量子计算原理及研究进展

韩永建,李传锋,郭光灿

中国科学技术大学;中国科学院量子信息重点实验室,合肥 230026

摘要 量子计算机是量子力学与计算问题相结合的产物,是近几年的研究热点,引起了广泛的社会关注。本文回顾量子计算机的发展,介绍了量子算法和量子计算模型,并以离子阱和超导线路为例阐述了量子计算机的物理实现,然后介绍了为了克服消相干而发展出的量子编码,以玻色取样为例讨论了量子霸权。展望未来,近期内可以展示量子霸权,进而实现解决特定问题的量子模拟器,但是普适的量子计算机的研制仍然需要很长的时间。

关键词 量子计算;量子算法;量子编码;离子阱;超导线路

随着现代微电子加工技术的不断提高,电子线路的尺寸越来越小。当不同线路之间的距离达到原子尺寸时,电子在不同线路之间的隧穿将不可忽略,经典电子线路模型将不再适用。要研究电子在这种线路种的性质,需要使用量子力学。此外随着电子线路集成度的不断提高,散热成为一个关键问题。根据Landauer擦除定理,在不可逆过程中,热量与不可逆操作的规模密切相关:集成度越高,单位面积上产生的热量越多。在集成度很高时,如何散热成为电子线路的巨大挑战,处理不好就会将电路烧坏。基于量子力学基本原理的量子计算机,由于其计算的可逆特性,不会因非可逆操作带来热量。量子计算机不仅能解决经典计算机所面临的一些瓶颈问题,更重要的是,它原理上就不同于经典计算机,在解决某些困难问题时,相比经典计算机具有压倒性优势。

将量子力学和计算问题相结合的思想[1]是由费曼(Feynman)于1982年提出的,按照他的设想可以用标准量子系统(容易操控的系统)实现对复杂量子系统的模拟,进而解决经典计算机无法解决的量子问题,特别是量子多体物理问题(多体系统的希尔伯特空间随着系统尺寸指数增长,经典计算机无法有效处理)。虽然当时人们并不知道如何去实现这样一台量子模拟器,但费曼的这一思想直接影响了后来量子计算的发展。1985年,Deutsch[2]提出了量子图灵机的概念,它类似于经典图灵机在经典计算机中的角色。量子图灵机在理论上告诉人们存在普适的基于量子力学的模型来实现计算。简单来讲,经典计算机能够实现的计算功能也可以在量子模型下实现。那么,相对于经典计算,量子计算有什么特别的优势,1992年,Deutsch和Jozsa[3]给出了第一个量子算法(即Deutsch-Jozsa算法),在他们提出的这个问题中,量子计算相对于经典计算具有指数的加速。随后1993年Bernstein和Vazirani[4]以及Simon[5]均提出了以他们名字命名的量子算法。这些算法都表明在解决某些特定问题时量子计算机相对于经典计算机具有优势。然而这些特定问题都是人为设计出来的,不对应现实问题,其影响力还仅仅局限于学术圈内。

1 量子算法

是否能找到一个现实的问题,量子计算机比经典计算更优越呢?1994年,Shor[6-7]提出了著名的大数因子算法,这个算法表明量子计算机可以有效地求解大数因式分解问题。大数因式问题是指:给定一个整数Q,它是2个质数的乘积,找出这2个质数。此问题是一个NP问题(给一个问题的答案可以多项式时间内验证正确性),到目前为止,还没有找到有效的经典算法,最好的算法其复杂度也会随着问题的规模指数增长。更为重要的是,大数因式分解问题的复杂性是目前广泛使用的RSA密钥系统的理论基础,Shor算法不仅证明了量子算法的优越性,更动摇了现行的RSA密码系统的安全性基础。另一个非常重要的量子算法是Grover[8]在1996年提出的对无序数据库的搜索算法,这一算法的复杂度为$\frac{\pi}{4}\sqrt{N}$,而经典计算机的搜索复杂度是N(N为数据库的规模)。由于搜索算法本身的广泛性,Grover算法充分的表明了量子计算的优越性。这些量子算法,特别是Shor和Grover算法的提出体现了量子计算的强大计算能力,在国家安全和商业价值方面都具有极大的潜力。

