中国科学: 信息科学 2016 年 第 46 卷 第 8 期: 982–1002
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
信息科学与技术若干前沿问题评述专刊

量子计算若干前沿问题综述

孙晓明

中国科学院计算技术研究所, 北京 100190
E-mail: sunxiaoming@ict.ac.cn

收稿日期: 2016–04–05; 接受日期: 2016–05–31
国家自然科学基金 (批准号: 61222202, 61433014, 61502449) 和中组部万人计划青年拔尖人才资助项目

摘要 量子计算, 由于其在大整数分解等问题上所显示出来的强大计算能力, 被认为是一种可能对未来产生颠覆性影响的新型计算模型, 它为一些困难的计算问题的解决提供了新的思路. 本文围绕着量子算法、量子计算复杂性、量子程序理论、量子电路、量子密码学等研究方向, 对近 20 年来量子计算所取得的一些重要进展进行了全面综述, 希望能够为从事相关研究工作的学者提供参考. 同时本文还列出了上述研究方向中一些相对重要的研究问题, 抛砖引玉, 希望能够推动其中一些问题的研究乃至解决.

关键词 量子算法 量子计算复杂性 量子程序理论 量子电路 量子密码学

1 引言

量子计算被认为是一种可能对未来产生颠覆性影响的新型计算模型, 它为一些困难的计算问题的解决提供了一种新的思路, 同时量子密码具有不依赖问题难解性假设 (例如 P≠NP) 的可证明安全性, 关于量子计算的研究日益得到学术界和工业界的重视.

量子计算的思想最早由 Feynman 在 20 世纪 80 年代提出, Deutsch [1] 定义并研究了量子图灵机和量子电路模型. 1993 年 Bernstein 和 Vazirani [2] 开始考虑量子图灵机的计算复杂性问题, 同年姚期智 [3] 证明了量子电路模型与量子图灵机在计算复杂性上等价, 从而完成了量子计算机的理论奠基. 早期的量子算法研究包括 Deutsch-Jozsa 算法 [4], Simon 算法 [5] 等. Shor [6] 在 1994 年提出的大整数分解的量子多项式时间算法和 Grover [7] 在 1996 年提出的无序数组元素查找的快速量子算法, 分别比相应的经典算法具有指数量级和平方量级的加速, 这些工作都展示出了量子计算潜在可能的超越经典计算的能力.

为了厘清量子计算的能力到底能否真正意义上超越经典计算, 最近 20 年间学者们对量子计算展开了更加深入和系统研究, 取得了诸多重要的进展, 例如提出并发展了基于量子随机游走 [8] 和振幅放大 [9] 等的新型量子算法设计技术, 在求解线性方程组等多个计算问题上设计了对数量级计算复杂性的新型量子算法 [10,11], 使用半正定规划等工具给出了量子判定树复杂性的精确刻画 [12,13], 证明了量子交互式证明系统的计算能力和多项式空间的计算能力等价 [14] 等, 此外在密码学领域还提出了设备

引用格式: 孙晓明. 量子计算若干前沿问题综述. 中国科学: 信息科学, 2016, 46: 982–1002, doi: 10.1360/N112016-00084

无关的量子密钥分发 [15,16] 等新的研究方向. 这些工作使得我们对量子计算的能力有了新的认识, 同时也加深了我们对于经典计算的理解.

关于量子计算的很多重要的科学问题还远未解决, 对很多问题目前的研究还非常有限, 例如量子计算机多项式时间能否解决经典计算机在多项式时间所不能求解的问题, 即 BQP 是否等于 BPP? 像 P vs. NP 问题一样, 这一问题的解决需要对量子多项式时间所能计算的问题的内部结构有充分的了解及刻画, 这方面研究还有很长的路要走. 一些相对简单的计算模型下 (例如判定树模型、通信模型) 量子算法比经典算法的优势极限到底有多大目前也尚不清楚, 此外量子计算机所需要使用的量子程序和量子软件也还有很多核心问题没有能够解决, 目前还没有可以实用的设备无关的量子密码机制. 上述这些问题都有待进一步探索.

量子计算是一个非常广阔的研究领域, 本文限于篇幅, 将集中围绕量子计算复杂性、量子算法、量子电路、量子软件与程序理论和量子密码学等 5 个方面对量子计算近年来国内外的发展现状做系统性的介绍, 并在此基础上提出未来五到十年一些需要重点开展研究的具体方向. 关于量子计算另外的几个重要的研究方向, 包括量子体系结构、量子通信、量子器件以及量子调控等在本文中未能涉及. 本文的组织如下: 文章共分 4 部分, 其中第 1 节引言, 第 2 节按照量子计算复杂性、量子算法、量子电路、量子软件与程序理论、量子密码学等 5 个方向综述近年来国内外的研究进展, 第 3 节提出未来量子计算的一些重要研究方向和研究问题, 第 4 节将对全文进行总结.

2 国内外发展动态与现状分析

2.1 量子计算复杂性

(1) **量子多项式时间复杂性类 (bounded-error quantum polynomial-time, BQP)**

多项式时间复杂性类 P 是指所有能够在经典的图灵机上在多项式时间内求解的问题所组成的集合, 而 (有界错误的) 概率多项式时间复杂性类 BPP (bounded-error probabilistic polynomial-time) [17] 是指所有能够在经典的概率图灵机上在多项式时间内求解的问题所组成的集合, 通常学术界普遍认为 BPP 代表了所有经典计算能够有效解决的问题. 与之类似, (有界错误的) 量子多项式时间复杂性类 BQP [2] 是指所有能够在量子图灵机上在多项式时间内求解的问题所组成的集合, 一般认为 BQP 代表着所有可以被量子计算机有效解决的问题所组成的集合. 由于量子的测不准原理, 量子算法通常会有一定的错误率, BQP 要求错误率必须低于某个 1/2 以下的常数 (通常取为 1/3).

BQP 复杂性类的严格定义如下 [2]: 一个问题 $A \in \mathrm{BQP}$ 当且仅当存在一个多项式时间可生成的量子电路族 $Q = \{Q_n | n \in \mathbb{N}\}$, Q_n 接受长度为 n 的量子比特输入 x, 然后输出一个量子比特, 满足下面的关系: 如果 $x \in A$, 则 $\Pr(Q \text{ 接受} x) \geqslant 2/3$; 如果 $x \notin A$, 则 $\Pr(Q \text{ 接受} x) \leqslant 1/3$.

现在已经知道 BQP 复杂性类中包含很多重要的计算问题, 例如大整数分解问题 [6]、离散对数问题 [6]、量子系统模拟 [18] 等. 上述 3 个问题是否能够在经典计算下多项式时间内解决 (即是否在 BPP 中), 目前尚不清楚, 如果它们不在 BPP 中, 那么量子计算就比经典计算能力更强.

自从提出量子计算的模型之后, 学者就一直在探讨 BQP 复杂性类与经典复杂性类之间的关系. 根据定义, 显然有 $\mathrm{P} \subseteq \mathrm{BPP} \subseteq \mathrm{BQP}$. 1997 年 Bernstein 和 Vazirani [19] 首次给了一个 BQP 复杂性类的上界: $\mathrm{BQP} \subseteq \mathrm{PSPACE}$, 这里 PSPACE 是多项式空间复杂性类, 即经典图灵机使用多项式空间能够解决的所有问题构成的集合, 上述各复杂性类之间的关系如图 1 所示. 随后 Adelman 等 [20] 改进了这一上界: $\mathrm{BQP} \subseteq \mathrm{PP}$, 这里 PP 是概率多项式复杂性类, 它与 BPP 的唯一差别是 PP 不需要错误的概率

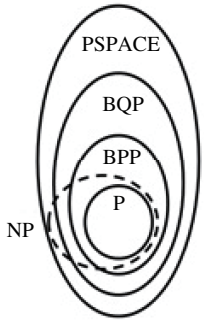


图 1　各复杂性类之间关系

Figure 1　The relationship between P, BPP, BQP and PSPACE

有界, 即 PP 只需要错误率低于 1/2 即可.

如前所述, 学者普遍认为 BQP 中存在着不在 BPP 中的计算问题 (例如大整数分解等备选问题), 即 BPP 真包含于 BQP [1)], 但这一问题目前还远未解决. 对角化技术是用来证明两个复杂性类不相等的一种重要手段, 理论计算机科学领域在此基础上发展出了使用神谕 (oracle) 图灵机来区分复杂性类的方法, Bernstein 和 Vazirani [2] 设计一个神谕 A, 使得 $\mathrm{BPP}^A \neq \mathrm{BQP}^A$. Watrous [21] 证明了存在另外一个神谕 B, 使得 BQP^B 不能被 MA^B 包含. Bennett 等 [22] 设计了一个神谕 A, 使得 BQP^A 不能包含 NP^A, 此外还有一些其他关于带神谕的复杂性关系, 例如 BQP^A 不能包含 SZK^A [23] 等. 如果允许进行测量后选择 (post-selection) 的话, Aaronson [24] 证明了 PostBQP 等于 PP. 完全问题是一个复杂性类中最难的一部分问题, 像很多常见的计算问题都是非确定性多项式时间复杂性类完全的 (即 NP 完全的), BQP 中也存在着完全问题, 例如近似计算 Jones 多项式 [25,26] 就是 BQP 完全的, 其他的一些 BQP 完全问题还包括由局部 Hamilton 量引出的局部 Hamilton 量特征值采样问题 [27], 由 Forrelation 问题自然推广而来的 k-fold Forrelation 问题 [28] 等.

(2) **量子判定树复杂性 (quantum decision tree, QDT)**

由于理解和研究通用图灵机计算模型下的计算复杂性所遇到的巨大困难, 学者们提出了一些数学上相对更加简明的计算模型, 包括电路复杂性模型, 判定树复杂性模型 [29], 通信复杂性模型 [30] 等, 希望通过对这些组合模型的研究, 能够加深对一般计算复杂性类的理解.

判定树模型的复杂度是用算法对问题输入的查询次数来衡量的. 根据所使用的计算模型不同, 判定树可以分为: 经典判定树复杂度 $D(f)$、(有界错误的) 随机判定树复杂度 $R_\epsilon(f)$, 和量子判定树复杂度 $Q(f)$、量子判定树复杂度又可以根据模型是否允许出错分为 (有界错误的) 量子判定树复杂度 $Q_\epsilon(f)$ 和无差错量子判定树复杂度 $Q_E(f)$. 通常错误率 ϵ 被取为 1/3 [2)].

1996 年 Grover [7] 提出了 Grover 量子搜索算法, 该量子算法在一个无序的数组上查找一个元素所需的查询时间只要 $\Theta(\sqrt{n})$, 该算法还可以用于查找最小元素. 2006 年孙晓明和姚期智 [31] 解决了在低维空间中查找局部最小元素的量子下界问题. 如果从判定问题 (算法输出的结果只能是 Yes 或者 No) 的角度来看, Grover 量子搜索算法事实上给出了一种计算有 n 个输入的 "或" 函数 ($\mathrm{OR}_n = x_1 \vee x_2 \vee \cdots \vee x_n$) 的量子判定树算法, 即 $Q\ (\mathrm{OR}_n) = \Theta(\sqrt{n})$. 与之对比, 如果采用经典算法, 即使是使用随机算法, 都需要至少 $\Omega(n)$ 的查询时间, 两者之间存在着平方量级的差别.

1) 这一问题与 BQP vs. NP 并没有直接的联系, 即使证明了 BPP ≠ BQP, NP 仍然可能和 BQP 不可比较, 见图 1.
2) 在上下文明确的情况下通常错误率会省略不写.

