科学通报 2016 年 第 61 卷 第 4-5 期：404 ~ 408

《中国科学》杂志社
SCIENCE CHINA PRESS

Science125个科学前沿问题系列解读(II)

What are the limits of conventional computing?

计算的极限

季铮锋[①②*]，夏盟佶[①*]

① 中国科学院软件研究所计算机科学国家重点实验室，北京 100190;

② Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L3G1, Canada

* 联系人, E-mail: jizhengfeng@gmail.com; mingji@ios.ac.cn

2015-12-07 收稿, 2016-01-04 修回, 2016-01-06 接受, 2016-01-25 网络版发表

摘要 计算深刻地影响着人们的日常生活和生产活动，也推动了诸多其他科学领域的发展和变革. 本文从几个不同的方面探讨计算的能力和极限. 从计算的模型和丘奇图灵论题，到P和NP问题的深远影响及量子计算对传统计算的冲击，我们深入讨论了对计算极限的理解.

关键词 图灵机，丘奇图灵论题，量子计算，大数分解，量子模拟

小学课堂上，学生们正在学习加减乘除四则运算. 奔波的旅途中，车内的GPS导航引导驾驶员以最短路径驶向目的地. 国家超级计算中心的机房里，“天河二号”超级计算机正在进行C919客机的高精确度空气动力学参数的运算. 在这些景象的背后，计算无处不在，悄无声息地改变着人们的生产生活方式. 与此同时，计算机科学在理论和技术2个方面向其他包括天文、地理、气象、生物、物理、材料等学科输出其特有的方法、观点和强大的工具，推动了整个科学研究的高速发展.

计算如此重要，那什么是计算呢？有趣的是，早在20世纪30年代，在电子计算机诞生之前，这个问题就已经有了完满的回答. 很多种后来被证明为等价的关于计算的模型被相继提出，其中包括递归函数、λ演算、图灵机等.

由于图灵机的定义最为直观，最类似人类进行计算的方式，图灵机作为计算理论模型被广泛接受. 一条可读写符号的无限长的带子，一组有限的转移规则就定义了一个图灵机. 图灵机读入符号，根据当前机器状态，移动读写头，写入符号，进入新的状态，并循环反复这一过程，直至机器进入停机状态，从而得到计算结果. 值得指出的是，图灵机定义中符号集合、状态集合、规则集合都是有限的，只有带子是无限长的. 图灵机的有限可描述的性质让我们可以对图灵机进行编码，对应到特定的自然数.

著名的丘奇图灵论题说如果一个问题在某个合理的计算模型下可计算，那么它在图灵机上也是可计算的. 这一论题奠定了用图灵机作为计算理论模型的地位. 由于不存在关于“合理”模型的准确定义，因此这一论题是无法证明、只可证伪的. 迄今为止，所有提出的合理的计算模型都符合这个论题.

1 计算的极限之外：停机问题

有了严格的计算的定义，首先要问的关于计算极限的问题就是是否所有问题都可以计算. 图灵机所定义的计算概念是一种特定方式的有限的描述对无限的驾驭——通过有限的规则计算一个无穷定义域上的问题. 有限的规则，只有可数无穷多个，而问题有不可数无穷多个，所以必然存在不可计算的问题. 著名的图灵停机问题就是一个例子. 设输入实例是自然数x，这个问题问编码为x的图灵机计算输入x时是否停机. 这个结论可以用康托对角线方法证明，

引用格式: 季铮锋，夏盟佶. 计算的极限. 科学通报, 2016, 61: 404–408
Ji Z F, Xia M J. The limits of computation (in Chinese). Chin Sci Bull, 2016, 61: 404–408, doi: 10.1360/N972015-01363

与罗素悖论也有自然的联系.

图灵机有一个重要性质, 存在通用图灵机. 一个图灵机是一组有限的规则, 可以编码成有限长度的字符串. 通用图灵机, 可以机械地读懂任何图灵机编码, 从而模拟编码所对应的图灵机的计算.

2 计算的效率

计算能力的极限, 一方面有停机问题这种不可计算的问题的极限限制, 另一方面, 是算法解决计算问题时的效率. 但是这里的效率不是现代的通用计算机每秒钟可以运算多少次, 而是所需的计算资源与问题实例的编码长度之间的关系. 最常见的计算资源是时间和空间, 分别是图灵机的运算步数, 和使用的带子格子数目. 如果一个算法时间复杂度是n^2, 就是说它计算任何长度为n的实例, 最多需要n^2步.