收稿日期:2017-07-26;修回日期:2017-11-06

基金项目:国家重点研发计划项目(2017YFA0304100)

作者简介:韩永建,教授,研究方向为量子信息,电子信箱:smhan@ustc.edu.cn;李传锋(通信作者),教授,研究方向为量子信息,电子信箱:cfli@ustc.edu.cn

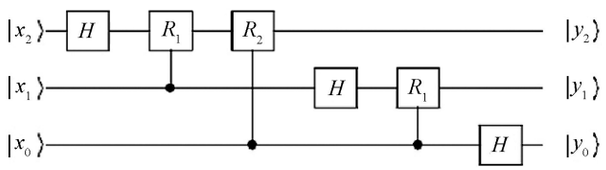
引用格式:韩永建, 李传锋, 郭光灿. 量子计算原理及研究进展[J]. 科技导报, 2017, 35(23): 70-75; doi: 10.3981/j.issn.1000-7857.2017.23.011

2 量子计算模型

量子图灵机为人们提供了量子计算的原始模型[2]。量子计算机除了和经典计算机有相似的计算模型以外,还有自身的一些新的计算模型。到现在为止,已有量子线路模型、One-way量子计算模型、绝热量子计算模型、量子随机行走模型以及拓扑量子计算模型。这些不同的量子计算模型的计算能力一致,可以相互转换,但在具体问题分析中,某些模型使用起来会更方便。

量子线路模型是和经典线路并行的模型,无论是它使用的语言还是构造方法都和经典计算相似,只需要将经典的逻辑门换成量子的逻辑门即可。一般来说,一个量子计算的过程,可以表示成整体系统的幺正变换(中间无测量,测量放到最后)。可以证明,任意系统的幺正变换都可以表示成两比特受控非门(CNOT)和单比特旋转门生成的组合,这个组合过程就是量子线路。所以,从量子线路的角度来看,只要能实现完美的两比特受控非门和任意的单比特旋转就可以实现普适的量子计算。不同的量子算法,对应于不同的量子线路,如图1表示实现3量子比特的量子傅里叶变换的线路图。量子线路模型的优点是可以借鉴经典计算线路的思想、概念和经验来设计新的量子算法。

量子计算的超强能力来自于量子态的超经典关联特性。如果能够大规模的制备拥有某种纠缠特性的量子态,就可以通过简单的单比特测量来实现普适的量子计算。这种有别于经典计算模式的计算方式称为One-way量子计算或基于测量的量子计算[9]。一般而言,使用具有某种拓扑结构(比如二维方格)的图态来实现普适的量子计算(并非任意图态都能实现普适量子计算,例如一维的图态就不适用)。图态本身具有某些非常好的量子特性,比如经过局域的测量之后,剩下的部分仍然是一个图态(可能需要做局域转动才会变成标准图态)。单比特测量的测量方式会依赖于前面其他单比特测量的结果。如果仅仅使用Clifford测量(例如Pauli算符测量),One-way量子计算的计算能力与经典计算机能力相当,无法完成普适的量子计算。非Clifford的测量在实现量子优越性的过程中起着关键性的作用。因而在实现量子计算的过程中,为了减少量子比特的数目,可以把Clifford测量的效果进一步编码到多体量子态的制备中去,图2显示了该计算过程。One-way量子计算是量子计算所特有的计算模型,对理解量子计算过程有非常好的作用。



