美国《量子计算：进展与前景》报告概要

● 李利　欧阳伟　杜晓梅[译]
江南计算技术研究所 无锡 214083

摘要：
2018年12月4日，由来自美国国家科学院、工程院和医学院的13位知名量子计算专家组成的一个专家委员会，公布了一份长达205页的《量子计算：进展与前景》报告，概述了量子计算的原理、优势与缺陷，客观地评估了量子计算的进展、风险及前景，给出了相关研究结论和建议，本文为该报告的概要部分。

关键词：量子计算，量子位，量子纠错，量子霸权，Shor算法

量子力学属于物理学的子领域，它描述极小粒子的行为，为新的计算范式奠定了基础。量子计算（QC）最初是在20世纪80年代作为一种改进超小型（“量子”）物理系统计算建模的方法而提出的。上世纪90年代，随着Shor算法的出现，人们对该领域的兴趣不断增长。如果Shor算法在量子计算机上实现，其将以指数方式加速一类重要的密码分析，从而潜在地威胁到某些用于保护政府和民用通信及存储数据的加密方法。事实上，量子计算机是唯一已知可比当今计算机快指数级的计算模型。虽然这些结果在20世纪90年代非常令人振奋，但它们只是理论上让科学家感兴趣：没有任何人知道如何构建一台量子计算机系统。大约25年后的今天，人们在创建和控制量子信息位或称“量子位（qubit）”方面取得了显著进展，许多研究组织已经演示了小规模的原理验证型量子计算机。这一进步重振了该领域，并吸引了大量的私营部门投资。

1. 为什么制造和使用量子计算机具有挑战性

传统计算机使用位（比特）来表示它正在运算的值；量子计算机则使用量子比特或量子位（qubit）。一个位可以是0或1，而量子位可以同时表示值0、1或两者的组合（称为“叠加”态）。传统计算机的状态是由一组位的二进制值确定，而在任何一个时间点，具有相同数量量子位的量子计算机的状态可以跨越相应传统计算机的所有可能状态，因此可在一个呈指数级增加的问题空间中工作。然而，利用这个空间的能力必须要求所有量子位本质上相互连接（称为“纠缠”），与外部环境完全隔离，并且能非常精确地控制。

在过去的25年中，许多创新技术使得研究人员可以构建能逐步为量子计算提供所需隔离与控制的物理系统。2018年，在大多数量子计算机中使用了两种技术（由超导电路产生的囚禁离子和人造“原子”），但是针对量子位基本物理实现（或称“物理量子位”）的许多不同技术当前也都正处于探索之中。虽然该领域进展迅速，但仍需要重大改进，现在就“投注”于量子计算的一种技术还显得为时过早。

即使能够制造出很高质量的量子位，要成功创建和使用量子计算机还是会面临一系列新的挑战。它们使用与传统计算机完全不同的运算，需要新的算法、软件、控制技术和硬件抽象。

2. 技术风险

（1）量子位在本质上无法杜绝噪声

传统计算机和量子计算机之间的主要区别之一，就在于如何处理系统中不需要的小偏差，或称“噪声”。一个传统的位不是1就是0，即使该值稍有偏差（即系统中有些噪声），该信号上的运算也能很容易地消除噪声。实际上，目前在位上运算并被用来创建计算机的传统门具有非常大的噪声容限，它们可以摒弃输入中较大的偏差，仍然可以生成干净、无噪声的输出。由于量子位可以是1和0的任意组合，所以量子位和量子门不能很容易地杜绝物理电路中发生的小错误（噪声）。其结果就是，创建所需量子运算时的小错误或是任何进入物理系统中的杂散信号，最终都可能导致计算中出现错误

的输出。因此，对于在物理量子位上运行的系统，最重要的设计参数之一就是其错误率。低错误率很难实现，即使到2018年，在具有5个以上量子位的系统上进行2量子位运算的错误率也超过了数个百分点。较小规模的系统有着更低的错误率，但是量子计算要想取得成功，就要把这种更好的运算保真度转移到更大规模的量子位系统上。

