



国防科学技术大学

全国优秀博士学位论文丛书 [第二辑]

纠缠的提取和正交量子态的局域区分

陈平形 著

国防科技大学出版社

纠缠的提取和正交量子态的局域区分

陈平形 著

国防科技大学出版社
·长沙·

图书在版编目(CIP)数据

纠缠的提取和正交量子态的局域区分/陈平形著. —长沙:国防科技大学出版社,
2007.7

(国防科学技术大学全国优秀博士学位论文丛书. 第2辑/曾淳主编)

ISBN 978 - 7 - 81099 - 416 - 3

I . 纠… II . 陈… III . 量子论 IV . O413

中国版本图书馆 CIP 数据核字(2007)第 072314 号

国防科技大学出版社出版发行
电话:(0731)4572640 邮政编码:410073
<http://www.gfkdcbs.com>
责任编辑:耿 筠 责任校对:肖 滨
新华书店总店北京发行所经销
国防科技大学印刷厂印装

*

开本:787 × 1092 1/16 印张:7.5 字数:152 千

2007 年 7 月第 1 版第 1 次印刷

ISBN 978 - 7 - 81099 - 416 - 3

全套定价:150.00 元

序 言

积淀孕育创新，智慧创造价值。

寒窗苦读，拼搏奋斗的积淀凝聚成一本本厚积薄发的论文。博士学位论文是博士生学术水平、科研能力、创造性成果的集中体现，也是学校研究生教育水平、学术水平和创新能力的重要标志。全国博士学位论文水平反映了我国高层次创新型人才培养的质量。作为国家 21 世纪教育振兴行动计划的重要内容，教育部每年评选 100 篇左右的全国优秀博士学位论文。该举措已成为提高研究生培养质量，鼓励创新，促进高层次创造性人才脱颖而出的重要措施。

自 1999 年教育部开展全国优秀博士学位论文评选以来，我校积极参加评选工作，同时参加湖南省和军队优秀博士、硕士学位论文的评选，并以此为契机，在我校研究生中大力倡导科学严谨的学风和勇攀高峰的精神，营造鼓励人才积极创新、支持人才实现创新的浓厚氛围，为学生的禀赋和潜能的充分开发创造一种宽松的环境；采取切实可行的措施，加强学科建设；通过深化研究生学位论文评阅制度改革，完善学位论文抽检制度，实施研究生创新工程，加强研究生导师队伍建设，建立激励机制，鼓励优秀人才脱颖而出等措施不断完善质量保证体系和监督机制，全面提高研究生培养质量。迄今为止，我校已有 7 篇学位论文获全国优秀博士学位论文，另有 7 篇博士学位论文被评为全国优秀博士学位论文提名论文。

睿智颖悟,优秀博士学位论文展现给我们的不仅仅是丰硕的科研成果,更是巨大的精神财富。全国优秀博士学位论文是我国优秀博士学位论文中的杰出代表,全国优秀博士学位论文作者是具有创造能力和竞争能力的高层次创造性人才,是支撑国家掘起的骨干创新力量。认真总结全国优秀博士学位论文的成功经验,对于进一步提高博士生教育的整体水平,培养数量更多、水平更高的高层次创造性人才,具有十分重要的启示作用。在2005年3月汇集出版的我校2004年及之前获得的全国优秀博士学位论文和全国优秀博士学位论文提名的10篇论文基础上,现将我校2005—2006年获得的4篇全国优秀博士学位论文和全国优秀博士学位论文提名论文汇集出版。旨在为广大在学博士生及其导师树立高水平博士学位论文的范本和学习榜样,也期望进一步推动我校研究生教育改革的深入发展,以培养高层次创新性人才为目标,认真总结创新性人才的培养经验和方法,深入探讨博士生教育改革的思路 and 措施。

当今世界,科学技术日新月异,科技创新已经成为社会生产力解放和发展的重要标志。科学技术的迅猛发展,正在引发一场广泛而深刻的军事变革,信息化战争时代已经来临。在新的历史条件下,面对世界新军事变革的严峻挑战,面对推进中国特色军事变革和军事斗争准备的紧迫需求,军队研究生教育的地位和作用比以往任何时候都更加突出。

