量子复杂性理论进展概述

刘宇攀*

浙江大学计算机学院

2016 年 6 月 20 日

摘要

本文论述了量子 (计算) 复杂性理论的部分近年进展. 从经典计算复杂性理论的自然对应, 复杂性类 BQP 和 QMA 的定义及其完全 (Complete) 问题; 到哈密顿量复杂性 (Hamiltonian complexity) 及其与凝聚态物理间的联系, 以及量子 PCP 猜想; 再到量子交互式证明系统 (Quantum interactive proof system) 和量子计数复杂性; 最后论述量子至上 (Quantum supremacy) 与扩展 Church-Turing 论题 (Extended Church-Turing thesis) 的关系.

目录

*yp_liu@zju.edu.cn

1 引言

关于可计算性的讨论, 很可能要追溯到上个世纪初, David Hilbert 提出的第十问题:

定义 1.1 (Hilbert 第十问题)**.** *给定有多个未知数和有理整数系数的丢番图方程 (Diophantine equation), 设计一个过程在有限步操作内判定方程是否存在有理整数解.*

如何进一步将这一问题的求解过程定义良好 (well-defined) 呢? 一些人尝试给出算法, 这一自然的概念的形式化定义. 对于算法定义的讨论, 引出了对算法和可计算性的定义, 以及作为计算机科学最为核心的分支之一的计算复杂性理论.

剩下的事情很多人都知道, 三十年后, Kurt Gödel(原始递归函数), Alonzo Church(Lambda Calculus), Alan Turing(Turing 机), 一些人试图定义什么是可计算性, 什么是计算模型, 什么是算法; 再过了三四十年, Stephen Cook(NP 完全性, 证明复杂性), Richard Karp(多项式规约), Andrew Yao(通信复杂西性和密码学), Leslie Valiant(计数复杂性和 PAC Learning), László Babai(交互式证明系统和图同构), 一些人试图考虑资源对计算的影响, 种种情形下计算的有效性, 如何对不同的问题分类并找到内禀的深刻联系.

而上世纪三十年代之后, 伴随着对"以太"的否定和对黑体辐射的解释, 新的物理学出现了. 不同于基于分析方法 (微积分) 的经典力学, 基于代数理论 (线性代数) 的物理解释了上述的所有现象. Werner Heisenberg(量子力学的矩阵描述), Erwin Schrödinger(量子力学的波动方程描述), John von Neumann(量子力学的公理化及算子代数), Paul Dirac(量子力学的公理化), 一些人在尝试公理化新的物理, 并联系背后的数学 (如群表示论或算子代数).

令人惊讶的是, 五十年后, 人们突然发现两个领域之间的令人吃惊的深刻联系: 从 Richard Feynman 和 David Deutsch 对于用量子力学来进行计算的讨论开始, 他们试图用纷繁的自然现象来刻画计算. Umesh Vazirani, Alexei Kitaev, Peter Shor, 一些人开始从复杂性理论的角度刻画量子计算的计算能力, 并试图找到具体的例子 (或者说关键应用) 来给出令人信服的证据.

让我们把目光聚集到 1998 年丹麦的奥胡斯大学, 那里举办了第一届 QIP(当时称作 *Algorithms in Quantum Information Processing*), 一个为期五天的研讨会. 他们讨论着 BQP(或者说 Quantum P), 或者几年前刚发现的一系列隐含子群问题 (Shor 算法), 或者说平方加速的搜索算法 (Grover 算法). 参会者中的一些人活跃至今, 其中一些出现在后面的章节中: Dorit Aharonov, Gilles Brassard, Richard Cleve, Lov Grover, Peter Høyer, Richard Jozsa, Michele Mosca, Barbara Terhal, Wim van Dam, Umesh Vazirani, John Watrous. 一些人还在读 PhD, 也许很少会有人在当时意识到, 自己所在的领域会走向何方; 一些人日后的工作斩获了许多个最佳论文奖, 甚至开拓了全新的子领域.

本文试图从理论计算机科学的视角, 给出这一仅有三十几年历史的全新领域的介绍. 第二节从讨论经典计算复杂性理论的量子对应开始, 介绍复杂性类 P 的量子对应 BQP 的定义, 它在复杂性类中的位置, 它的完全问题的来源, 和典型的完全问题. 第三节介绍复杂性类 NP 的量子对应 QMA, 典型的完全问题, 以及与 Cook-Levin 定理的关系; 再进一步讨论其背后的复杂性理论与凝聚态物理的对应, 即哈密顿量复杂性理论, 包括量子 PCP 猜想、张量网络和面积定律. 第四节介绍量子交互式证明系统的主要结果, 包括一个或者多个 Merlin, 及其与 Arthur 一次或多次通信的结果; 我们会惊讶地发现, 一些情况下量子计算并不会带来任何优势; 最后介绍计数复杂性相关的结果. 第五节讨论了 Shor 算法及其背后的隐含子群问题, 以及 Shor 算法没有对应的多项式时间经典算法的直接后果; 最后介绍了量子至上 (Quantum Supremacy)、扩展 Church-Turing 论题与玻色子采样问题的关系. 第六节给出了作者在复杂性理论的观点下, 对量子信息科学 (Quantum Information Science) 的看法.

囿于作者水平以及篇幅, 即使把话题限制在复杂性理论, 仍然有很多重要结果没有提及, 包括但不限于通信复杂性和查询复杂性相关的结果. 有两个结果需要特别提及:

- 2009 年, Aram Harrow, Avinatan Hassidim 和 Seth Lloyd 提出的 HHL 算法 [39]: 求解满足约束 (如良好的条件数和初态能有效制备等) 的线性方程组的量子算法, 相对最好的经典算法达到指数级加速. 由于线性方程组在科学和工程的广泛应用, 很快这一算法就被应用到了一些统计学习算法, 和某些常微分方程的边值问题的求解 (有限元方法) 中, 可以说近年的量子机器学习热潮也与此不无关系;
- 2013 年, Patrick Hayden 和 Daniel Harlow 用量子复杂性理论解决黑洞防火墙问题的尝试 [38], 以及背后一系列与量子引力 (Quantum Gravity) 和 AdS/CFT 对偶相关的问题.

好了, 这里不再过多评述. 让我们看看复杂性理论与量子计算之间, 会有什么样的出人意料的联系吧!

2 经典计算复杂性理论的自然对应

2.1 随机性与量子力学: 复杂性类 BQP

关于量子计算的讨论大致始于上世纪最后的十数年: 1982 年, Caltech 的 Richard Feynman[35] 等物理学家提出了关于用基于量子力学的计算机模拟量子系统的基本想法. 三年之后, Oxford 的 David Deutsch 试图将这一想法形式化 [32], 即定义量子 Turing 机, 以及 Church-Turing 论题的对应版本. 当然, 这些尝试也并没有服众.

事情开始发生转折的时候是 1993 年. 那年的 STOC 上, 刚刚涉足量子计算的 Umesh Vazirani(UC Berkeley) 和他的博士生 Ethan Bernstein 进一步形式化了 David Deutsch 的想法 [21]:

定义 2.1 (量子 Turing 机)**.** *量子 Turing 机 (QTM)M 是一个三元组 (Σ, Q, δ), 这里的 Σ 是有限字母表 (包括空字符 #), Q 是一个有限状态集 (初态为 q_0, 末态为 $q_f \neq q_0$), δ 则是量子转移函数 $\delta : Q \times \Sigma \to \tilde{C}^{\Sigma} \times Q \times \{L, R\}$, $\tilde{C}$ 中包含所有在 $ploy(n)$ 内计算实部和虚部误差小于 2^{-n} 的复数.*

QTM 有一个用 $\mathbb{Z}$ 索引的双向无穷长纸带, 以及一个可以自由移动的读写头. 对于格局, 初始格局, 以及终止格局的定义与确定性 Turing 机相同.

令 $\mathcal{S}$ 为 M 的格局的有限复线性组合构成的内积空间 (度量为 Euclid 距离), 我们把每个 $\phi \in S$ 称为 M 的叠加. 这样的 QTM M 定义了线性算符 $U_M : \mathcal{S} \to \mathcal{S}$, 称为 M 的时间演化算符: 如果 M 始于状态 p 和已扫描符号 σ 的格局 c, 那么一步推导后, M 是格局 $\psi = \sum_i \alpha_i c_i$ 的线性叠加. 这里每个非零 α_i 对应于转移 $\delta(p, \sigma, \tau, q, d)$, 而 c_i 是对 c 作用变换之后的新的结果. 把这样的线性映射拓展到整个空间 $\mathcal{S}$ 上, 即给定了线性时间演化算符 U_M.