（2）无错（Error-Free）量子计算机需要量子纠错

尽管物理量子位运算对噪声敏感，但是可以在物理量子计算机上运行量子纠错（QEC）算法来模拟无噪声或“完全纠错的”量子计算机。没有量子纠错，就不可能有复杂的量子程序（例如一个实现Shor算法的量子程序）能在量子计算机上正确地运行。然而，量子纠错会在两个方面产生显著的开销：一是为了模拟更可靠和稳定的所谓“逻辑量子位”所需的物理量子位数量；二是为了模拟逻辑量子位上的运算而必须在物理量子位上执行的原始量子位运算量。所以，尽管量子纠错对于未来创建无错误的量子计算机至关重要，但短期内它们由于资源消耗太密集而无法使用；近期的量子计算机很可能都会有错误。这类机器被称为“嘈杂中型量子（NISQ）计算机”。

（3）量子计算机无法高效地加载大量数据输入

虽然量子计算机可用少量量子位来表示呈指数级增长的数据，但目前还没有一种方法可将大量的传统数据快速转换为量子态（如果数据能用算法生成，则不受此限制）。对于需要大量数据输入的问题，创建输入量子态所需的时间通常会占用绝大部分计算时间，并大幅减少量子优势。

（4）量子算法的设计非常困难

测量量子计算机的状态会使大规模量子态“崩塌（collapse）”成为一个传统的结果。这意味着人们从量子计算机中提取的数据量，只等同于从相同规模的传统计算机中提取的数据量。为了发挥量子计算机的优势，量子算法必须利用干扰和纠缠等独特的量子特征来得出最终的传统结果。因此，实现量子加速需要全新的算法设计原则和非常精巧的算法设计。量子算法开发是该领域一个极为关键的方面。

（5）量子计算机需要一种新的软件栈

对于所有计算机而言，建造一台有用的设备都要比仅仅发明硬件复杂得多——人们需要工具来创建和调试量子计算机专用的软件。由于量子程序与传统计算机程序不同，因此需要进一步研究和开发软件工具栈。由于软件工具能推动硬件发展，因此同时开发硬件和软件工具链可有效缩短实用量子计算机的研发时间。事实上，使用早期工具来完成端到端设计（应用设计到最终结果）有助于阐明隐藏的问题并推动设计获得整体成功，这也是传统计算机设计中所采用的方法。

（6）量子计算机的中间状态无法直接测量

调试量子硬件和软件的方法至关重要。目前，传统计算机的调试方法依赖于内存和读取机器的中间状态。对于量子计算机，这两者都是不可能的。量子态不能简单地复制（根据所谓的“无克隆”定理）以供后续检查，并且任何对量子态的测量都会使其崩塌成一组传统位，从而使计算终止。新的调试方法对于开发大规模量子计算机至关重要。

3. 实现量子计算的时间表

预测未来总是有风险的，但是当感兴趣的产品相比当前设备并不跨越太多数量级时，则可以尝试预测未来。然而，要创建一台能够运行Shor算法以在1024位RSA加密消息中查找私钥的量子计算机，则需要制造一台比现有机器大五个数量级，且错误率好两个数量级的机器，此外还要开发软件环境来支持这台机器。

填补此差距所需的进展使得人们无法预测实现大型纠错量子计算机的时间表，而且尽管这些领域正在不断取得重大进展，但仍无法保证能够克服所有挑战。在弥补这一差距的过程中，还可能会暴露出意料之外的挑战，需要尚未被发明的技术，或是由于基础科学研究出现新成果而改变人们对量子世界的理解。该委员会没有推测给出一个具体的时间表，而是确定了将会影响技术创新速度的相关因素，并提出了用于监测本领域之进展的两个衡量指标和若干里程碑。

鉴于量子计算机的独有特性和挑战，它们不太可能直接取代传统计算机。事实上，它们需要许多传统计算机来控制它们的操作并执行量子纠错所需的计算。因此，它们目前被设计作为与传统处理器互补的专用设备，类似于协处理器或加速器。

在快速发展的领域，往往存在着许多未知和难题，其整体发展的速度取决于整个业界利用新方法和提出新见解的能力。而在那些研究结果保密或设有专利限制的领域，进展则要缓慢得多。幸运的是，许多量子计算研究者一直在公开分享他们的最新进展，这一理念将使该领域受益匪浅。