国防科技大学承担着为国家安全和军队信息化建设、研究开发国防高科技和先进武器装备、培养军队高级工程技术和指挥人才的历史使命,是我军实现新军事变革和军队信息化建设的高层次人才培养和科学研究重要基地。提高人才培养的质量已成为我们现阶段亟需关注的问题之一。我们要在培养大批各类专业和指挥人才的同时,努力为优秀创新人才的脱颖而出

出创造条件。尤其要下功夫造就一批真正能站在世界科学技术前沿的学术带头人和尖子人才，以应对世界新军事变革的严峻挑战，为推进中国特色军事变革做出新的更大贡献。

国防科学技术大学研究生院 曾淳

2007 年 4 月于长沙

2005—2006 年国防科技大学 全国优秀博士学位论文及 全国优秀博士学位论文提名论文

2005 年二篇全国优秀博士学位论文:

信息与通信工程学科,成礼智博士的论文《离散与小波变换新型算法及其在图像处理中应用的研究》,导师梁甸农教授;

原子与分子物理学科,陈平彤博士的论文《纠缠的提取和正交量子态的局域区分》,导师李承祖教授。

2005 年一篇全国优秀博士学位论文提名论文:

光学工程学科,侯静博士的论文《共光路/工模块自适应光学与位相畸变光束频过程研究》,导师姜文汉研究员。

2006 年一篇全国优秀博士学位论文提名论文:

信息与通信工程学科,黄知涛博士的论文《循环平稳信号处理及其应用研究》,导师周一宇教授。

摘要

量子信息是用量子态来编码信息、按量子态的演化规律来处理信息、按量子态的测量规则来提取信息的。由于量子态不同于经典物理态,它本质上是空间非定域的,即具有量子非局域性,这就使量子信息具有一些超出经典信息的新功能。深入研究量子非局域性不仅具有理论意义,而且对量子信息的物理实现具有指导作用。本文研究了量子信息基本理论中与非局域性有关的几个重要问题:纠缠态的判别,纠缠的纯化和提取,正交量子态的局域区分,以及信息熵、纠缠的纯化与提取、正交量子态的局域区分三者之间的关系。主要包括:

(1) 纠缠是量子非局域性的一个重要体现方式,在量子信息的理论和实验研究中都有重要的意义。判断一个量子态是否是纠缠态是一个很基本又至今未完全解决的问题。目前,虽然有不少关于一般纠缠态的充分必要判据,但利用这些判据去判别量子态是否是纠缠态时,都涉及很复杂的数学,因此这些判据实际上只能判别部分量子态。本文提出了一种通过把高维 Hilbert 空间投影到多个低维子空间的方法,来研究纠缠态的判据,得到了纠缠态的一个充分必要判据。具体使用这个判据时,虽然要解方程组,但该方程组是一个二次齐次方程组,而且其解有较好对称性,因此该判据对很多态都可方便地使用。有趣的是这个方法和结论显示出一个清晰的物理图像:一个混合态 ρ 即使在任何一个 $2 \otimes 2$ 子空间上的投影都是分离态,但从整个空间看它不一定是分离的,这说明高维系统和低维系统的纠缠方式存在区别(主要结论发表在 Phys. Rev. A V63, 052306 (2001.5))。

用同样的方法本文还给出了一个可计算的,而且有明确物理意义的 $2 \otimes n$ 系统中量子态结构纠缠的下限(主要结论发表在 Phys. Lett. A V295, 175 (2002))。

(2) 在量子信息中纠缠纯态作为一种物理资源,在隐形传态、量子数据压缩、稠密编码、密钥分配、量子纠错、量子计算等方面都起着重要的作用。然而,一个处于纠缠纯态的系统不可避免地要与环境相互作用并导致消相干,使纠缠纯态变成混合态。使用

这种混合纠缠态进行量子通信和量子计算将导致编码在态中的量子信息失真。为了避免信息的失真,一个办法就是把混合纠缠态尽可能地恢复成接近纠缠纯态或纠缠纯态,这就是所谓纠缠的纯化和提取。纠缠的纯化和提取不仅有理论意义,而且对发展量子信息技术有重要的实用价值。

