·量子信息技术专题· 文章编号:1000-3428(2018)12-0028-05 文献标志码:A 中图分类号:O413

量子非局域性与量子通信复杂度研究

张弘弛[1a,2],刘百祥[1a,1b,2],文 捷[1a,1b,2]

(1. 复旦大学 a. 计算机科学技术学院 上海市智能信息处理重点实验室; b. 校园信息化办公室,上海 200433;
2. 复旦-众安区块链与信息安全联合实验室,上海 200433)

摘 要: 论述国内外量子通信研究现状,研究量子非局域性问题和量子通信复杂度问题,通过纠缠态粒子解决 GHZ 问题,利用分布式算法讨论传递比特的最小数目。分析非局域性与通信复杂度之间的关联关系,进而研究同时消息传递模型。分析结果表明,与经典通信相比,量子通信效率较高,且量子非局域性问题和量子通信复杂度问题可以相互转换。

关键词: 量子通信;量子计算;纠缠态粒子;通信复杂度;量子非局域性

中文引用格式: 张弘弛,刘百祥,文 捷. 量子非局域性与量子通信复杂度研究[J]. 计算机工程,2018,44(12):28-32.
英文引用格式: ZHANG Hongchi, LIU Baixiang, WEN Jie. Research on quantum non-locality and quantum communication complexity[J]. Computer Engineering,2018,44(12):28-32.

Research on Quantum Non-locality and Quantum Communication Complexity

ZHANG Hongchi[1a,2], LIU Baixiang[1a,1b,2], WEN Jie[1a,1b,2]

(1a. Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science;
1b. Informatization Office, Fudan University, Shanghai 200433, China;
2. Fudan and Zhong'an Blockchain and Information Security Joint Lab, Shanghai 200433, China)

【Abstract】 The research status of quantum communication at home and abroad is discussed. The problem of quantum non-locality and quantum communication complexity is studied. The GHZ problem is solved by entangled particles, and the minimum number of transmitted bits is discussed by using distributed algorithm. The relationship between non-locality and communication complexity is analyzed, and then the simultaneous message passing model is studied. The results show that compared with the classical communication, the quantum communication efficiency is high, and the quantum non-locality problem and the quantum communication complexity problem can be mutually converted.

【Key words】 quantum communication; quantum computation; entangled particle; communication complexity; quantum non-locality

DOI: 10.19678/j.issn.1000-3428.0052199

0 概述

量子计算的优势在于大幅缩短所需信息的时间,比如文献[1-2]提出 Shor 因数分解算法和 Deutsch 算法。但量子通信[3-4]仍存在较多问题,例如同时消息传递(Simultaneous Message Passing, SMP)模型下的 k 等价性问题(k-equality problem),此问题可描述为:有 k 个团体,每个团体都有一个串,表示为 $x_1, x_2, \cdots, x_k$,他们之间不能直接通信,而是通过传递消息给第 $k+1$ 个团体,让第 $k+1$ 个团体判定 k 个人手上的串是否相等。此问题是 SMP 模型的基本问题,对问题难易度的刻画是量子通信复杂度[5],表示在计算过程中传输的量子比特(quantum bit)数目。量子非局域性和量子通信复杂度可以建立一种量子通信方法,两者对复杂度的刻画不同。

量子非局域性是在空间上相互分离的纠缠态粒子能够相互告知各自状态。若允许参与团体持有纠缠态的量子比特(entanglement quantum bit),则在物理上测量量子的可观测量时会引起另一个纠缠粒子的状态发生改变,进而完成任务。在此基础上,国内外学者提出诸多应用场景,如文献[6]提出 GHZ 问题场景。

在量子通信复杂度方面,参与团体传递量子位

基金项目: 国家自然科学基金(61672166);上海市科技创新行动计划(16JC1402700);上海市优秀学术带头人计划(16XD1400200);上海市领军人才计划(JLH2301003)。

