用经典计算机对量子多体系统进行模拟是非常困难的。但是，量子计算机没有这个问题。如果经典计算机无法精确[1)]模拟量子多体系统而量子计算机可以，那么不言而喻，量子计算机优于经典计算机。

1) 这里“精确”一词指误差可以通过算法中参数的选取趋近于零，并且算法对信息存储空间和时间等资源的需求随着精确度缓慢增长。

1985年，多伊奇(D. Deutsch)提出了量子计算机的模型——通用量子计算机(或量子图灵机)[4]。任意一种量子算法均可以利用通用量子计算机实现。量子计算机是由许多量子比特(二态量子系统)组成的物理系统。对每个量子比特，$|0\rangle$和$|1\rangle$是两个完全可区分的量子态，它们分别对应二进制数中的0和1。量子比特和经典比特的差别在于，量子比特可以处于0和1的量子叠加态，用$a|0\rangle+b|1\rangle$表示，这里系数a和b刻画了量子比特的具体状态。量子计算有很多方式，其中广泛使用的模型是量子线路，也就是通过在量子比特上执行一系列的逻辑操作来实现量子计算，如图1所示。这些逻辑操作包括：量子比特的初始化、量子态的幺正变换以及对量子比特信息的读取。

与经典计算机中的通用逻辑门类似，在量子计算机中任意的幺正变换均可以通过一组有限的幺正变换(量子门)的组合以任意的精确度近似。这样一组量子门被称为通用量子门。例如，Hadamard门(***H***)、π/4相位门(***S***)、π/8相位门(***T***)以及受控非门(***CNOT***)构成一组通用量子门[5]。这里面***H***、***S***和***T***为单量子比特门，***CNOT***为两量子比特门(图1)。利用这些量子门，不仅可以实现任意的量子算法，还可以实现任意的经典算法。从这个意义上说，显然量子计算机的计算能力是大于等于经典计算机的。

1986年，多伊奇和乔沙(R. Jozsa)提出了一个计算问题来表明量子计算机的确在解决某些问题上具有优势[6]。他们提出的问题是判断一个函数f：$\{x\}\rightarrow\{0,1\}$对于不同的输入x是否给出相同的输出0或1。函数f需要满足一定的条件，这里不再赘述。对于输入为一个比特的情况，也就是x有两个取值0和1，用经典计算机解决这个问题需要计算f至少两次。而用量子计算机只需要计算f一次，这个量子算法被称为多伊奇—乔沙(Deutsch—Jozsa)算法。当输入比特增多的时候，确定性经典算法需要计算f的次数随着比特数量指数增长，而量子算法仍然只需要计算f一次。

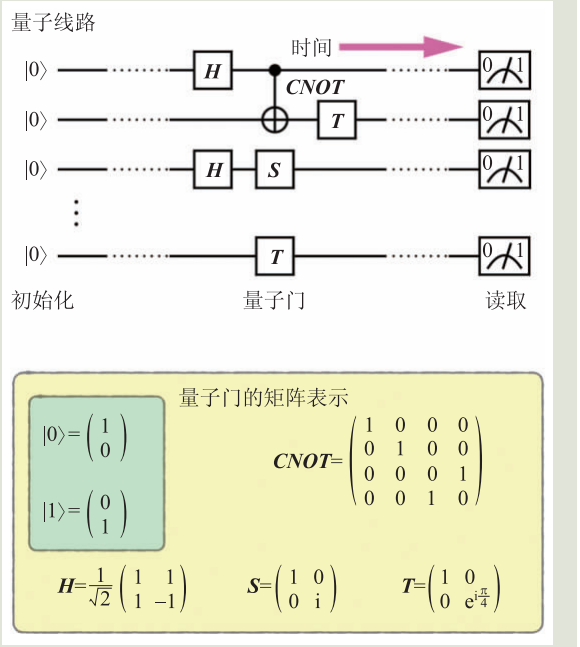


图1 量子线路和量子门。量子线路由量子比特的初始化、一组量子门以及最终的信息读取组成。其中的量子门可以由矩阵表示

1994年，肖尔(P. Shor)提出了能够解决因数分解问题的量子算法，被称为肖尔(Shor)算法[7]。利用已知最好的经典算法，因数分解所需的时间随着整数长度次指数增长。由于指数函数增长非常快，当整数达到一定长度时，经典计算机无法有效地进行因数分解。广为使用的RSA密码系统正是基于这一点。然而，量子算法所需的时间随着整数长度代数增长，要远远慢于指数函数。因此，量子计算机可以更快地对大整数进行因数分解。利用量子计算机，我们可以破解经典计算机无法破解的密码，给密码系统的安全性带来了挑战。当然，对于有些密码算法，还没有发现像肖尔算法这样可以进行破解的量子算法。因此，抵

多伊奇—乔沙问题

在多伊奇—乔沙问题中，函数f需要满足如下条件：要么所有的输出均相同；要么在所有的输入x中，一半的输出为0，一半的输出为1。对于n个输入比特的情况，总共有2^n种可能的输入x，有可能在查看$2^n/2+1$种输入以后才发现有不同的输出。因此，在经典计算中确定性的解决多伊奇—乔沙问题需要进行$2^n/2+1$次计算。