x—输入比特;*y*—输出比特;*H*—*Hardamard*门;*R*—相位门

图1 3量子比特的量子傅里叶变换的线路

Fig. 1 Quantum circuit for three-qubit quantum Fourier transformation

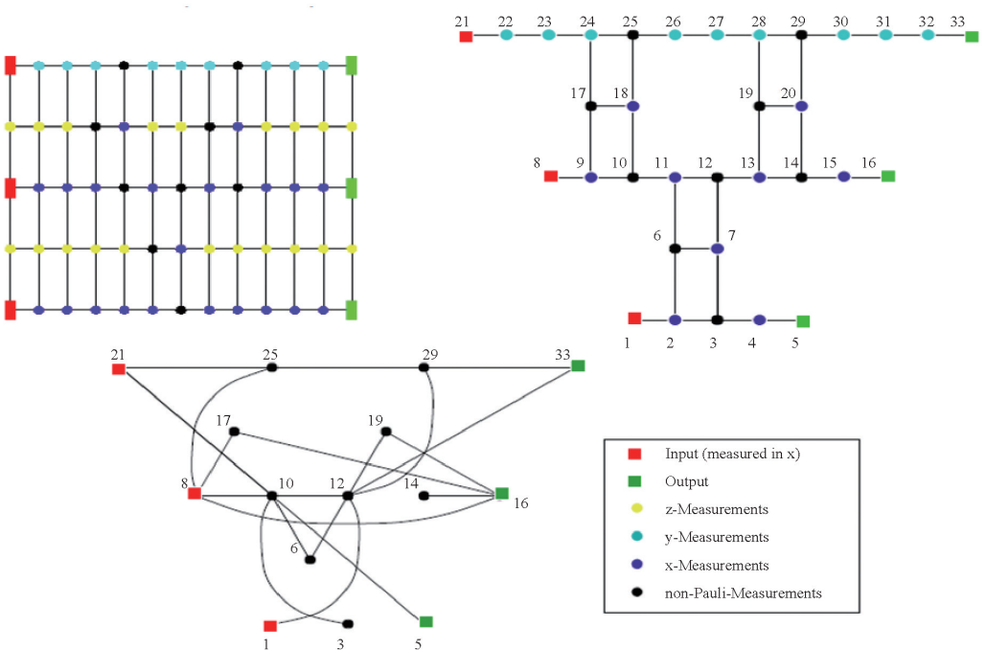


图2 3比特量子傅里叶变换的One-way算法

Fig. 2 One-way quantum algorithm for three-qubit Quantum Fourier transformaton

绝热量子计算模型也是量子计算特有的模型。这一计算模型基于量子绝热定理。量子绝热定理表明:如果量子系统初始处于该系统的基态,足够缓慢地变化系统的哈密顿量,系统如果有能隙保护将一直处于基态。哈密度量变化的速度将受限于能隙的大小。事实上,很多问题都可以映射到求解某个哈密顿量的基态问题上,特别是一些求极值的组合学问题可以非常方便地得到相应的哈密度量。然而这样的哈密顿量的基态通常都非常难于直接获得。量子绝热算法给出了一套获得一般哈密顿量的基态的方法[10]。在量子绝热模型中,系统初始哈密顿量的基态非常容易获得,将系统哈密顿量缓慢的从初始哈密顿量变到待求的哈密顿量,根据量子绝热定理,如果初始系统处于基态并且哈密顿量变化足够缓慢,则末态就是要求的基态。绝热量子计算的核心问题就变成了估计哈密顿量的能隙(计算时间由哈密顿量的变化快慢决定,而变化快慢是由整个过程中的哈密顿量的最小能隙决定的),由于实际问题对应的哈密顿量的复杂性(一般不具有平移对称性,相互作用也不是局域的),这是非常困难的任务。D-wave公司推出的超导系统量子计算装置就是基于绝热量子计算模型的。这一模型将一个量子计算的问题转化成了一个量子多体问题。对于量子多体问题,已有一些研究结果可以借鉴参考。反过来,也可以利用这样的量子计算机来研究一些复杂的多体物理问题。

拓扑量子计算模型也是量子计算中一个非常有意思的模型。在二维量子系统中,存在一种被称之为非阿贝尔统计的任意子,如果2个任意子之间进行了一次交换,它们的整体波函数就会做一个幺正变换。如果这种任意子还满足某种类型(比如Fabonacci型)[11],那么通过交换不同的任意子就可以实现普适的量子计算(图3示意通过Braiding来实现拓扑量子计算的过程)[11]。由于任意子统计本身的拓扑性质,这样