对处于叠加态 $\psi = \sum_i \alpha_i c_i$ 的 QTM M, 当它被测量 (或者说观察) 时, 看到格局 c_i 的概率是 $|\alpha|^2$. 而 M 的叠加也变成了 $\phi' = c_i$.

这样的 QTM 的定义看起来更像是经典的 Turing 机的定义, 加上来量子力学的五大公设: 态的叠加变成了字符串的叠加, 时间演化变成了 Turing 机的推导 (当然算符要符合 Schrodinger 方程), 测量就是简单的投影测量. 在定义了量子 Turing 机之后, 一个自然的问题就是考量这样的模型的计算能力. 首先需要定义 QTM 接受的语言.

定义 2.2 (EQP 与 BQP). *考虑静止的正规形式的多带 QTM M, 它的最后一条纸带的字母表为 $\{\#, 0, 1\}$. 如果我们用字符串 x 在第一条纸带上运行 M, 并保持其他地方为空, 直到 M 停机. 然后测量最后一条纸带上的起始位置, 我们得到 1 的几率是 p, 那就说: M 接受 x 的几率是 p, 拒绝 x 的几率是 $1-p$.*

考虑语言 $\mathcal{L} \subseteq (\Sigma - \#)^*$. 对于不同的复杂性类, 如果 QTM M 接受 $\mathcal{L}$, 如果 M 接受所有的 $x \in \mathcal{L}$ 的几率是 p, 拒绝字符串 $x \in (\Sigma - \#)^* - \mathcal{L}$ 的概率是 p. 如果取 $p = 1$, 那就是复杂性类 EQP(无错误量子多项式时间); 如果取 $p = \frac{2}{3}$, 那就是复杂性类 BQP(有界误差量子多项式时间).

随即, Umesh 等人给出了一个宽松的范围, 来 BQP 在复杂性类中的位置

定理 2.1 (BQP 的计算能力).

$$\mathsf{P} \subseteq \mathsf{BPP} \subseteq \mathsf{BQP} = \mathsf{BQP}^{\mathsf{BQP}} \subseteq \mathsf{P}^{\#\mathsf{P}} \subseteq \mathsf{PSPACE}.$$

看起来量子计算的能力似乎可能好于概率计算, 但在多项式时间里能访问的也只有多项式的空间了, 合情合理. 此外, $\mathsf{BQP} = \mathsf{BQP}^{\mathsf{BQP}}$ 意味着多个量子计算机的串并联并不会改善它的计算能力.

当然, 正如我们设计经典算法的时候几乎不会显式的写出对应的 Turing 机一样, 这样的计算模型虽然数学上严格, 但是可操作性并不好. 所幸, Princeton 的姚期智几个月后在 FOCS 上给出了量子 Turing 机的另一种刻画 [60]. 他证明了任何量子 Turing 机在多项式意义下可计算的函数, 均存在多项式规模的量子线路.

姚期智事实上给出了 BQP 的另一种定义: 多项式规模量子线路的一致 (uniform) 线路族在误差至多 $\frac{1}{3}$ 的情形可以解决的判定问题. 他把量子力学的作用理解为一类特殊的概率分布, 这样的做法后来颇被大家所接受. 更具体地说, 他定义量子线路的方式如下:

定义 2.3 (量子线路). *考虑量子线路 K, 其输入变量为 $x_1, x_2, \cdots, x_n$, 输出变量为 $y_1, y_2, \cdots, y_n$ (输出线网的子集). 我们把输入 $\tilde{x} \in \{0,1\}^n$ 对应于 $\{0,1\}^m$ 上的概率分布 $\rho_{\tilde{x}}$. 这样的概率被量子计算以一种自然的方式所的定义. 对输入 $\tilde{x}$, 终态 v 对应于所有输出线网 (不仅仅是输出变量 y_i) $v = \sum_{\tilde{y} \in \{0,1\}} = v_{\tilde{y}}$, 这里 $v_{\tilde{y}}$ 是当输出变量取 $\tilde{y}$ 时 v 的投影. 那么有 $\rho_{\tilde{x}}(\tilde{y}) = \|\tilde{y}\|^2$. 我们说 $\{\rho_{\tilde{x}} | \tilde{x} \in \{0,1\}^n\}$ 是由 K 产生的分布.*

很自然地, 为了刻画 BQP 的计算能力和结构, 我们想知道更紧的 bound. 其中的结果之一是 2004 年尚在 UC Berkeley 读 PhD 的 Scott Aaronson[1] 的结果:

定理 2.2 (BQP 与 PostBQP).

$$\mathsf{BQP} \subseteq \mathsf{PP} = \mathsf{PostBQP}$$

与通常的 QTM 不同, 这里的延迟选择操作 (不同于量子光学中的意义) 保证在第一个量子比特为 $|1\rangle$ 的情况下, 第二个量子比特为 $|1\rangle$ 的几率至少 $\frac{2}{3}$. 或者说 BQP 考虑的演化仅仅是酉变换 (保证几率守恒), 而 PostBQP 考虑的则是任何线性变换, 而一般的 Turing 即处理的则是 $0-1$ 矩阵. 转移函数的繁杂程度很自然的给出了计算能力分层的一个直观理由: 允许更复杂的转移很可能会得到更强的计算能力.

从另一方面来说, 由于 $\mathsf{PP} = \mathsf{PostBQP}$, 我们很自然的得到了处理 PP 的另一种手段: 不管是证明 $\mathsf{BQP} \subseteq \mathsf{PP}$, 还是证明 PP 对交封闭 [19]. 要知道后者甚至曾经在 18 年内无人解决. 这样的应用无关量子计算机存在与否, 量子计算复杂性理论无疑提供了新的视角和工具, 不论是对于理论计算机科学 (包括但不限于复杂性理论) 本身, 还是对于更多的学科 (比如凝聚态物理和统计物理), 我们将在后面的章节中看到更多的例子.

2.2 BQP 完全问题举隅: k-fold FORRELATION

当我们在讨论复杂性类的时候, 论及其种种性质, 最重要的大抵是它在整个层次中的位置, 以及它的完全 (Complete) 问题. 某个复杂性类的完全问题被认为是整个复杂性类中最难的问题, 因为它的有效解决意味着整个复杂性类中问题的有效解决 (想想 SAT 问题的确定性多项式时间算法意味着什么); 而另一方面, 它也是整个复杂性类中最具代表性的问题, 比如说二人博弈的纳什均衡是 PPAD 完全的 [28]. 于是作为复杂性类的 PPAD(有向图的多项式校验参数) 刻画的是纳什均衡点的存在性, 也就意味着 PPAD 作为复杂性类对于计算经济学而言有着重要的意义.

正因为某一复杂性类的完全问题是其中最具代表性的问题, 它当然可以视作这一复杂性类的等价定义. 这样的例子不胜枚举, 比如说常见的 BQP 的定义多使用与量子线路相关的 BQP 完全问题. 更多的 BQP 完全问题的例子见张胜誉等人的综述 [58].

这里介绍的问题是 k-fold FORRELATION, 它被认为是迄今为止发现的最简单的 BQP 完全问题: 描述它不但不需要任何量子力学, 甚至不需要任何非平凡的数学概念 (比如矩阵的条件数或者扭结对应的 Jones 多项式). Forrelation 的想法源于 Scott Aaronson(MIT) 及其师兄 Andris Ambainis 分离经典查询复杂性和量子查询复杂性的尝试 [3].

定义 2.4 (k-fold FORRELATION)**.** *给定 k 个布尔函数 $f_1, \cdots, f_k : \{0,1\}^n \to \{-1,1\}$. 我们想估计如下形式的"缠绕和":*

$$\Phi_{f_1,\cdots,f_k} := \frac{1}{2^{(k+1)n/2}} \sum_{x_1,\cdots,x_k \in \{0,1\}^n} f_1(x_1)(-1)^{x_1 \cdot x_2} f_2(x_2)(-1)^{x_2 \cdot x_3} \cdots (-1)^{x_{k-1} \cdot x_k} f_k(x_k)$$

不难证明 $|\Phi_{f_1,\cdots,f_k}| \leq 1, \forall f_1, \cdots, f_k$. 那么, 如果 $|\Phi_{f_1,\cdots,f_k}| \leq \frac{1}{100}$ 视为接受; 如果 $\Phi_{f_1,\cdots,f_k} \geq \frac{3}{5}$ 视为拒绝.