前人从理论上考虑了如何从无限个相同的混合态(简称为混合态的无限个拷贝)中提取纠缠纯态,这些方案的缺点是,实验室不可能有无限个相同的混合态;这些方案需要目前实验上很难实现的粒子间的控制非操作。本文考虑了从有限个相同混合态(混合态的有限个拷贝)中提取纠缠纯态。定义了准分离态和提取子空间的概念,得到了在有限个相同混合态情况下,二体和多体混合态纠缠提取的必要条件、充要条件及最有效的提取方案;计算了 $2 \otimes 2$ 系统的混合态的提取纠缠。并把这些结论推广到了二体混合态在无限个拷贝情况下的纠缠提取。我们的结论表明,从一个混合态的有限个拷贝中可提取纠缠的充要条件是:在混合态有限拷贝的 Hilbert 空间中存在一个子空间,有限拷贝在该子空间的投影为一个纯纠缠态。所谓纠缠提取操作就是把整个 Hilbert 空间中的存在纠缠纯态的子空间投影出来,纠缠提取原则上可由联合的投影测量和经典通信实现,控制非操作在纠缠提取中不是必不可少的(主要结论发表在 Phys. Rev. A V65, 012317 (2002. 1); Phys. Rev. A V66, 022309 (2002. 8); Phys. Rev. A V69, 012308 (2004. 1))。

(3) 一个由两个或两个以上部分组成的复合系统,处在几个可能态之一,这些可能态都是已知的,但不知道该系统究竟处在哪一个态。通过相对各部分的局域操作和部分间的经典通信来判定该系统所处的确切状态,这个过程称为量子态的局域区分。由量子力学的基本原理可知,不管区分操作是全局的还是局域的,两个非正交态都不能 100% 地被区分。如果一组态是正交的,则肯定可以通过全局操作区分,但并不一定能通过局域操作区分。复合系统正交量子态不一定能被局域区分是量子非局域性的重要表现形式之一。因此研究正交量子态的局域区分,可加深对非局域性的理解,同时也可推动与非局域性有关的其他问题研究。

前人得到了任意两个正交态可局域区分的充要条件;一些特殊系统多个正交态可局域区分的必要条件或充要条件。本文研究了多体正交量子态的局域可区分性。得到了一个适于所有正交量子态的可局域区分的必要条件:如果一个多体系统的一组正交

态 $\{|\Psi_i\rangle\}$ 是可肯定地局域区分,则存在一组线性独立的乘积矢量,使得每个态 $|\Psi_i\rangle$ 是这些乘积矢量的迭加,且 $|\Psi_i\rangle$ 中的每个乘积矢量都和这组正交态中所有除 $|\Psi_i\rangle$ 外的态正交。这个结论显示了任意一组态的正交性与局域可区分性的更深层的联系,即一组态可局域区分,不仅要求这组态中的每个态和别的态正交,而且要求每个态中的乘积态都和别的态正交。利用这个必要条件,不仅可得到很多新的不可局域区分的态组,还可对目前文献报道的大多数不可局域区分的态组很容易地作出正确的判定。本文还研究了多体正交乘积态的局域区分性,讨论了没有纠缠的非局域性的起源,证明了如果一组完备的正交乘积态是可局域区分的,则只需要局域的投影测量和经典通信就可区分这组态(主要结论发表在 Phys. Rev. A V68, 062107 (2003.12); Phys. Rev. A V70, 0223xx (2004.8))。

(4) 系统的信息熵(即 von Neumann 熵)描述了系统的不确定程度,有一些迹象表明信息熵与量子非局域性有内在的联系。本文开创性地研究了信息熵和量子非局域性的关系,得到了一些初步但有趣的结论。首先我们从信息熵的角度考察了纠缠的纯化与提取以及量子态的局域区分。我们发现,纠缠的纯化或提取过程可以描述为以消耗辅助系统的纠缠资源为代价,减少或消除目标系统的不确定性,并保持目标系统仍为纠缠态的过程。而量子态的局域区分是用局域操作和经典通信精确知道系统处于哪个态。区分之前系统处在几个可能态之一,具有不确定性,一旦区分了这些可能态,则系统的不确定性消除了。因此量子态的局域区分可描述为通过局域操作和经典通信排除系统不确定性或获得系统信息的过程。然后在一个特殊的方案下我们得到了信息熵、提取纠缠和可区分信息(其定义见第五章第三节)三者之间的一个关系式。利用这个关系式还可讨论无限拷贝下混合态的提取纠缠和提取纠缠的下限(主要结论发表在 Quantum Information and Computation V3, 203 (2003.5))。