对于完全布尔函数 (total functions), 学者们一直猜想量子判定树复杂度与经典判定树复杂度之间的差距最多就是平方量级的, OR_n 已经是最差的例子了. 但是就在几个月前, Ambainis 等 [32] 推翻了这一猜想, 他们构造了一组新型的布尔函数, 使得量子判定树复杂度与经典判定树复杂度之间有着 4 次方量级的差距, 即 $D(f)=\Omega(Q(f)^4)$. 这一结果发表之后, 吸引了学术界重新来思考量子查询复杂度与经典查询复杂度之间的关系. 如果将经典判定树复杂度换成更强的随机判定树复杂度, Aaronson 等 [33] 在之前 Ambainis 工作的基础上进一步提出了一族函数, 将 $Q(f)$ 和 $R(f)$ 之间的差距也从原来的平方量级提升到了 2.5 次方量级, 即满足 $R(f)=\Omega(Q(f)^{2.5})$.

在上界方面, 学者们已经证明, 量子判定树复杂度与经典判定树复杂度之间的差距最多不超过 6 次方量级 [34], 即 $D(f)=O(Q(f)^6)$, 由于随机判定树模型比经典判定树更强, 因此同样有 $R(f)=O(Q(f)^6)$, 如何缩小 2.5 与 6 次方之间的差距是目前量子研究领域的一个热点. 研究布尔函数的量子查询复杂度 $Q(f)$ 的一个重要工具是半正定规划, 学者已经证明 $Q(f)$ 可以由一个与函数相关的半正定规划来完全刻画 [12,13].

目前关于无差错量子判定树复杂度 $Q_E(f)$ 的研究相对较少, 很长一段时间学者们认为无差错量子判定树复杂度和经典的判定树复杂度之间可能是线性量级相关的, 2011 年 Ambainis 等 [35] 给出了第一个函数, 使得 $Q_E(f)$ 可以相比于 $D(f)$ 达到超过线性量级的加速, 具体来说 $Q_E(f)=O(D(f)^{0.8675\cdots})$. 目前已知的 $Q_E(f)$ 与 $D(f)$ 之间最大的差距也是前文中提到的 Ambainis 等 [32] 的工作中得到的, 他们使用同一个函数证明了 $Q_E(f)=O(\sqrt{D(f)})$. 此外 Ambainis 等 [36] 还证明了对于几乎所有的布尔函数 (除了与 OR_n 函数同构的函数以外), $Q_E(f)$ 都严格小于 $D(f)$, 这表明无差错的量子查询算法具有比想象中更普遍的计算能力优势.

对于部分布尔函数 (partial functions), 即定义域不是整个空间 $\{0,1\}^n$ 的函数, 量子算法可以达到比经典随机算法指数量级的加速, 甚至更大. Aaronson 和 Ambainis 在文献 [28] 中给出了 $Q(f)$ 和 $R(f)$ 之间最大的差别, 他们使用了一类称为 Forrealtion 的问题 (判断一个 Boolean 函数是否与另一个函数的 Fourier 变换高度相关), 该问题只需要一次量子查询即可被解决, 但随机算法却需要 $\Omega(\sqrt{n}/\log n)$ 次查询. 可以证明这里的 $Q(f)$ 和 $R(f)$ 是所能达到的最大差距, 因为任何 t 次查询的量子算法都可以用 $O(n^{1-1/2t})$ 次随机查询来模拟.

(3) **量子有穷自动机** (quantum finite automata, QFA)

量子有穷自动机可以看作经典有穷状态自动机的量子推广. 1971 年 Bainau [37,38] 首先定义了 QFA 的概念. 1997 年 Kondacs 和 Watrous [39] 证明了单向的 QFA 接受的都是正则语言, 而双向的 QFA 可以接受非正则语言, 因此双向的 QFA 具有比经典有穷自动机更强的计算能力. 尽管单向的 QFA 接受的都是正则语言, 但 Ambainis 等 [40,41] 证明了 QFA 的状态数相对于识别相同语言的经典自动机可以是指数量级的小, 具体来说, 他们证明了对于语言 $L_n=\{a_i|i$ 能被 n 整除$\}$, L_n 能够被一个有 $O(\log n)$ 个状态的 QFA 识别, 而识别 L_n 的经典有穷自动机需要有 n 个状态. Kondacs 和 Watrous [39] 证明了非正则语言 $L=\{a^mb^m\}$ 能够被双向的 QFA 在线性时间识别, 但双向的确定性有穷自动机不能识别 L. Ambainis 和 Watrous [42] 定义了 QCFA, 即头部的运动是经典的但中间的状态是量子的自动机. QCFA 能够在多项式时间内识别语言 $L=\{a^mb^m\}$, 在指数时间内识别回文语言, 这些都是确定性有穷自动机所不能够识别的. 2000 年 Moore 和 Crutchfield 研究并证明量子正则语言的封闭性质和泵引理 (pumping lemma) [43]. 2008 年邱道文等 [44] 给出了判定两个多次测量的量子有限自动机的等价性的多项式时间算法. 2012 年邱道文和 Mateus 等 [45] 利用实数有序域上的判定性问题方面的结论证明了量子有限自动机的状态最小化问题是可判定的, 属于指数空间复杂性类. 另外, 文献 [46] 提出了一类带经典和量子状态的单向量子有限自动机, 并证明了该模型在状态复杂性方面的优势.

(4) **量子证据的有效验证**

在复杂性类 BQP 之上还有很多重要的计算复杂性类, 量子 Merlin-Arthur 复杂性类 (quantum Merlin-Arthur, QMA) [47,48], 是指所有存在着 "量子证明" 的问题所组成的集合. 这里的 "量子证明" 类似于经典的 NP 问题的证据, 它是指一个由量子态组成的证据, 可以被一台量子计算机有效的验证. 就像一般认为 BQP 是所有能够被量子计算机有效解决的问题一样, QMA 一般被认为是所有可以被量子计算机有效验证的问题.

QMA 的形式化定义如下: 一个问题 $L \in$ QMA 当且仅当存在一个多项式时间可生成的量子电路族 $Q = \{Q_n : n \in \mathbb{N}\}$ 以及一个多项式有界函数 $p(x)$, Q_n 接收一个长度是 $(n + p(n))$ 量子比特的输入, 输出一个量子比特, 满足下面的条件.

完备性: 如果 $x \in A$, 则存在一个长度是 $p(|x|)$ 量子比特的量子态 ρ 使得 $\Pr(Q$ 接受$(x, \rho)) \geqslant 2/3$;

合理性: 如果 $x \notin A$, 则对于任意长度是 $p(|x|)$ 量子比特的量子态 ρ 都有 $\Pr(Q$ 接受$(x, \rho)) \leqslant 1/3$.

前文中提到的局部 Hamilton 量问题 (local Hamiltonian problem) 是第一个被证明的 QMA 完全问题 [47], 它可以看成 MAX-k-SAT 的量子版本, 它的完全性证明也可以被认为是关于 NP 完全问题的 Cook-Levin 定理的量子版本. 除此之外还有很多 QMA 完全问题, 例如 2-local Hamiltonian problem [49], density matrix consistency problem [50], group non-membership problem [51] 等. 已知的 QMA 复杂性类和一些经典复杂性类的关系如下: MA $\subseteq$ QMA$\subseteq$ PP [52]. 关于 QMA 复杂性的一个非常重要问题是: 多个互相不纠缠的量子证明者是否严格比一个量子证明者强, 即 QMA(k) 是否等于 QMA? 2013 年 Harrow 和 Montanaro [53] 证明了多个量子证明者的能力和两个量子证明者的能力是一样的, 即对于任意的 $k \geqslant 3$, 都有 QMA(k) = QMA(2). 关于其他一些 QMA(2) 复杂性类的变种也有类似的结果 [54]. 目前最好的关于 QMA(2) 的经典复杂性类上界是由 Schwarz [55] 在 2015 年证明的 QMA(2) $\subseteq$EXP.

(5) **量子交互证明系统** (quantum interactive proofs, QIP)

量子交互证明系统 QIP 由 Watrous [56] 提出, 它是经典交互证明系统模型在量子计算模型上的自然推广. QIP(k) 是指包含 k 轮信息交互的量子交互证明系统, QIP(0) 即 BQP, QIP(1) 即 QMA, Kitaev 和 Watrous [57] 在 2000 年证明了 QIP(3) =QIP. 2010 年 Jain 等 [14] 证明了 QIP = PSPACE, 这说明了利用量子机制并不会提升交互证明系统的计算能力. 关于多证明者交互式证明系统, Ito 等 [58] 证明了 NEXP$\subseteq$ $\mathrm{MIP}^*_{1,1-1/\mathrm{poly}}(3,1)$, 这里 MIP* 是一种多证明者交互式证明系统, 在这个模型中, 证明者之间允许共享量子纠缠态, 但不允许通信. 2012 年 Ito 等 [59] 中证明了 NEXP$\subseteq$MIP*. 2014 年 Fitzsimons 和 Vidick [60] 给出了局部 Hamilton 量问题的一个 MIP* 系统下的证明协议, 这个结论暗示着允许证明者之间共享纠缠态的交互证明系统很可能比不允许共享纠缠态的交互证明系统更为强大. 2015 年 Natarajan 和 Vidick [61] 又设计了一个解决局部 Hamilton 量的两轮的量子交互证明系统, 该系统的证明者数量、证明者的证明长度都为常数. 2016 年季铮锋 [62] 设计了一个经典的交互协议用于验证局部 Hamilton 量的量子证据状态的有效性, 通过这个协议可以证明以倒多项式的精度 (1/poly) 来近似多人一轮游戏的非定域值是 QMA 难的.

2.2 量子算法

除了量子大整数分解算法 (Shor 算法) 和量子搜索算法 (Grover 搜索算法) 两个最重要的量子算法以外, 近年来学者们在量子随机游走、量子模拟、求解线性方程组等多个方面的量子算法研究也取得了显著的进展.

(1) **量子随机游走** (quantum random walk)

随机游走以及马氏链是一种非常强大的经典算法设计技术, 被广泛的应用到搜索问题、采样问题以及近似估计. 同样地, 量子随机游走也为量子算法设计提供了一种一般化的框架. 与经典的随机游走不同, 给定了一个图结构, 量子随机游走算法按照量子的机制 (酉变换) 在图结构上模拟粒子的行为. 相比于经典随机游走, 量子随机游走一般具有更快的首达时间 (从源点出发到达目标点所需的期望时间). 对于一些特殊的图, 量子随机游走的首达时间可以比经典随机游走的首达时间指数量级的小. 另外量子随机游走有着更快的混合时间 (从源点出发到达所有顶点所需的期望时间). 存在着一些图结构, 使得量子随机游走的混合时间可以达到经典随机游走的混合时间开平方根量级, 并且可以证明平方量级的差距也是最大可能的差距.

Ambainis 等 [63] 提出了一种利用量子随机游走技术来计算布尔公式值的算法, 可以在 $O(n^{0.5+o(1)})$ 时间内计算任何一个长度是 n 的布尔公式的值. 特别地, 使用该算法可以更快地计算 AND-OR 树的值, 也就是说可以更快地计算一个两人博弈中哪一方有必胜策略. 与之对比, 学者已经证明存在一大类布尔表达式, 任何经典 (随机) 算法在最坏情况下都需要 $\Omega(n^{0.753\cdots})$ 的时间 [64].