上面的定义的 $k-$fold FORRELATION 是一个承诺问题 (Promise Problem). 我们可以找到一个有界误差 (Bounded-error) 的量子算法, 在 $\lceil k/2 \rceil$ 次量子查询后得到结果. 如此简单的问题是甚至"捕捉了量子计算的全部能力":

定理 2.3. *如果 $f_1, \cdots, f_k$ 是可以精确描述 (即通过线路计算) 的, 且 $k = poly(n)$, 那么 $k-fold\ FORRELATION$ 是一个 BQP 完全问题.*

既然完全问题如此重要, 那么我们如何才能找到类似的完全问题呢? 考虑一些典型的复杂性类的例子 [16], 譬如说

- NP 的完全问题是 k-SAT($k \geq 3$), 又称 Cook-Levin 定理. 最早是 Stephen Cook 使用 Turing 机的计算历史规约: 把每一步推导对应的纸带一条条的接在一起, 形成平面; 再把这样的平面中每一步推导对应的约束, 和起止状态用布尔表达式编码, 即得到了布尔表达式; 考虑这样的布尔表达式的取值, 那么就得到了 SAT 问题. 类似地, 我们可以通过一些构造 (这样的规约是多项式时间的, 称为 Karp 规约) 把其他问题也对应到 SAT 问题上, 如此这般可以得到一系列完全问题. 但是这样的规约并没有一般之法, 不同问题之间甚至很可能毫无可借鉴之处.
- PSPACE 的完全问题是 $TQBF$(全带量词布尔公式), 规约构造类似 Cook-Levin 定义[1]. 另一些常见的完全问题是棋类或解密游戏, 比如六贯棋 (Hex), 单人纸牌游戏形式的麻将 (Mahjong solitaire) 或仓库番 (Sokoban). 除此之外, 还有一些自动机理论相关的问题. 比如已知字母表, 判定给定的正则表达式 R 是否能够产生该字母表产生的所有字符串.

[1]后面我们会发现这样的构造在稍加修改的情况下, 甚至适用于证明 k-local Hamiltonian 是 QMA 完全的.

- #P 的完全问题是 Permanent(积和式), 或者是二分图完美匹配个数, 或者是无向图的不相交圈覆盖个数 (不难证明这三者等价), 以及特定类型的 Ising 模型的配分函数 (实际上是带权求和问题). 当然, 精确计数问题的难解性近年来得到了非常好的刻画, 蔡进一、陆品燕、陈汐等人证明了一系列二分定理 [26][27]: 即能够用可满足约束问题或图同构问题描述的技术问题, 要么存在多项式时间算法, 要么是 #P 完全的; 他们还给出了刻画这一二分定理的精确条件.

而对于量子复杂性理论主要的复杂性类, 如本节讨论的 BQP 和之后讨论的 QMA 而言. 我们寻找完全问题仍然是对不同例子采用不同处理方式, 并没有类似计数复杂性这样的漂亮的二分定理. 当然, 对于量子计算而言, 定义不同的等价计算模型的同时, 也就自然的定义了一系列 BQP 完全问题.

譬如 Michael Freedman 和王正汉等人, 在 2002 年从拓扑量子计算模型中, 得到了计算 Jones 多项式近似算法 [36], 并证明了它也是 BQP 完全的. 再如 Itai Arad 和 Zeph Landau(UC Berkeley) 给出了张量网络的收缩在累加近似 (Additive Approximation) 意义下的近似算法 [13][2], 并指出这一问题也是 BQP 完全的. 除此之外, 这样的张量网络的收缩过程的顺序选择, 也可以看做量子线路中一系列量子门的作用, 从而给这一问题的困难程度分类一个较为直观的解释.

3 哈密顿量复杂性与凝聚态物理

3.1 QMA 与 k 局部哈密顿量问题

在刻画了 P 的量子对应之后, 一个自然的问题是它的 NP 问题的量子对应是什么? 它们之间会有类似 $\mathsf{P} \stackrel{?}{=} \mathsf{NP}$ 这样数十年悬而未决的问题吗? 很快一些人给出了部分答案.

Alexei Kitaev(Caltech) 于 1999 年 1 月份芝加哥的德保罗大学的 AQIP[3]上介绍了量子版本的 NP, 即 BQNP[46][48](现在的 QMA):

命题 3.1 (QMA 定义及其完全问题)**.** *如果一个计算问题的解能够被在量子计算机上多项式时间内验证, 那么我们说这样的问题在复杂性类 BQNP(即"有界误差, 量子非确定多项式"的缩写, 又称 QMA) 中. 下面的问题是 BQNP 完全的:*

判定一个局部哈密顿量 (local Hamiltonian), 即一系列 k-local 厄米 (Hermite) 算符的和 (每个算符只涉及常数 k 个量子比特), 是否存在小于 a 或大于 b 的特征值, 这里的 $\frac{1}{b-a}$ 是关于输入规模 n 的多项式.

应该说 Kitaev 的证明的主要想法来自 Cook-Levin 定理中利用计算历史规约, 以及 Feynman 把哈密顿量对应于酉演化的想法 [35]($U = e^{iHt}$). 类似纸带排列对应的布尔表达式, Kitaev 给出了态演化算符对应的哈密顿量 $H = H_{in} + H_{out} + H_{prop}$. 这样做的动机也不难理解, 如果我们只考虑 $k - LH$ 的基态的话 (即没有任何线性叠加), 那么它就退化成了经典的 $MAX - k - SAT$ 问题. 直接的构造给出 $k = O(\log(n))$, 通过对构造过程的进一步优化和改进 $H^{'} = H^{'}_{in} + H^{'}_{out} + H^{'}_{prop} + H^{'}_{clock}$ 可以提高到 $k = 5$[10].

除了完全问题, 我们也关心 QMA 在复杂性类层次中的位置, Dorit Aharonov 在她的综述 (来自她 2001 年在特拉维夫大学的一系列课程讲义)[10] 中介绍了一些结果:

[2]Additive Approximation 的定义类似 FPRAS, 但是误差 $\Delta(n)$ 并不一定是输入规模 n 的多项式.

[3]时称 Algorithms in Quantum Information, 后更名为 Quantum Information Processing, 量子信息科学领域 (理论方面) 的顶级会议, 始于 1998 年丹麦的奥胡斯大学.

定理 3.1. $\mathsf{BPP} \subseteq \mathsf{BQP} \subseteq \mathsf{QCMA} \subseteq \mathsf{QMA} \subseteq \mathsf{PP}$

这里的 QCMA 从证明者 (Merlin) 传递到验证者 (Arthur) 的信息, 仅仅为字符串而不是量子态. 这样的结果与 BQP 相比并无太多改善. Dorit Aharonov 也在上面的综述中给出了一系列公开问题 (open problem):

- 如何找到更多 (自然) 的 QMA 完全问题?
- $k-LH$ 对于 $k=2,3,4$ 的情况?
- $\mathsf{QMA} \stackrel{?}{=} \mathsf{QMA}_1$, 即允许双边误差和允许单边误差的 QMA 计算能力是否相同[4].
- $\mathsf{QCMA} \stackrel{?}{=} \mathsf{QMA}$
- 给定局部哈密顿量, 是否存在多项式规模量子线路来生成它的基态? 即 $\mathsf{BQP} \stackrel{?}{=} \mathsf{QMA}$ [5].
- 是否存在 PCP 定理的量子对应? 我们能否证明量子计算的不可近似性?

十五年时间过去了, 一些问题得到解决; 一些问题悬而未决, 但是新的想法产生了更深远的影响:

- 我们在凝聚态物理中找到了很多的 QMA 完全问题 [37], 即使是一维线性系统的基态精确求解, 这样的计算上的困难几乎遍布凝聚态物理, 十分出乎意料;
- Julia Kempe 和 Alexei Kitaev 用微扰论的思想证明了 $2-LH$ 是 QMA 完全的 [45]. 更多的 QMA 完全问题见 Adam Bookatz 的综述 [22];
- 为了讨论 QMA_1, Sergey Bravyi 定义了量子 SAT 问题 [23], 并证明了量子 $3-SAT$ 问题是 QMA_1 完全的. 除此之外, 对于带某些限制的 SAT 问题, 我们也知道了一些有效求解算法, 如量子 $2SAT$ 的线性时间算法 [15][31], 虽然寻找这样的问题的经典算法的对应并不容易.

实际上 $k-LH$ 和 QMA 背后的思想意味这一个全新的领域, 哈密顿量复杂性 (Hamiltonian complexity) 理论. 这一领域极为深刻的联系了量子复杂性理论和凝聚态物理, 给出了一系列组合优化问题与凝聚态物理中的问题的对应关系, 而整个领域最核心的公开问题就是刻画量子不可近似性的量子 PCP 猜想 [7], 以及凝聚态物理中表示纠缠结构的 (高维) 面积定律. 我们将在下一节介绍这一领域的更多结果.

