

摘要

量子力学诞生于 20 世纪初期,但是这个理论从它诞生开始,就存在着不同的理解和争论。随着科学家之间的争论,人们对量子力学的认识更加深刻和确信。20 世纪 90 年代,量子力学与信息科学的相结合,更是将信息科学的发展带入了一个新天地。量子信息科学主要包括量子通信和量子计算,而量子信息科学的基础则是量子态的制备、变换、传输、存储以及测量。很多系统可以被用来作为研究量子信息科学的平台,常见的有光学体系、核磁共振体系(NMR)、腔动力学体系(Cavity QED)、量子点(Quantum Dot)和原子系综等。光学体系相对于其它体系相对全面,而且光子具有环境消相干小,便于操纵等优点。首先,现代通信的基础便是光纤网络,光子是天然的飞行比特,因而量子通信的研究基本都在光学体系中展开;其次,随着 2001 年,Knill, Laflamme 和 Milburn 三人在自然杂志发表一篇论文,证明了线性光学方法实现大规模量子计算的可能性,推动了光学体系在量子计算方面的研究。

单光子多比特体系是线性光学方法研究量子信息问题的基本内容之一。其基本思想是,利用光子的各种性质在单个光子上编码两比特或更多比特的信息,用来作为研究量子信息问题的载体。常见编码光子比特的有光子偏振、光子空间动量和光子轨道角动量,而光子空间动量和光子角动量可以用来编码高维体系(qudit)。单光子多比特体系可以用来很好的研究量子态的叠加性质,也是向多体、高维推广的基础。我们在实验上利用单光子多比特体系,研究了量子随机行走算法,量子博弈问题和单比特量子么正操作完美区分。

I、光子轨道角动量和量子随机行走

光子轨道角动量与光场的空间模式有着密切的关系。对于 Laguerre-Gaussian (LG) 模式光,每个光子携带 $l\hbar$ 的轨道角动量,其中 l 为整数,表示轨道角动量量子数,也表示 $\exp(il\varphi)$ 螺旋波前的单模光的模式。不同 l 的轨道角动量构成完备的 Hilbert 空间,所以可以用来编码 qubit 或者 qudit。我们用全息照相技术,制作用来产生各种模式激光的计算全息片,并将其应用于量子随机行走的实验。

量子随机行走是一种量子算法，与经典随机行走有着完全不同的现象和结果。量子随机行走算法已经在很多体系中实现，包括光学体系。在我们实验中，利用光子的路径编码 qubit，光子的轨道角动量编码 qudit，实现光子在轨道角动量空间上的随机行走。具体是先将光子制备到路径叠加态，然后根据不同路径，通过计算全息片实现轨道角动量的改变，最后探测光子处于各个轨道角动量态的几率，便得到了量子随机行走的结果。我们巧妙地将光子轨道角动量的高维特性应用于实验，得到了更为漂亮的结果，并且讨论了将量子随机行走向更多步数推广的实验可行性。这些内容将在第二章和第三章中详细讨论。

II、量子博弈

量子博弈是运筹学与量子理论结合的产物，是量子信息论的一个重要分支。量子博弈主要分为三类问题：PQ 翻硬币问题、“囚徒困境”问题和量子赌博。我们在实验上，利用线性光学方法，实现了量子赌博机，并对结果进行了分析，得出博弈方获得最大收益的最佳方案。实验中，我们使用两块双折射晶体作为偏振分束器，解决了 Mach-Zehnder 干涉稳定性的问题，获得了长时间的干涉稳定，使得实验结果更具说服力。第四章我们将详细介绍量子博弈论的基本问题和实验实现量子赌博机的具体情况。

III、量子么正操作的完美区分

量子态的区分是量子信息中的基本问题，科学家在研究量子态局域操作可区分性方面做出了大量的工作，取得了很大的进展。量子么正操作的区分与量子态区分类似，有着重要的意义，但是又不同于量子态的区分。理论上已经证明，任意两个不同的么正操作 U 和 V ，不论它们是否正交 ($U^\dagger V = 0$)，我们总可以通过并行运行该操作有限次的方法或者串行加入辅助么正操作的方法将它们完美区分。第五章我们将详细介绍量子么正操作完美区分的两种方案——并行方案和串行方案，并说明我们在实验上如何利用这两种方案，成功地实现了单比特么正操作的完美区分。最后通过实验结果，讨论了两种方案的优缺点和实验扩展问题。

Abstract

Quantum mechanics was born in the beginning of the twentieth century, and there were different understandings and debates on this theory through the century. But with the arguments between the scientists, it is clear that the quantum mechanics is a powerful theory in many fields. With the combining of information science and quantum mechanics in ninety years of twentieth century, quantum information science attracts much attention. Quantum information science mainly includes quantum communication and quantum computation. The process of preparation, operation, transmission, storage and measurement quantum state is the fundamental question of quantum information. There are several systems can be used to study the quantum information process, such as linear optics, NMR system, cavity QED, quantum dot, atom system et al. Linear optical system is a good candidate for implementing quantum information process for two reasons. First, the modern communication is based on fiber net, and photons are natural flying bit. So the research of quantum communication is most in the optics system. Second, Knill, Laflamme, and Milburn show that probabilistic two-qubit operations implemented in linear optical circuits with ancilla photons can be used to build a scalable quantum computer. Their work has stimulated much attention on the experimental realization of linear optics quantum computation protocols.

Single-photon few-qubit system is one of the basic linear optics system on quantum information research. The basic idea of single-photon few-qubit system is to encode two or more qubits on a photon by using different characters of photon. Usually, the quantum bit (qubit) can be encoded by polarization, space momentum and orbital angular momentum of photons. Especially, the space momentum and the orbital angular momentum (OAM) of photons can be used to encode high dimensional system (qudit). Single-photon few-qubit system can be used to study the superposition of quantum states, and can be easily extend to many-body or high dimensional systems. We experimentally implemented quantum random walk, quantum gambling

machine and perfect discrimination of unitary operations by using single-photon few-qubit system.

1. Orbital angular momentum of photons and quantum random walk

Orbital angular momentum of photons has the relationship with the mode of light. As we know, light beams can carry OAM associated with helicity of their phase fronts, described by a phase term $\exp(il\varphi)$, carries an OAM of $l\hbar$ per photon, where l can take any integer value. The OAM can make up an infinite dimensional Hilbert space, so it can be used to encode qubit or qudit. Orbital angular momentum of photons can be generated by computer generated holograms which are used in our experiment of quantum random walk.

Quantum random walk is a kind of quantum algorithm, and it is quite different from classical random walk. Numerous schemes of quantum random walk have been proposed using many kinds of system, including linear optics system. We encode space momentum of photon as a qubit and OAM of photon as a qudit, experimentally study the quantum random walk on the one-dimensional OAM space. We initialize the photons on a superposition of different routes, then change their OAM by using computer generated holograms due to different route. At last, we detect the probabilities of photons on each OAM state, which are also the results of quantum random walk. Because the photons “random walk” on the OAM space, the experimental setup is much simpler and easy to adjust. These contents will be discussed in the chapter two and chapter three.

2. Quantum game

Quantum game is a new region combined with operational research and quantum theory. It is an important embranchment of quantum information. Quantum game contains three main questions: PQ penny flipover, prisoner’s dilemma and quantum gambling. We experimentally realize the quantum gambling machine by using optical method, and discuss the best strategy of the participator to maximize their gains. We use two pieces of birefringent material calcites as polarizing beam splitters, which make the Mach-Zehnder interferometer inherently stable, and get the convictive

results of the quantum gambling. We will introduce some quantum game theory and our experimental setup in the chapter four.

3. Perfect discrimination of unitary operations

Distinguishable of quantum states is an fundamental question of quantum information, and a lot of works have been done on it. Similar to discrimination of quantum states, discrimination of quantum operation is also very important. But there are some differences between states and operation discrimination. It is shown that two unitary operations U and V can be perfectly discriminated by using parallel scheme or sequential scheme with finite number copies of unknown operation, no matter U and V are orthogonal or not. We will detailed introduce the two schemes of perfect discrimination of two unitary operation and our experiment based on these two schemes. The complexity and resource consumed are analyzed and compared with some other schemes of discrimination of unitary operations.

论文原创性和授权使用声明

本人声明所呈交的学位论文,是本人在导师指导下进行研究工作所取得的成果。除已特别加以标注和致谢的地方外,论文中不包含任何他人已经发表或撰写过的研究成果。与我一同工作的同志对本研究所做的贡献均已在论文中作了明确的说明。

本人授权中国科学技术大学拥有学位论文的部分使用权,即:学校有权按有关规定向国家有关部门或机构送交论文的复印件和电子版,允许论文被查阅和借阅,可以将学位论文编入有关数据库进行检索,可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

保密的学位论文在解密后也遵守此规定。

作者签名: 张沛

2018年4月28日

第一章 光量子信息处理的基本理论

量子理论和相对论是在 20 世纪初文化和政治蓬勃发展时产生的，它如同当代艺术、音乐、文化和政治的新发展一样，具有本质上的革新性。它们是物理界两项伟大的成就，已经成为当今物理学发展的两块基石。它们的出现是人们对客观物质世界的本质认识的一大进步。

十九世纪末，以黑体辐射实验规律为代表，一些经典理论不能解释的现象吸引了一代科学家的努力探索，最终导致了量子力学的诞生。量子力学可以解释经典力学不能解释的现象，它被大量实验事实证明是一个成功的物理理论。但是这个理论从它诞生开始，就存在着不同的理解和争论。A. Einstein, B. Podolsky 和 N. Rosen (EPR) 在 1935 年发表了一篇简短而重要的论文[1]，对正统的量子力学原理和概念的诠释提出了质疑，N. Bohr 随即发表文章进行答辩[2]，并由此引发了一场科学巨匠之间的大争论[3]。争论的焦点是：量子力学理论是否完备，定域实在论是否正确。随后 Bohm 在 1952 年提出隐变量假说，而 Bell 则根据定域实在论和隐变量假说，在 1964 提出了著名的 Bell 不等式[4]，用来支持 EPR 的观点。

1982 年 Aspect 等人做了 Bell 不等式验证的实验[5]，以及后来的其它人又做了一些更精密的实验，这些实验几乎都肯定了量子力学理论的正确性，否定了定域隐变量理论。从而激发了一大批后来的研究量子基本理论及其应用的开创性工作。以量子通信和量子计算为主要内容的量子信息学，就是以基本量子理论为基础迅速发展起来的新兴交叉学科。