基于经典随机游走的搜索算法设计一般可以抽象成如下形式: 构建关于状态空间的一个马氏链并模拟在上面的随机游走, 经过特定步数的随机游走后, 检查状态是否转移到了需要的状态. 这类算法都可以通过量子随机游走来进行加速. 决定此类算法效率的一个关键指标是马氏链的谱隙 (状态转移矩阵的最大特征值和第 2 大特征值之间的差异), 量子游走可以平方量级地提高计算时间对谱隙的依赖关系, 即从 δ^{-1} 提高到 $\delta^{-1/2}$. 量子随机游走的一个重要应用是 “判定一个图中是否存在三角形” 问题, 直接应用 Grover 搜索可以给出一个查询复杂度为 $O(n^{1.5})$ 的量子算法, Buhrman 等 [65] 利用振幅放大技术设计了一个复杂度为 $O(n+\sqrt{mn})$ 的量子算法. 结合振幅放大技术与组合技巧, 2007 年 Szegedy [66] 设计了一个复杂度为 $O(n^{10/7})$ 的量子算法, 关于 “查找三角形” 的量子算法竞赛就此展开. 利用量子游走技术, 2007 年 Magniez 等 [67] 把复杂度降低到 $O(n^{1.3})$, 2012 年 Belovs [68] 提出了一种基于量子张成方案 (quantum span program) 的 “学习图” (learning graph) 量子算法设计技术, 并利用这种技术设计了一个复杂度为 $O(n^{35/27})$ 的量子三角形查找算法. Lee 等 [69] 应用改进后的 “学习图” 技术得到了一个复杂度为 $O(n^{9/7})$ 的量子算法, Jeffery 等 [70] 直接利用量子随机游走也得到了具有相同复杂度的量子算法. 另一方面, 孙晓明等 [71] 证明了任何图性质函数的量子算法复杂度至少是 $\Omega(N^{1/4})$ 的, 这里 N 是图中边的数目. Belovs 等 [72] 证明了对于边有权重的寻找三角形问题, 上述 $O(n^{9/7})$ 的量子算法是最优的 (至多相差一个对数因子). 对于无权的三角形查找问题, Le Gall [73] 将复杂度进一步提升到 $O(n^{5/4})$. 此外应用改进后的 “学习图” 技术, Belovs 还改进了 “相异元素问题”(k-distinctness, 判定是否有 k 个元素相同) 的量子算法 [74, 75].

(2) **振幅放大** (amplitude amplification)

给定一个启发式搜索问题, 假设存在一个算法 A 以及一个 “检查” 函数 f, 满足每次 A “猜中” 的概率等于 ϵ, 即 $\Pr(A$ 输出 w 满足 $f(w)=1)=\epsilon$. 如果不断重复运行算法 A, 并且每次都用 f 来检查 A 的输出, 那么将可以把成功找到 w 的概率提高, 这种技术被称为概率放大技术. 具体来说, 如果单次成功的概率是 ϵ, 那么平均需要 ϵ^{-1} 次就能够找到一个满足 $f(w)=1$ 的 w. 2002 年 Brassard 等 [76] 提出了一种量子算法来加速这一搜索过程, 以很高的概率只运行 $O(\epsilon^{-1/2})$ 次算法 A, 就可以找到一个 w 使得 $f(w)=1$, 该技术被称为振幅放大技术, 与经典的概率放大技术对应.

应用振幅放大技术可以对很多计算问题进行量子加速, 例如 3-SAT 问题, 目前解决 3-SAT 问题最快的经典随机算法的运行时间约为 $O((\frac{4}{3})^n)$ [77], 应用振幅放大技术将可以得到一个运行时间为 $O((\frac{4}{3})^{\frac{n}{2}})$ 的量子算法. 除此之外, 应用 Grover 搜索算法或者振幅放大还可以加速查找最小数问题, 该问题经典算法需要 $\Omega(n)$ 的时间, 而量子算法的运行时间只要 $O(\sqrt{n})$ [78], 相比于经典算法达到了平方

量级的加速. 同样的图连通性问题的量子算法的运行时间只要 $O(n^{1.5})$ [79]. 模式匹配问题是生物信息学和文本处理领域内的一个基本问题, 目标是在一个长度是 N 的文本中找到一个长度为 M 的模式 P. 该问题的经典算法复杂度为 $O(M+N)$, 2003 年 Ramesh 和 Vinay [80] 使用振幅放大技术设计了一个时间复杂度为 $\tilde{O}(\sqrt{N}+\sqrt{M})$ 的量子算法.

(3) **求解线性方程组的量子算法**

解线性方程组是一个基本的数学问题, 在工程等领域有着重要应用. 给定一个 $N\times N$ 的矩阵 A, 以及一个 N 维向量 b, 算法需要输出一个向量 x 使得 $Ax=b$. 众所周知 Gauss 消元法可以在 $O(N^3)$ 的时间内计算 x. 2008 年 Harrow 等 [81] 提出了一种可以在对数时间内求解线性方程组的量子算法 (HHL 算法): 输入一个 $\log_2 n$ 位的量子态 $|b\rangle=\sum b_i|i\rangle$, 如果可以在常数时间内实现酉变换 e^{-iAt}, 则算法可以在 $O(\log_2 n)$ 的时间内近似得到一个量子态 $|x\rangle=\sum x_i|i\rangle$ 满足线性方程 $Ax=b$. 由于写下 x 都需要 N 的时间, 所以在经典情形下不可能存在比 N 更快的算法.

在实际应用 HHL 算法时需要有一些限制: 1) 由向量 $b=(b_1,\ldots,b_n)$ 需要能快速制备量子态 $|b\rangle$; 2) 需要能够高效地实现酉变换 e^{-iAt}; 3) 算法的运行时间随矩阵的条件数 $\kappa=\|\lambda_{\max}(A)/\lambda_{\min}(A)\|$ 线性增长, 因此 κ 不能很大; 4) 该量子算法最终输出一个量子态 $|x\rangle$, 如果需要 x 某一比特的信息, 需要再对 $|x\rangle$ 进行测量, 而由于量子的测不准原理, 测量后将会破坏掉该状态. 尽管 HHL 算法有上述的这些限制, 但是在一些特定的应用场景下上述限制可以被满足, HHL 算法可以实现 $O(\log_2 n)$ 时间求解.

学者们已经将 HHL 算法推广到机器学习领域, 比如 k-means 聚类 [82], 支持向量机 [83], 数据拟合 [84], 以及计算 Pagerank 向量 [85] 的某些性质等. 但上述的应用仍需要满足对 HHL 算法的 4 点限制, 例如 2013 年 Lloyd 等 [82] 提出了一种进行二分类的量子算法: 给定一个 $\log_2 n$ 比特的向量 $|u\rangle$, 以及两组向量 $|v_1\rangle,\ldots,|v_m\rangle$ 和 $|w_1\rangle,\ldots,|w_m\rangle$, 该算法可以在 $O(\log_2 mn/\epsilon)$ 时间内判定 $|u\rangle$ 与 $|v\rangle=\sum|v_i\rangle/m$ 和 $|w\rangle=\sum|w_i\rangle/m$ 哪个距离更近, 从而判定 $|u\rangle$ 应该属于哪一个聚类, 这里 ϵ 表示算法精度. 这里的一个问题在于如何快速制备出状态 $|u\rangle,|v_k\rangle$ 和 $|w_k\rangle$, 一种方案是利用量子 RAM, 要想利用量子 RAM 的直接制备方案就需要向量 u,v,w 是相对一致的 (relatively uniform), 然而如果增加相对一致的限定, 那么经典的随机采样算法也可以以 ϵ 的精度在 $O(\log_2 mn/\epsilon^2)$ 的时间内估计出 $\langle u|v\rangle$ 和 $\langle u|w\rangle$, 也就是说量子算法重新回到平方量级加速, 而非指数量级. 另外 HHL 算法还可应用于有限元方法, 2013 年 Clader 等提出了一种利用 HHL 算法解决电磁散射问题的有限元方法 [86].

(4) **绝热优化算法**

绝热优化是指采用绝热计算的方法来求解最大约束满足问题. 最大约束满足问题 (constraint satisfaction problem, CSP) 是指给定变量的一系列约束, 求出对变量的一个赋值, 使得能够满足尽可能多的约束, 包括 MAX-SAT, 最大子团问题等组合优化问题都可以看作是 CSP 问题的特例. Farhi 等 [87] 提出了使用绝热计算来求解 CSP 问题的算法: 系统先制备一个简单的 Hamilton 量并使其处于基态, 然后缓慢地让系统进行绝热演化, 使其演化为一个复杂的 Hamilton 量, 这个 Hamilton 量的基态编码了 CSP 问题的解. 如果这个演化过程进行得足够慢, 那么量子绝热定理就能保证系统一直处于基态, 最后的状态也一定就是优化问题的解. 这里需要该过程 "足够慢", 学者已经证明对于某些问题实例, 该过程需要指数时间 [88]. 加拿大 D-wave 公司所采用的技术就是绝热优化算法, 据报道对于一些特定的优化问题, D-wave II 的求解速度远超标准计算机上的经典算法 [89], 尽管上述结论比较非常依赖于问题的实例、选取的经典算法, 以及比较的度量方式等.

(5) **量子模拟及波色子采样**

最早 Feynman 提出量子计算概念的初衷主要是用来模拟量子化学、超导、高能物理等量子系统, 帮助人们更好地理解复杂量子系统的演化 [90]. 具体来说, 假设输入一个系统的初始状态以及系统的

Hamilton 量, 通过求解 Schrodinger 方程来输出给定时刻的系统状态. 由于描述系统状态的复杂度通常是指数量级的, 经典计算机很难进行快速的模拟. 然而利用量子的叠加和纠缠等特性, 通过量子计算机却可以快速地模拟很多现实中的量子系统, 例如只具有局部交互作用的系统 [91], 显示出了量子计算的威力. 此外 Berry 和 Childs [92] 还提出了使用量子随机游走来模拟 Hamilton 量的演化的方法.

2010 年 Aaronson 和 Arkhipov [93] 提出了量子波色采样的设想: 它主要由一组简单的交错导波管构成, 导波管的入口和出口数量相同, 我们从导波管入口处向光子回路注入大量相同的光子 (波色子), 那么通过采样光子从哪个出口离开, 就可以得到一个概率分布. 基于一定的计算复杂性假设, 这个概率分布是不能用经典计算机去快速产生的, 甚至是不能快速近似计算的. 另一方面, 作为一种专用的量子计算装置, 量子波色采样机只需要单光子源、线性的态演化和探测, 因而更容易在更大尺度上进行实验实现和实际应用. 目前在实验实现方面, 物理学家已经取得了初步的进展 [94~97].

2.3 量子软件与程序理论

由于量子不可克隆原理等量子特性, 经典的软件与程序理论、方法和技术在很大程度上不能直接适用于量子软件和程序, 这就使得量子软件理论与方法成为一个十分困难而富有挑战性的课题. 1996 年 Knill [98] 最先开展了关于量子软件理论的研究, 他提出了将量子算法转为量子伪代码的一系列基本原则, 这些原则对于后来量子程序语言的设计有很大的影响.

1998 年 Omer [99] 提出了第一个量子程序设计语言 QCL, 它的语法和数据结构都类似于经典 C 语言的语法和数据结构, 同时又具有许多重要的高层量子特征. 2000 年 Sanders 与 Zuliani [100] 提出了一种与 QCL 完全不同的量子程序设计语言 qGCL, 它本质上可以看作是 Dijkstra 的 Guarded-command 语言的扩展. qGCL 的语法中包含高层的数学符号, 并具有逐步精化的机制. 2001 年 Bettelli 等 [101] 在 Omer 的工作基础上提出了 C++ 的量子扩展, 同时该语言也具有一系列基于量子 RAM 的低层次操作.