御量子计算对密码安全的威胁有两种方式，一种是基于量子物理的量子密钥分发，另一种是后量子密码，也就是量子计算还无法破解的经典密码算法[8]。

1996年，劳埃德(S. Lloyd)提出了可以模拟局域相互作用量子系统演化的通用量子计算机算法[9]。根据这个算法，模拟量子系统演化的误差可以趋近于零，而算法所需的资源随着子系统个数、误差等参数的变化是一个代数函数。因此，通用量子计算机可以有效模拟量子系统演化。基于对演化的模拟，量子计算机还可以用来求解某些量子系统的基态能量等问题。量子系统的演化和基态能量是两个非常重要的计算问题，在物理、化学和材料等学科的研究中均有应用。

目前计算机已经广泛应用于日常生活的方方面面。但在计算机技术普及以前，它的两个主要应用是密码破译以及科学计算和模拟。非常巧合的，量子计算机两个重要的算法——肖尔算法和量子模拟算法分别对应了这两种应用。这两个算法有清晰的应用背景以及对经典算法的优势，因此极具代表性。如果能够在量子计算机上演示这两个算法，并且用来解决经典计算机无法解决的实例，或许可以认为最终实现了通用量子计算机。

除了本文介绍的，目前还有很多其他的量子算法[10]。应该注意到，不是对于所有的计算问题量子算法都有指数加速。在算法方面量子计算机和经典计算机的对比有大量计算复杂性理论的研究[5]。

退相干导致的两种计算错误

我们可以将量子计算机中的错误分为两种：比特错误和相位错误。比特错误导致量子比特0和1的取值发生改变，相位错误导致叠加态的相位发生变化。对于一个处于叠加态 $a|0\rangle+b|1\rangle$ 的量子比特，比特错误导致状态改变为 $a|1\rangle+b|0\rangle$，相位错误导致状态改变为 $a|0\rangle-b|1\rangle$。在经典计算机中也存在比特错误，但相位错误是量子计算机独有的。量子计算机中任何的错误都可以分解为两种错误的组合。

到目前为止，所有的结论都是基于拥有通用量子计算机这一假设。那么，我们有可能制造一台通用量子计算机吗？事实上，由于普遍存在的退相干现象，严格的幺正变换量子门是不可能百分百实现的。关键是这种退相干对计算结果有多大影响，是否在许可误差范围内。

3 退相干

量子计算所需的量子门是幺正变换。在量子力学理论中，幺正变换描述了一个封闭系统的演化。然而，在自然界中我们还没有发现真正的封闭系统：一个物理系统总是或多或少地与外界环境存在相互作用。由于相互作用的影响，系统演化不仅由系统本身决定还取决于环境的状态。其结果是系统演化一般不再是幺正变换。我们用完全正定映射来描述量子系统最一般性的演化。有些非幺正演化会使量子系统逐渐失去相干性，也就是量子叠加态无法持续，这个过程被称为退相干。

退相干会导致量子算法失去优势。1998年，本文作者之一及其合作者讨论了退相干对肖尔算法的影响，发现退相干会降低成功求解因数的概率[11]。当概率过低时，量子算法的效率不再高于经典算法。事实上，在物理系统中执行的量子门相对理想量子门的任何偏离都有可能导致量子计算的结果错误，进而量子算法失效。

退相干在自然界中是广泛存在的。与此同时，有一些物理机制可以用来抑制退相干。当环境对系统的影响具有某些对称性的时候，可能存在一个不发生退相干的量子态子空间，因此存储在子空间内的量子信息可以不受退相干的影响[11—13]。如果环境引起的噪声在时间上有关联，动态解耦等方法可以用来抑制退相干的发生[14, 15]。这些方法可以在很大程度上改进物理系统在量子计算中的性能，但计算错误的发生仍然是无法避免的。因此，需要在算法的层面对计算错误进行处理：虽然在计算过程中还是会发生错误，但可以避免错误对最终计算结果的影响。

4　量子纠错码和容错量子计算

量子纠错码可以用来解决退相干等硬件的不完美导致的计算错误问题。在错误的分布满足某些条件的情况下，我们可以把最终计算结果出错的概率降得任意低，这被称作容错量子计算。当然，量子纠错是有代价的。为了降低最终出错率，需要使用很多的量子比特来进行编码。进行容错量子计算的首要条件，也就是错误率低于容错阈值(亚阈值)的初始化、量子门以及读取等操作已经能够在实验中被演示。目前看来，在错误率低于阈值的条件下，巨大的量子比特数量是最终实现容错量子计算的主要障碍。

4.1　量子纠错码

量子纠错码是经典纠错码在量子信息的推广。首先来了解什么是经典纠错码。最简单的纠错码是重复码(repetition code)，也就是将要保护的信息重复存储(图2)。在日常生活中，我们会经常使用这种保护信息的方式，例如将重要的文件复制一份。事实上，这同样也是经典信息比量子信息更稳定的原因之一。在机械硬盘上，我们通过控制铁磁材料的极化方向来存储信息。其中少数粒子极化方向的错误不会影响对整体信息的读取。纠错码也是类似的。如果只有少数比特的信息发生了错误，我们可以将出错的比特找出来，进而实现对信息的保护。找出错误的方式有两种：一种是多数决定法，也就是数一数哪一种比特(0或1)比较多，多的那一种应该代表了正确的信息；另一种是宇称查验，也就是查验相邻比特的取值是否相同，不同则意味着其中一个出错了。对于经典纠错来说，两种纠错方式都有效。