3.2 量子 PCP 猜想的源与流

上一节对 QMA 和 $k-LH$ 的讨论, 引出了哈密顿量复杂性 (Hamiltonian complexity) 的第一个非平凡的结果. 关于哈密顿量复杂性, 可以参考 Sevag Gharibian, 黄溢辰, Zeph Landau 和 Seung Woo Shin 在 UC Berkeley 的讨论班上整理的综述 [37]. 一方面, 它揭示了量子复杂性理论和凝聚态物理间的深刻的对应关系:

[4] 类似经典复杂性理论中, 复杂性类 BPP 和 RP 的关系.

[5] 即 $\mathsf{P} \stackrel{?}{=} \mathsf{NP}$ 的量子对应.

$k-LH$	约束可满足问题 $(MAX-k-SAT)$
$H=H_1+\cdots+H_m$	$f(x_1,\cdots,x_n)=C_1\wedge\cdots\wedge C_m$
k 局部项 $H_1=\|010\rangle\langle 010\|$	子句 $C_i=x_1\vee\neg x_2\vee x_3$
基态能量	未满足的子句个数
对材料性质的描述	组合优化问题
QMA 完全	NP 完全

表 1: $k-LH$ 与 $k-SAT$ 的对应关系

甚至最后两者作为复杂性类的完全问题也有类似之处, 我们在之前讨论复杂性类 QMA 时也曾提及: $k-LH$ 的 QMA 完全性证明把时空量子线路映射到哈密顿量上, 而 $k-SAT$ 的 NP 完全性证明把纸带和计算历史映射到布尔表达式上.

从另一方面来说, 对于 N 体系统, 描述经典系统只需要 $O(N)$ 个参数; 而由于量子系统的线性叠加性质, 描述量子系统 (或者说希尔伯特空间) 需要 $2^{O(N)}$ 个参数. 可是, 对于某些量子态来说, 比如特定约束下的矩阵乘积态 (Maxtrix Product State, MPS), 它的计算在经典计算机上只需要多项式时间. 于是, 一个自然的问题是, 模拟量子系统究竟有多难? 或者说什么样的量子态能够被简洁的描述? 某些量子系统的基态 (比如矩阵乘积态就是一类物理模型的基态, 如 AKLT 链) 可能是答案之一.

然而, 描述量子系统的困难出乎意料: 2007 年, Dorit Aharonov 和 Daniel Gottesman 等人证明了精确求解一维量子系统 (一般意义下) 的基态是 QMA 完全的, 不管在任何温度下. 那么, 这样的系统能有效近似吗? 对于经典的 $MAX-k-SAT$ 问题, 由于 PCP 定理, 一方面, 近似估计未满足的子句个数仍然是 NP 困难的; 而另一方面, 这样的证明可以只检查一部分, 而且在一定概率下整个证明是完全正确的, 这就是所谓的概率可检查证明 (Probabilistic checking of proofs, PCP).

PCP 定理很可能是上世纪末理论计算机科学最重要的结果. 它由 Sanjeev Arora 和 Shumuel Safra, 在 1992 年的 FOCS 上提出, 并给出了复杂性类 NP 的另一种刻画 [17]. 凭借这一结果, 以及之后一系列相关的应用, Sanjeev Arora 和其他人分享了 2001 年的哥德尔奖. PCP 定理给出了一种不可近似性的刻画方式: 不但求解问题是困难的, 甚至得到足够好的近似也是困难的, . 但是这一证明过于繁杂, 后来 Irit Dinur[33] 在 2006 年用间隙放大技术 (gap amplification) 简化了 PCP 定理的证明, 这一工作拿到了当年的 STOC 最佳论文奖. 下面我们对间隙放大描述的 PCP 定理及其证明稍作评述.

定理 3.2 (PCP 定理 (间隙放大描述, Gap amplifiation)[33]). *对任何大小为 d 的字母表, 存在常数 $0<\gamma<1$ 和 $W>1$, 以及有效算法使得字母表 (大小为 d) 上的约束图 $G=(V,E)$, 能够被转换到另一个在通用字母表 (大小为 d_0) 上的约束图 $G^{'}=(V^{'},E^{'})$ 上, 并且满足下述论断:*

1. $|E^{'}|\leq W|E|$ 且 $|V^{'}|\leq W|V|$;
2. (完备性) 如果 $UNSAT(G)=0$, 那么 $UNSAT(G^{'})=0$;
3. (坚固性) 如果 $UNSAT(G)>0$, 那么 $UNSAT(G^{'})\geq\min(2\cdot UNSAT(G),\gamma)$.

这里的约束图从对应的约束可满足问题构造而来. Irit Dinur 的证明主要包括三个部分:

(1) 预处理 (Preprocessing): 把约束图 (Constraint graph) 转换为扩展图 (Expander graph);

(2) 间隙放大 (Gap amplifcation);

(3) 字母表规约 (Alphabet reduction).

那么是否存在类似的量子 PCP 定理呢? 这是上一节提及的 Dorit Aharonov 的综述中的公开问题之一 [10]. 这样的概率可检查证明的量子版本, 意味着对于量子系统, 我们只需要局部测试 (local test) 就能了解整体性质. 量子 PCP 猜想问的是, 量子系统的基态能量的近似求解也是 QMA 困难的吗? 或者更物理地说, 量子系统在高温情形下仍然是指数复杂性的吗? 关于量子 PCP 猜想的进一步介绍, 可以参考 Dorit Aharonov, Itai Arad 和 Thomas Vidick 在 ACM SIGACT News 上的专栏文章 [7].

这里简单的讨论一下为什么量子 PCP 猜想难以证明. 如我们所说, 绝大多数经典结果的量子对应都不是显而易见的, 不管是经典的确定性算法 (比如 2SAT 和量子 2SAT 的线性算法 [15][31]), 还是经典的随机算法 (比如量子 Lovasz 局部引理 [11]). 这里的量子 PCP 猜想的证明也不例外, 原因之一是量子不可克隆定理 (Quantum No-cloning Theorem), 使得复制任意量子态并不可行 (当然可以随意复制某些量子态, 比如希尔伯特空间的基). 在 2009 年, Dorit Aharonov, Itai Arad, Zeph Landau 和 Umesh Vazirani 提出了可检测性引理 (The detectability lemma), 并用这一工具证明了量子情形的间隙放大和一维面积定律. 但是 Irit 证明中的字母表规约部分仍然困难重重, 这也是哈密顿量复杂性理论中最重要的公开问题之一.

3.3 张量网络与面积定律

张量网络是一种工具, 它用无向图来刻画多个张量的关系 (如连接方式和它们的张量积): 每个顶点意味着一个张量, 顶点间的连线意味着张量收缩; 每个顶点对应一个有限维的希尔伯特空间, 而每个顶点的度的个数被称为张量的秩; 它的边界不一定是顶点, 也可以是开放的边. 内部的边的维度称为连接维度 (bond dimension), 它与这一类张量网络的复杂程度息息相关: 比如说矩阵乘积态 [25] 在连接维度非常大 (如顶点个数 N 的指数大小) 的时候, 甚至对于整个希尔伯特空间都是稠密的; 而只有连接维度为常数的时候, 它是经典计算机上能够有效计算的.

对于物理学家 (主要指凝聚态物理) 而言, 研究张量网络的动机就是找到偌大的希尔伯特空间上能被经典计算机有效计算的角落. 于是有了一系列特定的张量网络, 比如矩阵乘积态 (Matrix Product State) 和投影纠缠对态 (Projected Entangled-Pair State). 不过物理学家们用的方式 (包括一系列重整化群方法) 大都是启发式的, 几乎没有严格的算法分析. 这样做仍然可以找到一些实际应用中效果很好的方法, 但是很难对其中的思想以及背后隐藏的工具进一步抽象和一般化. 一些计算机科学家们试图给出解释, 比如 Itai Arad, Zeph Landau, Umesh Vazirani 和 Thomas Vidick 最近的工作 [14], 对一类重整化群方法进行了严格的算法分析, 并且给出了部分简并情形的低能态 (low energy state) 的计算方法.

对于计算机科学家们来说, 张量网络是在哈密顿量复杂性框架下的具体工具之一. 研究它的动机也不仅仅是物理上的, 它更像是一个数学工具: Shawn Cui 和 Machael Freedman 等人在其上定义了最大流/最小割, 并证明了对应的弱对偶定理 [30]. 这样的想法从哈密顿量复杂性的角度看非常自然: 寻找凝聚态物理中的问题与组合优化问题的对应.