与上述命令式的量子程序设计语言不同, 2004 年 Selinger [102] 提出了第一个函数式量子程序设计语言 QFC. 在 QFC 中, 函数不能作为数据处理, 因此尚缺乏像 ML 与 Haskell 等典型的函数式程序设计语言所具有的高层特征. 与此相关, 但不属于函数式量子程序设计语言研究的一个工作是 Sabry [103] 于 2003 年用 Haskell 实现了对量子计算的模拟.

在上面提到的量子程序设计语言中, 遵循的都是 “量子数据、经典控制” 的原则, 即数据是以量子态形式表现的量子信息, 对数据的处理采用量子操作, 但是基本的程序控制是经典的, 这类工作还包括文献 [104]. 2005 年 Altenkirch 与 Grattage [105] 提出了一种有限类型的函数式量子程序语言 QMC, 其中引入了高阶的量子控制结构, 但其关于量子化的程序控制仍然只是一种想法. 最近应明生 [106] 提出了二次量子化实现带量子控制的量子递归的思想, 真正的实现了量子化的程序控制.

2016 年 3 月微软公司发布了其最新的量子软件架构和工具包 Language-Integrated Quantum Operations: LIQUi|⟩. 通过 LIQUi|⟩ 可以将用户用高级语言所编写的量子程序转化成为可以在硬件上运行的机器语言. 另外由 Selinger 小组开发的 Quipper 量子编程语言 [107] 实现了多个重要的量子算法, 包括量子表达式求值算法 [63]、量子三角形查找算法 [67] 等.

近年来关于量子软件理论的更加高层的研究工作也逐渐开展起来. Abramsky 和 Coecke [108, 109] 致力于量子系统 (特别是量子纠缠) 的范畴论语义的研究. 2004 年 Tonder [110] 利用一个基于线性逻辑的类型系统建立了一种包括操作语义等的量子 Lambda 演算, 并证明了其计算能力与量子图灵机等价. 这些工作有望应用于克服量子不可克隆原理在量子软件中引起的本质困难. 2003 年 Oskin 和 Petersen [111] 提出了描述量子系统的量子代数, 试图为量子程序设计语言提供一个代数基础. 2004 年

Girard [112] 提出的量子相干空间有可能用于建立高层量子计算的形式语义. 同年 Jorrand 和 Lalire 提出了量子进程代数, 2005 年 Gay 和 Nagarajan [113] 提出了量子进程演算, Labire [114] 定义了量子进程代数的概率互模拟. 2011 年应明生 [115] 建立了第一个成熟的量子 Floyd-Hoare 逻辑并证明了它的完备性. Floyd-Hoare 逻辑是由图灵奖得主 Floyd 和 Hoare 提出并由 Cook 证明其完备性的形式逻辑系统, 该系统的用途是使用严格的数理逻辑推理来为计算机程序的正确性验证提供一组逻辑规则. 2012 年冯元等 [116] 定义了一种新型的量子进程的互模拟, 可以允许同时包含量子通信和经典通信. 应明生和冯元 [117] 给出了量子程序在有限状态的 Hilbert 空间上停机的充分必要条件.

2.4 量子密码

Bennett 和 Brassard [118] 提出的 BB84 量子密钥分配协议从理论上被证明是绝对安全的 [119, 120], 然而在实际中量子密钥分配所采用的具体实现方案, 以及所采用的量子器件的非理想性, 给窃听者带来了新的攻击手段 [121]. 是否能够从理论上排除掉所有可能的攻击手段? Mayers 和姚期智 [122] 最先提出了现在被称作 “设备无关” 的思想: 是否有可能仅对设备做最基本的空间上需要分离的假定, 除此以外对设备不做任何限制, 其安全性完全由对设备本身的测试来完成. 这一思想突破了安全性对系统设备的依赖性, 成为最近十几年量子密码学界研究的重点.

2006 年 Colbeck 在其博士论文 [123] 中提出了使用 Bell 测试来检查设备的安全性的设想, 2014 年 Vazirani 和 Vidick [15] 给出了首个完全安全的设备无关的量子密钥分发协议, 该协议不需要假设设备的独立性, 以及信道的噪声为零, 即使窃听者在设备与自身之间建立了某些量子纠缠, 使用者仍然能够成功地制备密钥或者识别出攻击. 经过仔细分析, Lo 等 [124] 发现量子密钥分配系统的侧信道大多出现在测量端, 他们于 2012 年提出了测量端设备无关协议, 该协议不仅能抵抗所有针对测量端的攻击, 而且对于探测器的要求也可降低到目前技术条件可实现的水平, 并很快就在实验上演示成功 [125]. 实验表明, 测量仪器无关量子密钥分配方案原则上是可行的. 但是, 实际系统需要两个单光子探测器同时响应, 因此其安全密钥生成效率十分低下, 目前离实际可用还有一定距离. 2014 年 Sasaki 等 [126] 提出了 Round-Robin 差分相位量子密钥分配协议, 受到了学术界的高度重视, 该协议不需要顾及光源的抖动, 且容忍的误码率很高, 这在环境干扰特别大的特殊环境下, 或许具有优势. 在空间量子密钥分配实验方面, 2013 年 Weinfurter 小组 [127] 利用飞机运动平台, 实现了 20 km 的量子密钥分发实验, 验证了星地系统之间相对运动情况下的 QKD 可行性.

2014 年 Sasaki 等提出了 Round-Robin 差分相位量子密钥分配协议 [128] (RRDPS). 2015 年潘建伟等 [129] 率先完成了改造的 RRDPS 方案的实验验证, 该实验系统在 50 km 距离, 误码率为 29% 的情况下仍能够生成安全的密钥. 随后韩正甫团队 [130] 等按照原 RRDPS 协议完成了实验, 验证了 RRDPS 协议的实际可行性和未来的可用性. 在针对量子协议的安全性分析和攻击方法方面, 温巧燕、高飞团队做了大量的工作, 包括对德国、瑞典、新加坡等学者联合提出并实验实现的量子拜占庭协议给出了一种截获 – 重发攻击, 证明了其协议是不安全的 [131], 以及利用量子隐形传态 (quantum teleportation) 进行攻击 [132].

2.5 量子电路

本节的讨论主要集中在量子门、量子线路、电路集成等, 而不涉及任何具体的量子器件. 1985 年 Deutsch [1] 首次提出了量子图灵机的概念, 并引进了量子电路模型和通用量子逻辑门组, 将经典的转移函数扩展到了量子酉变换. 1993 年姚期智 [3] 证明了量子电路模型与量子图灵机在计算复杂性意义

上等价. 1995 年 Barenco 等 [133] 证明了 CNOT 门和单量子比特门对量子计算而言是通用的. 1996 年 Shor 等 [134] 提出了量子纠错编码, 为量子电路模型在编码和容错方面提供了完善的理论保证.

量子电路的设计既不等同于经典的逻辑电路设计, 也不等同于传统的可逆逻辑电路的设计. 量子逻辑门的搜索空间远超经典电路, 用 2- 比特量子电路实现一个一般的 $n \times n$ 酉变换需要 $\Omega(4^n)$ 个门 [135]. 目前只针对一些量子比特和门数目很少的可逆函数找到了其相应的最优电路. Shende 等 [136] 设计了一个迭代加深的 A^* 算法, 给出了所有三输入的可逆函数的最优电路. 杨国武等 [137] 在最多只使用 12 个非门, CNOT 门和 Peres 门的限定下, 给出了部分四输入可逆函数的最优电路. Golubitsky 等 [138] 观察到部分可逆函数的最优电路可以从其他函数的最优电路得到 (例如通过反转 f 的最优电路就可以得到 f^{-1} 的最优电路), 利用这种电路之间的对称性和 Hash 的技巧, 给出了所有四输入的可逆函数的最优电路. 对于输入个数大于 4 的可逆函数的最优电路, 学者们利用了形式证明领域里的一些技巧, 如 Hung 等 [139] 使用的符号可达性分析, Grosse 等 [140] 使用的布尔可满足性等.

2004 年 Aaronson 和 Gottesman [141] 证明了任意的稳定电路能够被重构成一个由 Hadamard 门、相位门和线性可逆电路构成的 11 级的电路. 2008 年 Patel 等 [142] 提出了一种针对线性电路的综合算法, 在最坏的情况下使用 $\Theta(n^2/\log n)$ 个 CNOT 门, 在渐近的意义上达到最优. 2007 年, Maslov [143] 提出了一种在渐近的意义上深度最优的针对稳定电路的算法, 电路由 90^+ 个阶段拼接而成, 每一个阶段都只包含一类门.

学术界还提出了很多启发式算法来搜索最优电路, 根据编码模式的不同可以分为基于变型的方法 [144, 145], 基于搜索的方法 [146, 147], 基于循环的方法 [148] 等. 另外彭斐和解光军 [149] 提出一种新的一维编码模式, 利用遗传算法优化了量子隐形传态的电路. 杨国武等 [150] 利用抽象群论的方法进行了电路的综合.

对实现标准门的高效电路的研究也是一个重要的方向. DiVincenzo 和 Smolin [151] 给出了需要 5 个两比特量子门才可以实现 Toffoli 门的数值证据, 2013 年俞能昆等 [152] 从理论上证明了 4 个两比特量子门不可能计算 Toffoli 门, 即 5 个量子门实现 Toffoli 门是最优的. Margolus [3)]提出了一种只用 3 个 CNOT 门实现一个增加了相位变化后的 Toffoli 门、Song 和 Klappenecker [153] 证明了这一实现是最优的. 遗憾的是只对很少的一些情况, Margolus 门可以代替 Toffoli 门. 2009 年 Shende 和 Markov [154] 证明了无论是否使用辅助系统, 至少需要 6 个 CNOT 门才能完全实现 Toffoli 门.

在单量子比特优化方面, 微软研究院的量子体系结构和计算小组做出了很多重要结果. 2012 年, Bocharov 和 Svore [155] 考虑了如何高效地把一个单量子比特门分解成一系列容错的量子操作. 对一个给定的单量子比特电路, 他们可以构造一个最优的由容错 Hadamard 门和 $\pi/8$ 旋转门构成的门电路序列. 2013 年, Bocharov 等 [156] 首次提出了一个用于把单量子比特酉正门编译成通用 V 基 (the universal V basis) 上的电路的构造性算法. 2015 年 Bocharov 等 [157] 提出了一个概率多项式时间的算法来综合 RUS (repeat-until-success) 电路, 以一定的精度在 Clifford+T 基上近似任何单比特幺正门. 此外 Selinger 的小组也深入研究了 Clifford 门以及与其他量子门电路的关系 [158~160].

为了验证量子电路综合算法的性能, 已经有很多可用的标注集函数. MasLov [161] 开发和维护了一个可逆逻辑综合标注集网站, 网站上提供了广泛使用的标注集函数, 以及它们目前已知的最优电路实现. RevLib 数据库 [162] 中不仅包含一些函数已知最优的电路实现, 还包含一些次优的电路实现. 开源工具箱 RevKit [163] 中包含了一些可逆电路综合算法的实现. 用经典电路模拟量子电路可以用来帮助评价量子电路的性能, 为了减少时间和内存消耗, 施尧耘等 [164] 提出了一些高效的量子电路模拟算法.

3) Margolus N. Simple quantum gates, Unpublished manuscript (circa 1994).