作者简介: 张弘弛(1992—),男,硕士研究生,主研方向为量子计算、计算复杂性;刘百祥、文 捷,工程师。

收稿日期: 2018-07-24 **修回日期:** 2018-09-20 **E-mail:** 16210240022@fudan.edu.cn

(qubit)告诉对方信息,进而完成通信。文献[7]提出分布式 Deutsch-Jozsa 算法,解决等价性问题(Equality Problem,EQ),与经典通信相比,量子通信有较高的效率。

本文阐述量子通信近年来的主要研究成果,列举量子非局域性和量子通信经典问题,并给出解决办法,研究量子通信复杂度与量子的非局域性之间的关联关系。通过将量子通信中的分布式 Deutsch-Jozsa 算法转化为量子非局域性上的算法,以解决通信协议问题转换为量子非局域性的问题。

1　量子非局域性

局域性原则描述为:如果 2 个系统之间不存在因果关系,那么对其中一个系统测量得到的结果,不可能影响对第 2 个系统的测量。但若对分离的纠缠态粒子中的一个进行测量,则另一个粒子必然会产生对应的结果。根据文献[8],自旋态粒子$|\psi\rangle$可表示为:

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|+-\rangle-|-+\rangle) \tag{1}$$

其中,$|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$,$|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$为 σ_x 的本征态。如果一个人测量得到 σ_x 量的观测值为 +1,则整个状态坍塌到$|+-\rangle$,另一个人测量必定会得到 σ_x 的观测值为 −1。因此,在空间上不同 2 点测量,信息的传递速度快于光速。然而,纠缠态粒子并不能用来传递信息,其主要原因是何时进行测量需要经典的信道进行通信,但可以通过纠缠态粒子解决问题。具体描述如下述 GHZ 问题。

假设存在 3 个空间分离的参与者 A、B、C。每个人接收输入 s、t、u,对应输出 a、b、c,输入满足 $s\oplus t\oplus u=0$(⊕代表异或),参与者接收到信息后不可互相交流。参与者的目标共同计算如下:

$$a\oplus b\oplus c=\begin{cases}0, & stu=000\\ 1, & stu\in\{011,101,110\}\end{cases} \tag{2}$$

经典方法不存在完美的策略使输出满足式(2),每个人只能根据接收到的信息进行输出。假设每个人对于输入 0 输出 a_0、b_0、c_0,对于输入 1 输出 a_1、b_1、c_1,则有:

$$\begin{cases}a_0\oplus b_0\oplus c_0=0\\ a_0\oplus b_1\oplus c_1=1\\ a_1\oplus b_0\oplus c_1=1\\ a_1\oplus b_1\oplus c_1=1\end{cases} \tag{3}$$

从式(3)可以看出,4 个等式不能同时成立,但其中 3 个可以同时满足。因此,利用随机策略,开始时 3 个参与者协商确定随机串 r,根据串确定 4 个等式中哪 3 个成立,分离后按策略计算,则该随机策略正确率是 3/4。随机策略成功的概率表示为:

$$\sum_r q_r\frac{1}{4}\sum_{s,t,u}P(s,t,u,r)\leqslant\max_r\frac{1}{4}\sum_{s,t,u}P(s,t,u,r)=\frac{3}{4} \tag{4}$$

其中,q_r 为随机串 r 被选中的概率,不等式右侧为该策略下式(3)回答正确的概率,且在经典情况下正确概率至多为 3/4。

根据量子非局域性特征,存在可以产生正确结论的策略。假设 3 个参与者各持有一个纠缠态粒子,该粒子是 3 个量子位的合并态:

$$\frac{1}{2}|000\rangle-\frac{1}{2}|011\rangle-\frac{1}{2}|101\rangle-\frac{1}{2}|110\rangle \tag{5}$$

在该策略中,3 个人可以对纠缠态比特进行操作。即用幺正变换来改变粒子状态,一个幺正算子即一个幺正矩阵,行和列为正交归一的。则 2×2 的幺正矩阵可表示为:

$$\boldsymbol{U}=\begin{bmatrix}e^{i\left(\delta-\frac{\alpha}{2}-\frac{\beta}{2}\right)}\cos\frac{\theta}{2} & -e^{i\left(\delta-\frac{\alpha}{2}+\frac{\beta}{2}\right)}\sin\frac{\theta}{2}\\ e^{i\left(\delta+\frac{\alpha}{2}-\frac{\beta}{2}\right)}\sin\frac{\theta}{2} & e^{i\left(\delta+\frac{\alpha}{2}+\frac{\beta}{2}\right)}\cos\frac{\theta}{2}\end{bmatrix} \tag{6}$$