更一般地来说, 计算张量的代价是巨大的. 不难构造一个张量网络来计算平面图的边染色 (Edge Coloring), 作为判定问题的边染色已经是 NP 完全的, 而对应的计数问题版本则是 #P 完全的. 我们知道, 如果任何一个 #P 完全问题, 可以找到多项式时间算法, 那么我们可以轻易推出 P = NP, 所以张量网络在计算上的困难几乎是根深蒂固的. 除此之外, 既然张量网络能计算特定的计数问题, 那么显而易见, 它也能计算配分函数 [13].

当然, 我们很可能并不一定需要精确结果, 足够好的近似 (包括随机) 算法也是可以接受的. 然而对于一般的张量网络的收缩计算, 在可加性近似 (additive approximate) 情形[6]下这一问题是 BQP 完全的 [13], 这意味着我们有一个效果并不是很好的量子算法来计算任何张量网络. 我们需要面对的情形也往往是类似的: 某一类技术在一般情形下往往表现平平, 只有在某些具体情况会有出人意料的表现.

哈密顿量复杂性的核心问题是物理模拟的复杂性, 或者说我们要理解一个哈密顿量在计算上究竟有多困难. 如果要严格保证张量网络系列方法的有效性 (即有经典计算机上的多项式时间算法), 对于间隙哈密顿量 (gapped Hamiltonian) 的基态, 我们现在有一维面积定律: 面积定律说的是, 量子系统的纠缠熵与系统的边界成正比 (面积定律), 而不是与系统的面积成正比 (体积定律). 这样的想法类似高能物理中的全息原理 (Holographic Principle), 如黑洞的性质与其边界有关.

看起来一维面积定律的证明似乎容易入手: 这时的纠缠熵与常数成正比 (对于一维系统), 对于二维及其以上的情形, 我们还需要考虑如何度量边界 (譬如如何选取测度?). 2007 年, Matthew Hasting 用分析手段, 即 Lieb-Robinson 界证明了一维情形的面积定律 [41]. 次年, Dorit Aharonov, Itai Arad, Zeph Landau 和 Umesh Vazirani 用组合方法, 即可检测性引理, 再次证明了一维面积定律 [6]. 2013 年, Alexei Kitaev 和他们合作, 使用近似基态空间投影 (Approximate Ground Space Projection, AGSP) 技术进一步简化了证明, 并提出了连接维度为亚指数的矩阵乘积态的亚指数时间近似算法.

高维面积定律与量子 PCP 猜想是整个哈密顿复杂性理论中最核心的问题, 而隐匿在它们背后的量子复杂性理论所揭示的东西与量子计算机无关. 复杂性理论本身意味着对资源与计算能力的度量, 这样的资源可能是时间、空间、随机性或者量子力学; 可计算性也有着更丰富的含义, 譬如说, Toby Cubitt 等人证明了一般情形下谱隙 (Spectral gap) 是不可判定的 [29]; 而这时候的复杂性理论的意义, 也早已不再限于理论计算机科学本身, 也许我们所熟知的复杂性理论中的命题 (如 $\mathsf{P} \stackrel{?}{=} \mathsf{NP}$) 意味着更基础的事实, 只是我们未曾知晓而已.

4 更多的复杂性类: 量子计算的局限性

4.1 量子交互式证明系统

量子计算最核心的问题之一, 即是量子计算的加速的来源. 人们试图从很多角度寻求答案, 比如限制计算资源的使用, 或者试图找到某些量子计算资源于计算能力没有提升的情况. 对于这一论断, $\mathsf{QIP} = \mathsf{IP}$[43] 是近十年内最令人惊讶的结果之一. 季铮锋, Rahul Jain 和 John Watrous 等人, 在量子交互式证明系统被提出约十年之后, 证明了这一出乎意料的结论, 这一工作获得了 STOC 2010 的最佳论文奖.

经典的交互式证明系统 (IP) 包括了全知全能的证明者 (Merlin), 和能力有限的验证者 (Arthur). Arthur 并不相信 Merlin 的证明, Merlin 要想方设法的说服他. 在这一过程中 Arthur 可以对 Merlin 提出问题 (如对证明提出问题), 这样一来自然理解的更快. 典型应用之一是密码学中的零知识证明 (Zero Knowledge), 在不泄露任何技术细节的情况下, 说服对方自己已经得到结果. 定义了 IP 之后, 自然的问题就是它有多大, 结果是它大的几乎超乎所有人想象: $\mathsf{IP} = \mathsf{PSPACE}$[53].

[6] **可加性近似**即得到的解允许与输入规模 n 相差的误差 $E(n)$, 但是 $E(n)$ 不一定是多项式的; 准确来说, 这时候它是一系列表示收缩的线性算符.

在 1999 年, Alexei Kitaev 和 John Watrous 定义了复杂性类 QIP(量子交互式证明系统)[47], 它的定义类似 IP, 但是现在 Arthur 和 Merlin 都有自己的量子计算机, 并且可以接受发送量子信息 (量子态). 量子力学有着"指数并行"的内禀性质: n 个量子比特的量子态需要 2^n 个复数构成的矢量来描述. 拥有了如此强大的传送系统, 似乎 Merlin 找到了机会说服 Arthur 更多的东西了, 即

定理 4.1. $\mathsf{IP} = \mathsf{PSPACE} \subseteq \mathsf{QIP} \subseteq \mathsf{EXP}$

这里的时间复杂性类 EXP 的定义类似 P, 但是它包括了所有需要指数时间计算的问题. 它的完全问题包括西洋跳棋 (Draughts) 和日本规则下的围棋 (Go). Watrous 等人在持续改进这一结果, 直到 2009 年, 他和 Rahul Jain 证明了 $\mathsf{QIP}(2) \subseteq \mathsf{PSPACE}$, 即 2-信息的量子交互式证明系统. 他们使用了多重权重更新方法 (*multiplicative weights update method*), 来使得描述 QIP(2) 中验证者最大接受概率的半正定规划 (semidefinite programming), 得以近似最优求解. 季铮锋加入后, 他们在原有证明方法的基础上继续改进, 最终于次年证明了 $\mathsf{QIP} \subseteq \mathsf{PSPACE}$.

而在几个月后, 伍骁迪独立给出了 $\mathsf{QIP} \subseteq \mathsf{PSPACE}$ 的另一种证明方法 [59]. 他考虑计算两个可容许量子信道 (admissible quantum channel) 的方块范数 (diamond norm), 这一 QIP 完全问题; 然后将方块范数的计算转换为某些均衡值 (equilibrium value) 的计算.

当然, 上述结果仅仅是量子交互式证明系统相关的复杂性类的冰山一角. 量子交互式证明系统的潜在实际用途, 是用以验证大规模量子系统的正确性. 譬如说考虑 Merlin 的计算能力是量子力学对应的计算能力, 而 Arthur 用来验证这样的量子系统.

回到交互式证明系统本身, 多个共享纠缠的 Merlin, 似乎也意味着更强的计算能力. 2010 年, 尚在 Bristol 的 Aram Harrow 和 Ashley Montanaro 讨论了乘积态测试[7], 并用在量子交互式证明系统上得到了下述结果.

定理 4.2. $\mathsf{QMA} \stackrel{?}{=} \mathsf{QMA}(2) = \mathsf{QMA}(k)$

即只考虑一次 Merlin 到 Arthur 间的通信, 多个 Merlin 说服 Arthur 的能力和两个 Merlin 一样多. 尽管很多人猜测这样的结果可以拓展到单个 Merlin 的情况, 不过目前这一问题仍然未解决. 另一个重要结果是考虑多个 Merlin 的情形下, 他们之间共享纠缠和无纠缠时计算能力的差别. Tsuyoshi Ito 和 Thomas Vidick 在 2012 年证明了下述定理. 在得到了 MIP^* 的第一个非平凡下界的同时, 这一工作得到了 FOCS 2012 的最佳论文奖.

定理 4.3. $\mathsf{NEXP} = \mathsf{MIP} \subseteq \mathsf{MIP}^*$

4.2 计数复杂性与量子计算

最后介绍一些量子计数复杂性相关的结果. 如我们所知, 经典的计数复杂性理论有着非常漂亮的二分定理, 来刻画问题是可以有效计算的还是 #P 完全的[8]; 而经典计数复杂性的近似理论同样有出人意料的结果, 尽管类似的二分定理很可能并不存在, 但是存在类似素因子分解 (Factoring) 或图同构 (Graph Isomorphism) 这样的中间复杂性 (Immediate complexity) 问题, 二分图上的独立集计数 ($\#BIS$)[50], 即它并不是能够有效近似的 (FPTAS), 也不是 NP 困难的. 更有趣的是, 近似比的讨论于它而言并没有显著意义.

[7]判断是量子态是纠缠态还是乘积态, 由于绝大多数张量相关的计算都是 NP 困难的, 很明显精确的乘积态测试的时间代价也是指数的.