3 需重点开展研究的科学问题

量子计算是一个广阔的领域, 众多问题都有待解决, 在这里抛砖引玉, 列出一些我们认为相对重要、值得优先研究的问题, 其中与量子算法相关的几个问题 (问题 3, 4, 8 和 9) 很有希望在 5 年内取得突破, 与量子软件、量子复杂性、量子电路、量子密码等相关的问题 (问题 2, 5, 6 和 7), 极有可能在五至十年内取得重要的进展, 关于量子计算能力的问题 (问题 1) 则需要进行更长时间的探索研究. 但这只是一个粗略的判断, 并非绝对, 期待更多研究结果的出现.

3.1 图灵机模型下量子计算的优势极限

在量子计算领域最重要的研究问题无疑是去搞清楚量子计算的能力, 也就是说, 在最一般的图灵机计算模型下, 采用量子算法到底能够比经典算法量级上有多少提升? 特别是是否有可能有指数量级的提升? 用计算复杂性的语言来说, 即需要搞清楚量子多项式时间复杂性类 (BQP) 与经典概率多项式时间复杂性类 (BPP) 之间的关系, 以及 BQP 与 NP 之间的关系.

目前只知道 BPP⊆BQP⊆PSPACE, 这里 PSPACE 是多项式空间复杂性类. 一个重要的研究问题是能否进一步改进这里的上下界. Adelman 等 [20] 已经证明 BQP⊆PP, 这里 PP 是概率多项式时间复杂性类, 它与 BPP 的差别是不需要算法的错误率有界. 能否把上述上界替换成多项式层次复杂性类 PH? Aaronson [24] 给出了一些证据显示很可能 BQP⊈PH, 如果这一论断成立的话, 那么立即就能推出 BQP⊈NP, 也就是说量子图灵机在多项式时间内可以计算某些不在 NP 类里的问题. 另外还将推出 P≠PSPACE, 这些对我们理解经典计算复杂性也有着巨大的帮助.

经典计算复杂性理论中的 PCP 定理指出, 任何 NP 问题的实例, 例如可满足性, 都可以被适当地编码, 使得仅通过随机探查其中的 3 个比特, 就可以判断该实例是否可满足. 该定理不但加深了学术界对于 NP 问题的理解, 还给出了证明计算问题不可近似性的新方法. 建立量子版本的 PCP 定理是目前量子复杂性的一个重要研究课题.

在量子交互式证明系统方面, Jain 等 [14] 证明了量子交互式证明系统 QIP 的计算能力等价于多项式空间 PSPACE, 但是关于有多个证明者的量子交互证明系统 QMIP 的计算能力, 甚至是只能够采用量子纠缠的经典多证明者的交互式证明系统 MIP* 的计算能力都还没有搞清楚. 另外量子 Merlin-Arthur 复杂性类 QMA 的计算能力有多强? 如果有多项式个 Merlin, 即 QMA (poly), 是否一定比 QMA 本身要强?

3.2 其他计算模型下量子计算的优势极限

为了全面搞清楚量子计算的能力 (极限), 除了在最一般的图灵机模型下进行研究外, 还需要在特定的计算模型下去研究采用量子算法到底比经典算法在量级上能够有多少提升. 姚期智 [3] 已经证明, 在电路模型下量子计算复杂性与量子图灵机等价, 其他的一些重要的计算模型包括: 判定树复杂性模型, 通信复杂性模型, 量子自动机等.

在判定树模型下, Buhrman 等 [34] 已经证明量子判定树比经典判定树至多有开 6 次方量级的加速, 另一方面 Ambainis 等 [32] 最新构造的函数使用量子判定树可以达到比经典判定树开 4 次方量级的加速. 如何进一步缩小甚至关闭两者之间的差距是目前判定树领域研究的一个重点. 想要解决这一问题不光需要对量子判定树继续进行深入研究, 同时需要对经典判定树复杂度有更加深刻的认识. 经典判定树研究领域中一个 20 多年没有解决的重要的猜想 – 敏感度复杂性猜想断言说, 敏感度复杂性 $s(f)$ 与判定树复杂性 $D(f)$ 之间是多项式量级相关的, 目前还没有例子能够给出 $s(f)$ 与 $D(f)$ 之间

超过平方量级的差距. 如果两者的差距真的只有平方量级, 即 $s(f)^2 \geqslant D(f)$, 那么结合之前 Buhrman 等 [34] 已经证明的 $Q(f)^2 \geqslant s(f)$, 就可以得到 $Q(f)^4 \geqslant D(f)$, 也就是说两者的差距就是 4 次方量级的, 目前的例子已经是紧的了. 此外关于随机判定树复杂度与量子判定树复杂度之间的关系也还没有完全搞清楚, 目前最好的上下界分别是 2.5 次方和 6 次方.

在通信复杂度模型下, 学者们猜想采用量子通信不能够比经典的随机通信有指数量级的提升, 但是该问题还远未解决, 即使针对一些限制更强的模型, 例如单向量子通信模型, 以及采用 XOR 函数方式的双方通信模型. 后者与通信复杂性中长期悬而未决的 log-rank 猜想有关.

3.3 经典难解问题的量子算法

在 Shor 提出大整数分解问题和离散对数问题的量子多项式时间算法之后, 20 年来学者们一直致力于寻找其他重要的计算问题, 能够在量子计算机上获得高效的解决, 而 (目前为止) 不存在任何有效的经典算法, 图同构问题是其中一个备受学者们关注的备选问题. 图同构问题, 即判定两个图之间是否存在一个顶点间的 1-1 映射, 使得第 1 个图经过映射后变为第 2 个图. 该问题本身是计算复杂性领域中非常重要的一个未解问题, 关于它的经典算法的研究已经进行了 30 多年, 最近 Babai [165] 在此问题的经典算法上取得了重要突破, 给出了准多项式时间的算法.

图同构问题是非 Abel 群上的隐子群问题的一个特例, 隐子群问题 (hidden subgroup problems, HSP) 一般性的描述如下: 已知某个黑盒函数 $f: G \to X$ 将群 G 映射到集合 X, 并且满足: 存在 G 的某个子群 $K \leqslant G$, 使得任给 $a, b \in G$, $f(a) = f(b)$ 当且仅当 $a + K = b + K$, 也就是说函数 f 在 K 的任何一个陪集上的函数值都相同, 而在 K 的不同的陪集上函数值不同. 问题的目标是设计出一个有效的 (即多项式时间的) 量子算法来确定子群 K. 这里所谓黑盒函数是指, 我们唯一可以访问函数 f 的方式是选取群元素 $a \in G$, 并查询 $f(a) =?$ 除此之外不可以对函数 f 进行其他的操作.

当 G 是 Abel 群时, 此问题称为 Abel 群上的隐子群问题, 很多非常著名的问题, 例如大整数分解问题等都属于此类. 对于 Abel 群上的隐子群问题, 借助量子 Fourier 变换可以给出一个多项式时间的量子算法 [166]. 当 G 是非 Abel 群时, 此问题称为非 Abel 群上的隐子群问题. 图同构问题, 以及某种形式的最短向量问题都属于此类. 目前非 Abel 群上的隐子群问题尚无多项式时间的量子算法, 仅对一些特殊的非 Abel 群, 例如二面体群有部分结果. 而且学者已经证明, 仿照 Shor 算法简单的使用量子 Fourier 变换对该问题无效.

3.4 面向特定领域的新型量子算法

通用的量子计算机在较短的时期内可能还不能够很快地被制造出来, 但是针对某些特定领域、特定问题的特定算法的专用量子计算设备则有可能先于通用量子计算机问世.

Harrow 等 [81] 提出的 HHL 量子算法能够在 $O(\kappa^2 \log N)$ 的时间求解线性方程组, 但其算法复杂度与矩阵 A 的条件数 κ 之间是平方量级相关的, 如果 A 的条件数很大, 那么算法就会很慢, 甚至可能比经典的算法 (例如共轭梯度下降法) 要慢. Ambianis [167] 提出了一个新的量子算法, 复杂度为 $O(\kappa \log^3 \kappa \log N)$, 改进了算法对条件数 κ 的依赖. 是否能够进一步的改进算法与条件数之间的关系是目前的一个研究热点, 另外能否给出一个用条件数表示的求解线性方程组的量子算法的下界? 事实上如何使用条件数给出一个经典算法的下界也是一个重要的研究问题.

Lloyd 等在求解线性方程组的基础上还提出了包括聚类 [82], 支持向量机分类 [83] 等一些量子算法, 对于更加复杂的机器学习问题是否能够有量子算法进行加速? 例如神经元网络的参数训练问题, 甚至

深度机器学习中的参数训练问题等 (例如像 AlphaGo 这种下棋的深度学习算法). 在另一个方向上, 与求解线性方程组类似的一些问题, 像矩阵 SVD 分解, PCA 等是否可以有更好的量子算法, 甚至包括矩阵相乘最好的量子算法能够有多大幅度的提升? Le Gall 等 [168] 关于矩阵相乘有一些初步的结果.

针对目前大数据领域涌现出的一些新的计算问题, 量子算法能否提供新的解决思路? 例如在社会网络上的社区发现问题, 在大图中找三角形、四边形等都可以看作是该问题的特例. 目前关于在图中找三角形问题的量子算法, 学术界研究的最多 [67~70, 72], 关于 K_4 和更大的图, 也有一些部分结果 [74], 但上下界之间还有很大的差距.

3.5 量子软件和程序理论

量子程序设计早期的研究主要包括量子随机存储模型的提出, 以及经典程序设计语言的量子扩充等, 这类语言虽然数据是量子的, 但是其程序控制还是经典的, 真正意义上的量子程序应当是 "量子数据"+"量子控制". 经过近十多年的研究, 带经典控制流的量子程序理论已经基本成型, 包括操作语义、指称语义、最弱前置条件以及范畴论语义等都已建立起来.

递归是程序设计中最重要的技术之一, 例如分治算法、深度优先搜索等都需要用到递归. 带有量子控制流的递归程序, 包括其操作语义、指称语义等该如何定义? 更简单的像量子循环程序, 特别是有嵌套的循环程序的定义以及程序的终止问题等, 都是目前研究的热点. 另外一些重要的研究方向还包括: 能否建立一套量子递归的 Floyd-Hoare 逻辑? 如何从物理上来实现带量子控制流的量子递归? 能否借助带量子控制的量子程序更好地解决现有的一些问题等. 这些都需要对于相关问题的物理本质有更加深刻的理解.

量子模型检测和量子程序的自动验证是发展量子软件理论不可或缺的重要基石, 目前这方面的研究工作才刚刚起步, 一些重要的进展包括应明生等提出的量子 Hoare 逻辑以及在其上完成的对 Shor 算法和 Grover 算法的验证工作等, 这一方向还需要更加深入的进行研究. 此外并发量子程序、分布式的量子程序、量子通信协议等的自动验证, 以及量子程序的自动生成等也都是未来重要的研究方向.

3.6 设备无关的量子密码

密码协议的安全性除了依赖于所选取的困难问题的计算复杂性假设外, 还要依赖于随机数的选取, 随机数质量的好坏直接关系到密码协议的安全性, 如果每次都使用相同的随机数那么密码协议也是不安全的. 目前大多数的随机数产生方案都依赖于随机数产生器的特殊结构, 或者需要假设两个以上随机源的独立性. 这两个假设都无法进行验证, 在实际中也很难加以保证, 如何用最低的要求来保证产生的 "随机数" 的随机性是一个具有重要现实意义的问题.