随着量子信息科学的蓬勃发展，一些全新的概念，如量子密码，量子保密通信，量子计算机，量子调控等，都开始进入了人们的研究视野。量子信息科学正在以惊人力量改变着我们的生活：以量子隧穿效应为理论根据的量子隧穿显微镜，使人们能够看清原子，操纵原子；激光冷却、原子囚禁是光粒子性的最直接应用；量子计算机以惊人的计算速度冲击着现有的密码体系，而同时量子理论又提供了更为安全的量子密码和量子保密通信[6-8]……

量子通信和量子计算已经在很多体系中实现，最常见的有光学体系、核磁

共振体系 (NMR)、腔动力学体系 (Cavity QED)、量子点 (Quantum Dot)、原子系综和低温超导体系等。在量子计算方面, 线性光学系统在光子态操作、光子纠缠和消相干方面有着独有的优势, 并且实现了很多线性光学量子计算的基础实验。单光子源可以从相干性极好的激光衰减获得, 也可以通过自发参量下转化系统, 获得单光子或者纠缠的光子。而光子的偏振态可以通过线性光学元件, 例如半波片、 $\lambda/4$ 波片、分束器、偏振分束器等实现量子么正操作。而在量子通信方面, 基于目前的通信网络建立在光纤通信, 因而量子通信的研究也集中在光波通信。我们在实验上正是利用光学体系作为平台, 研究了一些量子信息的基本问题, 包括量子随机行走算法、量子博弈和量子么正操作的完美区分。

在量子信息的研究中, 量子力学用于描述物质系统的基本数学语言就是量子态, 而系统的演化则是用量子态的么正演化来描述。在详细论述这些量子信息理论之前, 在本章节我们先介绍量子信息的一些基本概念, 包括量子比特, 量子纠缠, 量子干涉, 单光子多比特体系以及在实验上用线性光学方法研究量子信息的基本知识。

1.1 量子比特

比特 (bit) 是经典信息论的基本概念。从物理角度讲, 比特就是一个拥有两个可以区分的状态的系统, 如是或非, 真或假, 0 或 1, 这两种状态之间存在巨大的能量壁垒。经典计算机中, 用高低电压来表示比特, 经典光纤通信中, 使用亮、暗光信号作为信息比特。量子信息与量子计算中建立了类似于经典比特的量子比特 (quantum bit 或 qubit)。像经典比特一样, 量子比特也是用实际的两态 (0 或 1) 物理系统来实现, 分别将这两种状态记为 $|0\rangle$ 或 $|1\rangle$, 对应于经典的 0 和 1。

量子态区别于经典态的最重要性质在于它的相干叠加性, 也就是说量子比特的状态除了可以是 $|0\rangle$ 或 $|1\rangle$, 还可以是 $|0\rangle$ 和 $|1\rangle$ 的线性组合态, 常称作量子叠加态 (superposition), 表示为:

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1. \quad (1-1)$$

其中 $\alpha, \beta \in \mathbb{C}$ 。换句话说, 量子比特的状态是二维复向量空间中的向量。特殊的

$|0\rangle$ 和 $|1\rangle$ 状态成为计算基态 (computation basis state)，是构成这个向量空间的一组正交基。

经典情况下，我们可以通过检查一个比特，来确定它是处于 0 状态还是 1 状态。但是在量子情形下，我们不能通过检查一个量子比特来确定它的量子状态，也就是得到 α 和 β 的值。如果我们测量式(1.1)的量子态，我们只能发现有 $|\alpha|^2$ 的几率得到“0”， $|\beta|^2$ 的几率得到“1”。经典比特可以看作是量子比特的特例 ($\alpha=0$ 或者 $\alpha=1$)。量子比特可以处于叠加态与我们理解身边物理世界的常识相矛盾。经典比特像丢一枚硬币：要么正面朝上，要么反面朝上。与之相反，量子比特可以处于 $|0\rangle$ 和 $|1\rangle$ 之间的连续状态——直到它被观测（量子比特被观测时，只能得到非“0”即“1”的测量结果）。

尽管这么奇特，量子比特的存在确实是真实的。他们的存在和行为被大量实验所证实，并且有许多不同的物理系统，可以用来实现量子比特。常见的实现方法有：光子的两种不同偏振 (polarization)；均匀电磁场中电子或原子核的自旋取向；原子或量子点中的能级等。

除了二维量子比特外，我们还经常会用到高维量子比特 (qudit)。对于 n 维量子比特，它的基态不是两个，而是 n 个。例如，三维量子比特 (qutrit) 的基态为 $|0\rangle$ 、 $|1\rangle$ 和 $|2\rangle$ ，它的一般形式为：

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle, \quad |\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1. \quad (1-2)$$

同二维量子比特类似，如果我们进行测量，得到“0”、“1”和“2”的几率分别为 $|\alpha|^2$ 、 $|\beta|^2$ 和 $|\gamma|^2$ 。以此类推，我们可以得到 n 维量子比特的情况。对于 m 个 n 维量子比特来说，它们所张的空间就是 n^m 维希尔伯特 (Hilbert) 空间，具有 n^m 个完备正交基。而 n 维量子比特的实验实现则需要 n 态量子系统，常用的有：光的空模式（第二章会介绍）和多能级原子或量子点等。

1.2 量子纠缠

对于一个两体的两子体系 (A 和 B)，假设体系 A 的一组完备力学量集的共同本征态为 $\{|\psi_i\rangle_A\}$ ，体系 B 的一组完备力学量集的共同本征态为 $\{|\psi_j\rangle_B\}$ 。这里

i 和 j 分别代表体系的 A 和 B 的一组完备量子数。如果整个体系的态矢量 $|\psi\rangle_{A,B}$ 不可能写成子系统态矢量的直积形式时, 即 $|\psi\rangle_{A,B} \neq |\psi_i\rangle_A \otimes |\psi_j\rangle_B$, 称态 $|\psi\rangle_{A,B}$ 为纠缠态, A, B 两子系统被称为是互相纠缠的。这个定义可以推广到多体或多自由度体系: 若整个体系的量子态不能表示为各个子系统的直积形式, 则该量子态成为纠缠态。

上面的描述只是体系的量子态为纯态时的情况, 如果体系处于混合态, 则纠缠的定义要复杂一些。以两子系统为例, 若体系的量子态密度矩阵可以表示为

$$\rho_{AB} = \sum_{i,j} P_{ij} \rho_{Ai} \rho_{Bj} \quad (1-3)$$

则 A, B 体系之间不存在纠缠, 反之, 则两体系是纠缠的。

如果处于纠缠的两个 (或者多个) 粒子的自由度都是二, 那么它们所处的态称为二维纠缠态。二维纠缠是最常见、最基本的一类纠缠, 如果讨论中没有特别指出是高维纠缠, 那么一般都讨论的是二维纠缠。在两体纠缠态中, 最重要的是称作 Bell 态[9]的四种纠缠态:

$$|\Psi\rangle_{A,B}^{\pm} = (|+\rangle_A |-\rangle_B \pm |-\rangle_A |+\rangle_B) / \sqrt{2}, \quad (1-4)$$

$$|\Phi\rangle_{A,B}^{\pm} = (|+\rangle_A |+\rangle_B \pm |-\rangle_A |-\rangle_B) / \sqrt{2}. \quad (1-5)$$

其中 $|\Psi\rangle_{A,B}^{\pm}$ 称为单重态 (具有交换反对称性), 其他三个态称为三重态 (具有交换对称性)。这四个态构成两比特体系所张的四维 Hilbert 空间的一组标准正交基, 也称作 Bell 基。Bell 态时具有最大纠缠度的两比特纯态, 通常也称作最大纠缠态。由于 Bell 态的这一独特性质, 使得它在量子信息中有着极为重要的应用。多体纠缠态中, GHZ 态[10]和 W 态[11]是比较重要的两种纠缠态。

处于纠缠态的系统在被测量时, 表现出一种相当奇特的关联性质。我们以 Bell 态为例, 式(1-4)中的两个 Bell 态, 当我们对 A 进行 $|+\rangle$ 、 $|-\rangle$ 正交基测量时, 如果测得 A 的结果为 $|+\rangle$, 那么 B 此时必然处在 $|-\rangle$ 上, 反之, 则 B 一定处在 $|+\rangle$ 上。不管我们怎么变换正交测量基, B 的状态一定与 A 的相反。这种强烈的关联性质已经超出了经典力学体系所可能具有的经典关联。而且这种关联可以很远距离的保持, 即, 即使 A, B 在空间上相距很远, 只要它们纠缠, 则上面提到的关联依然存在 (量子力学的非局域性)。这一结果曾经使爱因斯坦 (Einstein) 也

感到无法接受,以至他于 1935 年与 Podolsky 及 Rosen 一起提出了著名的 EPR 佯谬[1]。此后,对于此佯谬的论证,更加揭示了量子力学的本质。

1.3 量子干涉

干涉来源于物质的不可区分性,任何不可区分性都可以导致干涉。光子的干涉随时都在发生,但是由于没有选择正确的探测方式而忽略它的存在。经常是因为探测测器的响应时间太长,不同的干涉结果互相叠加而表现出平均效应,使得原本明显的干涉现象消失。因此获得稳定高可见度的干涉现象,也是人们一直研究的课题。首先,利用相干性好的光源,从源头开始就引入不可区分性。常见的做法是选择模式稳定,具有良好相干性的激光作为光源。其次,在测量的时候通过消除光子的一些可区分信息来提高干涉可见度。除了这些提高不可区分性的方法,稳定干涉过程也是非常重要的环节。

从最早的单光子干涉,例如杨氏双缝干涉, Mach-Zehnder 干涉(简称 M-Z 干涉),到双光子干涉,例如 Hong-Ou-Mandel 干涉以及 Franson 干涉,人们对光子的干涉理解一步步的加深,也使得干涉在量子信息中的应用越来越广泛。单光子的干涉在演示量子态叠加性方面有着广泛应用,而且单光子量子密钥分发的光学部分就是利用单光子干涉做成的干涉环[6,12];而线性光学量子计算和很多量子态的制备和测量方面几乎都是以多光子干涉为核心来完成的[13,14]。下面以 M-Z 干涉和 Hong-Ou-Mandel 干涉为例,简单介绍一下单光子和双光子干涉。