[8]更具体的说, 问题是在任何情况都是 #P 完全, 还是在平面情形有多项式时间算法; 后者可以用全息算法 (Holographic Algorithm) 有效解决.

关于计数复杂性早期的重要结果是 $0-1$ 矩阵积和式问题是 #P 完全的, 以及 $\mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}}$(Toda 定理). 但鲜见对于量子计数复杂性的讨论, 为数不多的结果是施尧耘和张胜誉在 2009 年证明的下述结论.

定理 4.4. $\mathsf{BQP} \subseteq \mathsf{PP} \subseteq \mathsf{P}^{\#\mathsf{P}} = \mathsf{P}^{\#\mathsf{BQP}}$

也就是说对于 Turing 机而言, 不管是经典的 #P, 还是两字的 #BQP 作为喻示, 它的多项式时间内的计算能力并没有差别. 这里的 #BQP 定义如下:

定义 4.1. *$f \in \#\mathsf{BQP}$ 如果 $\exists$ 一致量子线路族 $\{V_x\}$ 关于输入规模 $|x|$ 为多项式, 使得*

1. *$\prod_{init} \prod_{acc} \prod_{init}$ 的特征值要么至少是 $2/3$, 要么至多是 $1/3$;*
2. *$f(x) = |eigenvalue(\prod_{init} \prod_{acc} \prod_{init}) \geq 2/3|$.*

其中投影算符定义如下, 这里 V_x 为量子线路作用的酉变换:

- *$\prod_{acc} = V_x^\dagger \prod_{acc} V_x$: 投影到第一个量子比特为 1 的对应子空间, 如果 V_x 已经作用.*
- *$\prod_{init} = I_m \otimes |0^k\rangle_S \langle 0^k|_S$: 投影到 S 包含 $|0^k\rangle$ 的子空间.*

这样的定义与 #P 稍显不同, 但另一方面我们对 #BPP 和 #BQP 同样知之甚少. 包括它们的完全问题, 内部结构的刻画 (如是否存在类似二分定理的结果). 当然, 量子计数复杂性也许会和其他领域存在着一些出人意料的联系, 只是不为人所知而已. 毕竟在几十年前, 几乎不可能有物理学家意识到他们得不到某些 Ising 模型的有效求解算法, 事实上和计数复杂性的结果有关.

5 扩展 Church-Turing 论题与量子至上

5.1 Shor 算法及其启示

在量子计算研究初期, 为了刻画它的计算能力, 除了对复杂性类 (如 BQP 和 EQP) 的讨论, 也有一些使用量子算法解决具体问题的尝试. 当时人们并不相信量子计算能解决 NP 完全问题, 所以大家把目光聚集到了素因子分解 (Factoring) 和图同构 (Graph Isomorphism) 这两个可能的间隔复杂性 (immediate complexity) 问题上.

在 1994 年末的 FOCS, 来自 AT&T 的贝尔实验室的 Peter Shor 给出了量子计算机上的"随机多项式时间算法", 来求解离散对数 (Discrete Log) 和素因子分解问题 (Factoring): *Algorithms for Quantum Computation: Discrete Log and Factoring*[55]. 这一工作后来在 1999 年获得了哥德尔奖[9] 从技术上说, Shor 把离散对数和素因子分解问题, 转化为了一类周期寻找问题 (Period Finding). 而周期寻找问题, 可以通过 $\mathbb{Z}_n$ 上的量子 Fourier 变换有效解决, 而 Fourier 变换与群表示相关; 特别的在交换群情形下, 这样的群的表示恰好是数. 这里的 $\mathbb{Z}_n$ 即为描述这一问题的隐含子群 (Hidden Subgroup).

同年的 FOCS 上, Daniel Simon 发表了 *On the power of quantum computation*, 提出了另一类隐含子群算法 (Simon 算法)[56], 解决了隐含子群为 $\mathbb{Z}_2$ 的情形. 当然, 隐含子群问题 (Hidden Subgroup Problem), 是后来为了进一步研究作为量子算法原语的量子 Fourier 变换而提出的.

[9]哥德尔奖是理论计算机科学最高奖, 由欧洲理论计算机协会 (EATCS) 和美国计算机协会算法与计算理论组 (ACM SIGACT) 联合颁发.

除此之外, 同时期的 Alexei Kitaev 也在试图寻找这样的量子算法, 不过 Kitaev 关注的是图同构. 不幸的是, 图同构作为隐含子群为非交换群的情形, 由于找不到简单的群表示 (这时候不是数而是矩阵), 至今悬而未决[10]. 而 Kitaev 提出的相估计算法 [49], 甚至可以解决隐含子群为 $\mathbb{Z}$ 的情形. 关于隐含子群问题和量子算法的介绍到此为止, 更多的近年进展可以参考 Ashley Montanaro 的综述 [51].

这里对 Shor 算法本身的意义进行一些讨论. 除了 RSA 公钥体系的广泛应用使得此类密码系统能够被量子计算机破解[11]之外, Shor 算法的提出还有更惊人的意义:

命题 5.1. *Shor 算法提出导致的直接结果, 下述三个论断必有一个为真:*

- *扩展 Church-Turing 论题 (Extended Church-Turing Thesis) 是错的;*
- *量子力学在大规模尺度是错的;*
- *素因子分解问题有多项式时间的经典算法 (类似素性测试与 AKS Test[5]).*

下面给出 (扩展) Church-Turing 论题的表述, 并对其进行简单地讨论. 由于我们不知道如何定义计算模型的"合理"与否, Church-Turing 论题是无法证明且只可证伪的. 而到目前为止, 所有合理的计算模型都符合这一论题.

命题 5.2 (Church-Turing 论题)**.** *如果一个问题在某个合理的计算模型下可计算, 那么它在 Turing 机上也是可计算的.*

命题 5.3 (扩展 Church-Turing 论题)**.** *如果一个问题在某个合理的计算模型上有多项式时间算法, 那么它在 Turing 机上也有多项式时间算法.*

乐观的说, 我们当然希望上述扩展 Church-Turing 论题是错的, 即 Shor 算法是对的, 且没有类似时间复杂性的经典算法. 量子计算机的出现意味着我们可以对这一论题进行检验, 早期对此的质疑主要集中在量子系统的退相干和周围环境的噪声的破坏性影响, 上世纪末期一系列关于量子容错计算及纠错编码的研究给出了完美的回应. 特别是 Michael Ben-Or 和他当时的博士生 Dorit Aharonov 给出的量子阈值定理 (Quantum threshold theorem)[8] 刻画了下述事实: 只要计算过程中每个部件的噪音都控制在阈值之下, 那么任何大规模量子计算都能实现.

5.2 量子至上与玻色子采样问题

为了检验扩展 Church-Turing 论题, 我们希望找到这样的问题: 它毋庸置疑地展示了对于这样的数学上定义良好的问题, 量子计算机达到了最好的经典算法无法企及的加速; 无论这样的问题是多么的出乎意料, 多么的特殊 (没有实际用途), 甚至在硬件上无法规模化 (non-scalable). 这样的问题称为量子至上 (Quantum Supremacy), 这一说法最早由 Caltech 的 John Preskill 在 2011 年的第二十五届索尔维会议上提出 [52]. 从技术上说, 这样的问题的有效经典模拟算法的存在会引起复杂性类多项式层次 (PH) 塌陷.

量子至上近年也有了一些进展, 比如: 2011 年, Scott Aaronson 和他的博士生 Alex Arkhipov 提出的玻色子采样 (Boson Sampling) 问题 [4]; 同年 Michael Bremner, Richard Josza 和 Dan

[10] 当然图同构 (GI) 本身已经有了很大的进展, László Babai 去年提出了拟多项式时间算法 [18], 在图同构的基础上解决了更一般的字符串同构问题, 算法本身用到了少量群论. 这一工作拿到了今年 STOC 的最佳论文奖.

[11] 但是这里需要相当多的量子比特, 实验上在二三十年内达到这样的进展甚至都很渺茫. 此外, 现在也有一些密码系统对于量子计算机来说仍然难以解决, 比如格上的密码系统 (lattice cryptography).

Shephed 提出的 Fourier 采样问题 [24]; 以及今年年初 Edward Farhi 和 Aram Harrow 讨论的量子近似优化算法 (QAOA)[34].

下面我们简单的介绍一下玻色子采样 (BosonSampling) 问题 [4]. Aaronson 师徒讨论的是线性光学量子计算 (Linear Optics Quantum Computing), 这一模型并不能实现通用量子计算. 他们的结果意味着如果存在多项式时间的经典算法, 能够从线性光学网络的概率分布中采样, 那么 $\mathsf{P}^{\#\mathsf{P}} = \mathsf{BPP}^{\mathsf{NP}}$ 且因此 PH 坍缩至第三层. 下面引述玻色子采样问题的定义.