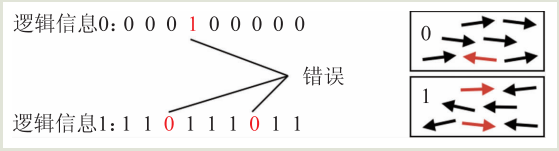


图2　经典纠错码和经典信息存储

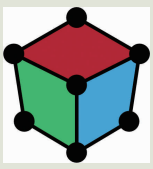
和经典纠错相比，量子纠错不仅需要处理比特错误，还需要处理相位错误。1995年，肖尔提出了第一个量子纠错码——肖尔(9量子比特)码，通过两次利用重复码来处理两种错误[16]。基于相同的思想，通过结合两个经典纠错码分别用来处理比特错误和相位错误，考得本克(R. Calderbank)、肖尔和斯特恩(A. Steane)提出了一系列的量子纠错码，并以他们三个人的名字命名为CSS码[17, 18]。当然，有的量子纠错码是以其他方式构造的。

由于对量子比特的读取会破坏量子叠加态，量子信息不能以读取信息再按照多数决定的方式纠错。在量子纠错中，纠错的方式是宇称查验，也就是通过查验量子比特之间的关系查找错误。量子纠错中的宇称查验是对一组物理可观测量(厄米算符)的测量，一般来说是一组相互对易的泡利算符。不同的量子纠错码对应了不同的一组算符。任何一个量子比特上的错误都会反映为算符测量结果的改变，也就是说能够在测量中被观测到。

宇称查验会牺牲一些量子比特的自由度。对于n个量子比特的纠错码，如果宇称查验涉及s个独立的泡利算符，那么我们可以存储$k \leqslant n-s$个被保护的量子比特信息。这是由于这些泡利算符正确值对应的量子态空间的维度是2^{n-s}，因此在这个子空间内可以存储最多$n-s$个量子比特信息。

宇称查验和斯特恩7量子比特码

我们用$\boldsymbol{X}$和$\boldsymbol{Z}$表示两个泡利算符，每个泡利算符有+1和−1两个本征值。比特错误会改变$\boldsymbol{Z}$的值，相位错误会改变$\boldsymbol{X}$的值。图中每一个圆对应了一个量子比特。对于斯特恩码，需要进行6种宇称查验，分别是每一个四边形上4个量子比特泡利算符的乘积，$\boldsymbol{ZZZZ}$和$\boldsymbol{XXXX}$。经过观察可以发现，任何一个比特错误或相位错误都会导致特定一组宇称查验结果（即$\boldsymbol{XXXX}$和$\boldsymbol{ZZZZ}$的取值）的改变。因此，这些错误可以被发现并且纠正。



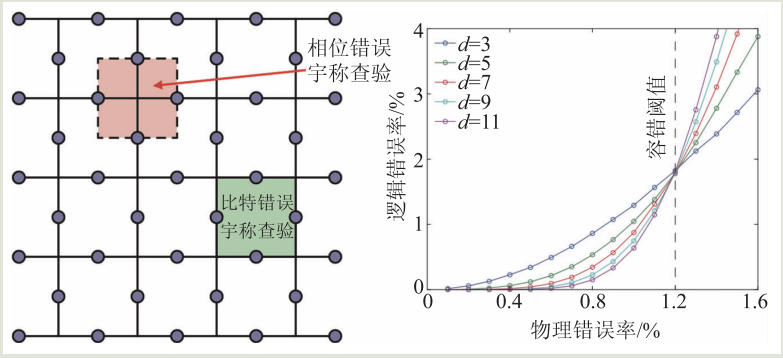


图3　表面码和容错阈值

编码用到的n个量子比特被称为物理量子比特，被保护的k个量子比特被称为逻辑量子比特。在量子纠错中，每一个物理量子比特都对应了一个具体的两量子态物理系统，而一个逻辑量子比特则涉及到多个甚至所有物理量子比特，是最终用来存储信息和计算的量子比特。

有没有一种量子纠错码，它的宇称查验和重复码类似，只是对近邻量子比特的测量？由于在物理系统中量子比特之间往往是近邻相互作用，这样的纠错码更容易实现。1997年，凯达耶夫(A. Kitaev)提出了拓扑码[19]，根据边界条件的不同，也被称为环面码或表面码(图3)。此后又发现了其他具有类似性质的量子纠错码。对于量子计算来说，目前综合看来表面码可能是纠错码最好的选择。