理论计算机科学家认为, 多项式时间是衡量计算是否有效的合理标准. 太慢的算法, 例如, 指数时间算法, 在不太大的输入长度n的时候, 计算时间2^n就会指数爆炸而无法在实际中使用. 另一方面, 同样一个问题, 在图灵机上可能需要n^3时间, 在随机访问模型下可能只需要n^2时间. 用多项式时间衡量有效性避免了计算模型相关性. 所有存在多项式时间算法的判定问题构成的集合记为P. 丘奇图灵论题可以扩展到有效计算的情形. 扩展版的丘奇图灵论题说, 如果一个问题在某个合理的计算模型上有多项式时间的算法, 那么它在图灵机上也有多项式时间算法. 虽然还没有定论, 但是量子计算已经对这个扩展论题发出了挑战.

3 有效计算的未知极限: NP完全问题

P和NP问题是计算机科学中最广为人知的问题, 也是一个深刻的数学问题. 粗略地讲, NP是可以有效验证的问题类. 对一个问题和一个可能的解答, 如果有一个图灵机可以在多项式时间内验证解答的真伪, 那这样的问题就属于NP.

等价地, NP也是多项式时间不确定型图灵机所能计算的问题类. 不确定型图灵机的每一步计算有2种可能选择, 它计算一个问题只要存在一个不确定选择的序列完成这一计算. 这种不确定选择的能力可以用来猜到一个解. 也正因为这种能力, 我们无法物理上造出这样的图灵机, 也不认为它是合理的计算模型, 不认为它打破了扩展版的丘奇图灵论题.

对很多NP中的问题, 可以使用归约的方法证明, 如果它们中有一个问题有多项式时间算法, 那么所有的NP问题都有多项式时间算法. 这类问题被叫作NP完全问题, 目前已知的NP完全问题有成千上百个, 几乎遍布各个计算机科学的研究领域. NP完全问题是否存在多项式时间算法, 也就是P和NP问题, 被克雷数学研究所在千禧年大奖难题中收录, 列为七大问题之一. 这个问题在理论计算机科学复杂性研究中具有核心地位, 是认识计算极限的核心问题.

4 突破计算极限的新方向: 量子计算

量子信息与量子计算研究基于量子力学原理的信息处理和计算方法, 是探索物理可实现计算能力极限的新方向. 本文后半部分介绍量子计算理论领域的新进展, 重点讲述量子计算研究带给我们在计算极限方面的认识和启示.

如果说比特是经典信息的基本单位, 那么量子比特则是量子信息的基本单位. 一个经典比特要么是0, 要么是1, 一个量子比特可以是0和1的量子叠加. 更加数学地, 一个量子比特所处的叠加态可表示为$\alpha|0\rangle+\beta|1\rangle$. 其中$\alpha$, β称为概率振幅, 分别描述0和1的权重, 满足$|\alpha|^2+|\beta|^2=1$. 量子叠加与概率凸组合有2点本质的区别. 首先, 量子叠加中的概率振幅可以是负数或者复数, 而概率组合中的概率总是非负的实数, 正的和负的概率振幅可以叠加相消. 其次, 量子叠加的概率振幅按照2范数归一化的向量, 而概率组合是按照1范数归一化的向量.

理解量子叠加对深入理解量子计算的能力有着重要的意义. 如果$|0\rangle$, $|1\rangle$是2个可能的量子状态, 那么根据量子叠加原理, $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$和$\frac{|0\rangle-|1\rangle}{\sqrt{2}}$都是合法的量子状态. 进一步地, $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$和$\frac{|0\rangle-|1\rangle}{\sqrt{2}}$也可以叠加, 又回到$|0\rangle$和$|1\rangle$. 这种正负概率振幅相消的量子现象是量子干涉产生的原理, 也是量子计算优势的基础. 量子叠加通常也被解读成一种量子并行性, 并被认为是量子算法加速计算的核心.

除了量子叠加概念, 另一个理解量子计算的重要概念是量子测量. 量子测量是沟通量子系统与经典世界的桥梁, 通常是量子计算获得计算结果的最后一步. 如果测量时系统处在某量子叠加态, 测量的结果将由概率振幅的模平方定义的概率分布随机决

定. 比如在$\frac{|0\rangle+|1\rangle}{\sqrt{2}}$上做测量将以$\frac{1}{2}$的概率得到0, $\frac{1}{2}$的概率得到1.