由于量子力学的测不准原理使得量子机制具有天然的随机性, 因此通过量子机制来产生随机数得到了学者们越来越多的关注. 2006 年 Colkbeck [123] 在其博士论文中最先提出了通过检查是否违背贝尔不等式来生成可信的随机数. 在 Colkbeck 提出的协议中, 通信双方在一个不可信的量子设备上反复运行非定域的贝尔测试, 如果该设备能够超过经典的上界, 即违背贝尔不等式, 则证明了该设备一定是量子机制的, 因此可以相信该设备制备的随机数是按照量子测不准原理得到的.

2014 年施尧耘等 [16] 给出了一种只需要极少的理论假设的量子随机数产生方案, 该方案只需要假设初始有一个弱随机源, 设备之间不能通信, 以及基本量子力学定律的正确性, 就能保证从一个不可信的量子设备中抽取出任意长的随机数. 这里弱随机源只需对量子设备随机, 甚至不需要对窃听者随机 (即可以和窃听者的随机数正相关). 但该方案所需要的量子测量精度等技术指标仍旧过高, 无法应

用于实际中像量子密钥分发等商用量子设备, 甚至目前在实验室中都还不能够进行实验的验证. 如何进一步降低在不可信量子设备上产生安全的量子随机数的实验要求是目前这一方向研究的重点.

3.7 量子电路优化

要想构建出实用的量子计算机, 量子电路的设计和优化必不可少. 近些年量子电路优化和综合领域取得了很多进展, 但依然还有很多重要的问题需要解决. 在构建任意 n 输入量子门的研究方面, 2003 年 Shende 等 [136] 构造性地证明了任何偶排列能够在不使用辅助系统的条件下由非门、 CNOT 门和 Toffoli 门实现. 另一方面存在一个 n 输入的可逆函数, 实现这个函数需要使用 $\Omega(n2^n/\log n)$ 个量子门. 2010 年 Saeedi 等 [148] 改进了 Shende 等的构造, 将门电路的规模降至 $8.5n2^n + o(2^n)$, 这与 $\Omega(n2^n/\log n)$ 的下界还存在不小的差距, 如何改进实现可逆函数需要的量子门电路数目的上界和下界有重要理论和实际意义.

在构建一些特殊的量子门电路方面, 1995 年 Barenco 等 [133] 用 CNOT 门实现了 Toffoli 门, 在不使用辅助系统时 Barenco 等的构造一共使用了 $\Theta(n^2)$ 个 CNOT 门, 如果允许使用辅助系统, 则只需要 $\Theta(n)$ 个 CNOT 门即足够. 实现一个 n 比特输入的 Toffoli 门所需要的最少的 CNOT 门的数目到底是多少? Barenco 的设计是否已经达到最优? 另外其他重要的量子门, 例如 Fredkin 门等所需要的 CNOT 数目也尚未完全搞清楚.

在量子电路构建方面, 一些特殊的量子电路, 例如稳定电路 (stabilizer circuit), GF(2) 线性电路等, 由于其自身的特性, 在量子信息领域发挥着重要的作用, 关于构建特殊量子电路的最小规模、最优深度等优化问题目前还有待解决. 这里稳定电路是指由 Hadamard 门、相位门、CNOT 门和测量操作构成的量子电路 [141], 稳定电路在量子纠错、量子编码和量子传输等领域有重要的作用.

3.8 无差错量子算法

常见的量子算法, 像 Shor 大整数分解算法 [6]、Grover 搜索算法 [7] 等, 算法都是可能出错的, 量子多项式时间复杂性类 BQP 在定义的时候也允许以小概率出错 (错误率小于 1/3). 但是最早的两个量子算法, Deutsh-Jozsa 算法 [4] 和 Simon 算法 [5], 都是百分之百正确的. 因此一个重要的研究方向是无差错的量子算法到底能够对哪些计算问题带来加速? 其最多能在量级上带来多少提升? 如果只是采用类似 Simon 算法的思想, 将可以把算法复杂度从 n 加速到 $n/2$, 最近 Ambainis [35] 设计了一个新的无差错量子算法, 在一个复合型的布尔函数上可以把计算复杂度从 n 加速到 $Q_E(f) = O(n^{0.8675\cdots})$, 2015 年 Ambainis 等 [32] 再次提出一个新的函数, 其无差错量子算法复杂度可以到 $O(n^{0.5})$, 而经典的随机算法复杂度也要 $\Omega(n)$, 即量子无差错算法可以达到平方量级的加速. 另一方面, 目前已知的 $Q_E(f)$ 最好的下界是 $Q_E(f) \geqslant D(f)^{1/3}$, 上下界之间还有 1/6 的差距. 最近邱道文等 [169] 研究了一次量子无错查询复杂性的对称部分布尔函数. 一个自然的问题是, 如何刻画具有 k 次量子无错查询复杂性的对称部分布尔函数?

另外一个重要的研究方向是确定无差错的量子算法的计算能力到底有多强, 即研究无差错的量子多项式时间复杂性类 ZQP (zero-error quantum polynomial time), 显然 ZQP 包含于 BQP 内, 同时 ZQP 包含无差错概率多项式时间复杂性类 ZPP, 即 ZPP$\subseteq$ZQP$\subseteq$BQP, 但是目前还不清楚这两边是否是紧的, 包括是否可以使用神谕来区分开它们, 即是否存在神谕 A, 使得 $\mathrm{ZPP}^A \subsetneq \mathrm{ZQP}^A$.

3.9 量子模拟及波色采样算法

构建大规模的量子系统以模型量子化学、高温超导, 以及高能物理中的真实量子系统, 其中一个关键问题是如何克服退相干性等环境噪声影响, 制备高质量的多光子纠缠态, 潘建伟教授领导的团队在这方面的研究处于世界领先地位.

多光子纠缠态还可以用来进行波色采样, 目前还不清楚经典计算能否对波色采样的分布进行模拟, 该问题与经典复杂性理论中如何计算一个矩阵的积和式 (permanent) 有着直接的联系, 2011 年 Aaronson 和 Arkhipov [93] 基于 "近似一个 Gauss 矩阵的积和式是 #P 困难的" 等复杂性假设证明了近似波色采样概率问题不在多项式层次复杂性类 (PH) 中. 能否移除这一假设前提? 或者证明这一假设前提是正确的? 这样将会给出量子算法比经典算法有指数量级能力提升的直接证据.

在实际中, 如何验证一个波色子采样的正确性? 具体来说, 能否向一个只有经典计算能力的验证者 (BPP) 证明波色采样的正确性? 能不能对波色采样给出容错的机制? 特别是只利用线性光子的容错方案, 因为目前的波色采样方案都是基于光子的. 能否找到更多可以借助波色采样的技术来解决的经典计算问题, 特别是一些经典计算中的难解问题, 也是一个重要的研究方向.

4 结论

在过去 20 年间, 量子计算得到了快速的发展, 取得了一系列重要的研究成果. 但在很多方面, 研究才刚刚起步, 显露出来的问题仅仅是冰山一角, 需要学者们付出更大的努力. 未来五到十年, 将是量子计算发展至关重要的阶段, 我们预计在求解困难问题的量子算法、面向特定领域的新型量子算法、无差错量子算法和量子波色采样等方面的研究中可能会取得突破, 在量子程序理论、量子复杂性、量子密码和量子电路等方面的研究工作会取得一些重要的进展, 对量子计算的能力会有更加全面的认识.

致谢 在本文的撰写过程中得到了包括应明生教授、肖侬教授、冯元教授、段润尧教授、季铮锋教授、高飞教授、邱道文教授、吴热冰教授、张靖教授等的大力支持和帮助, 在此表示真诚的感谢! 另外李乾、何昆、陈志怀等对本文亦有重要贡献.

参考文献

1 Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer. Proc Royal Soc A-Math Phys Eng Sci, 1985, 400: 97–117
2 Bernstein E, Vazirani U. Quantum complexity theory. SIAM J Comput, 1997, 26: 1411–1473
3 Yao A C-C. Quantum circuit complexity. In: Proceedings of the 34th Annual Symposium on Foundations of Computer Science, Palo Alto, 1993. 352–361
4 Deutsch D, Jozsa R. Rapid solution of problems by quantum computation. Proc Royal Soc A-Math Phys Eng Sci, 1992, 439: 553–558
5 Simon D R. On the power of quantum computation. SIAM J Comput, 1997, 26: 1474–1483
6 Shor P W. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, 1994. 124–134
7 Grover L K. A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on the Theory of Computing. New York: ACM, 1996. 212–219
8 Ambainis A. Quantum walk algorithm for element distinctness. SIAM J Comput, 2007, 37: 210–239
9 Brassard G, Høyer P, Mosca M, et al. Quantum amplitude amplification and estimation. Quant Comput Inf, 2002, 305: 53–74

10 Harrow A, Hassidim A, Lloyd S. Quantum algorithm for linear systems of equations. Phys Rev Lett, 2009, 15: 150502
11 Lloyd S, Mohseni M, Rebentrost P. Quantum algorithms for supervised and unsupervised machine learning. arXiv: 1307.0411
12 Hoyer P, Lee T, Spalek R. Negative weights make adversaries stronger. In: Proceedings of the 39th Annual ACM Symposium on Theory of Computing. New York: ACM, 2007. 526–535
13 Reichardt B W. Reflections for quantum query algorithms. In: Proceedings of the 22nd Annual ACM-SIAM Symposium on Discrete Algorithms. Philadelphia: Society for Industrial and Applied Mathematics, 2011. 560–569
14 Jain R, Ji Z F, Upadhyay S, et al. QIP = PSPACE. J ACM, 2011, 58: 30
15 Vazirani U, Vidick T. Fully device independent quantum key distribution. Phys Rev Lett, 2014, 113: 140501
16 Miller C A, Shi Y Y. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. In: Proceedings of the 46th Annual ACM Symposium on Theory of Computing. New York: ACM, 2014. 417–426
17 Gill J. Computational complexity of probabilistic Turing machines. SIAM J Comput, 1977, 6: 675–695
18 Lloyd S. Universal quantum simulators. Science, 1996, 273: 1073
19 Bernstein E, Vazirani U. Quantum complexity theory. SIAM J Comput, 1997, 26: 1411–1473
20 Adleman L, de Marrais J, Huang M-D. Quantum computability. SIAM J Comput, 1997 26: 1524–1540
21 Watrous J. Succinct quantum proofs for properties of finite groups. In: Proceedings of the 41st Annual Symposium on Foundations of Computer Science, Redondo Beach, 2000. 537–546
22 Bennett C H, Bernstein E, Brassard G, et al. Strengths and weaknesses of quantum computing. SIAM J Comput, 1997, 26: 1510–1523
23 Aaronson S, Shi Y Y. Quantum lower bounds for the collision and the element distinctness problems. J ACM, 2004, 51: 595–605
24 Aaronson S. Quantum computing, postselection, and probabilistic polynomial time. Proc Royal Soc London A: Math Phys Eng Sci, 2005, 461: 3473–3482
25 Aharonov D, Jones V, Landau Z. A polynomial quantum algorithm for approximating the Jones polynomial. Algorithmica, 2009, 55: 395–421
26 Freedman M, Larsen M, Wang Z. A modular functor which is universal for quantum computation. Commun Math Phys, 2002, 227: 605–622
27 Wocjan P, Zhang S Y. Several natural BQP-Complete problems. arXiv:quant-ph/0606179
28 Aaronson S, Ambainis A. Forrelation: a problem that optimally separates quantum from classical computing. In: Proceedings of the 47th Annual ACM on Symposium on Theory of Computing. New York: ACM, 2015. 307–316
29 Buhrman H, de Wolf R. Complexity measures and decision tree complexity: a survey. Theor Comput Sci, 2002, 288: 21–43
30 Yao A C-C. Some complexity questions related to distributive computing (preliminary report). In: Proceedings of the 11th Annual ACM Symposium on Theory of Computing. New York: ACM, 1979. 209–213
31 Sun X M, Yao A C-C. On the quantum query complexity of local search in two and three dimensions. In: Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science, Berkeley, 2006. 429–438
32 Ambainis A, Balodis K, Belovs A, et al. Separations in query complexity based on pointer functions. arXiv:1506.04719
33 Aaronson S, Ben-David S, Kothari R. Separations in query complexity using cheat sheets. arXiv: 1511.01937
34 Beals R, Buhrman H, Cleve R, et al. Quantum lower bounds by polynomials. In: Proceedings of the 39th Annual Symposium on Foundations of Computer Science, Palo Alto, 1998. 352–361
35 Ambainis A. Superlinear advantage for exact quantum algorithms. In: Proceedings of the 45th Annual ACM Symposium on Theory of Computing. New York: ACM, 2013. 891–900
36 Ambainis A, Gruska J, Zheng S G. Exact quantum algorithms have advantage for almost all Boolean functions. Quant Inf Comput, 2015, 15: 435–452
37 Baianu I. Organismic supercategories and qualitative dynamics of systems. Bulletin Math Biophys, 1971, 33: 339–354
38 Baianu I. Categories, functors and quantum automata theory. In: Proceedings of the 4th International Congress of Logic, Methodology and Philosophy of Science, Bucharest, 1971
39 Kondacs A, Watrous J. On the power of quantum finite state automata. In: Proceedings of the 38th Annual Symposium on Foundations of Computer Science, Miami Beach, 1997. 66–75
40 Ambainis A, Freivalds R. 1-way quantum finite automata: strengths, weaknesses and generalizations. In: Proceedings of the 39th Annual Symposium on Foundations of Computer Science, Palo Alto, 1998. 332–341