重要结论：一个可以实现思想和群体自由交流的开放生态系统，将会推动技术的快速发展。

众所周知，某一技术的进步取决于投入其中的人力和资本。虽然许多人认为会有一个类似于摩尔定律的法则适用于系统中量子位数量的扩展，但

务必记住的是，摩尔定律是从良性循环中产生的：技术进步产生了指数级增长的利润，促进了对研发（R&D）的再投资，吸引了新的人才和行业加入创新，从而又将技术提升至更高一级。如果像硅工业一样，类似于摩尔定律的量子位持续指数级增长需要指数级增加的投资，那么就需要量子计算机有类似的良性循环来维持这种投资，即让小型机器取得足够的商业成功以吸引增加对整个领域的投资。如果没有可以产生商业利润的中间进展，那么就只能依靠政府机构不断地增加对该领域研究的资助。即使在这种情况下，成功实现中间里程碑也是极为重要的。

鉴于量子纠错的开销，近期的机器几乎肯定都是嘈杂中型量子（NISQ）计算机。尽管大型纠错量子计算机会有许多令人感兴趣的应用，但对于NISQ计算机而言，目前并没有实际的应用。为NISQ计算机创建实际应用是一个相对较新的研究领域，需要开发新型量子算法。到2020年初为NISQ计算机开发出商业应用，对于启动良性投资循环至关重要。

重要结论：研究和开发NISQ计算机的实际商业应用是该领域亟待解决的问题。这项工作的成果将对大规模量子计算机的发展速度和量子计算机商用市场的规模和稳健性产生深远影响。

量子计算机一般可以分为三大类。“ 模拟量子计算机 ”直接操控量子位之间的相互作用，并且不会将这些动作分解为原始的门操作。模拟量子计算机包括量子退火器、绝热量子计算机和直接量子模拟器等。“ 数字NISQ计算机 ”通过在物理量子位上使用原始的门操作来执行感兴趣的算法。这两种类型的机器都存在噪声，这意味着其质量（以误差率和量子位相干时间测量）将制约它们所能解决问题的复杂度。“ 完全纠错型量子计算机 ”是一种基于门的量子计算机，由于部署了量子纠错（QEC）而更加鲁棒，使得有噪声的物理量子位能够模拟稳定的逻辑量子位，从而保证了这类计算机能够可靠地进行任何计算。

4. 里程碑

量子计算发展的第一个里程碑是模拟和数字系统的简单理论验证。小型的数字NISQ计算机于2017年问世，拥有数十个量子位，其错误率高到无法校正。量子退火研究工作大约在十年前就开始了，采用一种相干时间较低但可以更快速扩展的技术来构建量子位。因此，到2017年，实验性量子退火器已经发展到具有大约2000个量子位。以此为起点，量子计算的进展可以用几个可能的里程碑来划分。其一是证明“ 量子霸权 ”，即完成一项在传统计算机上难以处理的任务，无论该任务是否具有实用性。虽然有几个团队致力于实现这一目标，但都未能得到证实（截至2018年中）。另一个重要的里程碑是创建一台具有商业价值的量子计算机，这要求量子计算机能比任何传统计算机更有效地执行至少一项实际任务。尽管理论上后一个里程碑比实现“ 量子霸权 ”难——因为其应用必须比现有传统方法更好、更有用——但实际上，证明“ 量子霸权 ”更不容易，尤其是对于模拟量子计算而言。因此，在证明“ 量子霸权 ”以前，很可能就会出现一种有效的应用。在量子计算机上部署量子纠错，以创建错误率显著降低的逻辑量子位，是又一个重要的里程碑，也是创建完全纠错系统的第一步。

5. 度量标准

基于门的量子计算进展可以通过跟踪确定量子处理器质量的关键属性来进行监控，这些属性包括：单量子位和双量子位运算的实际错误率、量子位之间的连通性，以及单个硬件模块中包含的量子位数量。

重要结论：基于本委员会目前获得的信息，现在要预测可扩展量子计算机出现的时间表还为时尚早。不过，短期内的进展，可以通过监控在恒定的平均门错误率下物理量子位的扩展速度来了解，其扩展速度使用随机的基准测试进行评估；而长期的进展，则可以通过监控一个系统的逻辑（纠错）量子位有效数量来跟踪。

跟踪逻辑量子位的规模和扩展速度能让人们更好地预估未来里程碑出现的时间点。

重要结论：如果研究界都采用明确的报告规范，以实现不同设备间的比较，并能转化成如本报告中所提出的度量标准，那么就能更容易地监控该领域的发展状况。一套能够在不同机器之间进行比较的基准测试应用有助于提高量子软件的效率并改进底层量子硬件的架构。