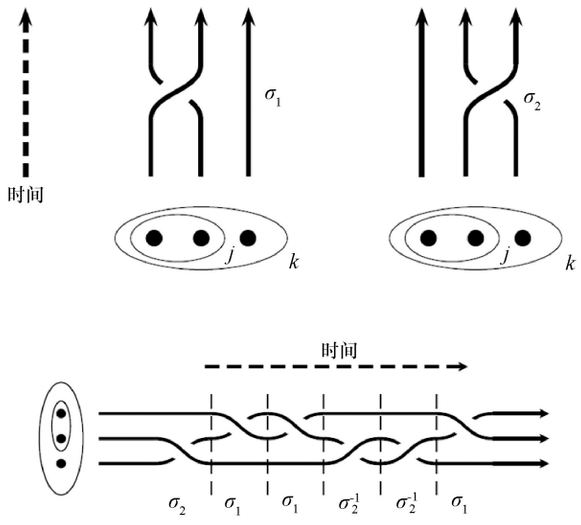


图3 拓扑量子计算示意

Fig. 3 Illustration of topological quantum computation

实现的量子计算天然具有对噪声的免疫性,是实现量子计算的理想载体。从这一模型出发,还可以直接的将量子计算与拓扑分类研究相联系[12],比如可以直接利用量子计算得到Jones多项式的一些值,进而可以研究拓扑分类。然而,要实现和操控这样的非阿贝尔任意子还远远超出了现阶段在固态系统中的能力。最有可能在实验中实现的非阿贝尔任意子是马约拉那任意子[13],但它的交换并不能实现普适的量子计算[14]。

3 量子计算机的物理实现

量子计算的优越性可以从Shor算法和Grover算法中得到充分体现。要实现这样的算法,必须要建立一台基于量子力学原理的计算机。什么样的系统才能够用来实现量子计算的功能,DiVincenzo在2000年提出了以他的名字命名的判据[15],主要包括以下要求。

1)系统由可扩展的量子比特组成。

2)量子比特的状态可以被有效初始化(例如制备到|0>态)。

3)可以可靠的实现一组普适逻辑门(比如两比特CNOT加上任意单比特旋转)。

4)相对于逻辑门操作时间,系统有长的相干时间。一般而言,要求在相干时间内能完成10^4个门操作,才能完成编码和纠错的过程。

5)可以对每个比特实施有效的测量。

6)可以在静止比特(即做计算的比特)和飞行比特(即用于信息传输的比特,一般是光子)之间进行转换。

最后一条并不包含在Divincenzo最初的判据中,这主要是为了将量子计算和量子通信相结合,或者是为了实施分布式的量子计算而加入的要求。

按照这一判据,哪些系统适合作为量子计算的载体?到目前为止,人们已经在各种系统(离子阱系统、超导系统、冷原子系统、量子点系统、光学系统、核磁共振NMR系统、稀土系统和里德堡原子系统等)上进行了探索和尝试,不少系统可以满足其中的某些要求,但还没有哪个系统能很好地满足所有要求。不同的系统都有自身的优缺点,如果可以把不同系统的优点组合在一起,就有可能实现真正的量子计算机。就目前的实验技术发展水平而言,离子阱系统和超导系统是最领先的,以这2个系统为例来说明量子计算的发展现状。

离子阱系统是最早用于量子计算的物理系统。一般的离子阱是将一串离子囚禁在线性阱中。每个离子的2个内能级形成一个量子比特。单比特操作可以通过激光作用在相应的离子上来实现。2个离子之间的受控非门(CNOT)可以通过2束激光作用在相应的2个离子上,在声子的协助下完成。DiVincenzo条件在离子阱中都可以在一定程度上实现,很多条件也已经在实验上得到了验证,具体如下。

1)人们已经在一维离子阱中实现了7比特的量子算法[16],10多个比特的量子态制备[17]和约300个离子的量子模

拟[18]。原则上,离子阱的可扩展性可以通过与芯片技术相结合来实现[19]。这方面的实验还在继续,可扩展性问题是基于离子阱系统的量子计算的主要障碍。

2)离子阱中的离子可以通过激光冷却来实现初态制备,单比特的初态制备实验误差已经可以小于10^{-3}[20]。

3)单比特操作的误差已可以低于10^{-6}[20],两比特的操作误差已低于10^{-3}[21]。这已经超过了实现普适容错量子计算的阈值(如果采用合适的编码,比如表面码,阈值约为10^{-2})。超快的单量子门操作时间已经可以达到50 ps[22],这一技术极大的提高了相干时间内能操作的量子门个数(已超过10^4的阈值)。这一技术正在被用于两比特的量子门。