4.2　容错阈值

在量子计算中，需要通过对物理量子比特的操作来实现量子纠错所需要的宇称查验。而每一次操作都有一定概率引入错误，有可能导致纠错本身起到负面作用。因此，如果量子纠错能够起到预期效果，其前提条件是宇称查验过程中产生的错误不会使得错误没有减少反而增加了。这个条件被量化为容错阈值：当单次操作的错误率小于阈值的时候，量子纠错才能起到应有的作用。

对于表面码来说，当物理量子比特单次操作的错误率低于阈值的时候，纠错后逻辑量子比特的错误率随着表面码尺寸(码距)的增加而降低，如图3所示。事实上，这种情况下逻辑错误率随着码距指数衰减。因此，我们可以通过增加码距，也就是使用更多的物理量子比特，来降低逻辑错误率。只要物理量子比特足够多，逻辑错误率就会足够低。数值模拟表明表面码的错误率阈值大约是1%[20]。

4.3　容错量子计算

通过查验物理量子比特之间的关系，逻辑量子比特被保护起来了。除此以外，我们还需要对逻辑量子比特进行操作来实现通用量子计算。并且这些操作不应该破坏对逻辑量子比特的保护。在这方面已经有大量的研究。为了能够进行通用量子计算，需要一组逻辑量子比特操作，包括初始化、通用量子门以及读取。其中某些操作可以直接进行而不明显增加逻辑错误率，另外一些操作需要通过引入魔术态[21]等处理方法来进行。容错量子计算的过程如图4所示，这里不再赘述。总的来说，理论上基于逻辑量子比特的通用量子

关于容错阈值的两点说明

(1)阈值一般是在对错误分布的合理假设下得到的，假设与真实的物理系统之间还存在着差异。一般来说，假设包括每次操作的错误是独立分布的。常用的模型是去极化模型，即当错误发生的时候，相应物理量子比特的量子态完全被破坏。

(2)阈值是对单次操作的错误率来说的。例如整个计算包括N次操作，每次操作的错误率为p，那么在物理量子比特上发生错误的个数大概是Np。即使在$Np>>1$的情况下，只要p小于阈值并且量子纠错码足够大，逻辑量子比特出错的概率还是可以足够低。

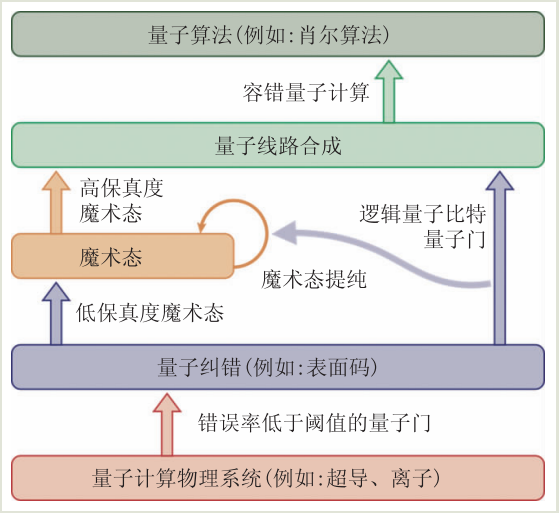


图4 容错量子计算

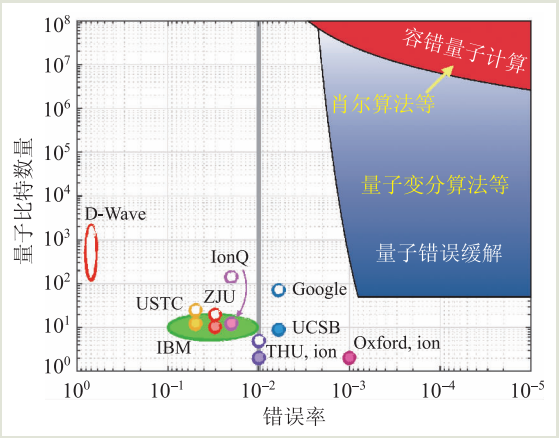


图5 量子计算系统参数。灰线对应错误率p=1%，为表面码的阈值。D-Wave系统为模拟量子计算机，没有两量子比特门错误率。空心代表没有找到报道两量子比特门错误率测量实验结果的文献。作者注意到关于USTC量子门错误率的文献中提到，利用随机校准测量的其系统中单个两量子比特门的错误率一般低于1%[30]

计算是可行的。

目前看来，表面码可能是实现容错量子计算最好的选择。首先，表面码具有较高的容错阈值(~1%)。其次，表面码仅需要在近邻量子比特之间进行宇称查验，容易在物理系统中实现。虽然通过CSS码的级联可以得到更高的阈值(~3%)[22]，但需要在远距离量子比特之间进行宇称查验，也就是需要量子计算机内部的高保真度量子态传输，因此在物理系统中实现的难度更高。

实现容错量子计算需要一台拥有大量低错误率量子比特的量子计算机。在亚阈值的条件下，只要物理量子比特数量足够多，码距足够大，我们就能够运行任意复杂的量子算法。需要的量子比特数量由错误率以及算法决定。对于表面码，操作逻辑量子比特的错误率可以用$P\sim d(100p)^{(d+1)/2}$来粗略估计，其中p是物理错误率，d是码距[23]。一个逻辑量子比特需要的物理量子比特数量大约为$(2d-1)^2$。如果我们考虑利用肖尔算法分解RSA系统中1000位的二进制整数，逻辑操作的数量大约在10^{11}的数量级，因此逻辑错误率P需要达到10^{-12}的水平。我们还假设需要1000个逻辑量子比特用于存储整数，并需要大约10倍的量子比特用于辅助，包括魔术态制备等。这样就能估计所需要物理量子比特的总数。这里仅做最简单粗略的估计，结果如图5所示。

