清华物理系量子信息研究的新进展*

龙 桂 鲁
(清华大学物理系 北京 100084)

摘 要 在清华大学物理系成立 60 周年之际,我们对近年来清华大学物理系量子信息研究的主要进展情况作一介绍,包括量子搜索算法研究,核磁共振量子计算的实验研究,量子通讯的理论与实验研究. 在量子搜索算法研究方面,我们提出了量子搜索算法的相位匹配,纠正了当时的一种错误观点,并且提出了一种成功率为 100% 的量子搜索算法,改进了 Grover 算法. 在核磁共振量子计算实验方面,我们实现了 2 到 7 个量子比特的多种量子算法的实验演示;在量子通讯方面,我们提出了分布式传输的量子通讯的思想,应用于量子密钥分配、量子秘密共享、量子直接安全通讯等方面,构造了多个量子通讯的理论方案. 在实验室,我们实现了 2 米距离的空间量子密码通讯的演示实验.

关键词 量子搜索算法,核磁共振量子计算,分布式量子通讯

Recent progress in quantum information research in the Deapartment of Physics, Tsinghua University

LONG Gui-Lu
(*Key Laboratory for Quantum Information and Measurements and Department of Physics, Tsinghua University, Beijing* 100084, *China*)

Abstract At the occasion of the 60 anniversary of the department, we give a brief introduction of the recent progress on quantum information research over the last few years, including quantum search algorithm, nuclear magnetic resonnace quantum computing experiment, quantum communication theory and experiment. In quantum algorithm study, we put forward the concept of phase matching in quantum searching, corrected a mistake at that time, and furthermore we constructed a quantum search algorithm with 100% successful rate which improves the Grover algorithm. In NMR quantum computing, we have demonstrated several quantum algorithms using 2 to 7 qubits NMR systems. In quantum communication, we have proposed the idea of distributed quantum communication and applied the idea to quantum key distribution, quantum secret sharing and quantum secure direct communication. We have constructed dozens of quantum communication protocols based on this idea. We have demonstrated quantum communication over a 2m distance in free space in laboratory.

Keywords quantum search algorithm, NMR quantum computing, distributed quantum communication

1 引言

自 1995 年以来,量子信息研究开始成为国际上的研究热点. 量子信息是量子力学与信息科学的交叉学科,包括量子计算与量子通讯等多个方向. 首先,Feynman 指出使用经典计算机模拟量子体系是不可行的,要模拟它们必须使用利用量子力学原理进行计算的量子计算机;第二,量子计算机具有量子平行性,具有经典计算机强大的功能,因此可以解决经典计算机很难解决的问题,如大数质因子分解和无序数据库的搜索等. 第三,随着计算机芯片越来越接近量子极限,量子计算机也成为未来计算机的一个探索方向. 而且,量子信息与国家安全紧密相关,因此受到世界各国的普遍重视.

清华大学量子信息的研究从 1998 年开始,8 年来在实验和理论上取得了一些进展. 现在从三个方面,简要介绍如下.

2 研究工作的进展情况

2.1 量子搜索相位匹配与全成功率的量子搜索算法

对无序数据库的搜索,Grover 算法可以在 $O(\sqrt{N})$ 的步骤里找到标记态,比经典算法有平方根的加速. Grover 算法中有两个相位取反. 在推广到任意相位转动的时候,当时在包括 Grover 本人在内一批专家有一种错误看法,认为任意的相位转动都可以. 我们的研究表明,这是错误的. 我们提出了相位匹配,只有在满足相位匹配条件时搜索才能成功[1—3].

* 国家重点基础研究发展计划(批准号 2001CB309308)、国家自然科学基金(批准号 10325521, 60433050)和教育部博士点基金资助项目
2006 - 04 - 18 收到

而相位匹配还会在误差中有重要的影响[4]. 量子相位匹配,后来被丹麦实验组的实验所证实,并且为多个理论研究组的理论研究所肯定.

Grover 算法有一个缺点,它的成功率并不是 100%. 我们构造了一个成功率为 100% 的量子搜索算法[5]. 这个算法在使用上比原始的 Grover 算法更好.

此外,我们还给出了其他一些量子算法. 通过把 NP 完全问题约化为无序数据库的搜索问题,我们给出了 NP 完全问题的量子算法,所有的计算步骤是 $O(\sqrt{N})$,比经典算法有平方根加速[6]. 我们提出了利用经典平行来加速量子算法的方法,可以进一步加速量子算法[7],而对无序数据库的搜索,利用这种方法,可以达到只需要一次搜索就可以找到标记态[8]. 但是这种加速是通过增加物理资源而取得的.

我们提出了玻色子体系的纠缠的刻划方法[9],对量子计算机的存储器进行有效初始化的方法[10].

2.2 核磁共振量子计算实验

核磁共振量子计算是一种重要的量子计算机的物理实现方案. 我们在核磁共振量子系统中实现了 2 个到 7 个量子比特的多个实验,实现了包括 Grover 算法、一次拿取算法、Bruschweiler 算法、量子时钟对准算法、模块化量子线路、Heisenberg 链的量子模拟等多个算法[11—17]. 目前,7 个量子比特是国际上已经实现的最多量子比特数目.