41 Ambainis A, Nahimovs N. Improved constructions of quantum automata. Theor Comput Sci, 2009, 410: 1916–1922
42 Ambainis A, Watrous J. Two-way finite automata with quantum and classical states. Theor Comput Sci, 2002, 287: 299–311
43 Moore C, Crutchfield J P. Quantum automata and quantum grammars. Theor Comput Sci, 2000, 237: 275–306
44 Li L Z, Qiu D W. Determining the equivalence for one-way quantum finite automata. Theor Comput Sci, 2008, 403: 42–51
45 Mateus P, Qiu D W, Li L Z. On the complexity of minimizing probabilistic and quantum automata. Inf Comput, 2012, 218: 36–53
46 Qiu D W, Li L Z, Mateus P, et al. Exponentially more concise quantum recognition of non-RMM languages. J Comput Syst Sci, 2015, 81: 359–375
47 Kitaev A Y, Shen A, Vyalyi M N. Classical and Quantum Computation. Providence: American Mathematical Society, 2002
48 Knill E. Quantum randomness and nondeterminism. arXiv:quant-ph/9610012
49 Aharonov D, Gottesman D, Irani S, et al. The power of quantum systems on a line. Commun Math Phys, 2009, 287: 41–65
50 Liu Y K. Consistency of local density matrices is QMA-complete. In: Approximation, randomization, and Combinatorial Optimization. Algorithms and Techniques. Berlin: Springer, 2006. 438–449
51 Watrous J. Succinct quantum proofs for properties of finite groups. In: Proceedings of the 41st Annual Symposium on Foundations of Computer Science, Redondo Beach, 2000. 537–546
52 Watrous J. Quantum computational complexity. In: Encyclopedia of Complexity and Systems Science. New York: Springer, 2009. 7174–7201
53 Harrow A W, Montanaro A. Testing product states, quantum Merlin-Arthur games and tensor optimization. J ACM, 2013, 60: 3
54 Li K, Smith G. Quantum de Finetti theorem under fully-one-way adaptive measurements. Phys Rev Lett, 2015, 114: 160503
55 Schwarz M. An exponential time upper bound for quantum Merlin-Arthur games with unentangled provers. arXiv:1510.08447
56 Watrous J. PSPACE has constant-round quantum interactive proof systems. Theor Comput Sci, 2003, 292: 575–588
57 Kitaev A, Watrous J. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In: Proceedings of the 32nd Annual ACM Symposium on Theory of Computing. New York: ACM, 2000. 608–617
58 Ito T, Kobayashi H, Preda D, et al. Generalized Tsirelson inequalities, commuting-operator provers, and multi-prover interactive proof systems. In: Proceedings of IEEE Conference on Computational Complexity, College Park, 2008. 187–198
59 Ito T, Kobayashi H, Watrous J. Quantum interactive proofs with weak error bounds. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. New York: ACM, 2012. 266–275
60 Fitzsimons J, Vidick T. A multiprover interactive proof system for the local Hamiltonian problem. In: Proceedings of the Conference on Innovations in Theoretical Computer Science. New York: ACM, 2015. 103–112
61 Natarajan A, Vidick T. Constant-soundness interactive proofs for local Hamiltonians. arXiv:1512.02090
62 Ji Z F. Classical verification of quantum proofs. arXiv:1505.07432
63 Ambainis A, Childs A M, Reichardt B, et al. Any AND-OR formula of size N can be evaluated in time N 1/2+o(1) on a quantum computer. SIAM J Comput, 2010, 39: 2513–2530
64 Santha M. On the Monte Carlo boolean decision tree complexity of read-once formulae. Random Struct Algorithm, 1995, 6: 75–87
65 Buhrman H, Durr C, Heiligman M, et al. Quantum algorithms for element distinctness. SIAM J Comput, 2005, 34: 1324–1330
66 Magniez F, Santha M, Szegedy M. Quantum algorithms for the triangle problem. In: Proceedings of ACM-SIAM Symposium on Discrete Algorithms, Vancouver, 2005. 1109–1117
67 Magniez F, Santha M, Szegedy M. Quantum algorithms for the triangle problem. SIAM J Comput, 2007, 37: 413–424
68 Belovs A. Span programs for functions with constant-sized 1-certificates: extended abstract. In: Proceedings of the 44th Symposium on Theory of Computing. New York: ACM, 2012. 77–84
69 Lee T, Magniez F, Santha M. Improved quantum query algorithms for triangle finding and associativity testing. In:

Proceedings of the 24th Annual ACM-SIAM Symposium on Discrete Algorithms, New Orleans, 2013. 1486–1502
70 Jeffery S, Kothari R, Magniez F. Nested quantum walks with quantum data structures. In: Proceedings of the 24th Annual ACM-SIAM Symposium on Discrete Algorithms, New Orleans, 2013. 1474–1485
71 Sun X M, Yao A C-C, Zhang S Y. Graph properties and circular functions: how low can quantum query complexity go? In: Proceedings of the 19th IEEE Conference on Computational Complexity, Amherst, 2004. 286–293
72 Belovs A, Rosmanis A. On the power of non-adaptive learning graphs. In: Proceedings of the 28th Conference on Computational Complexity, Stanford, 2013. 44–55
73 Le Gall. Improved quantum algorithm for triangle finding via combinatorial arguments. In: Proceedings of the 55th Annual Symposium on Foundations of Computer Science, Philadelphia, 2014. 216–225
74 Ambainis A. Quantum walk algorithm for element distinctness. SIAM J Comput, 2007, 37: 210–239
75 Belovs A. Learning-graph-based quantum algorithm for k-distinctness. In: Proceedings of the 53rd Annual Symposium on Foundations of Computer Science, New Brunswick, 2012. 207–216
76 Brassard G, Hoyer P, Mosca M, et al. Quantum amplitude amplification and estimation. Contemp Math, 2002, 305: 53–74
77 Schoning T. A probabilistic algorithm for k-SAT and constraint satisfaction problems. In: Proceedings of the 40th Annual Symposium on Foundations of Computer Science, New York City, 1999. 410–414
78 Durr C, Hoyer P. A quantum algorithm for finding the minimum. arXiv:quant-ph/9607014
79 Dürr C, Heiligman M, Høyer P, et al. Quantum query complexity of some graph problems. In: Automata, Languages and Programming. Berlin Springer, 2004. 481–493
80 Ramesh H, Vinay V. String matching in O(n+m) quantum time. J Discrete Algorithms, 2003, 1: 103–110
81 Harrow A W, Hassidim A, Lloyd S. Quantum algorithm for linear systems of equations. Phys Rev Lett, 2009, 103: 150502
82 Lloyd S, Mohseni M, Rebentrost P. Quantum algorithms for supervised and unsupervised machine learning. arXiv:1307.0411
83 Rebentrost P, Mohseni M, Lloyd S. Quantum support vector machine for big data classification. Phys Rev Lett, 2014, 113: 130503
84 Wiebe N, Braun D, Lloyd S. Quantum Algorithm for Data Fitting. Phys Rev Lett, 2012, 109: 050505
85 Garnerone S, Zanardi P, Lidar D A. Adiabatic Quantum Algorithm for Search Engine Ranking. Phys Rev Lett, 2012, 108: 230506
86 Clader B D, Jacobs B C, Sprouse C R. Preconditioned Quantum Linear System Algorithm. Phys Rev Lett, 2013, 110: 250504
87 Farhi E, Goldstone J, Gutmann S, et al. Quantum computation by adiabatic evolution. arXiv:quant-ph/0001106
88 van Dam W, Mosca M, Vazirani U. How Powerful is Adiabatic Quantum Computation? In: Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science, Las Vegas, 2001. 279–287
89 King J, Yarkoni S, Nevisi M M, et al. Benchmarking a quantum annealing processor with the time-to-target metric. arXiv:1508.05087
90 Feynman R. Simulating physics with computers. Int J Theor Phys, 1982, 21: 467–488
91 Lloyd S. Universal quantum simulators. Science, 1996, 273: 1073–1078
92 Berry D W, Childs A M. Black-box Hamiltonian simulation and unitary implementation. Quant Inf Comput, 2012, 12: 29–62
93 Aaronson S, Arkhipov A. The computational complexity of linear optics. In: Proceedings of the 43rd Annual ACM Symposium on Theory of Computing. New York: ACM, 2011. 333–342
94 Broome M A, Fedrizzi A, Rahimi-Keshari S, et al. Photonic boson sampling in a tunable circuit. Science, 2013, 339: 794–798
95 Crespi A, Osellame R, Ramponi R, et al. Integrated multimode interferometers with arbitrary designs for photonic boson sampling. Nature Photonics, 2013, 7: 545–549
96 Ralph T C. Quantum computation: Boson sampling on a chip. Nature Photonics, 2013, 7: 514–515
97 Spring J B, Metcalf B J, Humphreys P C, et al. Boson sampling on a photonic chip. Science, 2013, 339: 798–801
98 Knill E H. Conventions for Quantum Pseudo-Code. LANL report LAUR-96-2724. 1996
99 Omer B. A procedure formalism for quantum computing. Dissertation for Ph.D. Degree. Vienna: Technical University of Vienna, 1998
100 Sanders J W, Zuliani P. Quantum computing. In: Proceedings of Mathematics of Program Construction, LNCS,