4)离子阱中状态读出误差已可以低于10^{-4}[23]。

5)离子阱中的静止比特与光子(飞行比特)之间的量子态转化已在实验中实现[24]。

由此可以看出,除了可扩展性之外,离子阱系统已经对DiVincenzo其他条件进行了实验验证,而且都展现出了良好的特性。

超导线路是另一个非常有希望实现量子计算的系统,它与现有的微加工技术相结合可以很好地解决系统的可扩展问题。对应于DiVincenzo的判据,超导线路系统的表现如下。

1)9个比特的量子处理器已经获得了实验演示,可扩展性在此系统中没有原则性困难,且已部分获得实验支持。

2)利用反馈控制的比特初始化可以获得很好的效果[25]。

3)单比特操作的保真度已超过99.9%[26],2比特操作的保真度也已超过99.5%[26]。

4)相干时间在二维芯片上可达到约80 ms, 在三维芯片中可达约150 ms。

5)利用参数放大技术实现了保真度超过99%的量子状态读出[27]。

6)超导比特与飞行比特之间的转换还处于非常初期的阶段,仅演示了微波与光波之间的转换[28]。

由此可以看出超导系统也是一个非常有潜力的实现量子计算的系统。

4 量子编码

阻碍现普适量子计算的主要困难是量子系统的退相干特性。量子态本身非常脆弱,会不可避免地受到环境的影响,导致系统的退相干。而量子计算的优越性本身就来自于多体系统的相干特性,破坏相干性就破坏了量子计算的优越性。因而如何抵御退相干是实现量子计算的关键。

在经典计算中也会出错 ,即本来为0(1)的比特可能变成1(0),可以通过编码解决这一问题的。对于量子系统,可以将退相干看作是量子计算出错,也可以利用编码来解决。然而量子编码相对于经典编码有如下重大的不同。

1)单个量子态的出错方式有无穷多种,而经典计算的单比特出错方式只有2种。

2)经典比特可以通过测量来判断错误是否发生,而一般的量子测量会导致量子态的塌缩,进而破坏整个计算过程。

针对第一个问题,理论研究表明,任意的单比特错误都可以表示为2个不同错误:X(比特翻转)和Z(相位反转)的组合。这样就可以只考虑2种不同的出错了。对于第2个问题,为了在获取出错信息时不破坏对应的量子态,此量子态必须是获取信息的测量算符的本征态。这就要求仔细设计量子编码:既能获取出错信息又不破坏量子态的相干性。有鉴于此,Shor等[29-30]提出了著名的CSS码。在Shor的编码中,一个逻辑量子比特需要9个物理比特进行编码,在此编码中,2种不同的错误均能被发现并纠正。在Steane提出的编码中,一个逻辑比特需要7个物理比特来编码[30],也可以发现和纠正所有的错误。可以证明,如果要求编码比特能发现并纠正所有的错误,至少需要5个物理比特来编码一个逻辑比特。量子编码是利用编码的冗余来实现对出错的纠正。