1.3.1 Mach-Zehnder 干涉

在量子信息中,经常用到的一种单光子干涉就是 Mach-Zehnder 干涉(以下简称 M-Z 干涉)。很多其他的干涉仪都可以从基本的 M-Z 干涉仪演化而成,例如量子密钥分配中用到的干涉仪就是两个不等臂的 M-Z 干涉仪。M-Z 干涉仪的光路图如图 1.1 所示。一束光经过分束器(BS1)分成两束(a 路和 b 路),在其中一路通过调相介质引入位相 ϕ ,最后在另一个分束器(BS2)上重合。只要满足干涉条件,在 BS2 的两个输出端口(c 和 d)探测,便可以观测到干涉现象。

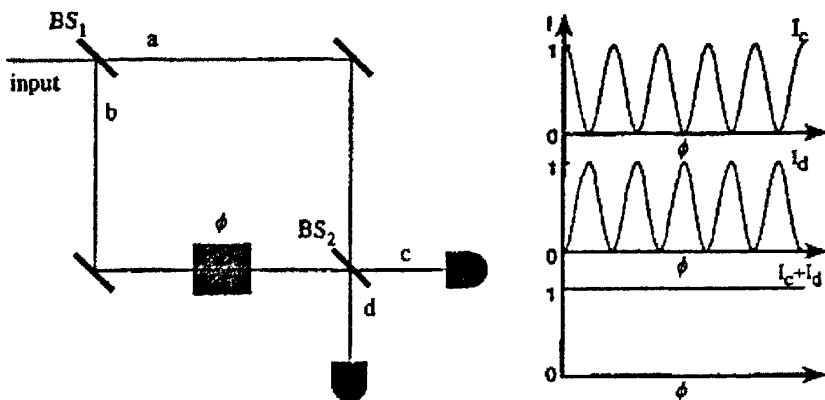


图 1.1 Mach-Zehnder 干涉仪及其干涉曲线

对于上面的这个 M-Z 干涉仪，要满足以下条件才能看到理想的干涉现象：

1). 输入光模式单一，相干性极好；2). a 路和 b 路的路径差小于入射光的相干长度；3). a、b 两路光在 BS2 上完全重合；4). 整个光路稳定性极好。满足这些条件，我们就可以通过改变 b 路径的相位调制器，观察到 c、d 两路的光强随相位 ϕ 的变化曲线。

假设两块分束器的透射率和反射率分别为 T 和 R，则分束器对光的变换矩阵[15]可以表示为：

$$U_{BS} = \begin{pmatrix} \sqrt{T} & -\sqrt{R} \\ \sqrt{R} & \sqrt{T} \end{pmatrix}. \quad (1-6)$$

当分束器的透射率和反射率相等时，即同为 50% 的平衡分束器（没有特指的情况下，我们所说的分束器都是指平衡分束器），则其演化矩阵为：

$$U_{SBS} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}. \quad (1-7)$$

利用变换矩阵的表述方式，M-Z 干涉仪的整个过程可以表示成如下：

$$\begin{aligned} E_{input} &\xrightarrow{BS_1} \frac{1}{\sqrt{2}} (E_a + E_b) \\ &\xrightarrow{\phi} \frac{1}{\sqrt{2}} (E_a + e^{i\phi} E_b) \\ &\xrightarrow{BS_2} \frac{1}{2} [(E_c - E_d) + e^{i\phi} (E_c + E_d)] \\ &= \frac{1}{2} [(1 + e^{i\phi}) E_c + (1 - e^{i\phi}) E_d] \end{aligned} \quad (1-8)$$

式中 E 表示电场强度。最后，在 c 路和 d 路探测光的强度 I 与相位 ϕ 的关系分别为：

$$I_c = \frac{1 + \cos \phi}{2} I_{input}; \quad (1-9)$$

$$I_d = \frac{1 - \cos \phi}{2} I_{input}. \quad (1-10)$$

其中 I_{input} 是输入光的光强。特别的，当入射光是单光子时，式(1-9)和(1-10)表示的是该光子出现在 c 路和 d 路的概率。干涉可见度 (visibility) 表示为：

$$V = \frac{|I_{cMax} - I_{dMin}|}{|I_{cMax} + I_{dMin}|}. \quad (1-11)$$

此干涉结果来自于探测器原则上对达到探测器的光来自于那一路的不可区分性。这一不可区分性表现在需要满足前面所提到的前三点干涉条件。如果光路的稳定性不好，最终将导致两路的相位差 ϕ 随时间漂移，记为 $\phi(t)$ ，则干涉结果将是：

$$I_c = [1 + \frac{1}{\Delta t} \int_{t-\Delta t}^{t+\Delta t} \cos \phi(t) dt] \frac{I_{input}}{2} \quad (1-12)$$

$$I_d = [1 - \frac{1}{\Delta t} \int_{t-\Delta t}^{t+\Delta t} \cos \phi(t) dt] \frac{I_{input}}{2} \quad (1-13)$$

当 $\phi(t)$ 在 Δt 时间内变化剧烈导致 $\frac{1}{\Delta t} \int_{t-\Delta t}^{t+\Delta t} \cos \phi(t) dt \rightarrow 0$ 时，干涉现象就会消失，干涉可见度为 0。

从式(1-9)和(1-10)中可以看出， ϕ 每变化 π ，光强就会发生明亮转变。而对应于相位 π 的光程差是半个波长，因此通过此干涉仪可以测量到波长量级的长度变化。同样，其他很多能引起相位变化的物理量，如温度、压强等，都可以用此类干涉仪进行高精度的测量。当入射光为单光子时，由式(1-8)可以看出， c 、 d 两路的光子态形式由相位 ϕ 决定，所以 M-Z 干涉仪也可以用来制备量子叠加态，这点在制备光子轨道角动量叠加态时应用最多[16]。

以 M-Z 干涉仪为原型，可以演化出众多的干涉仪，例如迈克耳逊干涉仪、Sagnac 干涉仪等。而在以相位编码的量子密钥分配实验中，整个光路可以被看作是一个大的 M-Z 干涉仪。

1.3.2 Hong-Ou-Mandel 干涉

前面简单介绍了单光子干涉及 M-Z 干涉仪，单光子干涉可以理解为光场的二阶干涉[17]，其可见度的大小对应着二阶相关度。对于二阶干涉的描述是可以建立在经典理论框架之中。然而，随着 H. Hanbury-Brown 和 R. Q. Twiss 在上世纪 50 年代完成光场的 HBT 实验[18]，尤其是在 1987 年 C. K. Hong, Z. Y. Ou 和 L. Mandel [19]完成著名的 HOM 干涉实验后，我们需要利用量子理论去描述此类光场的高阶干涉。或者说，我们能利用经典干涉理论解释的多个光子的干涉不是真正意义的多光子干涉。

双光子干涉仪主要有两种：Hong-Ou-Mandel 干涉[19]和 Franson 干涉[20,21]。下面我们主要介绍一下在量子信息中应用最为广泛的 Hong-Ou-Mandel 干涉，由此说明光场的四阶干涉现象和双光子干涉的本质。

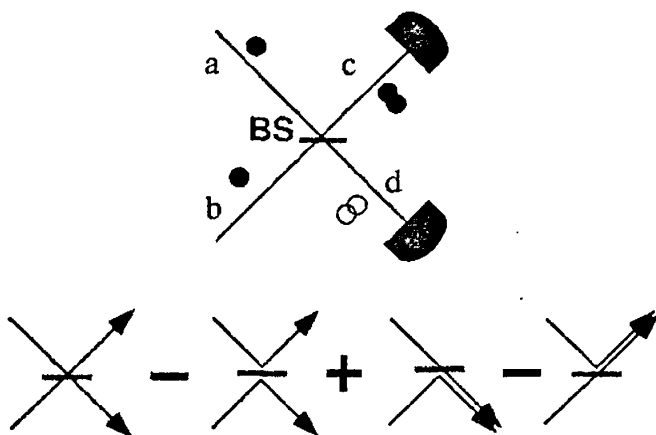


图 1.2 双光子干涉示意图

如图 1.2，我们考虑一种简单的双光子干涉，同时也是量子信息中经常用到的双光子干涉——Hong-Ou-Mandel 干涉。两个全同的单光子分别延 a、b 两路入射到分束器的两个输入端。根据不同的透射和反射，图 1.2 下方列出输出的 4 种可能情况。但是当两个光子同时到达分束器的同一点时，探测器不可能区分第一种和第二种情况，将发生干涉现象。并且它们之间由于分束器的透、反射引起的相位差为 π ，导致干涉相消，因而这时候光子只可能从同一出口离开分束器。表现在探测方面就是 c、d 两路的两个探测器的复合计数（同时探测到记为有符合计数，相当于逻辑运算的“与”）为 0。同时，如果在其中一路径上探测双光子

的概率，可以发现干涉时双光子的概率是不干涉时的两倍。也就是光子分别走两个路径的概率由于干涉而转移到了走同一路径，从而也保证了概率和为 1，或者能量守恒。

C. K. Hong, Z. Y. Ou 和 L. Mandel 在 1987 年首先完成了这样的双光子干涉实验。他们的实验光路图如图 1.3 所示。时间关联的双光子态是通过光学自发参量下转换过程[22]实现的。在自发参量下转换过程中，一束泵浦激光入射到非线性晶体中，一个泵浦光子将以一个很小的概率劈裂成两个参量光子。由于此过程时间非常短暂，可以认为这两个光子是同时产生的。图 1.3 中利用 I-型切割的晶体产生的偏振相同的两个光子入射分束器，通过调节分束器（BS）的位置可以调节光程差，即可以改变两个光子到达分束器的时间，从而得到了符合计数与相位差的关系曲线，如图 1.4 所示。