核磁共振量子计算是否是量子的,一致是个争论的话题. 我们认为核磁共振量子计算是量子性的[18]. 后来我们发现,争论的焦点来自一个量子力学的基本问题:具有相同密度矩阵的系综是否完全在物理上等价. 包括 Preskill 和 Peres 等大多数认为是完全等价的,而包括 Penrose 和 Despagnat 以及我们认为是不等价的. 我们定义了三种密度矩阵:完全密度矩阵、压缩密度矩阵、约化密度矩阵,提出了系综整体测量与系综抽样测量的概念,推广了 Despagnat 的一个 2 能级系综的例子,给出了一般的系综在整体测量的标准方差的表达式,指出通过这一方差就可以区分不同的系综. 经过多次波折,该论文最近被 Foundations of Physics 杂志接受发表[19]. 此外,我们还澄清了一个说法:如果具有相同密度矩阵的系综可以区分,则可以构造超光速通讯,我们指出这两者是没有联系的[20].

2.3 量子通讯

我们提出了利用分布式传输的方法进行量子通讯的思想,并将其应用于量子密钥分配、量子秘密共享、量子直接安全通信. 这些方案具有安全、容量高和高效率的有点. 量子直接安全通讯是不需要传递密钥,直接通过量子信道进行保密通讯的方案[21—28]. 我们在实验室演示了 2 米距离的空间量子密码通讯[29].

3 结束语

以上简单介绍我们在量子信息研究方面的一些进展. 最近几年,我们还开展了量子控制的研究工作[30].

参 考 文 献

[1] Long G L, Zhang W L, Li Y S *et al*. Commun. Theor. Phys., 1999, 32: 335 (quant-ph/9904077)
[2] Long G L, Li Y S, Zhang W L *et al*. Phys. Lett., 1999, A262: 27 (quant-ph/9906020)
[3] Long G L, Tu C C, Li Y S *et al*. J. Phys. A, 2001, 34: 861 (quant-ph/9911004)
[4] Long G L, Li Y S, Zhang W L *et al*. Phys. Rev. A, 2000, 61: 042305 (quant-ph/9910076)
[5] Long G L. Phys. Rev. A, 2001, 64: 022307
[6] Guo H, Long G L, Li F. Commun. Theor. Phys., 2002, 37: 424
[7] Long G L, Xiao L. Phys. Rev. A, 2004, 69: 052303
[8] Xiao L, Long G L. Phys. Rev. A, 2002, 66: 052320 (quant-ph/0112162)
[9] Li Y S, Zeng B, Liu X S *et al*. Phy. Rev. A, 2001, 64: 054302 (quant-ph/0104101)
[10] Long G L, Sun Y. Phys. Rev. A, 2001, 64: 014303 (quant-ph/0104030)
[11] Long G L, Yan H Y, Li Y S *et al*. Phys. Lett. A, 2001, 286: 121
[12] Xiao L, Long G L, Yan H Y *et al*. J. Chem. Phys., 2002, 117 (7): 3310
[13] Long G L, Xiao L. J. Chem. Phys., 2003, 119: 8473
[14] Zhang J F, Long G L, Deng Z W *et al*. Phys. Lett. A, 2004, 70 (6): 062322
[15] Zhang J F, Liu W Z, Deng Z W *et al*. J. Opt. B: Quantum Semiclass. Opt., 2005, 7: 22
[16] Zhang J F, Long G L, Zhang W *et al*. Phys. Lett. A, 2005, 72 (1): 012331
[17] 张竞夫, 谢竞祎, 王 川等. 中国科学, 2005, G35 (4): 390
[18] Long G L, Yan H Y *et al*. Commun. Theor. Phys., 2002, 38: 306
[19] Long G L, Zhou Y F, Jin J Q *et al*. quant-ph/0508207, accepted in Foundations of Physics
[20] Wang C, Long G L, Sun Y. Commun. Theor. Phys., 2005, 44: 822
[21] Long G L, Liu X S. Phys. Rev. A, 2002, 65: 032302-1-3
[22] Deng F G, Long G L. Phys. Rev. A, 2003, 68: 042315
[23] Deng F G, Long G L, Liu X S. Phys. Rev. A, 2003, 68: 042317
[24] Xiao L, Long G L, Deng F G *et al*. Phys. Rev. A, 2004, 69: 052307
[25] Deng F G, Long G L. Phys. Rev. A, 2004, 69: 052319
[26] Deng F G, Long G L. Phys. Rev. A, 2004, 70: 012311
[27] Liu X S, Long G L, Tong D M *et al*. Phys. Rev. A, 2002, 65: 022304-1-4
[28] Wang F G, Deng Y S, Li X S *et al*. Phys. Rev. A, 2005, 71 (4): 044305
[29] 王川, 张竞夫, 王平晓等. 中国科学, 2005, G35: 449; 448, 237
[30] Liu X S, Wu R B, Liu Y *et al*. J. Opt. B: Quantum Semiclass. Opt., 2005, 7: 268