我们可以发现，实现容错量子计算需要错误率明显低于阈值(到0.1%附近及以下)以及百万以上的物理量子比特。这对于目前的技术来说还是无法实现的。

容错量子计算需要经典计算机的参与。特别是表面码的解码过程(也就是根据宇称查验的测量结果查找错误的过程)，需要消耗一定的经典计算资源。而且码距越大，所需的计算资源越多。因此，量子计算机不会简单取代经典计算机，除非量子计算机在速度、成本特别是精确度等方面达到了经典计算机的水平。

5 量子计算的物理系统

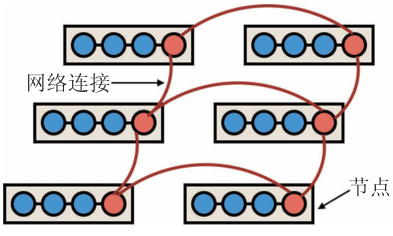
我们已经发展出了众多可以用于量子计算的物理系统，包括超导量子比特、囚禁离子、量子点、中性冷原子、光学量子计算和拓扑量子计算等。目前已经能够在实验中演示亚阈值的量子比特操作(包括初始化、量子门以及读取)。其中代表性的是2014年在超导量子比特系统中实现了错误率大约0.6%的两量子比特门，同年在囚禁离子系统中演示了错误率大约0.1%的两量子比特门。这些试验结果表明亚阈值的量子计算系统在技术上是可行的。

我们主要关心的是两量子比特门。这是由于一般来说相较于其他操作，两量子比特门的错误

率更高，并且在宇称查验中影响更大。在这些能够演示亚阈值操作的实验系统中，量子比特数量都比较少。因此，按照容错量子计算的方案，量子纠错可以降低操作逻辑量子比特的错误率，但目前还没有在实验中被成功演示。在接下来对实验系统的介绍中，我们提到的量子比特均为物理量子比特，而不是被纠错码保护的逻辑量子比特。

超导量子比特系统——作为固态系统具有较好的可扩展性。2011 年 D-Wave 发布的其第一台量子计算系统具有 128 个量子比特，至 2017 年最新的系统已经具有 2000 个量子比特[24]，体现了超导系统良好的可扩展性。但 D-Wave 的系统是模拟(analog)量子计算系统，不是本文主要讨论的基于量子线路的通用量子计算系统。在通用量子计算方面，加州大学圣巴巴拉分校(UCSB)的超导量子计算实验室的 9 量子比特系统可以实现错误率大约 0.6%的两量子比特门[25]。2018 年 Google 发布了基于相同设计的 72 量子比特系统[26]。自 2016 年起，IBM 投入大量资源研发并提供开放的量子计算系统，可以通过云访问。在其数个量子计算系统中，最早的系统有 5 个量子比特，目前在线的系统最多有 20 个量子比特，两量子比特门错误率由大约 1%到 10%不等[27]。

浙江大学(ZJU)的超导量子计算实验室可以在 10 量子比特系统中实现错误率大约 3%的两量子比特门，并且两量子比特门可以在任意一对量子比特之间进行，实现了全耦合[28]。基于相似的设计，他们还研发了能够全耦合的 20 量子比特系统[29]。中国科学技术大学(USTC)的超导量子计算实验室可以在 12 量子比特系统中实现错误率大约 5%的两量子比特门[30]。其最新的系统具有 24 个量子比特[31]。



节点量子比特数量	节点内错误率阈值	节点间错误率阈值
1	~ 0.01%	~ 0.01%
2	~ 0.1%	~ 1%
3	~ 0.1%	~ 10%
4	~ 0.2%	~ 30%
4	> 0.775%	10%
5	> 0.825%	10%

图6　网络架构量子计算

囚禁离子系统——具有很高的精确度，两量子比特门的错误率可以达到 0.1%以下，远远低于容错阈值。牛津大学(Oxford，2014 年)和美国国家标准技术研究所(NIST，2016 年)的囚禁离子实验室利用不同的离子分别成功演示了错误率大约 0.1%的两量子比特门[32, 33]。然而，这两个实验系统都仅有两个离子量子比特。2018 年，IonQ 发布了 160 个量子比特的系统，其技术可以在 13 个量子比特的系统实现错误率 2%以下的量子门[34]。清华大学(THU)的囚禁离子实验室目前可以囚禁 5 个离子量子比特并实现通用量子门，在两量子比特系统中能够达到大约 1%的两量子比特门错误率[35, 36]。一般认为通过增加单个离子阱中的离子个数来增加量子比特数量是不可扩展的。囚禁离子系统可以利用分段离子阱[37]或网络化的方式进行扩展。