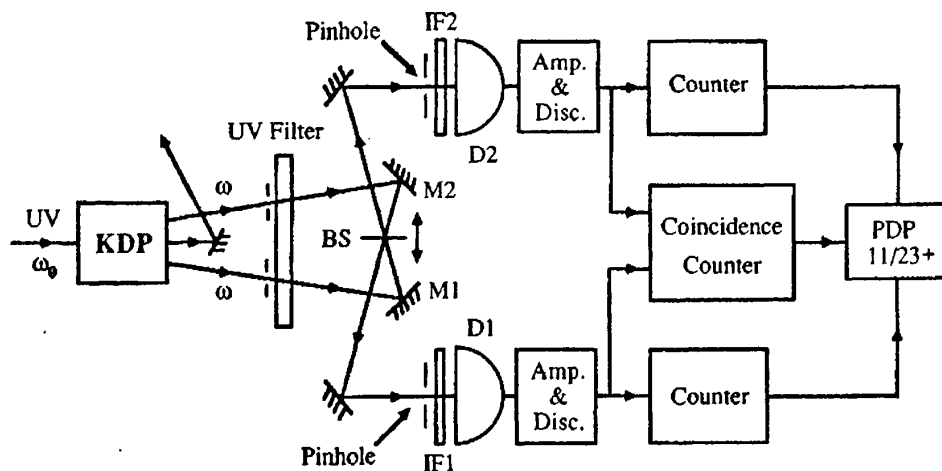


图 1.3 Hong-Ou-Mandel 干涉实验装置图

在实验过程中，由于 I-型相位匹配条件导致的自发参量下转换产生的光子的谱线展宽很宽，此时需要用窄带干涉滤波片（IF1 和 IF2）进行滤波。光子通过干涉滤波片之后，相干长度将可以提高一个量级，达到 10^{-13} 秒甚至更高。当两光子的光程差大于两光子的相干长度，即两光子在分束器上时间完全不重合，我们可以从到达探测器的时间上对光子进行区分，因而干涉不会发生，光子将以经典概率的方式进行传输，即两个探测器有 50% 的概率都响应；而在两光子光程差在相干长度之内时，光子波包在分束器有重叠，引起时间上的不可区分性，会存在部分干涉；直至到达时间完全相同，光子波包完全重合，可以得到最大干涉，

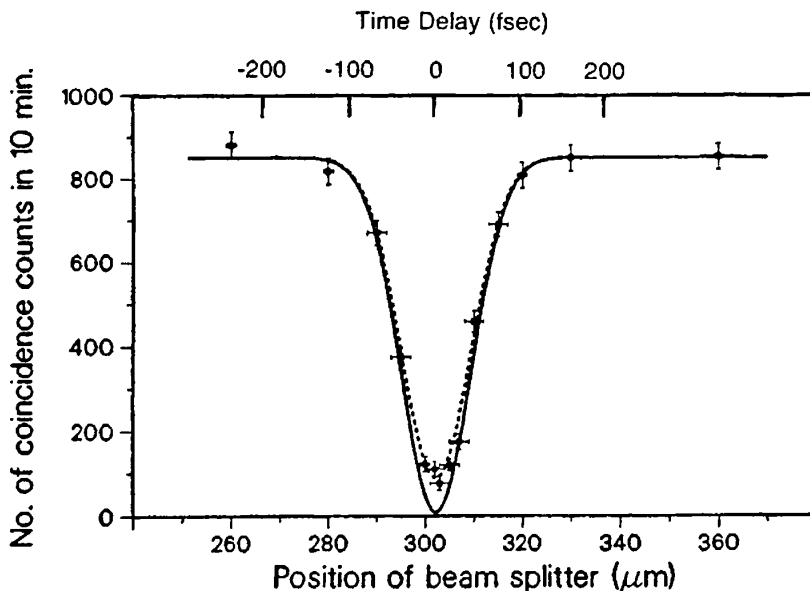


图 1.4 Hong-Ou-Mandel 干涉实验结果

并使符合计数为 0，出现符合计数的极小值点。假设干涉滤波片透过的谱呈高斯型，其相互交叠的积分也呈高斯型，因而两个探测器的符合计数也满足高斯分布，可以表达为：

$$R_c \propto 1 - e^{-\tau^2(\Delta\omega)^2}, \quad (1-14)$$

其中， τ 是两个光子到达分束器的时间差。 $\Delta\omega$ 是单光子的频谱宽度，在这个实验中主要由干涉滤波片决定。

实验中，双光子的符合计数不能完全到 0，主要有两个原因：首先，两个光子在空间模式上没有完全重合。这个通常在实验上利用小孔（Pinhole）或者单模光纤来滤波，用以提高干涉可见度。其次，虽然已经用了窄带干涉滤波片，但是两个光子在频谱上还是有一定的可区分性，这种可区分性就会导致干涉可见度下降。用小孔，单模光纤，和窄带干涉滤波片滤波，实际上就是一种擦除两个光子之间可区分性来提高干涉可见度的常用方法。

如上所述，当两个全同的光子同时入射一块分束器上，两个光子将在分束器的同一个输出端输出，此现象也成为光子聚束效应（Photon Bunching）。现在我们讨论当入射的双光子处于不同态的情况。一种简单的情况就是两个光子偏振态相互垂直。例如 a 路的光子处于水平偏振（H），而 b 路光子处于竖直偏振（V），则在分束器之后将不会出现光子聚束效应，因为两个光子在偏振上可以区分。但

是利用这种过程却可以用来制备双光子的纠缠态, 区泽宇等首先利用此方法制备了最大纠缠态[23], 其实验结果违反了贝尔不等式[24]并验证量子局域性。如果结合偏振分束器, 利用双光子 Hong-Ou-Mandel 干涉和后选择方法 (Post-selection), 将可以制备出更多的多光子态, 例如多光子 Greenberg-Horne-Zeilinger (GHZ) 态[10,25], W 态[11]和 Cluster 态[26]等。

考虑输入分束器的双光子态是贝尔态的情况。如果此双光子处于贝尔单态, 则呈现光子反聚束现象, 也就是两个光子将分别从两个输出端离开; 如果双光子处于贝尔三态上, 则呈现光子聚束现象。利用此性质, 一个分束器可以鉴别出的贝尔单态[27], 并在此基础上可以完成量子密集编码[28], 纠缠交换[29], 量子态隐形传输[30-32]。同时根据以上讨论, 我们可以发现, Hong-Ou-Mandel 干涉仪除了可以用作判断单光子源输出的两个单光子态性质是否相同[33], 而且可用作单光子态提纯[34]和纠缠纯化[35,36]。同时, 加上贝尔单态和贝尔三态的性质, 可以实现量子态普适克隆和非门[37,38]。辅以其他光子, 此干涉还可以构成量子比特的受控非门[39,40]。如果利用非对称的分束器, 相应的 Hong-Ou-Mandel 干涉可以完成非线性的相移[13,41], 并可以完成量子比特受控非门[42-44]。可见 Hong-Ou-Mandel 干涉是线性量子计算的核心。

1.4 单光子多比特体系的应用

量子信息问题可以在很多体系中实现, 最常见的有光学体系、核磁共振体系 (NMR)、腔动力学体系 (Cavity QED)、量子点 (Quantum Dot)、原子系综和低温超导体系等。量子信息问题在每种体系中都取得了很大的进展。2001 年, Knill, Laflamme 和 Milburn 三人在自然杂志 (Nature) 发表了一篇光学方法实现大规模量子计算可能性的文章[13], 引起了科学家对光学量子计算重视, 增强了人们用光学方法处理量子信息问题的信心。结合后面章节的需要, 本节主要介绍有关在单光子多比特体系中解决量子信息问题的一些基础知识。

在光学体系中, 常用到的量子比特有两维的光子偏振、多维的空间动量 (也称作路径比特) 和轨道角动量。具体来说, 用光子的两个正交的偏振态 (一般用 H 和 V 分别表示水平偏振和竖直偏振) 表示比特的 0 或 1, 写成态的形式就是分别用 $|H\rangle$ 和 $|V\rangle$ 表示 $|0\rangle$ 和 $|1\rangle$ 。这样, 对于偏振比特, 半波片 (HWP) 和 $\lambda/4$ 波

片 (QWP) 实现比特的任意旋转, 偏振分束器 (PBS) 实现 H 和 V 的分离。也可以用光子处于上路径或下路径来表示 0 或 1, 即路径比特。光子路径比特的旋转, 用能量分束器 (BS) 可以实现。当然光子的路径可以有更高的维度, 所以路径比特可以被用来表示 qudit。光子轨道角动量 (见第二章) 彼此正交, 可以组成高维的 Hilbert 空间, 任意两个光子轨道角动量态可以组一个 qubit 体系, 更多的轨道角动量态可以组成 qudit 体系。对于轨道角动量比特, 比特之间的旋转可以用计算全息片或柱状透镜实现。而轨道角动量比特的分离可以使用计算全息片来完成[45]。

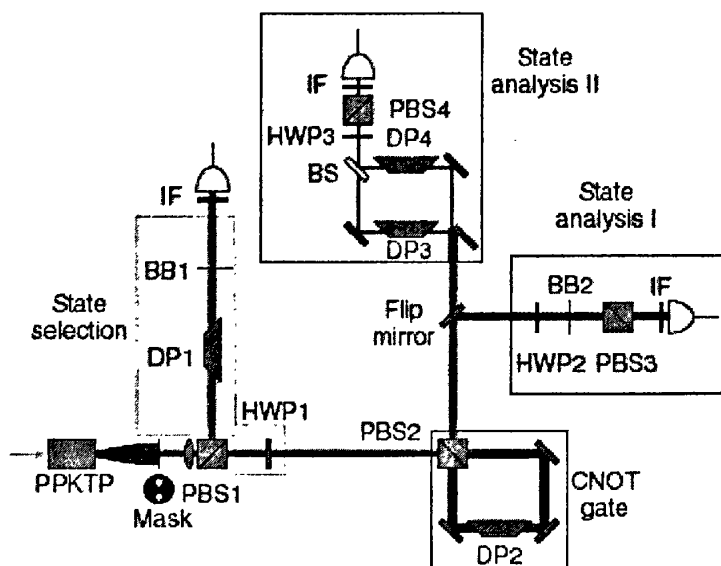


图 1.5 单光子两比特 C-NOT 门的实现

自然的, 基于这些量子比特, 我们可以推广到多光子体系或者单光子多量子比特体系。在多光子体系中, 应用最多的是用偏振来编码量子比特, 因为偏振态的旋转操作非常的高效便捷。例如量子密集编码实验[28]、量子隐形传态[30-32]。当然, 也有应用多光子轨道角动量纠缠的实验[46]。单光子多比特可以实现基本的确定性量子逻辑门[47-50], 虽然这种方法实现的量子逻辑门不能应用于真正意义的量子计算机 (需要资源随比特数指数增加), 但是利用这种方法仍然能够很好的验证一些基本的量子逻辑方案[51,52]。例如用光子偏振和轨道角动量编码两量子比特, 在实验上实现了 C-NOT 门和量子的 Deutsch 算法[53]。我们在实验上利用单光子多比特系统实现了量子随机行走算法[54]和量子赌博机[55]。