量子叠加和量子测量的讨论很大程度上揭示了量子计算的实质. 首先, 我们利用量子力学的原理操作量子叠加态, 使得对于计算没有实际意义的输出对应的概率振幅相消, 然后做量子测量并读出对计算有帮助的输出信息. 任何现有的量子算法都遵循这样的思路, 但是设计有效的量子算法却非易事.

5 大数分解量子算法及其影响

最重要最具深远影响的量子算法是肖尔的大数分解多项式时间量子算法. 这个算法输入为一个整数, 输出为这个整数的素数分解. 为什么解决这个简单数论问题的量子算法却是过去20年量子计算研究的核心推动力呢?

一方面, 大数分解问题被认为是经典计算不能有效解决的问题之一, 并广泛应用于构造公钥密码体系. 大数分解量子算法给基于大数分解问题的密码体系带来阴影. 更为致命的是, 除大数分解问题外, 其他一大类包括离散对数问题、椭圆曲线等在内的密码设计中常用的数论难题都可以用类似的量子傅里叶分析的方法设计出有效的量子算法. 如果大规模的量子计算机成为现实, 那么目前广泛应用的公钥密码体系将形同虚设, 互联网安全、电子商务将受到致命的威胁.

另一方面, 大数分解量子算法揭示了量子计算超越经典计算的可能性, 让我们对计算极限的认识有了新的高度. 特别地, 大数分解量子算法的提出意味着如下3个看似不可能的论断必有1个是真的. 一是扩展版丘奇图灵论题是错的, 二是量子力学在大规模尺度是错的, 三是大数分解问题有多项式时间的经典算法. 无论哪一论断确定为真, 都将是科学发展史上一次革命性的飞跃.

6 量子模拟

除了在数论问题上的突破, 量子计算在无结构数据搜索、模拟量子系统, 求解线性系统等重要问题中有望超越经典计算.

著名的物理学家费曼最早观察到用经典计算机模拟量子系统的困难, 并提出了用量子计算模拟量子系统的想法. 量子哈密顿量模拟问题是用量子电路来模拟稀疏哈密顿量演化的问题. 量子系统的演化由哈密顿量H按照薛定谔方程决定. 经过时间t, 系统的演化为$\exp(-\mathrm{i}Ht)$. 对于一个n量子比特的系统, 哈密顿量H是一个2^n乘2^n的厄米矩阵. 如果这个矩阵的每行绝大部分元素是0, 而只有最多多项式个非零元, 那么它就被称为稀疏的. 稀疏的哈密顿量的演化$\exp(-\mathrm{i}Ht)$可以有效地用量子计算机模拟. 大部分量子化学、材料科学中哈密顿量都是稀疏的, 这使得量子模拟算法可以在这些领域中取得广泛引用, 模拟并预测系统的行为. 量子模拟问题是量子计算的代表性应用, 除非所有的量子算法都可以被经典计算有效模拟, 否则量子模拟问题不可能有经典的算法.

量子线性系统算法是量子模拟算法的一个重要的应用. 这个算法给出了求解稀疏线性系统$Ax=b$的对数时间算法. 值得注意的是这个算法并不解决传统意义下的线性方程求解问题. 首先, 为了使用该算法, 需要把向量b制备成量子叠加态. 其次, 计算结束后, 系统处在正比于解x的量子叠加态上, 因此并不能有效地读出x的每个元素, 而只能按照x的概率振幅随机读出元素标号. 这些细节问题局限了这个算法的应用范围. 与其说它是一个算法, 不如说它是一个算法的框架, 在利用这个框架设计具体的量子算法时需要考虑输入态制备和结果读出这2个问题.

鉴于揭示和区分量子计算和经典计算极限的重要理论意义, 研究者开始考虑一些并不自然的、生造的、但现有的量子实验技术条件可实现而经典计算不能有效解决的问题. 玻色采样问题就是这方面尝试的代表. 玻色采样问题中, 多个输入光子经过一个分光镜网络到底输出端, 问题的要求是根据由量子力学给出的分布进行输出采样. 这样的特殊分光镜网络并不等价于通用量子计算机, 但实现相对容易, 有望在可以预期的将来较早展示出量子计算设备相对于经典设备的优越性.