6. 构建和使用量子计算机的参与方

显然，全世界都在努力开发量子计算机和其它量子技术。要开发出一台成功的量子计算机，必须进行规模庞大、协调一致的研究工作，以实现基础科学的进步和工程领域的新策略，这将横跨多个传统学科。

重要结论：虽然一直以来美国都在开发量子技术方面发挥着领头作用，但量子信息科学和技术现在已成为一个全球性领域。鉴于除美国之外的多个国家最近都确定了对该领域的巨额投资，美国要想保住其领先地位，持续的国家支持至关重要。

此外，私营企业目前在美国量子计算研发的生态系统中也发挥着很大的作用。

重要结论：如果近期量子计算机无法取得商业上的成功，为了防止量子计算研发的大幅萎缩，政府的投资就会变得至关重要。

7. 量子计算机与密码技术

密码技术依靠难以计算的问题来保护数据，量子计算将对其产生重大影响。对于用来保护几乎所有因特网通信和加密存储数据的非对称密码，在大型量子计算机上运行的Shor算法将大幅减少从中提取私钥所需的计算。在这样的量子计算机出现之前部署后量子密码技术，具有极高的商业价值。企业和政府都无法承受未来其私密的通信被解密，哪怕是在30年以后。鉴于此，必须尽可能快地启动向后量子密码技术过渡，要知道仅仅是作废现有Web标准，就需花费超过十年的时间。

重要结论：鉴于量子计算目前的状态和近期的发展速度，未来10年内，基本不可能出现能破解RSA 2048或类似基于离散对数的公钥密码系统的量子计算机。

重要结论：即使还要十多年后才会出现能够破解当前密码的量子计算机，其危害也是足够严重的，而过渡到新安全协议的时间漫长且充满着不确定性，因此优先开发、标准化和部署后量子密码技术，对于最大限度地降低潜在安全威胁和隐私灾难是至关重要的。

鉴于量子计算机使现有协议面临严重危险，人们正在积极研发后量子密码技术，即量子计算机无法破解的非对称密码。这些技术有可能在本世纪20年代实现标准化。在早期的量子计算研究中，利用Shor算法潜在地破解现有密码是一个主要推动因素，但是抗量子密码算法的存在将降低量子计算机对密码分析的效用，因此从长期来看，它将减小密码破译对量子计算研发的推动作用。

8. 追求量子计算的风险和效益

研制实用的量子计算机仍然面临着重大的技术障碍，而且不能保证这些障碍一定会被克服。构建和使用量子计算机，不仅需要先进的器件工程，还需要在多个融合科学领域取得根本性进展，包括计算机科学、数学、物理学、化学和材料科学等。这些努力都会带来潜在的益处。例如，量子计算的研发成果已经促进了物理学（如量子引力领域）进步；通过量子算法研究，推动了传统计算机科学进步。

重要结论：量子计算对于推动基础性研究非常有价值，从而有助于促进人类对宇宙的理解。与所有基础科学研究一样，该领域的发现会带来变革性的新知识和新应用。

构建大型纠错量子计算机的挑战十分巨大。成功的量子计算需要对量子相干性进行前所未有的控制，实现这一点需要改进现有工具和技术，或开发全新的工具和技术。同样依赖于量子相干性控制的其它技术，例如量子传感和量子通信等，也将受益于这些进步。

重要结论：虽然大规模量子计算机的可行性尚不确定，但开发一台实用量子计算机的努力仍将带来重大好处，并且会持续溢出至量子信息技术的其他近期应用，例如基于量子位的传感技术等。

除了知识和潜在的社会效益之外，量子计算也会影响国家安全。任何一个拥有大规模实用量子计算机的实体都可以破解当今的非对称密码系统，这是一项重大的信号情报优势。意识到这种风险，促使人们致力于开发和部署能够对抗量子密码分析的加密系统，目前已经有几种方案被认为能够实现量子安全。但是，在政府和民用系统中部署后量子密码技术只能保护后续的通信，却无法消除之前已被敌方所截获加密数据被破解的安全风险，尽管其风险程度会随着有能力运行Shor算法的量子计算机姗姗来迟、数据变得不那么相关而逐渐减弱。此外，新的量子算法或工具会带来新的量子密码分析技术；与网络空间安全一样，后量子可恢复性（弹性）也需要持续的安全研究。