然而,仅有量子纠错码,对实现量子计算还是远远不够的。因为除了环境导致的出错,量子操作,包括量子门操作、量子态制备和测量(特别是纠错过程中的测量)也存在操作误差。因此容错的概念被提出。一个编码被称为容错编码是指:在所有量子操作都可能出错的情况下,它仍然能够将整个系统纠回理想的状态。并非所有的量子编码都是容错的,例如上面提到的Steane码就不是容错的。但量子纠错码都可以通过适当增加量子比特将其改造成容错码。对于容错的编码,只要量子操作的出错率低于某个阈值,就可以把出错的量子态纠正回到它的理想状态去。直接利用容错编码实现量子计算需要极小的出错阈值,利用级联编码可以大大的降低要求。Knill等[31-32]最初的证明表明:实现容错量子计算的出错阈值约为10^{-4}~10^{-5}。后来,通过对编码和方法的改进将容错的阈值提高到0.03。然而Knill等[33]给出的这些阈值都没有考虑量子计算的实际实现问题,特别是没有考虑量子比特的空间排布问题,他们总是假设量子门可以作用在任意两个比特之间。Gottesman首先考虑了量子计算的实际构型问题,结果表明在实际的构型下容错量子计算仍然可以实现,但容错的阈值比Knill等最初考虑的情况要低。在一维或准一维的构型中,容错的阈值约为10^{-5}。对于二维的情况,人们发现如果利用表面码来编码比特,可以额外的获得拓扑保护,容错的阈值可以极大的提高。现阶段最好的阈值可以达到10^{-2}。实验上,现阶段离子阱和超导系统中的单比特操作以及两比特的实验精度都已达到容错量子计算的阈值。

容错量子计算虽然解决了量子退相干和实验操作误差的问题,但是极大地增加了实验实现量子计算机需要的量子比特规模。使得系统的可扩展性成为实现量子计算机的主要障碍。在可扩展性方面固体系统(超导系统,量子点系统等)具有天然的优势。因而解决非固体系统的可扩展性问题就非常重要。特别是前面提到的离子阱系统。离子阱系统在除了可扩展性问题以外的所有方面都非常适合做量子计

算机,而且它的门操作精度已经超过了实现普适的容错量子计算的阈值。为了解决可扩展问题,人们把离子阱技术与芯片技术相结合,将大量离子囚禁在芯片表面上,通过调节表面电极来移动不同阱中的离子,进而实现不同阱中离子之间的相互作用。表面离子阱现阶段的主要问题是在芯片表面有电场噪声,这些噪声会对离子进行加热。研究这种噪声的本质并降低这种噪声的影响是实现离子阱系统可扩展性的重要课题。将芯片放到低温系统或加强对芯片表面的处理都可以有效的降低噪声[34-35]。

5 量子霸权

尽管各个系统都取得了巨大进展,实现普适的容错量子计算仍然超出了现阶段的技术能力。那么在现有的技术条件下,是否可以体现量子计算的巨大威力?对某些特定的问题,并不需要量子编码过程,只需要几十个物理比特量子计算机(准确的说是专为解决具体问题而构建的量子模拟器,还不是普适的量子计算机)就可以超越现在的超级计算机的能力,这就是近期备受关注的量子霸权。玻色取样问题就是一个这样的问题。玻色取样问题可以描述如下[36-37]:给定m个输入模式,n个输入光子($n<m$)(图4),一个系统的幺正演化算符U,求这个装置的输出分布取样。

这个问题已经被证明是一个#p困难问题,其计算难度大于NP完全问题。对于这个问题,即使用中国最强大的超级计算机也无法处理$n>50$的情况。因而如果能够演示量子计算机在$n>50$的情况下仍能获得正确的结果,那么,在原理上就可以证明量子系统在解决玻色取样问题上相对于经典计算机具有压倒性优势。线性光学系统在演示玻色取样问题方面有其自身的优势。光学系统有非常好的相干性,对外界环境并不敏感,整个计算过程都不需要进行编码。当然,要实现多达50个光子的玻色取样仍然是一个巨大的挑战,它需要有高品质的单光子源和高效率的可分辨光子数的探测器。