网络量子计算系统——网络化是扩展量子计算系统的一个方式[38]。对于囚禁离子系统，可以利用光学系统将众多离子阱(节点)耦合起来，每个节点仅需有少数几个离子量子比特(图 6)。通过光子量子比特可以在不同的节点之间实现对离子量子比特的操作，进而整个离子阱网络可以作为一个可扩展的量子计算系统使用。一般来说节点间操作错误率较高。理论研究表明，只要节点内操作错误率显著低于 1%，即使节点间操作错误率远远高于 1%，仍然可以进行容错量子计算[39—41]。牛津大学网络量子信息技术中心以此为方案在发展离子阱网络量子计算机[42]。

网络化架构对于超导量子比特以及分段离子阱等系统同样具有意义。对于表面码量子计算，理想的状况是制备一个足够大的二维量子比特阵列，其中所有的近邻量子比特之间可以进行同样好的低错误率操作。但这样一个系统需要对量子比特的品质有很好的控制，并且能够同时优化这个多体系统中的所有操作。而在网络化架构中，通过牺牲一些操作的精确度以及部分量子纠错能力，

可以显著降低扩展系统的技术难度。

光学量子计算系统——在超导量子比特或囚禁离子等系统中，制备数百万的量子比特来实现容错量子计算是困难的，在近期内难以实现。有一种量子比特相对来说容易制备，也就是光量子比特。利用单光子源、线性光学器件以及单光子探测器可以实现通用量子计算[43]。虽然光量子比特相对容易制备，但实现量子计算需要整合大量的光学器件，不一定比其他系统的难度更低[44]。在光学量子计算和模拟方面，中国科学技术大学的实验室能够实现18个光量子比特的量子纠缠态[45]。

拓扑量子计算系统——对量子比特数量的需求是量子纠错导致的。如果不需要量子纠错，那么量子比特数量可以大大降低。理论上认为利用拓扑系统中的任意子进行量子计算有可能达到非常高的精确度，因此不需要复杂的量子纠错[46]。以马约拉纳(Majorana)费米子系统为例，在系统与环境间费米子交换被充分抑制的条件下，虽然还是需要量子纠错，但用到的量子比特数量会明显减少[47]。目前还没有马约拉纳量子比特的实验演示。有实验观测到在半导体—超导杂化系统中发生准粒子污染的时间在微秒量级[48]，与之可比较的是超导量子比特发生退相干的时间同样在微秒量级。

6　中等规模量子计算和错误缓解

容错量子计算是量子计算技术发展的远期目标，可能还需要很长一段时间才能实现。但另一方面，一台仅有几十个以上量子比特的量子计算机，其行为就很难用经典计算机模拟了。这意味着，在这样一个中等规模的系统上，就有可能进行有价值的量子计算[49]。近年来提出的量子变分算法[50]就适用于此类系统，可以用来求解量子系统的基态能量或模拟量子系统的演化[51, 52]。类似的算法还有量子近似最优化算法等[53]。除此以外，量子模拟器是一个重要的发展方向。

量子计算的指数加速(例如肖尔算法)意味着某些计算问题无法通过发展经典计算技术解决，而这些问题可以用量子计算解决。因此在两种计算方式的对比中，量子计算比经典计算更具优势。然而，当比较两个具体的计算系统的时候，一台量子计算机和一台经典计算机，我们应该关心一些更加实际的参数，例如处理器的速度或能耗等。如果以应用为目标，区分两种计算方式不是最重要的。假如可以在量子计算机上解决某个问题，是量子计算以外其他领域关心的，并在时耗或能耗等方面有一定的优势，那么应该可以认为量子计算机已经具备应用价值了。

在中等规模量子计算方面，除了要发展相应的量子算法，还需要解决计算错误的问题。由于量子比特数量的限制，容错量子计算方案显然是不适用的。接下来将介绍中等规模系统中错误处理的方式——量子错误缓解。

对于有一些计算问题来说，计算结果正确与否很容易查验。例如因数分解问题，我们很容易用经典计算机查验一个整数是否是另一个整数的因数。类似的问题包括NP(nondeterministic polynomial time)问题等。如果发生了计算错误而得到错误的结果，那么最简单的处理方法就是将计算再重复一次。只要重复的次数够多，总能得到正确的结果。假设一次计算需要的操作次数是N，单次操作的错误率是p，那么整个计算不出错的概率是$(1-p)^N$。这个概率越低，平均来说我们需要重复的计算次数越多。因此，这个方法在Np不大时是有效的。

对于另外一些计算问题来说，计算结果很难被查验。例如在量子模拟问题中，计算基态能量

量子模拟器

与本文主要讨论的基于量子线路的通用量子计算系统不同，一般来说量子模拟器(simulator)是模拟(analog)量子计算系统。量子模拟器是利用一种可控的量子系统(例如超导量子比特系统、囚禁离子系统或冷原子系统等)模拟另一种量子系统，进而研究被模拟系统的性质。虽然同样用于量子模拟(simulation)，一般来说模拟(analog)量子计算通过系统连续演化完成，而劳埃德提出的通用量子计算算法可以利用量子门实现。