Ponte de Lima, 2000. 1837: 80–99
101 Bettelli S, Calarco T, Serafini L. Toward an architecture for quantum programming. arXic:cs.PL/0103009
102 Selinger P. Towards a quantum programming language. Math Struct Comput Sci, 2004, 14: 527–586
103 Sabry A. Modeling quantum computing in Haskell. In: Proceedings of the ACM SIGPLAN Workshop on Haskell. New York: ACM, 2003. 39–49
104 Valiron B. A functional programming language for quantum computation with classical control. Dissertation for Master's Degree. Ottawa: University of Ottawa, 2004
105 Altenkirch T, Grattage J. A functional quantum programming language. In: Proceedings of the 20th Annual IEEE Symposium on Logic in Computer Science, Chicago, 2005. 249–258
106 Ying M S. Foundations of quantum programing. In: Proceedings of the 8th Asian Conference on Programming Languages and Systems. New York: ACM, 2016. 16–20
107 Valiron B, Ross N J, Selinger P, et al. Programming the quantum future. Commun ACM, 2015, 58: 52–61
108 Abramsky S. High-level methods for quantum computation and information. In: Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science, Turku, 2004. 410–414
109 Abramsky S, Coecke B. A categorical semantics of quantum protocols. In: Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science, Turku, 2004. 415–425
110 van Tonder A. A Lambda calculus for quantum computation. SIAM J Comput, 2004, 33: 1109–1135
111 Petersen A, Oskin M. A new algebraic foundation for quantum programming languages. In: Proceedings of the 2nd Workshop on Non-Silicon Computing at ISCA, San Diego, 2003. 88: 3544–3549
112 Girard J-Y. Between logic and quantic: a tract. Linear Logic Comput Sci, 2004, 316: 346–381
113 Gay S J, Nagarajan R. Communicating quantum processes. In: Proceedings of the 32nd ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages. New York: ACM, 2005. 145–157
114 Lalire M. Relations among quantum processes: bisimilarity and congruence. Math Struct Comput Sci, 2006, 16: 407–428
115 Ying M. Floyd-Hoare logic for quantum programs. ACM Trans Program Lang Syst, 2011, 33: 19
116 Feng Y, Duan R Y, Ying M S. Bisimulation for quantum processes. ACM Trans Program Lang Syst, 2012, 34: 17
117 Ying M S, Feng Y. Quantum loop programs. Acta Inform, 2010, 47: 221–250
118 Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing. New York: IEEE Press, 1984. 175–179
119 Mayers D. Unconditional security in quantum cryptography. J ACM, 2001, 48: 351–406
120 Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett, 2000, 85: 441–444
121 Bennett C H, Bessette F, Brassard G, et al. Experimental quantum cryptography. J Cryptol, 1998, 5: 3–28
122 Mayers D, Yao A. Quantum cryptography with imperfect apparatus. In: Proceedings of the 39th Annual Symposium on Foundations of Computer Science, Palo Alto, 1998. 503–509
123 Colbeck R. Quantum and relativistic protocols for secure multi-party computation. Dissertation for Ph.D. Degree. Cambridge: University of Cambridge, 2006
124 Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution. Phys Rev Lett, 2012, 108: 130503
125 Pirandola S, Ottaviani C, Spedalieri G, et al. High-rate measurement-device-independent quantum cryptography. Nat Photon, 2015, 9: 397–402
126 Sasaki T, Yamamoto Y, Koashi M. Practical quantum key distribution protocol without monitoring signal disturbance. Nature, 2014, 509: 475–478
127 Nauerth S, Moll F, Rau M, et al. Air-to-ground quantum communication. Nature Photonics, 2013, 7: 382–386
128 Sasaki T, Yamamoto Y, Koashi M. Practical quantum key distribution protocol without monitoring signal disturbance. Nature, 2014, 509: 475
129 Guan J-Y, Cao Z, Liu Y, et al. Experimental passive round-robin differential phase-shift quantum key distribution. Phys Rev Lett, 2015, 114: 180502
130 Wang S, Yin Z-Q, Chen W, et al. Experimental demonstration of a quantum key distribution without signal disturbance monitoring. Nature Photonics, 2015, 9: 832–836
131 Gao F, Guo F-Z, Wen Q-Y, et al. Comment on "experimental demonstration of a quantum protocol for Byzantine agreement and liar detection". Phys Rev Lett, 2008, 101: 208901

132 Gao F, Wen Q-Y, Zhu F-C. Teleportation attack on the QSDC protocol with a random basis and order. Chinese Phys B, 2008, 17: 3189–3193

133 Barenco A, Bennett C H, Cleve R, et al. Elementary gates for quantum computation. Phys Rev A, 1995, 52: 3457–3467

134 Calderbank A R, Shor P W. Good quantum error-correcting codes exist. Phys Rev A, 1996, 54: 1098–1105

135 Shende V V, Markov I L, Bullock S S. Minimal universal two-qubit controlled-NOT-based circuits. Phys Rev A, 2004, 69: 062321

136 Shende V V, Prasad A K, Markov I L, et al. Synthesis of reversible logic circuits. IEEE Trans Comput-Aided Design Integr Circ Syst, 2003, 22: 710–722

137 Yang G, Song X, Hung W N N, et al. Bi-directional synthesis of 4-bit reversible circuits. Comput J, 2008, 51: 207–215

138 Golubitsky O, Falconer S M, Maslov D. Synthesis of the optimal 4-bit reversible circuits. In: Proceedings of the 47th Design Automation Conference. New York: ACM, 2010. 653–656

139 Hung W, Song X, Yang G, et al. Optimal synthesis of multiple output Boolean functions using a set of quantum gates by symbolic reachability analysis. IEEE Trans Comput-Aided Des Integr Circ Syst, 2006, 25: 1652–1663

140 Grosse D, Wille R, Dueck G, et al. Exact multiple-control Toffoli network synthesis with SAT techniques. IEEE Trans Comput-Aided Des Integr Circ Syst, 2009, 28: 703–715

141 Aaronson S, Gottesman D. Improved simulation of stabilizer circuits. Phys Rev A, 2004, 70: 052328

142 Patel K N, Markov I L, Hayes J P. Optimal synthesis of linear reversible circuits. Quant Inf Comput, 2008, 8: 282–294

143 Maslov D. Linear depth stabilizer and quantum Fourier transformation circuits with no auxiliary qubits in finite neighbor quantum architectures. Phys Rev A, 2007, 76: 052310

144 Miller D M, Maslov D, Dueck G W. A transformation based algorithm for reversible logic synthesis. In: Proceedings of the 40th Annual Design Automation Conference. New York: ACM, 2003. 318–323

145 Maslov D, Dueck G W, Miller D M. Techniques for the synthesis of reversible Toffoli networks. ACM Trans Des Autom Electron Sys, 2007, 12: 1–28

146 Gupta P, Agrawal A, Jha N K. An algorithm for synthesis of reversible logic circuits. IEEE Trans Comput-Aided Des Integr Circ Syst, 2006, 25: 2317–2330

147 Donald J, Jha N K. Reversible logic synthesis with Fredkin and Peres gates. J Emerg Tech Comput Syst, 2008, 4: 1–19

148 Saeedi M, Zamani M S, Sedighi M, et al. Reversible circuit synthesis using a cycle-based approach. J Emerg Tech Comput Syst, 2010, 6: 1–26

149 Peng F, Xie G J. Optimum design of quantum teleportation circuit. J Appl Sci, 2010, 28: 313–317 [彭斐, 解光军. 量子隐形传态电路的优化设计. 应用科学学报, 2010, 28: 313–317]

150 Yang G, Song X, Hung W N, et al. Group theory based synthesis of binary reversible circuits. Lec Notes Comput Sci, 2006, 3959: 365–374

151 DiVincenzo D P, Smolin J A. Results on two-bit gate design for quantum computers. In: Proceedings of the Workshop on Physics and Computation, Dallas, 1994. 14–23

152 Yu N, Duan R, Ying M. Five two-qubit gates are necessary for implementing the Toffoli gate. Phys Rev A, 2013, 88: 010304

153 Song G, Klappenecker A. The simplified Toffoli gate implementation by Margolus is optimal. QIC, 2004, 4: 361–372

154 Shende V V, Markov I L. On the CNOT-cost of TOFFOLI gates. Quant Inf Comput, 2009, 9: 461–486

155 Bocharov A, Svore K M. Resource-optimal single-qubit quantum circuits. Phys Rev Lett, 2012, 109: 190501

156 Bocharov A, Gurevich Y, Svore K M. Efficient decomposition of single-qubit gates into V basis circuits. Phys Rev A, 2013, 88: 012313

157 Bocharov A, Roetteler M, Svore K M. Efficient synthesis of universal repeat-until-success quantum circuits. Phys Rev Lett, 2015, 114: 080502

158 Ross N J, Selinger P. Optimal ancilla-free Clifford+T approximation of z-rotations. arXiv:1403.2975

159 Selinger P. Generators and relations for n-qubit Clifford operators. arXiv:1310.6813

160 Selinger P. Efficient Clifford+T approximation of single-qubit operators. Quant Inf Comput, 2012, 15: 159–180

161 Maslov D. Reversible logic synthesis benchmarks page. http://www.cs.uvic.ca/dmaslov. 2011

162 Wille R, Grosse D, Teuber L, et al. RevLib: an online resource for reversible functions and reversible circuits. In: Proceedings of the 38th International Symposium on Multiple Valued Logic, Dallas, 2008. 220–225

163 Soeken M, Frehse S, Wille R, et al. RevKit: a toolkit for reversible circuit design. Multiple-Valued Logic Soft

Comput, 2012, 18: 55–65
164 Shi Y-Y, Duan L-M, Vidal G. Classical simulation of quantum many-body systems with atree tensor network. Phys Rev A, 2006, 74: 022320
165 Babai L. Graph isomorphism in quasipolynomial time. In: Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing. New York: ACM, 2016. 684–697
166 Mosca M. Quantum computer algorithms. Dissertation for Ph.D. Degree. Oxford: University of Oxford, 1999
167 Ambainis A. Variable time amplitude amplification and quantum algorithms for linear algebra problems. In: Proceedings of the 29th Symposium on Theoretical Aspects of Computer Science, Paris, 2012. 636–647
168 Le Gall F. Quantum complexity of Boolean matrix multiplication and related problems. In: Computing With New Resources. Berlin: Springer, 2014. 176–191
169 Qiu D W, Zheng S G. Characterizations of symmetrically partial Boolean functions with exact quantum query complexity. arXiv: 1603.06505

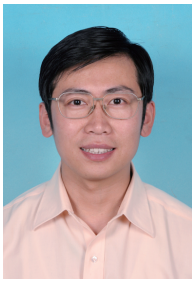
A survey on quantum computing

Xiaoming SUN

Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190*, China*
E-mail: sunxiaoming@ict.ac.cn

Abstract On the basis of its unrivalled potential to solve factorization problems and further application in cryptography, quantum computing is considered as one of the most promising computational models for the future. It provides a new angle for thinking of computation and a new approach for attack various computationally difficult problems. In this article, we give a comprehensive survey of developments in the last twenty years on quantum algorithms, quantum complexity, quantum programming theory, quantum circuits, and quantum cryptography that we hope will serve as references for researchers in related fields. We also outline various research directions and open problems in this area, with the hope of prompting further progress or even solutions.

Keywords quantum algorithms, quantum complexity, quantum programming theory, quantum circuits, quantum cryptography



Xiaoming SUN received B.S. and Ph.D. degrees in computer science from Tsinghua University, Beijing, China, in 2001 and 2005, respectively. Currently he is a professor at the Institute of Computing Technology, Chinese Academy of Sciences. He was previously an associate professor at the Institute for Advanced Study, Tsinghua University. His current research interests include approximation algorithms, computational complexity, and quantum computing. He is currently an associate director of the Technical Committee on Theoretical Computer Science of China Computer Federation (CCF TCTCS). He is also a member of the editorial board of the Journal of Software, Journal of Computer Science and Technology, and Computer Research and Development.