将量子纠缠于单光子多比特结合起来，可以成为解决一些特殊问题的有效工具。最有代表的一个工作是 F. Franco 和 N. C. Wong 利用单光子两比特体系实现确定性的 C-NOT 门[50]。他们利用光子的偏振作为控制比特，空间动量作为目标比特，实现偏振比特对空间动量比特的 C-NOT 控制。在这个实验中，图 1.5，波长 398.5nm 激光泵浦 PPKTP 晶体，产生 II 型参量下转化纠缠光子对。偏振纠缠的光子对经过 PBS1 后变为分离的单光子，上路光作为参考，下路光在经过 Mask 和 HWP1 后，已经编码了两比特的信息。经过一个 Sagnac 干涉环和德福（Dove）镜，实现了用偏振比特对空间动量比特的控制，详细的讨论参见文献 [50]。

参考文献

- [1] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935).
- [2] N. Bohr, Phys. Rev, **48**, 696 (1935).
- [3] E. Schrodinger, Proc. Cambridge Phil. Soc, **31**, 555 (1935).
- [4] J. S. Bell, Rev. Mod. Phys. **38**, 447452 (1966).
- [5] A. Aspect, P. Grangier and G. Roger, Phys. Rev. Lett. **47**, 460 (1981).
- [6] C. H. Bennett and G. Brassard, *Proceeding IEEE International Conference on Computers, System and Singal Processing*, Bangalore, India (IEEE, New York, 1984), pp. 175-179.
- [7] A. K. Akert, Phys. Rev. Lett. **67**, 661 (1991).
- [8] T. Jennewein, C. Simon et al, Phys. Rev. Lett. **84**, 4729 (2000).
- [9] S. L. Braunstein, A. Mann and M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992).
- [10] D. M. Greenberger, M. A. Horne, A. Shimony and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990)
- [11] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
- [12] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
- [13] E. Knill; R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
- [14] P. Kok, et al. eprint quant-ph/0512071.
- [15] R. A. Campos, B. E. A. Saleh, and M. C. Teich, Phys. Rev. A **40**, 1371 (1989).
- [16] A. Vaziri, G. Weihs and A. Zeilinger, J. Opt. B: Quantum Semiclass. Opt. **4**, s47 (2002).
- [17] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, (Cambridge, London 1995).
- [18] H. Hanbury-Brown and R. Q. Twiss, Nature (London), **178**, 1046 (1956).
- [19] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
- [20] J. D. IYanson, Phys. Rev. Lett. **62**, 2202 (1989).
- [21] Z. Y. Ou, X. Y. Zou, L. J. Wang, and L. Mandel Phys. Rev. Lett. **65**, 321 (1990).
- [22] 黄运锋, 博士学位论文, 中国科学技术大学 (2003).

- [23] Z. Y. Ou and L. Mandel, Phys. Rev. Lett. **61**, 50 (1988).
- [24] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
- [25] J.-W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger, Nature (London) **403**, 515 (2000).
- [26] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, Nature (London) **434**, 169 (2005).
- [27] S. L. Braunstein and A. Mann, Phys. Rev. A **51**, 81727 (1995).
- [28] K. Mattle, H. Weinfurter, P. G. Kwiat and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).
- [29] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).
- [30] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger Nature (London) **390**, 575 (1997).
- [31] J.-W. Pan, S. Gasparoni, M. Aspelmeyer, T. Jennewein, and A. Zeilinger, Nature (London) **421**, 721 (2003)
- [32] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, Nature (London) **421**, 509 (2003).
- [33] C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto, Nature (London) **419**, 594 (2002).
- [34] M. Ricci, F. De Martini, N. J. Cerf, R. Filip, J. Fiurask, and C. Macchiavello, Phys. Rev. Lett. **93**, 170501 (2004).
- [35] J.-W. Pan, C. Simon, C. Brukner and A. Zeilinger, Nature (London) **410**, 1067 (2001)
- [36] J.-W. Pan, S. Gasparoni, R. Ursin, G. Weihs, and A. Zeilinger, Nature (London) **423**, 417, (2003).
- [37] M. Ricci, F. Sciarrino, C. Sias, and F. De Martini, Phys. Rev. Lett. **92**, 047901 (2004).
- [38] W. T. M. Irvine, A. Lamas Linares, M. J. A. de Dood, and D. Bouwmeester, Phys. Rev. Lett. **92**, 047902 (2004).
- [39] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Phys. Rev. A **64**, 062311 (2001).

- [40] S. Gasparoni, J.-W. Pan, P. Walther, T. Rudolph, and A. Zeilinger, *Phys. Rev. Lett.* **93**, 020504 (2004).
- [41] K. Sanaka, T. Jennewein, J.-W. Pan, K. Resch, and A. Zeilinger, *Phys. Rev. Lett.* **92**, 017902 (2004).
- [42] T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White, *Phys. Rev. A* **65**, 062324 (2002).
- [43] H. F. Hofmann and S. Takeuchi, *Phys. Rev. A* **66**, 024308 (2002).
- [44] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, *Nature (London)* **426**, 264 (2003).
- [45] J. Leach, M. J. Padgett, S. M. Barnett, S. Franke-Arnold, and J. Courtial, *Phys. Rev. Lett.* **88**, 257901 (2002).
- [46] A. Mair, . Vaziri, G. Weihs and A. Zeilinger, *Nature (London)* **412**, 313 (2001).
- [47] N. J. Cerf, C. Adami, and P.G. Kwiat, *Phys. Rev. A* **57**, R1477 (1998).
- [48] J.C. Howell and J. A. Yeazell, *Phys. Rev. A* **61**, 052303 (2000).
- [49] B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, *Phys. Rev. A* **63**, 032303 (2001).
- [50] M. Fiorentino and Franco N. C. Wong, *Phys. Rev. Lett.* **93**, 070502 (2004).
- [51] P.G. Kwiat, J. R. Mitchell, P. D. D. Schwindt, and A.G. White, *J. Mod. Opt.* **47**, 257 (2000);
- [52] Y. Mitsumori, J. A. Vaccaro, S.M. Barnett, E. Andersson, A. Hasegawa, M. Takeoka, and M. Sasaki, *Phys. Rev. Lett.* **91**, 217902 (2003).
- [53] A. N. de Oliveira, S. P. Walborn¹ and C. H. Monken, *J Opt. B: Quantum Semiclass. Opt.* **7** 288–292 (2005).
- [54] P. Zhang, X.-F. Ren, X.-B. Zou, B.-H. Liu, Y.-F. Huang, and G.-C. Guo, *Phys. Rev. A* **75**, 052310 (2007).
- [55] P. Zhang, Y.-S. Zhang, Y.-F. Huang, L. Peng, C.-F. Li and G.-C. Guo, *Euro. Phys. Lett.* **82**, 30002 (2008).

第二章 光子轨道角动量

激光拥有很多种不同的空间模式，应用最多的是拉盖尔-高斯(Laguerre-Gaussian)—LG 模和厄米-高斯(Hermite-Gaussian)—HG 模。所有的 LG 模或者 HG 模之间彼此正交，构成了一个完备的希尔伯特(Hilbert)空间。对应于光子，即不同模式光的光子携带者不同的轨道角动量，在这方面的已经完成了很多基础研究[1-9]。在利用光子研究量子信息的过程中，可以利用其轨道角动量实现多比特、纠缠和高维体系。

2.1 LG 模光子轨道角动量

Allen 等人早在 1992 年就观察到不同的 LG 模光的光子携带着不同的光子轨道角动量[1]，但是对于轨道角动量是否是单个光子的性质科学家们还是存在着一些疑问。2001 年，Mair 等人实现光子轨道角动量纠缠的实验有力地消除了这一疑问[3]。

对于 LG 模，柱坐标系下归一化的电场分布为：

$$LG_p^l(\rho, \varphi, z) = \sqrt{\frac{2p!}{\pi(|l|+p)!}} \frac{1}{\omega} \left(\frac{\sqrt{2}\rho}{\omega}\right)^{|l|} L_p^{|l|}\left(\frac{2\rho^2}{\omega^2}\right) e^{-\frac{\rho^2}{\omega^2}} e^{-\frac{ik\rho^2}{2R}} e^{-i(2p+|l|+1)\varphi} e^{-il\varphi}, \quad (2-1)$$

其中 $L_p^l(x)$ 是拉盖尔(Laguerre)多项式：

$$L_p^l(x) = \sum_{m=0}^p (-1)^m \frac{(|l|+p)!}{(p-m)! (|l|+m)! m!} x^m, \quad (2-2)$$

对于高斯光束，各项的定义如下：

$\omega(z) = \omega_0 \sqrt{1 + (z/z_R)^2}$ ：光斑大小，

$R(z) = z(1 + (z/z_R)^2)$ ：波阵面的曲率半径，

$\varphi(z) = \arctan(z/z_R)$ ：Gouy 位相，

$z_R = \frac{1}{2} k \omega_0^2$ ：瑞利(Rayleigh)长度。

ω_0 为光的束腰， l 为光子的轨道角动量量子数，也称作光的旋转数， $(p+1)$ 是光

在径向的节点数目。在光的束腰位置（ $z=0$ ）,LG 模式可以简化为：

$$LG_p^l(\rho, \varphi) = \sqrt{\frac{2p!}{\pi(|l|+p)!}} \frac{1}{\omega_0} \left(\frac{\sqrt{2}\rho}{\omega_0}\right)^{|l|} L_p^{|l|}\left(\frac{2\rho^2}{\omega_0^2}\right) e^{-\frac{\rho^2}{\omega_0^2}} e^{-il\varphi}. \quad (2-3)$$

为了简化计算，通常我们采用这种表达形式。

图（2.1）给出了轨道角动量量子数 $l=1$ ， $p=0$ 的光场强度分布以及光的相位分布。 $p=0$ ， $l=0$ 的 LG 模就是我们通常所见到的高斯激光束。图（2.2）给出了模式 (p, l) 分别为 $(0, 1)$ ， $(2, 0)$ ， $(2, 1)$ 光的光场强度分布。