但是，国家安全问题超越了密码学。更大的战略问题是未来的经济和技术领导力。从历史上看，传统计算曾对社会产生变革性影响。尽管将量子算法用于工业和研究应用的探索才刚刚开始，但量子计算显然具有超越当前计算边界的潜力。量子计算有望能够提高多个计算领域的效率，因此在美国支持建立一个强大的量子计算研究社区具有战略价值。

9. 结束语

基于对迄今为止量子计算领域进展的公开信息评估，该委员会认为原则上并没有根本性的原因阻碍构建一台大型容错量子计算机。然而，要建立这样一台系统并将其部署到实际应用中，依然存在着巨大的技术挑战。此外，未来的投资决策不仅要看美国和全球研究社区的力量和开放性，还取决于能否实现近期成功和商业应用，这些都将影响在公开领域创建实用量子计算机的时间表。不论大型量子计算机何时出现或者是否会出现，对量子计算和量子技术的持续研发都将拓展人类科学认知的边界，那些尚未收获的成果将会改变我们对于宇宙的理解。

参考文献：
[1] R.P. Feynman, 1982, “Simulating physics with computers.” International journal of theoretical physics 21, no. 6-7: 467-488.
[2] S. Lloyd, 1996, “Universal quantum simulators.” Science: 1073-1078.
[3] E. Bernstein and U. Vazirani, 1993, “Quantum complexity theory. In Proceedings of the twenty-fifth annual ACM symposium on Theory of computing (STOC ‘93). ACM, New York, NY, 11-20. DOI=http://dx.doi.org.stanford.idm.oclc.org/10.1145/167088.167097
[4] P. Kaye, R. Laflamme, and M. Mosca, 2007, An introduction to quantum computing. Oxford University Press.
[5] M.A. Nielsen and I. Chuang, 2002, “Quantum computation and quantum information” Cambridge University Press: 558-559.
[6] D. Simon, 1997, “On the power of quantum computation.” In Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on, pp. 124-134. IEEE, 1994. SIAM journal on computing 26, no. 5: 1474-1483.

要闻集锦

HPE以13亿美元价格收购超级计算机制造商Cray

HPE近日宣布，已经以13亿美元的价格收购了Cray，这一举措有望将HPE推向不断增长的超级计算市场的前沿。

13亿美元的价格相当于每股35美元，比Cray的周四收盘价溢价17%。这次收购也是HPE自2015年从惠普公司分拆出来成为独立公司以来的最大一笔收购。

Cray由超级计算机行业开创者Seymour Cray于1972年创立，迄今为止打造了很多全球最快超级计算机TOP500榜单中的多套超级计算机。最近Cray还在美国政府推动的“百亿亿次级”计算项目中发挥了关键作用。

Cray目前正在为美国能源部建设两个百亿亿级超级计算机系统，第一个将耗资5亿美元，服务于位于芝加哥的阿贡国家实验室，第二台超级计算机预计耗资6亿美元，将为橡树岭国家实验室的研究人员提供1.5exa-flops的性能。

HPE在百亿亿级超计算机领域看到了巨大的收入机会。HPE在收购公告中表示，预计未来5年将有超过40亿美元的百亿亿级项目。反过来，高性能计算市场规模将从2018年的280亿美元增长到2021年的350亿美元。

Moor Insights＆Strategy总裁兼首席分析师Patrick Moorhead表示：“高性能计算是增长最快的市场之一，HPE已经表达了在了这个市场中做得更好的意图。所以对这次收购我并不感到惊讶，收购能否成功取决于两家厂商的整合。”

除了Cray的客户群和人才之外，此次收购还将为HPE带来一系列超级计算技术。Cray开发了一种名为Shasta的计算机体系结构，专门用于百亿亿级超算系统。此外，Cray还出售一种名为Slingshot的超级计算机优化网络技术，以及存储设备和人工智能软件等产品。

HPE本身对高性能计算市场也并不陌生。HPE已经为匹兹堡超级计算中心和世界上最大的化学品生产商巴斯夫集团等组织打造了超级计算机系统。

Moorhead表示：“HPE带来了更大的规模和一些独特的消费模式，Cray则带来了专业知识和独有的接入IP。”

HPE表示，完成收购收购会之后将向GreenLake产品阵容中增加一系列新的高性能计算产品，这将让企业能够以付费即用的方式购买高性能计算硬件，此外HPE还计划推出针对人工智能工作负载优化的高性能计算解决方案。

（陈继军）