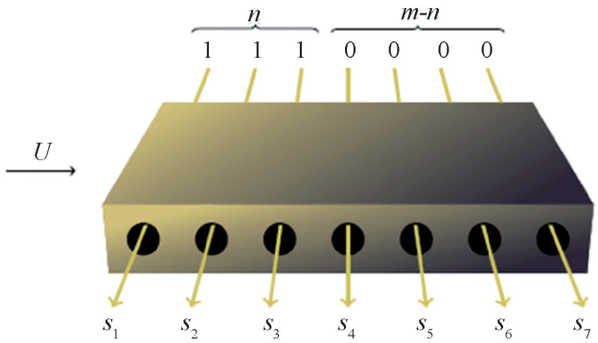


图4 玻色取样问题的示意

Fig. 4 Illustration of Boson sampling

6 结论与展望

实现普适的量子计算机仍然是一个长期的目标。在可以预见的未来几年内,有可能实现量子纠错码的错误探测,错误的纠正以及观察到逻辑比特相干时间的延长,实现量子计算的关键步骤。在未来的5~10年时间内有可能实现所谓的量子霸权,在玻色采样问题中的光子数超过50或者在量子退火算法中实现对经典计算机的超越。对于这些特定的问题,量子设备能够展现出其优越性。虽然到现在为止,还没有发现玻色取样在现实中的应用,但这种超越无论是在原理上还是在技术上都会对最终实现普适的量子计算机起到极大的推动作用。

参考文献(References)

[1] Feynman R P. Simulating physics with computers[J]. International Journal of Theoretical Physics, 1982, 21(6/7): 467-488.

[2] Deutsch D. Quantum theory, the Church-turing principle and the universal quantum computer[J]. Proceedings of the Royal Society A Mathematical Physical & Engineering Sciences, 1985, 400(1818): 97-117.

[3] Deutsch D, Jozsa R. Rapid solution of problems by quantum computation[J]. Proceedings of the Royal Society of London, Series A, 1992, 439 (1907): 553-558.

[4] Bernstein E, Vazirani U. Quantum complexity theory[C]//STOC '93: Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing. New York: ACM, 1993: 11-20.

[5] Simon D R. On the power of quantum computation[C]//Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science. Piscataway, NJ: IEEE, 1994: 116-123.

[6] Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring[C]//Proceedings of the 35th Annual IEEE Symposium on the Foundations of Computer Science. Piscataway, NJ: IEEE, 1994: 124-134.

[7] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Journal on Computing, 1997, 26(5): 1484-1509.

[8] Grover L K. Quantum mechanics helps in searching for a needle in a haystack[J]. Physical Review Letters, 1997, 79(2): 325-328.

[9] Raussendorf R, Browne D E, Briegel H J. Measurement based quantum computation on cluster states[J]. Physical Review A, 2003, doi: 10.1103/PhysRevA.68.022312.

[10] Farhi E, Goldstone J, Gutmann S, et al. Quantum computation by adiabatic evolution[J/OL]. [2017-04-30]. http://www.physast.uga.edu/~mgeller/quant-ph%200001106.pdf.

[11] Nayak C, Simon S H, Stern A, et al. Non-abelian anyons and topological quantum computation[J]. Review of Modern Physics, 2007, 80(3): 1083-1159.

[12] Pachos J K. Introduction to topological quantum computation[M]. Cambridge: Cambridge University Press, 2012.

[13] Xu J S, Sun K, Han Y J, et al. Simulating the exchange of Majorana zero modes with a photonic system[J]. Nature Communications, 2016, 7 (2): 13194.

[14] Xu J S, Sun K, Pachos J K, et al. Experimental simulation of Majorana-based quantum computation[J]. Quantum Physics, arXiv: 1702.08407.