引入 Hadamard 算子 $\boldsymbol{H}$ 和单位算子 $\boldsymbol{I}$。为别为:

$$\boldsymbol{H}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \tag{7}$$

$$\boldsymbol{I}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \tag{8}$$

当输入 1 时,作用 Hadamard 算子,输入 0 时,作用 $\boldsymbol{I}$。当输入 $stu=011$ 时,则有:

$$\begin{aligned}(\boldsymbol{I}\otimes\boldsymbol{H}\otimes\boldsymbol{H})\left(\frac{1}{2}|000\rangle-\frac{1}{2}|011\rangle-\frac{1}{2}|101\rangle-\right.&\\ \left.\frac{1}{2}|110\rangle\right)=\frac{1}{2}|0\rangle(|01\rangle+|10\rangle)-&\\ \frac{1}{2}|1\rangle(|00\rangle-|11\rangle)=\frac{1}{2}|001\rangle+&\\ \frac{1}{2}|010\rangle-\frac{1}{2}|100\rangle+\frac{1}{2}|111\rangle&\end{aligned} \tag{9}$$

操作后的状态在基$|0\rangle$和$|1\rangle$上进行测量,可得到 001、010、100、111,每种情况概率各$\frac{1}{4}$。但无论哪一种情况发生,都满足 $a\oplus b\oplus c=1$。因此,该问题在量子非局域性特征中有确定解答。

2　量子通信复杂度

通信的 2 个团体可以通过比特或者量子比特传递信息。在经典通信框架中[9],假设 2 个团体 A、B,需要计算函数 $f:D\to\{0,1\}$,其中 $D\subseteq X\times Y$。在通常情况下,$X=Y=\{0,1\}^n$,A、B 分别获得 n 比特输入串 x、y。因为函数基于 x、y,所以 A、B 进行通信合力计算 $f(x,y)$。在协议算法中,A、B 分别独立计算,相互发送消息给对方,每一条消息称为一轮,几轮过后输出结果。

经典情况主要研究等价性问题,判断 2 个人手上的信息是否一致:

$$EQ(x,y)=\begin{cases}1, & x=y\\ 0, & \text{其他}\end{cases} \tag{10}$$

文献[5]将通信复杂度扩展到量子计算领域,状态由 A 的私有状态、信道状态和 B 的私有状态 3 部分构成。因此,初始状态表述为$|x\rangle|0\rangle|y\rangle$。当 A 获得输入 x 后,用幺正算子对私有状态和信道进行操作,A 对自己的信息计算的同时把消息放入信道,B 用幺正算子操作信道和私有状态进行接收和计算。文献[10]通信过程中一个量子比特可以被非局域性特征中一个纠缠态比特加 2 个经典比特替换,且提出问题:在不共享纠缠情况下,量子通信协议是否与非局域性特征等价。

文献[11]提到算法协议是文献[2]中经典 Deutsch-Jozsa 算法的分布式版本。

经典 Deutsch-Jozsa 算法可解决问题[12]:对于函数 $f:\{0,1\}^n\rightarrow\{0,1\}$,其输出是否为常量,或输出中 0 和 1 有相同的个数。Deutsch-Jozsa 算法线路模型如图 1 所示。

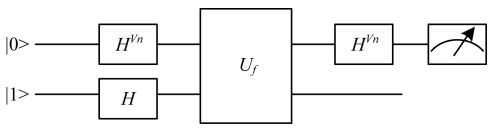

图 1 Deutsch-Jozsa 算法线路模型

图中 U_f 为向后传播算子:

$$U_f|x\rangle|y\rangle=|x\rangle|y\oplus f(x)\rangle \tag{11}$$

$$U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)=(-1)f(x)|x\rangle\cdot\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \tag{12}$$