或者关联函数等。对于这类问题，在Np不大的条件下，本文作者之一及其合作者以及IBM量子计算团队分别提出和发展了两种处理计算错误的方法，它们是错误外推[51, 54]和随机错误消除[54, 55]。

错误外推——由于计算错误的原因，计算结果可能会偏离正确值，如图7所示。如果我们知道错误率并且能够增加错误率，那么就可以利用不同错误率的计算结果，通过拟合外推的方法，估计在错误率等于0的情况下的正确值。2018年IBM超导量子计算实验室演示了错误外推法[56]。

随机错误消除——通过在计算中按照错误的统计分布随机地改变原本的量子线路，如图7所示，可以使得错误对计算结果正负两方面的影响相互抵消，进而得到正确的结果。2018年，浙江大学超导量子计算实验室在10量子比特系统上进行了演示[57]。2019年，清华大学离子阱实验室在实验中利用随机错误消除将量子门的等效错误率降低了一个数量级[36]。

除了错误外推和随机错误消除，还有其他一些在中等规模量子计算机上缓解计算错误的方法。有些量子算法本身带有对称性。例如在分子系统的量子模拟计算中，电子个数往往是一个守恒量。通过查验类似的守恒量，可以判断是否发生了错误，进而抑制错误对最终结果的影响[58, 59]。

利用量子错误缓解，我们可以扩展能够进行高精确度量子计算的参数空间。以随机错误消除为例，由于引入的随机性，计算平均值所需的取样次数(也就是耗时)将随之增加，增加的倍数可以用$\sim e^{4Np}$来估计[55]。当$Np\sim 2$的时候，这个倍数大约是3000，大概还是可以接受的。取样计算可以并行处理，因此可用的量子比特越多，耗时越短。考虑涉及50个量子比特以及具有一定线路深度的量子算法，也就是$N\sim 50^2$，我们可以粗略估计在中等规模系统上有效进行随机错误消除的参数范围，结果如图5所示。相较于容错量子计算，这个范围更加接近今天的实验技术水平。

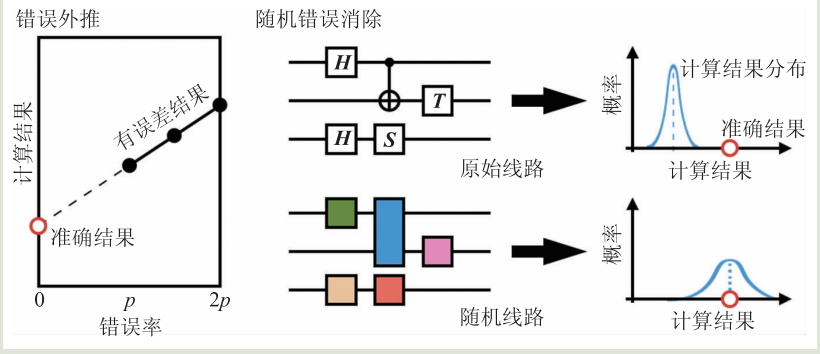


图7　量子错误缓解

7　结论

量子计算基于自20世纪初起经由大量实验验证的量子力学理论。它的计算方式不同于传统计算机。在量子计算中信息以量子叠加态的形式存储，并通过量子态的演化进行计算。量子计算机可以运行以肖尔算法为代表的量子算法，并且在解决某些计算问题方面，量子计算机可以远远快于经典计算机。

在量子计算机的物理实现方面，通过量子纠错可以解决退相干等因素导致的计算错误问题。使用量子纠错的首要条件是亚阈值操作，近年来的实验进展直接显示了这个条件是可以达到的。然而，进行密码破解规模的量子计算所需的量子比特数量巨大，成为了利用肖尔算法等量子算法的主要障碍。目前看来，超导量子比特和囚禁离子系统相较于其他系统具有一定优势。但鉴于到容错量子计算还有几个数量级的差距，很难说我们会在哪一种系统中最终实现通用量子计算机。

受限于现有技术所能提供的量子比特数量，中等规模量子计算有可能在近期内实现应用。我们可以利用量子错误缓解抑制计算错误，但仅能进行不需要大量操作的量子计算。量子变分算法能够在这些限制条件下运行，因此适用于中等规模量子计算，并且有希望解决某些经典计算机难以解决的量子化学和材料科学等研究中的重要问题。尽管如此，由于量子变分算法涉及到大规模参数优化并依赖于选取的尝试量子线路，我们还无法像肖尔算法一样严格从理论上证明其对经典算法的

优势。因此，在这方面还需要从理论上进一步研究量子算法，并在量子计算系统上对算法进行测试。

总之，量子计算是具有巨大潜在价值的颠覆性的科技发展方向，并且近年来在各方面都取得了快速发展。无论是远期的容错量子计算还是近期的中等规模量子计算，具有实用价值的量子计算机都需要一定数量的低错误率量子比特，当前的实验技术还无法完全满足条件。未来的发展既需要从理论上研究量子算法和错误处理方法，同时也需要实验技术在量子比特数量和错误率两方面的进步。这些工作需要踏踏实实的努力，并且要有十年磨一剑的信心和定力。