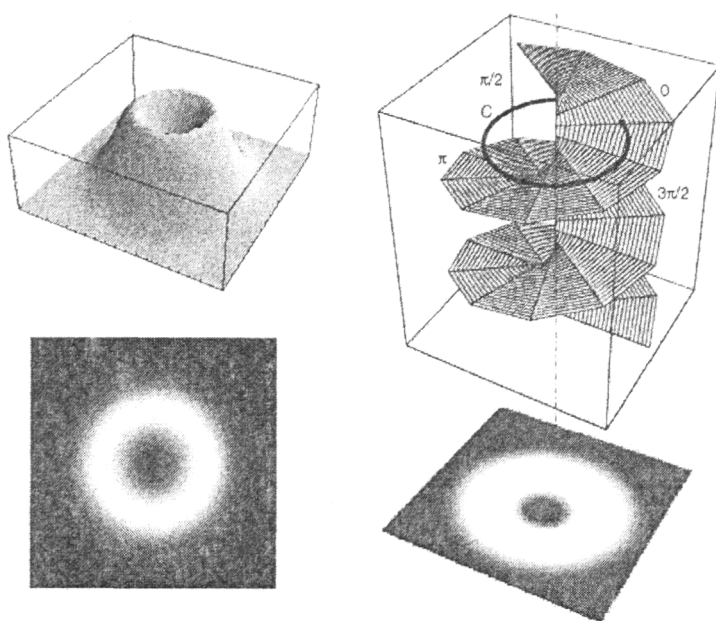


图 2.1 轨道角动量为 1 的光强分布及相位分布

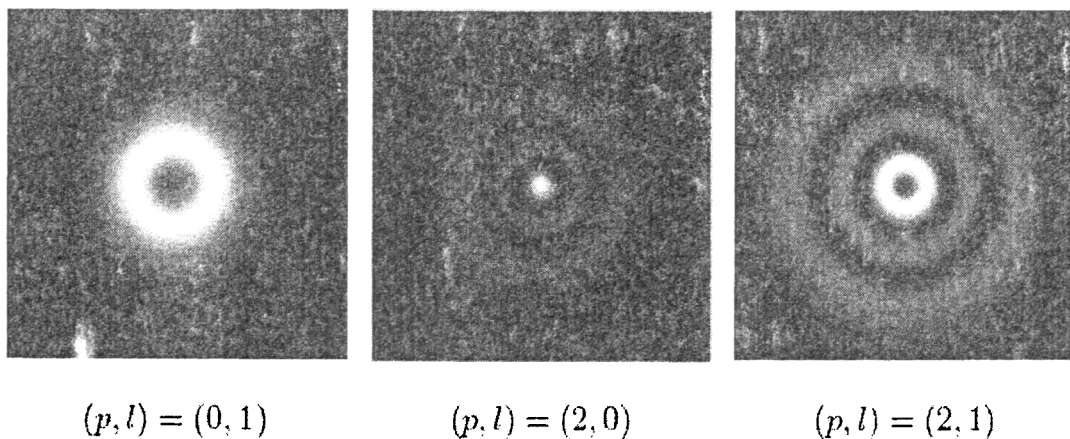


图 2.2 不同 (p, l) 的 LG 模光场强度分布

如果光的模式是一个旋转数为 l 的纯 LG 模，那么这束光中的每个光子的轨道角动量就为 $l\hbar$ ，对应于一个轨道角动量的本征态，本征值为 $l\hbar$ [1]。如果光的模式不是单一模式的 LG 模，而是不同 l 的 LG 模式叠加，那么光子就处于轨道角动量的叠加态上，叠加态的相对振幅由不同模式的光所占比重决定。

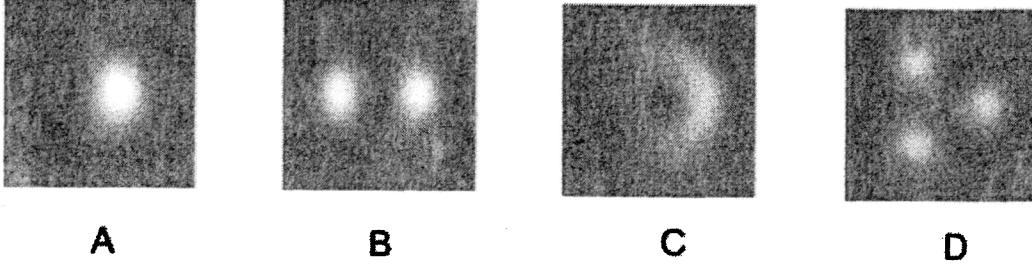


图 2.3 模式叠加后的光场强度分布

图 (2.3) 是一些 LG 模式叠加态的光场分布。A 是 LG_0^0 和 LG_0^1 模式光等权干涉（叠加态）后的光场分布，B 是 LG_0^1 和 LG_0^{-1} 等权干涉后的光场分布，C 是 LG_0^1 和 LG_0^2 等权干涉后的光场分布，D 是 LG_0^{-1} 和 LG_0^2 等权干涉后的光场分布。这些图形可以很容易的由 LG 模的数学表达是计算出来。设两束 LG 模式光分别为 $LG_0^{l_1}$ 和 $LG_0^{l_2}$ ，干涉后的光场分布表达式如下：

$$\left| LG_0^{l_1} + re^{i\theta} LG_0^{l_2} \right|^2 = \frac{\omega_0^2}{2\pi} e^{-A\rho^2} \{ \rho^{2|l_1|} + r^2 \rho^{2|l_2|} + 2r\rho^{|l_1|+|l_2|} \cdot \cos[(|l_1 - l_2|) \cdot \varphi + \theta] \} \quad (2-4)$$

其中 r 为两种模式之间的相对振幅， θ 为两者之间的相对相位。可以看出，光场分布与 $\cos[(|l_1 - l_2|) \cdot \varphi + \theta]$ 有密切关系。对应于光子的轨道角动量，可以看作是光子的动量分布。

2.2 HG 模光子轨道角动量

与 LG 模类似，光的另外一种空间模式 HG 模也构建了一个完备的 Hilbert 空间。因此也有很多研究用它来实现多比特、纠缠和高维体系。

对于 HG 模，归一化的模函数为：

$$HG_m^n(x, y, z) = \sqrt{\frac{2}{\pi}} \frac{1}{\omega(z)} \sqrt{\frac{1}{2^{m+n} m! n!}} H_m\left(\frac{\sqrt{2}x}{\omega(z)}\right) H_n\left(\frac{\sqrt{2}y}{\omega(z)}\right)$$

$$\exp\left(-\frac{x^2 + y^2}{\omega(z)^2} - i\frac{k(x^2 + y^2)}{2R(z)} - ikz + i(m+n+1)\varphi(z)\right) \quad (2-5)$$

其中 $H_l(x)$ 是厄米(Hermite)多项式:

$$H_l(x) = \sum_{k=0}^{l/2} (-1)^k \frac{l!}{(l-2k)!k!} (2x)^{l-2k} \quad (2-6)$$

对于高斯光束, 各项的定义如下:

$\omega(z) = \omega_0 \sqrt{1 + (z/z_R)^2}$: 光斑大小,

$R(z) = z(1 + (z/z_R)^2)$: 波阵面的曲率半径,

$\varphi(z) = \arctan(z/z_R)$: Gouy 位相,

$z_R = \frac{1}{2}k\omega_0^2$: 瑞利 (Rayleigh) 长度。

ω_0 为光的束腰, m 和 n 是模式参数。其中 $(m+1)$ 代表了光在 x 方向的节点数目, $(n+1)$ 代表了光在 y 方向的节点数目。在光的束腰位置 ($z=0$), HG 模式可以简化为:

$$HG_m^n(x, y) = \sqrt{\frac{2}{\pi}} \frac{1}{\omega(z)} \sqrt{\frac{1}{2^{m+n} m! n!}} H_m\left(\frac{\sqrt{2}x}{\omega_0}\right) H_n\left(\frac{\sqrt{2}y}{\omega_0}\right) \exp\left(-\frac{x^2 + y^2}{\omega_0^2}\right) \quad (2-7)$$

为了简化计算, 通常我们采用这种简化表达式。图 (2.4) 给出了模式 (m, n) 分别为 $(1, 0)$, $(2, 0)$, $(3, 2)$ 的光场强度分布。

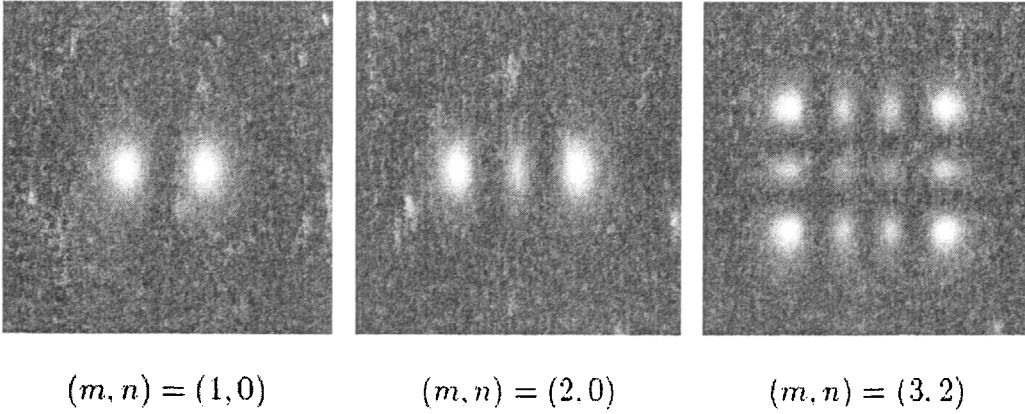


图 2.4 不同 (m, n) 的 HG 模光场强度分布

2.3 LG 模的产生

LG 模光场分布有着极好中心对称性质，便于产生和探测，在量子信息研究中有广泛的应用。我们着重介绍 LG 模光的产生和探测方法。

2.3.1 设计激光腔

在激光物理中，LG 模式属于激光腔的高阶横向模式。产生激光的过程中应尽量避免这种高阶模式存在，但是也可以通过设计激光腔来产生我们需要的 LG 模光 [10,11]。前面介绍可知，LG 模式光的分布是高度中心对称的，所以这也要求在调节激光腔时要做到中心对称，细微的散斑或者不对称会导致 HG 模的产生。所以只有设计特殊的激光腔，才能获得较好的 LG 模光。这也导致了这种方法的实际应用性很差。

2.3.2 柱状透镜模式转换

利用一对柱状透镜可以将高阶的 HG 模转换成 LG 模。由一对柱状透镜引入的 Gouy 相位可以把 HG_m^n 模转化成 LG_p^l 模，之间的参数关系是： $l = (m - n)$ 和 $p = \min(m, n)$ [12]。为了得到高阶 HG 模，通常做法是在激光腔中放入细的金属线，改变共振腔条件使之产生高阶的 HG 模。