其中,U_f 将函数值传递到相位上。

$$H^{\otimes n}|x\rangle=H\otimes H\cdots H|x\rangle=\frac{1}{2^{\frac{n}{2}}}\sum_y(-1)^{x\cdot y}|y\rangle \tag{13}$$

其中,$x\cdot y=x_{n-1}y_{n-1}\oplus\cdots\oplus x_0y_0$。

Deutsch-Jozsa 算法线路模型把$(H^{\otimes n}\otimes I)U_f(H^{\otimes n}\otimes H)$作用在$|00\cdots0\rangle|1\rangle$后产生输出:

$$\left(\frac{1}{2^n}\sum_{x,y}(-1)^{f(x)+x\cdot y}|y\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \tag{14}$$

因为$((-1)^{f(x)+x\cdot y})^2=(-1)^{2f(x)}=1$,所以测量必定得到状态$|00\cdots0\rangle$,如果 f 为常数,该状态的概率为 1。若函数 f 对应一半输入输出为 0,另一半输入输出为 1,则观测到状态$|00\cdots0\rangle$概率为 0。

该算法的分布式通信版本可以要求其满足 $x=y$,或 x、y 恰好在 $n/2$ 个位上不相同,则存在一个简单的量子协议使用 $\text{lb}\,n$ 个量子位解决问题。具体描述如下:

1)A 发送给 B 一个位的量子态$\frac{1}{\sqrt{n}}\sum_{i=0}^{n}(-1)^{x_i}|i\rangle$。

2)B 作用相位算子$|i\rangle\rightarrow(-1)^{y_i}|i\rangle$,再作用$H^{\otimes\text{lb}\,n}$。

3)如果测量给出$|0^{\text{lb}\,n}\rangle$,则 B 输出 1,其他情况 B 输出 0。

根据经典 Deutsch-Jozsa 算法,B 测量后的状态为:

$$H^{\otimes\text{lb}\,n}\left(\frac{1}{\sqrt{n}}\sum_{i=0}^{n}(-1)^{x_i+y_i}|i\rangle\right)=\frac{1}{n}\sum_i(-1)^{x_i+y_i}\sum_j(-1)^{i\cdot j}|j\rangle \tag{15}$$

从式(15)可以看出,如果 $x=y$,则观测到$|0^{\text{lb}\,n}\rangle$,如果 x、y 恰好在 $n/2$ 个位上不相同时,则是其他结果。

在经典情况下,文献[10]通过组合[13]分析证明在该问题中每一个没有误差的协议至少要传送 $0.007n$ 比特数,量子通信在该方面有较大改进。若允许有小概率误差,经典情况可以做到传输 $O(\text{lb}\,n)$ 比特数达到误差限。

3 非局域性和通信复杂度的关联

国内外研究者怀疑量子的非局域性和量子通信复杂度是否是同一个问题,非局域问题一般可以转化为通信复杂度问题。本文将分布式 Deutsch-Jozsa 算法映射到非局域性问题,问题描述:A 和 B 的任务是各提供输出 $a,b\in\{0,1\}^{\text{lb}\,n}$,当 $x=y$ 时,$a=b$,而当 x、y 恰好在$\frac{n}{2}$个位上不相同时,$a\neq b$。该过程描述如下:

1)A、B 共享一个纠缠态粒子,该粒子处在状态$\frac{1}{\sqrt{n}}\sum_i|i\rangle|i\rangle$。

2)A、B 分别通过相位算子附加局部相位信息得到$\frac{1}{\sqrt{n}}\sum_i(-1)^{x_i}(-1)^{y_i}|i\rangle|i\rangle$。

3)A、B 分别作用$H^{\otimes\text{lb}\,n}$算子得到$\frac{1}{n\sqrt{n}}\sum_a\sum_b\sum_i(-1)^{x_i+y_i+i\cdot(a\oplus b)}|a\rangle|b\rangle$。

4)对 A、B 分别进行测量。

对于每一个量子态 a,A、B 得到结果 a 的概率为$\left|\frac{1}{n\sqrt{n}}\sum_i(-1)^{x_i+y_i}\right|^2$。