定义 5.1 (BosonSampling)**.** *给定 A, 以及基 $S \in \Phi_{m,n}$, 其中的 $S = (s_1, \cdots, s_m)$ 是非负整数序列, 满足 $s_1 + \cdots + s_m = n$. 这里的输入 A 是 $m \times n$ 的列正交矩阵 $A \in \mathcal{U}_{m,n}$, 其中 $\mathcal{U}$ 是均匀同分布 (i.i.d.) 的高斯分布 $0-1$ 矩阵. 令 A_S 是由 A 的第 i 行的 s_i 次拷贝得到的所有 $n \times n$ 矩阵, 其中 $\forall i \in [m]$. $\mathcal{D}_A$ 可以用如下三种方式定义, 且他们等价:*

(1) 令 $\mathcal{D}_A$ 是 $\Phi_{m,n}$ 上的概率分布, 定义如下

$$Pr_{\mathcal{D}_A}[S] = \frac{|Per(A_S)|^2}{s_1! \cdots s_m!}.$$

(2) 定义 $\mathcal{D}_{\mathcal{A}}$ 为 $\Phi_{m,n}$ 上的分布, 由补全 A 到任意 $m \times m$ 酉矩阵 U, 然后用计算基测量量子态 $\phi(U)|1_n\rangle$ 得到.

(3) 定义 $\mathcal{D}_{\mathcal{A}}$ 为如下方式得到的分布: 第一次应用变量 U 的线性改变到多项式 $x_1 \cdots x_n$(这里 U 是任意关于 A 的 $m \times m$ 酉补全), 来得到新的 m 变量多项式

$$U[x_1 \cdots x_n] = \sum_{S \in \Phi_{m,n}} \alpha_S x^S$$

然后令

$$Pr_{\mathcal{D}_A}[S] = |\alpha_S|^2 s_1! \cdots s_m! = \frac{|\langle x^S, U[x_1 \cdots x_n]\rangle|^2}{s_1! \cdots s_m!}$$

这一问题 (BosonSampling) 的目标是, 对于给定的输入 A, 从 $\mathcal{D}_A$ 中精确或近似地采样.

不难从上面的定义中发现, 玻色子采样问题 (或者说线性光学量子计算) 与矩阵的积和式 (permanent) 计算有着密切的关系. 事实上线性光学量子计算也可以用来证明积和式是 #P 困难的 [2], 而这一结论是计数复杂性早期最重要的结果之一, 也在 Leslie Valiant 的图灵奖获奖文献 [57] 引用中.

这里不再讨论更多的证明细节. 需要额外说明的是, 由于玻色子采样问题只需要约 40 ∼ 50 个量子比特, 就可以超过目前最好的超级计算机在这一问题的表现. 而这个数量级的量子比特的量子计算机被很多实验组认为可以在十年内实现, 如 Google/UCSB 的 Martinis 组或中科大的潘建伟组. 也许在不长的时间后, 我们就能看到扩展 Church-Turing 论题被证伪. 这不但是理论计算机科学家们和实验物理学家们的一次完美的合作, 也是计算复杂性理论中的重要结果. 量子计算能否真正的带来计算极限的新突破, 以及量子力学能否在大规模尺度经受住考验, 让我们拭目以待.

6 小结: 复杂性理论观点下的量子信息科学

应该说, 基础科学的发展从来都没有停滞, 从来都会有全新的观点. 文小刚倡导的拓扑序 (Topological order) 当然是方向之一, 他的直觉把他引向了长程量子纠缠 (long-range quantum entanglement). 可全新的世界观并非仅仅如此. 也许物理学家们会觉得文小刚的想法疯

狂的有些民科的意味, 可这还是物理学家们能理解的"疯狂". 对于绝大多数物理学家来说, 他们几乎从来都没有意识到复杂性理论说的是什么.

大概十年前或稍远些的时候, 有一批 PhD 毕业了. 他们来自世界上不同的地方, 在不同的地方读的博士. 当然, 直到现在, 这些名字仍然在某种程度上鲜为人知: Fernando Brandao, Aram Harrow, Patrick Hayden, Scott Aronson, Thomas Vidick, Toby Cubitt, Dorit Aharonov, Alexei Kitaev. 其中的一些人早已暂露头角, 他们几乎都出现在最好的大学里那几个最好的位置. 我丝毫不会怀疑, 其中一些人的名字会找到它在历史中的位置, 其中一些人会成为几十年后一流的传主题材.

他们在尝试构建全新的世界观, 他们逐渐意识到 Alan Turing 和 Stephen Cook 的想法其实比大多数人所理解的更加基础和深刻: 用复杂性理论的观点来看待多体物理和量子引力. 这样的思想是极其胆大妄为的, 并且前无古人的, 宛如尝试用微积分描述经典力学的 Issac Newton, 用线性代数描述量子力学的 Werner Heisenberg, 用时空几何 (黎曼几何) 描述相对论的 Albert Einstein. 如文小刚所说, 新的物理需要新的数学来刻画. 而新的思维方式会带来全新的世界观, 这样的世界观对于正统的理论物理学家或者理论计算机科学家来说, 几乎都是疯狂的想法. 而只有我们觉得这些想法变得稀松平常的时候, 我们才真正理解了他们.

大概是在以色列的耶律撒冷访问的前一年, Kitaev 试图寻找复杂性类 NP 的量子对应. 他一点都不像正统的物理学家. 定义当然是最为非平凡的东西, 胡乱说几句的东西也并不能称为定义, Kitaev 定义 QMA 的时候, 顺便给出了它的完全问题 $k-LH$. 我们终于意识到 Stephen Cook 和 Leonid Levin 的构造的非凡意义并不仅仅局限在理论计算机科学中, 把一条条织带平铺在一起, 用滑动的窗口来约束纸带排列——历史留给我们当然不只有结局, 也许胜利者能决定史观, 可纷繁的细节中仍然隐藏着别的东西, 不管是明明暗暗的灯塔还是量子力学本身. 这条线索直接把我们拉到了凝聚态物理, 2 局部 (2-local) 的东西在物理中多得甚至有些稀松平常, 如 Ising 模型. 可图像的纷繁复杂程度也远在我们的想象之上, 即使是直线上的物理系统的哈密顿量, 精确有解也轻易的达到了 QMA 完全的界限. 正如我们不知道 $\mathsf{P} \stackrel{?}{=} \mathsf{NP}$ 意味着什么一样, 我们也不知道 $\mathsf{BQP} \stackrel{?}{=} \mathsf{QMA}$ 意味着什么. 也许, 仅仅是也许, 复杂性类间的分离 (seperate) 或是坍缩 (collapse) 意味着也不仅仅是数学上的纯粹智力游戏, 而是隐匿在大自然深处的无法突破的界限.

还有另一件事. 所谓量子至上 (Quantum Supremacy), 我们似乎十分乐观地笃信着扩展 Church-Turing 论题必将错误. 从 Alexei Kitaev 和 Peter Shor 早年关于隐含子群问题的工作开始, 我们开始发现量子力学提供的诡异的几率分布击打着那些广为人知的金科玉律, 或者说, 把它们变成了陈词滥调. 再到后来, Grover 算法和查询复杂性理论, (连续时间) 量子随机游走算法, HHL. 一系列关键应用 (killer applications) 的出现让人们变得乐观的几近无以复加. 我们在十几年前学会了如何用统计学来从数据中学习, 背后所依赖的优化理论和统计学的计算上的低效性仿佛给出了我们所能触及的问题的边缘, 而 HHL 却给出了摆脱束缚的方法.

当然, 这不是严格的量子至上. 当 2011 年 Scott Aaronson 师徒了 Boson Sampling, 今年 Aram Harrow 和他之前的博士生对量子近似优化算法进行了分析 (之前出现了经典和量子的近似算法轮流刷新下界的情况). 我们意识到这样的量子至上是非平凡的, 它并不是理论计算机科学家出于智力上的纯粹好奇. 它更像是 DQC1 或者簇态量子计算 (cluster state quantum computation) 这样在实验上有着充分理由的事物, 为了理解量子加速, 我们从不同的角度出发试图限制量子幽灵. 而量子至上, 借助复杂性理论间的层层假设, 给予了那些难以证明的论题以实际物理意义. 我们妄图用自然的力量来击打那些被认为难以证明的论题, 宛如 Archimedes 的杠杆, 只不过撬动的并非地球, 而是用自然规律挑战数学规律.

参考文献

[1] Scott Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 461, pages 3473–3482. The Royal Society, 2005.