7 量子计算与经典计算关系

总体来讲, 量子计算在可计算性的层面并不强于经典计算, 但是在有效计算的层面, 普遍的认识是量子计算比经典计算更加优越. 这些认识和信心来自于已知的量子算法, 包括大数分解算法、量子模拟算法、玻色采样等问题的理解. 同时, 我们也要客观地认识到, 量子计算并不是万能的, 我们只在这些特定的问题上找到了超越经典计算的应用. 特别地, 依

据量子叠加和并行性从而简单地认为量子计算能加速所有问题的观点是不正确的. 量子计算的加速似乎对问题的结构有着特殊的要求, 并不是所有的问题都能利用量子叠加找到更加高效的算法. 特别地, 目前研究者普遍认为量子计算机并不能有效解决NP完全问题.

8 量子计算实现: 可能性和困难

量子算法和理论的研究让人们欢欣鼓舞, 但是为什么自肖尔算法提出已过去20多年, 还没有通用量子计算机出现呢? 量子计算真的是可以物理实现的计算模型吗? 在量子计算研究初期, 对于量子计算的质疑主要集中在量子系统的退相干性和噪声对大规模量子系统的破坏性影响. 量子纠错解错码、量子容错计算等方面的研究逐步打消了这方面的担忧. 特别地, 量子阈值定理给出了确定的噪声阈值——只要计算过程中每个部件的噪声控制在阈值之下, 任意大规模的量子计算都能实现. 这在理论上铺平了量子计算发展的道路, 量子计算的实现看起只是一个工程技术问题. 当然, 在物理实现上, 我们离通用量子计算所需要的精度, 离阈值定理给出的阈值还有很大的距离. 真正实现大规模的通用量子计算机将是未来几十年各个大国、各大信息业巨头重要的攻关课题. 量子计算能否真实地带来计算极限的新突破, 量子力学能否在大规模尺度经受住考验, 让我们拭目以待.

参考文献

1 Turing A. On computable numbers, with an application to the Entscheidungs problem. London Math Soc, Ser 2, 1936, 42: 230–265
2 Cook S. The complexity of theorem-proving procedures. In: Harrison M A, Banerji R B, Ullman J D, eds. Proceedings of the 3rd ACM Symposium on Theory of Computing, 1971. 151–158
3 Levin L. Universal search problems (in Russian). Probl Inf Transm, 1973, 9: 115–116
4 Arora S, Barak B. Computational Complexity: A Modern Approach. Cambridge: Cambridge University Press, 2009
5 Feynman R. Simulating physics with computers. Int J Theor Phys, 1982, 21: 467–488
6 Nielsen M, Chuang I. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000
7 Lloyd S. Universal quantum simulator. Science, 1996, 273: 1073–1078
8 Shor P. Polynomial-time algorithm for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput, 1997, 26: 1484–1509
9 Harrow A, Hassidim A, Lloyd S. Quantum algorithm for linear systems of equations. Phys Rev Lett, 2009, 103: 150502
10 Aaronson S, Arkhipov A. The computational complexity of linear optics. In: Fortnow L, Vadhan S P, eds. Proceedings of the 43rd Annual ACM Symposium on Theory of Computing, 2011. 333–342

The limits of computation

JI ZhengFeng[1,2] & XIA MingJi[1]

[1] *State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China;*
[2] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L3G1, Canada*

The powerful idea of computation has accompanied the development of human civilization, has deeply changed the way we live and work, and has accelerated the advancement of many areas of sciences. In this article, we explore the power and limits of computation from several different perspectives. We will discuss topics from the models of computation and Church-Turing thesis, to the impact of the P versus NP problem and quantum computing on our understanding of the limits of computation. More concretely, we will explore the computability and the halting problem, the efficiency problem of computation, the P versus NP problem. We then move on to the discussion of quantum computation, quantum algorithm for factoring and its implications, quantum simulation and the relation between quantum and classical computations.

Turing machine, Church-Turing thesis, quantum computing, integer factorization, quantum simulation

doi: 10.1360/N972015-01363

季铮锋

清华大学计算机系博士，加拿大滑铁卢大学博士后. 现为中国科学院软件研究所助理研究员，研究方向为量子信息、量子计算和量子复杂性.

夏盟佶

中国科学院软件研究所副研究员，研究计数复杂性、全息算法、张量网络. 中国科学院软件研究所博士，美国威斯康星大学研究助理，德国马普所博士后，西蒙斯计算理论研究所学期主题计划“计数复杂性与相变”参与者，“中国科学院院长奖”获得者.