当 $x=y$,结果为 $1/n$,其他情况 $a\neq b$ 的概率为 0,即 $a=b$。当 x、y 在 $n/2$ 个位上不相同时,结果为 0,必有 $a\neq b$。因此,A 只要把结果 a 送给 B,B 就可以算出结果,该过程中传送的量子位为 $\text{lb}\,n$ 比特数。

3.1　单向量子通信复杂度和非局域性问题的映射

单向量子通信复杂度问题可以全部映射到非局域性问题[14]。存在 A、B2 个团体,从 A 到 B 在单向量子通信中交换的量子比特数 q 小于其经典模型的比特数 c。在通信过程中,假设 A 从状态 $|k\rangle$ 开始,A 先作用变换 $\boldsymbol{U}_{\mathrm{A}}(x)$ 在私有态和信道上,其中,$\boldsymbol{U}_{\mathrm{A}}(x)$ 变换只与 A 的输入 x 相关。B 获得信道上的信息,变换 $\boldsymbol{U}_{\mathrm{B}}(y)$ 在私有态上,然后对其进行测量,得到结果为 1 的概率为:

$$|\langle l|\boldsymbol{U}_{\mathrm{B}}(y)\boldsymbol{U}_{\mathrm{A}}(x)|k\rangle|^2 \tag{16}$$

根据 l、k、y 值确定方程 $f(x,y)$ 的值。对于量子非局域性,A 和 B 共享一个纠缠态:

$$|\psi\rangle=\frac{1}{2^{\frac{q}{2}}}\sum_{i=0}^{2^q-1}|i\rangle|i\rangle \tag{17}$$

A 作用一个局域变换 $\boldsymbol{U}_{\mathrm{A}}(x)^{\mathrm{T}}$,测量其状态,B 作用一个局域变换 $\boldsymbol{U}_{\mathrm{B}}(y)$,测量其状态。若 A 测出状态 l,B 测出状态 k,那么对应 x,y 观测到 l,k 的概率为:

$$P(k,l|x,y)=|\langle l|\boldsymbol{U}_{\mathrm{B}}(y)\boldsymbol{U}_{\mathrm{A}}(x)^{\mathrm{T}}|k\rangle|^2=2^{-q}|\langle l|\boldsymbol{U}_{\mathrm{B}}(y)\boldsymbol{U}_{\mathrm{A}}(x)|k\rangle|^2 \tag{18}$$

如果 A 将测量结果 k 送给 B,则 B 可以计算出 $f(x,y)$。

3.2　多团体量子通信复杂度与非局域性

单向量子通信复杂度问题映射到非局域性问题条件比较苛刻,2 个团体参加且必须只进行一轮通信。文献[15]在使用共享随机变量的情况下,将通信复杂度和非局域性关联扩到多团体量子通信,描述了多团体与 2 团体通信的不同,两者不完全相同,但只相差一个系数。共享随机变量使两者之间的通信不再依靠经典信道通信,只需将纠缠态通过操作到目标态。

现假设有 k 个团体,$A_1,A_2,\cdots,A_k$。在非局域情况下,他们共享一个纠缠态,初始为 σ,每位用算子操作使初始态达到计算目标 ρ。定义量子非局域性复杂度 $QNonl(\rho)$ 为所有可达成计算目标 ρ 中长度最短的 σ。在量子通信情况下,可定义 $QComm(\rho)$ 为 k 个团体之间交换的量子位数目,关系如下:

$$\frac{k}{k-1}Qcomm(\rho)\leqslant QNonl(\rho)\leqslant 2Qcomm(\rho)$$

文献[16]在两人通信情况下一个复杂度为 $Q-qubit$ 的量子通信协议可以转换为一个不使用本地存储的 $Q^2+2Q-qubit$ 的量子通信协议。转换过程中的主要思路是将一轮 $Q-qubit$ 通信转换为一个 Q 轮的 $1-qubit$ 通信。通过非局域性与通信协议在没有本地存储的情况下的等价性,给出问题在非局域性与通信协议下的等价性。结论表明,若一个不使用本地存储通信协议通过 $Q-qubit$ 成功计算函数 f 的概率 $p\geqslant 1/2+\varepsilon,\varepsilon>0$,则可以在非局域模型下使用 $O(Q^2)$ 个经典比特以概率 $p\geqslant 1/2+(1-2^{-Q})^{2Q}\varepsilon$ 成功计算函数 f。因此,一个需要 $Q-qubit$ 的通信协议,在非局域性模型下可能需要 $O(Q^4)$ 经典比特通信。