[2] Scott Aaronson. A linear-optical proof that the permanent is# p-hard. In *Proc. R. Soc. A*, volume 467, pages 3393–3405. The Royal Society, 2011.

[3] Scott Aaronson and Andris Ambainis. Forrelation: A problem that optimally separates quantum from classical computing. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, pages 307–316. ACM, 2015.

[4] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 333–342. ACM, 2011.

[5] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in p. *Annals of mathematics*, pages 781–793, 2004.

[6] Dorit Aharonov, Itai Arad, Zeph Landau, and Umesh Vazirani. The detectability lemma and quantum gap amplification. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 417–426. ACM, 2009.

[7] Dorit Aharonov, Itai Arad, and Thomas Vidick. Guest column: the quantum pcp conjecture. *Acm sigact news*, 44(2):47–79, 2013.

[8] Dorit Aharonov and Michael Ben-Or. Fault-tolerant quantum computation with constant error. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 176–188. ACM, 1997.

[9] Dorit Aharonov, Daniel Gottesman, Sandy Irani, and Julia Kempe. The power of quantum systems on a line. *Communications in Mathematical Physics*, 287(1):41–65, 2009.

[10] Dorit Aharonov and Tomer Naveh. Quantum np-a survey. *arXiv preprint quant-ph/0210077*, 2002.

[11] Andris Ambainis, Julia Kempe, and Or Sattath. A quantum lovász local lemma. *Journal of the ACM (JACM)*, 59(5):24, 2012.

[12] Itai Arad, Alexei Kitaev, Zeph Landau, and Umesh Vazirani. An area law and sub-exponential algorithm for 1d systems. *arXiv preprint arXiv:1301.1162*, 2013.

[13] Itai Arad and Zeph Landau. Quantum computation and the evaluation of tensor networks. *SIAM Journal on Computing*, 39(7):3089–3121, 2010.

[14] Itai Arad, Zeph Landau, Umesh Vazirani, and Thomas Vidick. Rigorous rg algorithms and area laws for low energy eigenstates in 1d. *arXiv preprint arXiv:1602.08828*, 2016.

[15] Itai Arad, Miklos Santha, Aarthi Sundaram, and Shengyu Zhang. Linear time algorithm for quantum 2sat. *arXiv preprint arXiv:1508.06340. (To appear at ICALP 2016)*, 2015.

[16] Sanjeev Arora and Boaz Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[17] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: A new characterization of np. *Journal of the ACM (JACM)*, 45(1):70–122, 1998.

[18] László Babai. Graph isomorphism in quasipolynomial time. *arXiv preprint arXiv:1512.03547*, 2015.

[19] Richard Beigel, Nick Reingold, and Daniel Spielman. Pp is closed under intersection. In *Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 1–9. ACM, 1991.

[20] Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM journal on Computing*, 26(5):1510–1523, 1997.

[21] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. In *Proc. 25th Annual ACM Symposium on Theory of Computing, 1993*, 1993.

[22] Adam D Bookatz. Qma-complete problems. *Quantum Information & Computation*, 14(5&6):361–383, 2014.

[23] Sergey Bravyi. Efficient algorithm for a quantum analogue of 2-sat. *Contemporary Mathematics*, 536:33–48, 2011.

[24] Michael J Bremner, Richard Jozsa, and Dan J Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 467, pages 459–472. The Royal Society, 2011.

[25] Jacob C Bridgeman and Christopher T Chubb. Hand-waving and interpretive dance: An introductory course on tensor networks. *arXiv preprint arXiv:1603.03039*, 2016.

[26] Jin-Yi Cai and Xi Chen. Complexity of counting csp with complex weights. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 909–920. ACM, 2012.

[27] Jin-Yi Cai, Xi Chen, and Pinyan Lu. Graph homomorphisms with complex values: A dichotomy theorem. *SIAM Journal on Computing*, 42(3):924–1029, 2013.

[28] Xi Chen and Xiaotie Deng. Settling the complexity of two-player nash equilibrium. In *2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)*.

[29] Toby S Cubitt, David Perez-Garcia, and Michael M Wolf. Undecidability of the spectral gap. *Nature*, 528(7581):207–211, 2015.

[30] Shawn X Cui, Michael H Freedman, Or Sattath, Richard Stong, and Greg Minton. Quantum max-flow/min-cut. *arXiv preprint arXiv:1508.04644*, 2015.

[31] Niel de Beaudrap and Sevag Gharibian. A linear time algorithm for quantum 2-sat. *arXiv preprint arXiv:1508.07338. (To appear at CCC 2016)*, 2015.

[32] David Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 400, pages 97–117. The Royal Society, 1985.

[33] Irit Dinur. The pcp theorem by gap amplification. *Journal of the ACM (JACM)*, 54(3):12, 2007.

[34] Edward Farhi and Aram W Harrow. Quantum supremacy through the quantum approximate optimization algorithm. *arXiv preprint arXiv:1602.07674*, 2016.

[35] Richard P Feynman. Simulating physics with computers. *International journal of theoretical physics*, 21(6):467–488, 1982.

[36] Michael H Freedman, Michael Larsen, and Zhenghan Wang. A modular functor which is universal for quantum computation. *Communications in Mathematical Physics*, 227(3):605–622, 2002.

[37] Sevag Gharibian, Yichen Huang, Zeph Landau, and Seung Woo Shin. Quantum hamiltonian complexity. *Foundations and Trends® in Theoretical Computer Science*, 10(3):159–282, 2015.

[38] Daniel Harlow and Patrick Hayden. Quantum computation vs. firewalls. *arXiv preprint arXiv:1301.4504*, 2013.

[39] Aram W Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Physical review letters*, 103(15):150502, 2009.

[40] Aram W Harrow and Ashley Montanaro. An efficient test for product states with applications to quantum merlin-arthur games. In *Foundations of Computer Science (FOCS), 2010 51st Annual IEEE Symposium on*, pages 633–642. IEEE, 2010.

[41] Matthew B Hastings. An area law for one-dimensional quantum systems. *Journal of Statistical Mechanics: Theory and Experiment*, 2007(08):P08024, 2007.

[42] Tsuyoshi Ito and Thomas Vidick. A multi-prover interactive proof for nexp sound against entangled provers. In *Foundations of Computer Science (FOCS), 2012 IEEE 53rd Annual Symposium on*, pages 243–252. IEEE, 2012.

[43] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. Qip= pspace. In *Proceedings of the forty-second ACM symposium on Theory of computing*, pages 573–582. ACM, 2010.

[44] Rahul Jain, Sarvagya Upadhyay, and John Watrous. Two-message quantum interactive proofs are in pspace. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 534–543. IEEE, 2009.

[45] Julia Kempe, Alexei Kitaev, and Oded Regev. The complexity of the local hamiltonian problem. *SIAM Journal on Computing*, 35(5):1070–1097, 2006.

[46] Alexei Kitaev. Quantum np. *Talk at AQIP*, 99, 1999.

[47] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 608–617. ACM, 2000.

[48] Alexei Yu Kitaev, Alexander Shen, and Mikhail N Vyalyi. *Classical and quantum computation*, volume 47. American Mathematical Society Providence, 2002.

[49] Alexi Yu Kitaev. Quantum measurements and the abelian stabilizer problem (1995). *arXiv preprint quant-ph/9511026*.

[50] Jingcheng Liu and Pinyan Lu. Fptas for# bis with degree bounds on one side. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, pages 549–556. ACM, 2015.

[51] Ashley Montanaro. Quantum algorithms: an overview. *npj Quantum Information*, 2:15023, 2016.

[52] John Preskill. Quantum computing and the entanglement frontier-rapporteur talk at the 25th solvay conference. 2012.

[53] Adi Shamir. Ip=pspace. *Journal of the ACM (JACM)*, 39(4):869–877, 1992.

[54] Yaoyun Shi and Shengyu Zhang. Note on quantum counting classes. *Available from Shengyu Zhang's homepage: http://www. cse. cuhk. edu. hk/syzhang/papers/Sharp-BQP. pdf*, 2009.

[55] Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124–134. IEEE, 1994.

[56] Daniel R Simon. On the power of quantum computation. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 116–123. IEEE, 1994.

[57] Leslie G Valiant. The complexity of computing the permanent. *Theoretical computer science*, 8(2):189–201, 1979.

[58] Pawel Wocjan and Shengyu Zhang. Several natural bqp-complete problems. *arXiv preprint quant-ph/0606179*, 2006.

[59] Xiaodi Wu. Equilibrium value method for the proof of qip= pspace. *arXiv preprint arXiv:1004.0264*, 2010.

[60] Andrew Chi-Chih Yao. Quantum circuit complexity. In *Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on*, pages 352–361. IEEE, 1993.