最近我们还把这个关系式推广到了一般的方案,推广后的关系式为: $E_D = \bar{E} - \frac{S}{I_{md}}$, 其中 E_D 是混合态的提取纠缠; $\bar{E}$ 是混合态的本征态的平均纠缠; S 是为提取纯纠缠态所必须排除的不确定性; I_{md} 是排除 1bit 的不确定性所需损失的纠缠。这个关系式简洁、普适,原则上适于任意多体量子态,并揭示了系统的不确定性与系统的非局域性之间的关系。这个关系式很类似与热力学的一个关系式: $F = U - TS$, 其中 F 是自由能;

U 是内能; T, S 分别是温度和熵。有趣的是,上面两个关系式虽然仅仅是类似,但两者的熵都有相同的物理意义,这说明信息熵在热力学过程和纠缠提取过程中起了相同的作用。我们的这些结论展示了信息熵与量子非局域性的关系。

关键词:非局域性;量子信息;纠缠态;纠缠提取;局域区分

ABSTRACT

This thesis will probe the property of non-locality from the following fields: inseparability criterion of quantum states, purification or distillation of the entanglement, local distinguishability of orthogonal quantum states, and the relations among information entropy, distillable entanglement and local distinguishability of orthogonal states. The main contents of this thesis are shown below:

(1) A necessary and sufficient condition of the separability of a mixed state in bipartite systems is presented by decomposing a higher dimension Hilbert space into many $2 \otimes 2$ subspaces. This condition comes down to the problem of finding the solution of a set of quadratic equations. The solution of this set of quadratic equations is a set of orthogonal vectors, which makes the equations more easily solved. It is shown that even if the projection of a mixed state on each $2 \otimes 2$ subspace is separable the state is still entangled probably. The style of entanglement in a lower dimensions system is different from that in a higher dimension system.

By the same means we present a lower bound on entanglement of formation of states in $2 \otimes n$ systems. This lower bound can be calculated easily and has distinct physical meaning.

(2) We discuss the distillation of entanglement from finite copies of a mixed state. Two conceptions of quasiseparable state and distillable subspace are introduced. First a necessary condition of distillability from finite copies is given, then a necessary and sufficient condition of distillability from finite copies and the most efficient distillation protocol are given. These conclusions can be generalized to multi-partite mixed states. It is shown that the distillation of entanglement (from finite copies or infinite copies of a mixed state) is to project out a subspace, the projection of all copies of the mixed state in this subspace is a pure entangled state. The distillation of entanglement can be achieved by joint projective measures and classical communication and doesn't involve Control-Not operations, in principle.

(3) We consider the orthogonality and the distinguishability of a set of arbitrary states in multi-partite systems. It is shown that if a set of orthogonal states are distinguishable by local operations and classical communication (LOCC), each of the states is a supposition of some

product vectors so that the product vectors in every orthogonal states are orthogonal to the other orthogonal states. Employing this conclusion we also prove a specially simple criterion: if the sum of the Schmidt numbers of a set of bipartite states in a quantum system is bigger than the dimensions of Hilbert space of the system, the states are not LOCC distinguishable. These results can improve the known conclusion in local distinguishability, and may be also useful in understanding the essence of non-locality and discussing the distillation of entanglement.

(4) We have discussed the connections between the information entropy (which describe the uncertainty of the system) and the quantum non-locality. First, The relations of information entropy, distillation of entanglement and distinguishability of orthogonal states are discussed. In terms of information an new interpretation for the distillation of entanglement and the distinguishability of orthogonal states is given. Then employing a special protocol we give a sufficient and necessary condition for the local distinguishability of states and the distillation of the entanglement, and gain the maximal yield of the distillable entanglement. It is shown that information entropy, the local distinguishability of states and the distillable entanglement are closely and generally related. This means that non-locality and the uncertainty in a quantum system are related. Recently, we generalize these conclusions and get an interesting formula:

$E_D = \bar{E} - \frac{S}{I_{md}}$, where E_D is the distillable entanglement of a mixed state; $\bar{E}$ is the average of the entanglement of the eigenstates of the mixed state; S is the amount of the necessarily gained information; I_{md} is the loss of the entanglement per bit information gained. This formula is similar to a form in the thermodynamics: $F = U - TS$ where F is the free energy; U is the inner energy; T, S is the temperature and the entropy respectively. Interestingly, the two formulas is just of similar form, but the entropy has the same physics. This show that the information entropy has the same role in the thermodynamics and the distillation of the entanglement. We also get a criterion for inseparability related to the information entropy (see arxiv: quant-ph/0403015, submitted). These conclusions show the connections between the information entropy and quantum non-locality.