此转换过程说明针对函数 $f(x,y)$,如果一个量子协议比经典协议能用更低的复杂度解决,则贝尔不等式不能完全满足,相应的量子通信复杂度和非局域性复杂度等价。

量子非局域性和量子通信协议在特定情况下等价,例如共享随机变量情况下的多人通信,以及任何情况下的 2 人通信。等价有 2 个优点:1)给将来量子通信的基础构建指明方向,量子通信复杂度和非局域性构建的通信方案,其复杂度差别不大;2)给今后量子通信复杂度提供研究方法。但在一些情况下的等价性仍未知,例如 SMP 模型。

4　SMP 模型

除了相互通信外,研究者会关注将消息发给第三方。此模型有一个裁判作为第三方,A 和 B 同时获得 n 比特输入,他们需要各自发送一轮消息 m_a 和 m_b 给第三方裁判,然后第三方裁判基于消息 m_a 和 m_b 计算出 $f(x,y)$,该模型称为 SMP 模型或裁判模型[17]。

针对等价性问题,近似最优经典协议算法思想如下:

选定一个大小为 $3n$ 的有限域 $\mathbb{F}$,A 输入 x,在域上构造多项式函数 $p_x(t)=\sum_i x_i t^{i-1}$,然后 A 随机选择域上一个点 $a\in\mathbb{F}$,并发送 $(a,p_x(a))$ 给裁判,B 做同样的处理发送 $(b,p_y(b))$,这串消息称为指纹。根据鸽笼原理,a、b 会以一个固定概率发生碰撞,等于元素 d。此外,如果 $x=y$,则 $p_x=p_y$,$p_x(d)=p_y(d)$;如果 $x\neq y$,则 p_x,p_y 最多为 n 次多项式。因此,$p_x(d)\neq p_y(d)$ 的情况发生的概率大于等于 2/3,裁判进行多次判定输出结果。如果 A、B 发送的消息列表中恰好存在一个公共点 d,当且仅当 $p_x(d)=p_y(d)$,则裁判必然会输出 1,且消息列表长度需要 $O(\sqrt{n}\,\mathrm{lb}\,n)$ 比特[18]。文献[19]基于发送信息长度下界算法提出量子计算方法,将指纹用量子态表示为:

$$|F_x\rangle=\frac{1}{\sqrt{m}}\sum_{a\in\mathbb{F}}|a\rangle|p_x(a)\rangle \tag{19}$$

则有:

$$\langle F_y|F_x\rangle=\frac{1}{m}\sum_{i,j\in\mathbb{F}}\langle p_y(i)|p_x(i)\rangle \tag{20}$$

当 $x=y$ 时,$p_x(i)=p_y(i)$,必为 1。当 $x\neq y$,最多有 $n-1$ 个点相同,其概率不超过 1/3。其中,$|F_x\rangle$ 由 $2\,\mathrm{lb}\,m=2\,\mathrm{lb}\,n+O(1)$ 个量子比特组成,需要发送的信息量为 $O(\mathrm{lb}\,2n)$,比经典通信效率高。

5 结束语

本文描述了目前量子通信的主要研究成果,阐述并验证了量子非局域性问题和量子通信复杂度问题之间的关联关系。分析结果表明,量子非局域性问题与量子通信复杂度问题可以转换,量子通信复杂度相近,且量子通信比经典通信效率高。同时研究了 SMP 模型,与经典通信相比,该模型效率较高。但量子通信相应的量子计算模型还没有定论,这将是下一步的研究方向。

参考文献

[1] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Review,1999,41(2):303-332.

[2] DEUTSCH D,JOZSA R. Rapid solution of problems by quantum computation[J]. Mathematical and Physical Sciences,1992,439:553-558.