[15] Divincenzo, David P. The physical implementation of quantum compu-

tation[J]. Fortschritte Der Physik, 2000, 48(9-11): 771-783.
[16]Nigg D, Müller M, Martinez E A, et al. Quantum computations on a topologically encoded qubit[J]. Science, 2014, 345(6194): 302.
[17] Monz T, Schindler P, Barreiro J T, et al. 14-Qubit entanglement: Creation and coherence[J]. Physical Review Letters, 2011, 106(13): 130506.
[18] Jurcevic P, Lanyon B P, Hauke P, et al. Quasiparticle engineering and entanglement propagation in a quantum many-body system[J]. Nature, 2014, 511(7508): 202.
[19] Chan M, Nicklason F, Vial J H. Scaling the ion trap quantum processor[J]. Science, 2013, 339(6124): 1164-1169.
[20] Harty T P, Allcock D T C, Ballance C J, et al. High-fidelity preparation, gates, memory, and readout of a trapped-ion quantum bit[J]. Physical Review Letters, 2014, 113(22): 220501.
[21] Ballance C J, Harty T P, Linke N M, et al. High-fidelity two-qubit quantum logic gates using trapped calcium-43 ions[J]. Physical Review Letters 2014, doi: 10.1103/PhysRevLett.117.060504.
[22] Campbell W C, Mizrahi J, Quraishi Q, et al. Ultrafast gates for single atomic qubits.[J]. Physical Review Letters, 2010, 105(9): 212-217.
[23] Myerson A, Szwer D, Webster S, et al. High-fidelity readout of trapped-ion qubits.[J]. Physical Review Letters, 2008, 100(20): 200502.
[24] Stute A, Casabone B, Brandstätter B, et al. Quantum-state transfer from an ion to a photon[J]. Nature Photonics, 2013, 7(3): 219.
[25] Ristè D, DiCarlo L. Digital feedback in superconducting quantum circuits[J/OL]. [2017-04-30]. http://lib-arxiv-008.serverfarm.cornell.edu/pdf/1508.01385v1.pdf.
[26] Barends R, Kelly J, Megrant A, et al. Superconducting quantum circuits at the surface code threshold for fault tolerance[J]. Nature, 2014, 508(7497): 500.
[27] Macklin C, O'Brien K, Hover D, et al. A near-quantum-limited Josephson traveling-wave parametric amplifier[J]. Science, 2015, 350(6258): 307-310.
[28] Regal C, Andrews R, Peterson R, et al. Bidirectional and efficient conversion between microwave and optical light[J]. Nature Physics, 2014, 10(4): 321-326.
[29] Calderbank A R, Shor P W. Good quantum error-correcting codes exist[J]. Physical Review A, 1995, 54(2): 1098-1105.
[30] Steane A M. Error correcting codes in quantum theory[J]. Physical Review Letters, 1996, 77(5): 793.
[31] Aharonov D, Ben-Or M. Fault tolerant quantum computation with constant error[J]. Quantum Physics, arXiv:quant-ph/9611025.
[32] Knill E, Laflamme R, Zurek W H. Resilient quantum computation: Error models and thresholds[J]. Proceedings Mathematical Physical & Engineering Sciences, 1997, 454(1969): 365-384.
[33] Gottesman D. Stabilizer codes and quantum error correction[J]. Thesis Preskill, 1997, arXiv: quant-ph/9705052.
[34] Labaziewicz J, Ge Y, Antohi P, et al. Suppression of heating rates in cryogenic surface-electrode ion traps[J]. Physical Review Letters, 2008, 100(1): 013001.
[35] Brownnutt M, Kumph M, Rabl P, et al. Ion-trap measurements of electric-field noise near surfaces[J]. Reviews of Modern Physics, 2015, 87(4), doi: 10.1103/RevModPhys.87.1419.
[36] Tillmann M, Dakic B, Heilmann R, et al. Experimental boson sampling [J]. Nature Photonics, 2012, 7(7):540-544.
[37] Spagnolo N, Vitelli C, Bentivegna M, et al. Experimental validation of photonic boson sampling[J]. Nature Photonics, 2013, 8(11): 6527-6532.

The principle and development of quantum computation

HAN Yongjian, LI Chuanfeng, GUO Guangcan

CAS Key Lab of Quantum Information, University of Science and Technology of China, Hefei 230026, China

Abstract Quantum computer is the combination of quantum mechanics and computing problem. It is a hot research topic of recent years and receives much attention from the society. In this paper we briefly review the principle and development of quantum computer. First, we introduce quantum algorithms and computing models, and explain physical implementation of quantum computer by taking ion trap and superconducting circuit as examples. Then we introduce quantum codes used to overcome decoherence. We also discuss quantum supremacy with Boson sampling as example. As we look into the future of quantum computers, we think quantum supremacy may be demonstrated in a few years and then quantum simulators to solve special problems. As for universal quantum computer, however, it may still need a long time.

Keywords quantum computing; quantum algorithm; quantum code; ion trap; superconducting circuit

（责任编辑　刘志远）