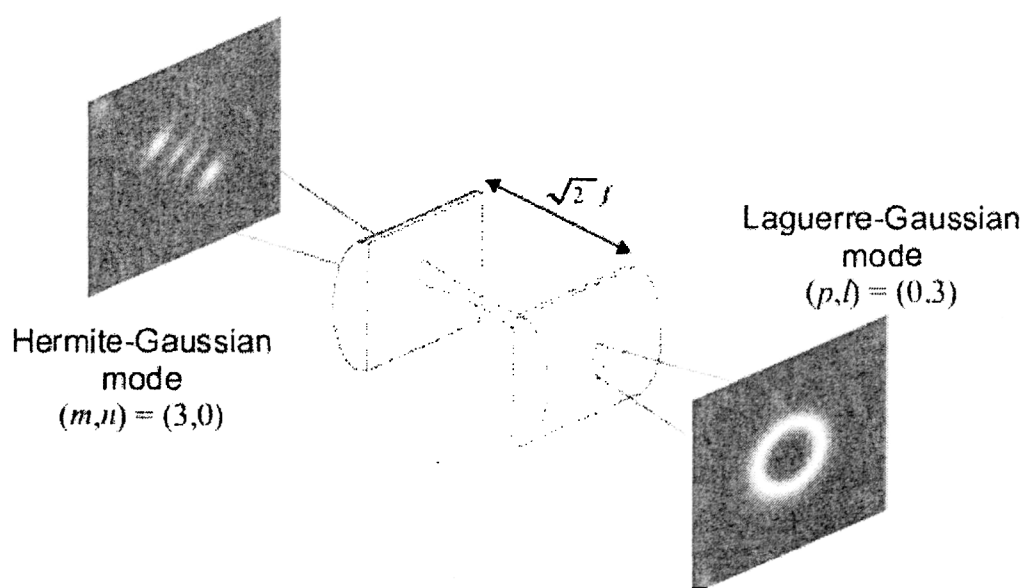


图 2.5 利用柱状透镜实现模式转化

用柱状透镜获得高阶 LG 模的示意图见图 (2.5)。这种方法的转换效率比较高,原则上只有透镜的反射损失。但是这种获得 LG 模光的前提是要先得到高阶 HG 模光,通常这个条件比较难实现,因为激光器在设计时,总是尽可能的避免产生高阶模式。

2.3.3 旋转相位片

LG 模光最重要的性质就是具有旋转相位,旋转的速度由 l 决定。因此可以设计这样一种相位片,见图 (2.6),它的光学厚度 h_s 随着方位角 α 改变,这样便可以给零阶的高斯光加上一个旋转相位。具体的关系是:

$$l = h_s(n - n_0) / \lambda \quad (2-8)$$

其中 l 是 LG 模的旋转数, n 和 n_0 分别是相位片的折射率和外界介质的折射率, λ 为高斯光束的波长。

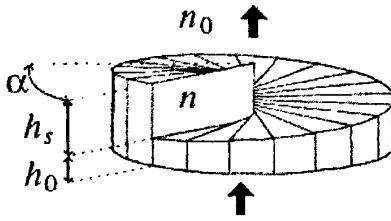


图 2.6 旋转相位片

由上面的公式可知, h_s 正比与波长 λ , 这对于旋转相位片的制作工艺要求极高,因为我们要把相位片光学厚度精确控制在 λ 量级。所以旋转相位片在毫米波段应用比较多,可见光波段应用很少[13, 14]。

2.3.4 计算全息片

计算全息片是光学实验中最常用到的通过零阶高斯模产生高阶 LG 模光的器件。而且通过计算全息片,可以很方便的由零阶高斯光束获得任何所需要高阶模式光[15, 16]。它是一种透射型的全息片,它的透射函数为:

$$T(r, \varphi) = \exp\left(\frac{i\delta}{2\pi} \bmod\left(m\varphi - \frac{2\pi}{\Lambda} r \cos \varphi, 2\pi\right)\right), \quad (2-9)$$

其中 δ 是位相调制的幅度, $\Lambda = 2\pi/k_x$ 是远离分叉点部分的条纹周期, k_x 是参考光在 x 方向的波矢分量, l 是光子轨道角动量 (光的旋转数)。针对不同的衍射级 n , m 分叉的全息片可以将入射光的旋转数改变 $\Delta l_m = nm$ 。衍射的效率由位相调制幅度 δ 决定。当 $\delta = 2\pi$ 时, 几乎 100% 的透射光都会集中到正一级衍射上。图 (2.7) 分别是 $m=1$, $m=2$ 和 $m=3$ 分叉的全息片的条纹图样。一般情况下, 都要求光正入射到条纹分叉中心, 当入射光偏离中心, 将会产生模式叠加的衍射花样。

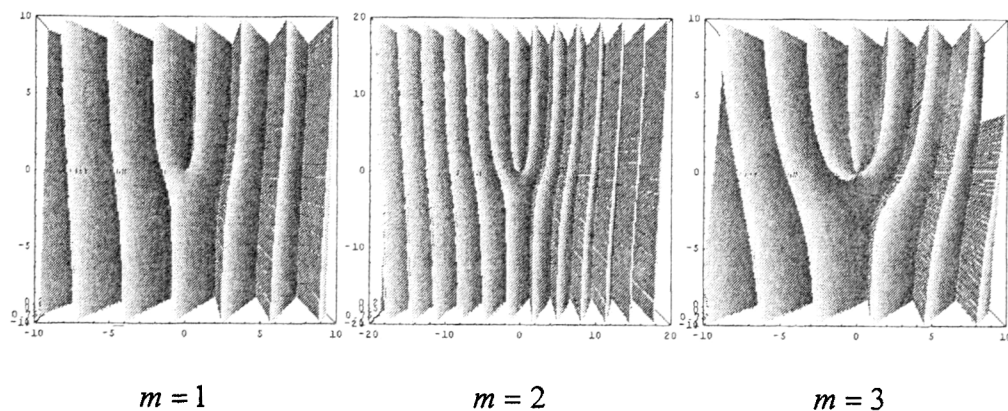


图 2.7 全息片条纹图样

2.4 计算全息片的制作

全息片的制作工艺分为以下几步: 首先, 根据需要计算全息片的透射函数, 将全息片条纹曝光在照相底片上, 然后再将底片上的条纹曝光到全息干板, 最后通过对全息干板的显影定影, 就会得到立体的条纹光栅, 也就是计算全息片。下面通过实例简要介绍全息片的制作工艺。

众所周知, 全息片纪录的是目标光与参考光干涉的干涉条纹。假设目标光为 LG_0^l 模式光, 则参考光波前函数可以简单的表示为:

$$R = R_0 e^{ik_x x + ik_z z} \quad (2-10)$$

参考光与目标光的夹角为 $\theta = \tan^{-1}(k_x/k_z)$ 。一般情况下, 考虑 $z=0$ 的情况, 这时干涉光场可以表示为:

$$I(x, y) = |R_0 e^{ik_x x} + u_0'(x, y)|^2 \quad (2-11)$$

全息片的透射函数 T 可以通过入射光场 E_m 和透射光场 E_T 这样定义:

$$E_T(x, y) = T(x, y)E_m(x, y) \quad (2-12)$$

对于相位型全息片，其透射函数可以写成：

$$T(x, y) = \exp(i\delta H(x, y)) \quad (2-13)$$

其中 δ 相位调制的幅度， $H(x, y)$ 为全息片的实际条纹。这样，将式(2-11)展开，可以得到：

$$I = R_0^2 + (E_l(r))^2 + 2R_0E_l(r)\cos(k_x x - l\phi), \quad (2-14)$$

其中 $E_l(r)$ 为 LG 光场的实振幅。(2-14)式的前两项为相对强度，第三项包含了干涉的相位信息。我们可以根据这个表达式写出透射函数的简单形式：

$$T = \frac{1}{2}(1 - \cos(k_x x - l\phi)) \quad (2-15)$$

由此可以得出 binary 全息片的透射函数为：

$$l \frac{\phi}{\pi} = n + \frac{2r}{\Lambda} \cos \phi \quad (2-16)$$

其中 $n = 0, \pm 1, \pm 2, \dots$ ， $\Lambda = 2\pi / k_x$ 表示光栅的远离中心分叉处的周期。

我们根据式(2-16)选择全息片的参数（ l 和 Λ ），设计出产生不同模式光的计算全息片条纹，通过仪器将其曝光在照相底片上。由于照相底片纪录的只是平面光强分布信息，不能用来作为光栅使用，所以我们要将其信息通过照相技术转移到全息干板上。

通过对全息干板的显影定影，便可以获得立体的条纹信息。而整个干板的显影定影过程，决定了光栅的品质，也就是说，全息干板的制作过程，决定了全息片光栅的衍射效率。我们在实验中参照了 J. Arlt 等人的经验[17]，大致过程将在附录中介绍。

这种衍射光栅的形状是中心分叉的条纹状衍射光栅，当入射的 LG_0' 经过其分叉中心，正一级衍射光便会出现 $LG_0'^{l+m}$ 模式的光。因为这种全息片是透射型光栅，立体条纹的得到是通过显影定影得到，这种方法很难获得完美的条纹。所以实际应用的全息片一级光的衍射效率通常比较低，我们经过多次测试后，得到的一级衍射效率 40%，达到国际先进水平[18,19]。图(2.8)是拍摄到的 He-Ne 激光经过 1 阶分叉计算全息片后衍射光斑，光斑的光场强度分布与我们前面的讨论一致。

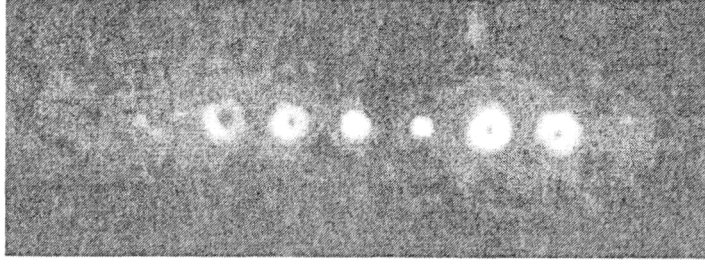


图 2.8 1 阶分叉计算全息片透射光分布

实验上，制备和测量不同轨道角动量的叠加态同样重要。一种简单易行的方法就是使用位置拉偏的全息片。这种方法特别适用于制备 LG_0^l 模和高斯模（也可以认为是 LG_0^0 模）的叠加态。叠加态的相对振幅和相对相位都由拉偏的位置决定