Key words: non-locality, quantum information, entangled state, distillation of the entanglement, local distinguishability.

目 录

摘 要.....	(i)
----------	-------

引 言

1 研究背景	(1)
2 本文的研究目的及主要工作	(5)
参考文献	(6)

第一章 部分与本文有关的基本概念和基础知识

1.1 纯态的 Schmidt 分解与 Schmidt 数	(10)
1.2 局域操作	(11)
1.3 部分转置操作.....	(12)
1.4 量子操作的线性性	(12)
1.5 作为纠缠度量的几个必要条件.....	(13)
1.6 几种基本纠缠度量	(14)
参考文献	(17)

第二章 二体量子态的可分离判据

2.1 二体量子态可分离的必要条件.....	(19)
2.1.1 Bell-CHSH 不等式判据	(20)

2.1.2 部分转置正定判据(Peres 判据)	(20)
2.1.3 HH-CAG 约化判据	(20)
2.1.4 α -熵不等式判据	(21)
2.1.5 纠缠度判据	(21)
2.2 可分离态的充分必要条件	(21)
2.3 结构纠缠的一个下限	(28)
本章小节	(30)
附 录	(31)
参考文献	(32)

第三章 纠缠的纯化和提取

3.1 引 言	(34)
3.2 无限个拷贝情况下可提取的条件	(35)
3.2.1 Werner 态的纯化	(35)
3.2.2 任意 $2 \otimes 2$ 系统混合纠缠态的纯化	(36)
3.2.3 束缚纠缠态	(37)
3.3 有限个拷贝情况下的提取	(39)
3.3.1 从有限个拷贝中提取纠缠的必要条件	(39)
3.3.2 从有限个拷贝中提取纠缠的充要条件	(41)
3.4 最有效的提取方案和提取纠缠的计算	(45)
3.4.1 有限个拷贝情况下最有效的提取方案和提取纠缠的计算	(45)
3.4.2 有限拷贝中任意 $2 \otimes 2$ 混合态的提取纠缠	(46)
3.4.3 无限个拷贝情况下最有效的提取方案	(47)
3.5 多体混合态有限个拷贝下的纠缠提取	(48)

3.5.1 多体混合态在有限个拷贝下可提取的必要条件	(48)
3.5.2 多体混合态在有限个拷贝下可提取的充要条件	(49)
本章小节	(51)
参考文献	(51)

第四章 正交量子态的局域区分

4.1 正交量子态局域区分研究的主要进展	(55)
4.1.1 可以局域区分的情况	(55)
4.1.2 不可局域区分的情况	(56)
4.2 多体系统中正交态可局域区分的条件	(57)
4.2.1 多体正交态可局域区分的一个充要条件	(57)
4.2.2 多体正交态局域可区分的必要条件	(59)
4.3 多体正交乘积态的局域区分	(63)
本章小结	(65)
参考文献	(66)

第五章 熵、纠缠的提取及正交量子态局域区分的关系

5.1 联合熵、条件熵和互熵	(69)
5.1.1 经典情况	(69)
5.1.2 量子推广	(70)
5.2 纠缠提取和量子态局域区分的信息论描述	(70)
5.2.1 纠缠提取的信息论描述	(71)
5.2.2 局域区分的信息论描述	(73)
5.3 局域区分与纠缠提取的关系	(74)

5.4 经典信息的损失与纠缠的损失	(78)
5.4.1 相对熵纠缠的损失与经典信息的损失	(78)
5.4.2 提取纠缠的损失与经典信息的损失	(79)
本章小结	(81)
参考文献	(81)
 第六章 总结与展望	 (83)
 致 谢	 (86)
 攻读博士学位期间发表和待发表的学术论文	 (87)
 后 记	 (89)