[3] 麻 敏,李志慧,徐廷廷. 可验证的(n,n)门限量子密码共享方案[J]. 计算机工程,2017,43(8):169-172.

[4] 冯晓华,孙永奇. 基于量子进化的给定围长构造算法[J]. 计算机工程,2017,43(10):141-146.

[5] YAO C C. Quantum circuit complexity[C]//Proceedings of the 34th IEEE Annual Foundations of Computer Science. Washington D.C.,USA:IEEE Press,1993:352-361.

[6] MERMIN N D. Extreme quantum entanglement in a superposition of macroscopically distinct states[J]. Physical Review Letters,1990,65(15):1838.

[7] BUHRMAN H,CLEVE R,WIGDERSON A. Quantum vs. classical communication and computation[C]// Proceedings of the 30th ACM Symposium on Theory of Computing. New York,USA:ACM Press,1998:63-68.

[8] BENENTI G,CASATI G,STRINI G. 量子计算与量子信息原理[M]. 王文阁,李宝文,译. 北京:科学出版社,2011.

[9] ARORA S,BARAK B. Computational complexity:a modern approach[M]. Cambridge,UK:Cambridge University Press. 2009.

[10] CLEVE R,BUHRMAN H. Substituting quantum entanglement for communication[J]. Physical Review A,1997,56(2):1201-1204.

[11] AMBAINIS A,SCHULMAN L J,TA-SHMA A,et al. The quantum communication complexity of sampling[C]// Proceedings of Symposium on Foundations of Computer Science. Washington D. C.,USA:IEEE Press,1998:342-351.

[12] 季 赛,陈思怡,瞿治国. 一种安全的大容量量子图像水印协议[J]. 计算机工程,2018,44(5):234-239.

[13] FRANKL P,RÖDL V. Forbidden intersections[J]. Transactions of the American Mathematical Society,1987,300(1):259-286.

[14] BUHRMAN H,CLEVE R,MASSAR S,et al. Nonlocality and communication complexity[J]. Review of Modern Physics,2010,82(1):665-698.

[15] JAIN R,WEI Z,YAO P,et al. Multipartite quantum correlation and communication complexities[J]. Computational Complexity,2014,26(1):1-30.

[16] BUHRMAN H,CZEKAJ L,GRUDKA A,et al. Quantum communication complexity advantage implies violation of a bell inequality[J]. National Academy of Sciences,2015,113(12):3191-3196.

[17] YAO C C. Some complexity questions related to distributive computing[C]//Proceedings of the 7th ACM Symposium on Theory of Computing. New York,USA:ACM Press,1979:209-213.

[18] AMBAINIS A. Communication complexity in a 3-computer model[J]. Algorithmica,1996,16(3):298-301.

[19] BEALS R,BUHRMAN H,CLEVE R,et al. Quantum lower bounds by polynomials[C]//Proceedings of the 39th Annual Symposium on Foundations of Computer Science. New York,USA:ACM Press,1998:352.

编辑 赵 辉

(上接第 27 页)

[12] DUAN R. Super-activation of zero-error capacity of noisy quantum channels[EB/OL]. [2018-04-01]. https://www.researchgate.net/publication/45856659_Super-Activation_of_Zero-Error_Capacity_of_Noisy_Quantum_Channels.

[13] DUAN R,SEVERINI S,WINTER A. Zero-error communication via quantum channels,noncommutative graphs,and a quantum lovász number[J]. IEEE Transactions on Information Theory,2013,59(2):1164-1174.

[14] DUAN R,SEVERINI S,WINTER A. On zero-error communication via quantum channels in the presence of noiseless feedback[J]. IEEE Transactions on Information Theory,2016,62(9):5260-5277.

[15] DAN S. Quantum zero-error source-channel coding and non-commutative graph theory[J]. IEEE Transactions on Information Theory,2016,62(1):554-577.

[16] LANCASTER P. Theory of matrices[EB/OL]. [2018-04-01]. https://www.researchgate.net/publication/270349125_Theory_of_Matrices?ev=auth_pub.

编辑 吴云芳