致　谢　感谢袁骁和张静宁两位博士提供参考文献和对部分表述的建议。

参考文献

[1] Richard F. Int. J. Theor. Phys., 1982, 21: 467
[2] Manin Yu I. Computable and Noncomputable. Sov. Radio, 1980. pp. 13-15
[3] National Academies of Sciences, Engineering, and Medicine. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press, 2019
[4] Deutsch D. Proc. Royal Soc. A, 1985, 400: 97
[5] Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. Cambridge University Press, 2010
[6] Deutsch D, Jozsa R. Proc. Royal Soc. Lond. A, 1992, 439: 553
[7] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press, 1994
[8] https://www.ncsc.gov.uk/information/quantum-key-distribution
[9] Lloyd S. Science, 1996, 273: 1073
[10] https://quantumalgorithmzoo.org/
[11] Sun C P, Zhan H, Liu X F. Phys. Rev. A, 1998, 58: 1810
[12] Duan L M, Guo G C. Phys. Rev. Lett., 1997, 79: 1953
[13] Zanardi P, Rasetti M. Phys. Rev. Lett. 1997, 79: 3306
[14] Viola L, Lloyd S. Phys. Rev. A, 1998, 58: 2733
[15] Viola L, Knill E, Lloyd S. Phys. Rev. Lett., 1999, 82: 2417
[16] Shor P W. Phys. Rev. A, 1995, 52: 2493
[17] Andrew S. Proc. Roy. Soc. Lond. A, 1996, 452: 2551
[18] Calderbank A R, Shor P W. Phys. Rev. A, 1996, 54: 1098
[19] Kitaev A Y. In: Proceedings of the Third International Conference on Quantum Communication, Computing and Measurement, edited by Hirota O, Holevo A S, and Caves C M. New York: Plenum Press, 1997
[20] Wang D S, Fowler A G, Hollenberg L C L. Phys. Rev. A, 2011, 83: 020302
[21] Bravyi S, Kitaev A. Phys. Rev. A, 2005, 71: 022316
[22] Knill E. Nature, 2005, 434: 39
[23] Fowler A G, Devitt S J, Jones C. Sci. Rep., 2013, 3: 1939
[24] https://www.dwavesys.com/d-wave-two-system
[25] Barends R *et al*. Nature, 2014, 508: 500
[26] https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html
[27] https://quantum-computing.ibm.com/
[28] Guo Q *et al*. Phys. Rev. Lett., 2018, 121: 130501
[29] Song C *et al*. arXiv: 1905.00320
[30] Gong M *et al*. Phys. Rev. Lett., 2019, 122: 110501
[31] Ye Y *et al*. Phys. Rev. Lett., 2019, 123: 050502
[32] Ballance C J *et al*. Phys. Rev. Lett., 2016, 117: 060504
[33] Gaebler J P *et al*. Phys. Rev. Lett., 2016, 117: 060505
[34] https://ionq.co/news/december-11-2018
[35] Lu Y *et al*. arXiv: 1901.03508
[36] Zhang S *et al*. arXiv: 1905.10135
[37] Kielpinski D, Monroe C, Wineland D J. Nature, 2002, 417: 709
[38] Dür W, Briegel H J. Phys. Rev. Lett., 2003, 90: 067901
[39] Li Y, Barrett S D, Stace T M *et al*. Phys. Rev. Lett., 2010, 105: 250502
[40] Li Y, Benjamin S C. New J. Phys., 2012, 14: 093008
[41] Nickerson N H, Li Y, Benjamin S C. Nat. Commun., 2013, 4: 1756
[42] https://nqit.ox.ac.uk/
[43] Knill E, Laflamme R, Milburn G. Nature, 2001, 409: 46
[44] Li Y, Humphreys P C, Mendoza G J *et al*. Phys. Rev. X, 2015, 5: 041007
[45] Wang X L *et al*. Phys. Rev. Lett., 2018, 120: 260502
[46] Nayak C, Simon S H, Stern A *et al*. Rev. Mod. Phys., 2008, 80: 1083
[47] Li Y. Phys. Rev. Lett., 2016, 117: 120403
[48] Albrecht S M. Phys. Rev. Lett., 2017, 118: 137701
[49] Preskill J. Quantum, 2018, 2: 79
[50] Peruzzo A *et al*. Nat. Commun., 2014, 5: 4213
[51] Li Y, Benjamin S C. Phys. Rev. X, 2017, 7: 021050
[52] McArdle S, Endo S, Aspuru-Guzik A *et al*. arXiv: 1808.10402
[53] Farhi E, Goldstone J. arXiv: 1411.4028
[54] Temme K, Bravyi S, Gambetta J M. Phys. Rev. Lett., 2017, 119: 180509
[55] Endo S, Benjamin S C, Li Y. Phys. Rev. X, 2018, 8: 031027
[56] Kandala A *et al*. Nature, 2019, 567: 491
[57] Song C *et al*. arXiv: 1812.10903
[58] McArdle S, Yuan X, Benjamin S. Phys. Rev. Lett., 2019, 122: 180501
[59] Bonet-Monroig X, Sagastizabal R, Singh M *et al*. Phys. Rev. A, 2018, 98: 062339