[16]。叠加态 $\frac{1}{\sqrt{1+\gamma^2}}(|u_{00}\rangle + \gamma e^{i\varphi}|u_{01}\rangle)$ 的光场分布如图 (2.9) 所示，其中 w_0 为激光的束腰大小。

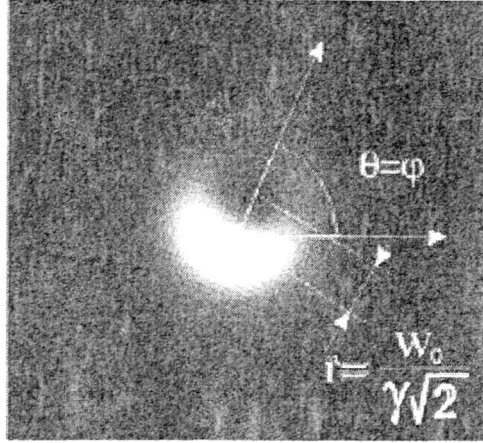


图 2.9 轨道角动量叠加态的光场强度分布

对于透射型的全息片，透射光刻一写为：

$$u_o(r, \varphi) = T(r, \varphi) u_i(r, \varphi) \quad (2-17)$$

如果入射光打在 1 分叉全息片偏离中心坐标为 (r_0, φ_0) 的位置，入射光为 LG_0^l 时出射光向 $p=0$ 的 LG_0^l 本征模上的投影就可以表示为[20]：

$$a_L^l(r_0, \varphi_0) = \iint (u_0^L(r, \varphi) \exp(-imr \frac{2\pi}{\Lambda} \cos \varphi))^* T(r - r_0, \varphi - \varphi_0) u_0^l(r, \varphi) r dr d\varphi$$

图 (2.10) 给出了全息片拉偏位置与模式所占比例之间关系的数值计算结果。

2.5 LG 模式的探测

对于基模高斯光 ($l=0, p=0$) 的探测, 可以利用单模光纤和探测器完成。因为其它的高阶模式 ($l \neq 0$) 有较大的空间分布, 因此不能有效的耦合进入单模光纤, 这也是单模光纤探测基模的原理。所以对于高阶模式光的探测, 我们需要使用一种特殊的模式探测器。这种探测器由全息片和单模光纤两部分组成。我

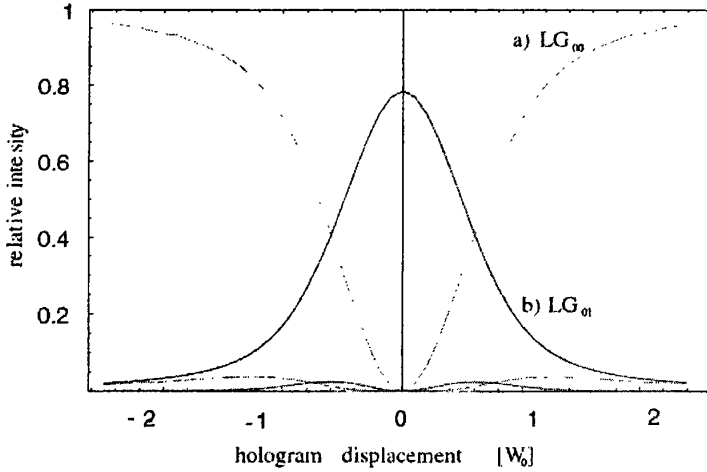


图 2.10 拉偏的 1 分叉全息片的模式分析

们首先利用全息片将高阶模式转变到基模高斯光, 然后再耦合进单模光纤进行探测。选用不同的全息片, 就能对不同的阶模式光进行探测。而叠加态的探测则是通过拉偏全息片的方法实现。

由于全息片条纹很细, 用精确拉偏全息片的方法来实现叠加态的产生和探测在实验上还是存在着一定难度。对于叠加态的产生, 可以使用干涉的方法来实现 [16], 但是对于轨道角动量叠加态的探测, 目前还没有其他更好的方法, 这也给使用光子轨道角动量叠加态的研究带来了一定的困难。

2.6 小结

本章主要讨论了拉盖尔-高斯(Laguerre-Gaussian)—LG 模和厄米-高斯(Hermit-Gaussian)—HG 模两种模式的定义和性质, 介绍它们与光子轨道角动量的关系。重点介绍常用的 LG 模的产生和探测, 详细说明了使用计算全息片产生高阶 LG 光和探测高阶模式光的方法。这些基础理论和实践为我们后面利用光子

轨道角动量研究高维多比特体系做好了铺垫。

参考文献

- [1] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw and J. P. Woerdman, *Phys. Rev. A* **45**, 8185 (1992).
- [2] H. H. Arnaut, and G. A. Barbosa, *Phys. Rev. Lett.* **85**, 286 (2000).
- [3] A. Mair, Vaziri, G. Weihs and A. Zeilinger, *Nature (London)* **412**, 313 (2001).
- [4] G. Molina-Terriza, J. P. Torres and L. Torner, *Phys. Rev. Lett.* **88**, 013601 (2002).
- [5] A. Vaziri, G. Weihs and A. Zeilinger, *Phys. Rev. Lett.* **89**, 240401 (2002).
- [6] J. P. Torres, A. Alexandrescu and L. Torner, *Phys. Rev. A* **68**, 050301(R) (2003).
- [7] A. Vaziri, J.-W. Pan, T. Jenewein, G. Weihs and A. Zeilinger, *Phys. Rev. Lett.* **91**, 227902 (2003).
- [8] X. F. Ren, G. P. Guo, B. Yu, J. Li and G. C. Guo, *J. Opt. B: Quantum Semiclass. Opt.* **6**, 243 (2004).
- [9] N. K. Langford, R. B. Dalton, M. D. Harvey, J. L. O'Brien, G. J. Pryde, A. Gilchrist, S. D. Bartlett and A. G. White, *Phys. Rev. Lett.* **93**, 053601 (2004).
- [10] C. Tamm and C. O. Weiss, *J. Opt. Soc. Am. B* **7**, 1034–1038 (1990).
- [11] M. Harris, C. A. Hill, P. R. Tapster, and J. M. Vaughan, *Phys. Rev. A* **49**, 3119–3122 (1994).
- [12] M. W. Beijersbergen, L. Allen, H. E. L. O. Vandeveen, and J. P. Woerdman, *Opt. Comm.* **96**, 123–132 (1993).
- [13] M. W. Beijersbergen, R. P. C. Coerwinkel, M. Kristensen, and J. P. Woerdman, *Opt. Comm.* **112**, 321–327 (1994).
- [14] G. A. Turnbull, D. A. Robertson, G. M. Smith, L. Allen, and M. J. Padgett, *Opt. Comm.* **127**, 183–188 (1996).
- [15] J. Arlt, K. Dholakia, L. Allen and M. J. Padgett, *J. Mod. Opt.* **45**, 1231 (1998).
- [16] A. Vaziri, G. Weihs and A. Zeilinger, *J. Opt. B: Quantum Semiclass. Opt.* **4**, s47 (2002).
- [17] J. Arlt, Thesis for the degree of Doctor of Philosophy, School of Physics and Astronomy, University of St Andrews, St Andrews, Fife Scotland (1999).
- [18] H. He, N. R. Heckenberg, and H. Rubinsztein-Dunlop, *J. Mod. Optics* **42**,

217–223 (1995).

[19] N. R. Heckenberg, R. McDuff, C. P. Smith, H. Rubinsztein-Dunlop, and M. J. Wegener, *Opt. Quant. Elec.* **24**, S951–S 962 (1992).

[20] M. W. Beijersbergen, R. P. C. Coerwinkel, M. Kristensen, and J. P. Woerdman, *Opt. Comm.* **112**, 321–327 (1994).

第三章 量子算法和量子随机行走

20 世纪是信息和计算机的世纪，同样，它也是一个量子领域快速发展的世纪。早在 1985 年，牛津大学的物理学家 David Deutsch 提出了将计算机和量子力学结合起来，能否在量子世界中实现计算[1]。之后，计算机科学家和物理学家对量子并行计算的强大能力产生了浓厚的兴趣，并着手寻找更多得引人入胜的例子，来显示量子计算机比经典计算机拥有更为出色的功能。量子算法无疑是最能体现量子计算机优越性最直观的表现。其中最令人瞩目的是 1994 年 Peter Shor 发现了能够解决大数因式分解算法（Shor algorithm）[2]，使得现在的经典加密手段变得不再安全。1997 年，L. K. Grover 等人又发现了量子搜索算法（Grover algorithm）[3]，大大提高了搜索的速度。人们对于量子算法的研究才刚刚开始，很多科学家都在致力于发现新的量子算法。在经典领域，随机行走问题在很多领域有着重要的应用，包括数学，生物，固体物理，天体物理，聚合化学，计算机科学甚至经济学[4, 5]。自然的，量子的随机行走问题在量子世界是否也能有其重要的应用，尤其在量子计算方面能否提供新的量子算法？人们从最基本的量子随机行走研究开始，发现了很多有趣的现象[6-21]，尤其是在发现了基于量子随机行走的量子算法以后[22, 23]，量子随机行走开始受到更多的关注和研究。

3.1 量子算法

经典的计算机只有逻辑 0 和 1，也就是所谓的经典比特。但是在量子领域，由于叠加态的存在，使得量子比特 0 和 1 有了更为丰富的存在形式： $\alpha|0\rangle + \beta|1\rangle$ 。这就令量子计算机在大容量存储和平行计算方面远远超过经典计算机。

设想我们每次储存的信息不再是一个个经典的比特，而是量子比特的叠加态，那么我们就可以在计算过程中对所有状态的几率幅直接进行运算，最后通过测量得到最终的计算结果，这样就可以大大的增加计算的速度。这也就是量子并行算法的基本原理。这一原理最早是 1981 年由物理学家 Richard Feynman 提出，1985 年 Deutsch 进行了论证和推广，提出了真正意义上的第一个量子算法，

Deutsch 算法[1, 24]。随后量子算法得到了更多的关注和研究，其中最具代表的两个量子算法是一种基于 Fourier（傅里叶）变换的 Shor 量子算法[2]和量子加速搜索的 Grover 算法[3]。下面我们主要介绍一下最简单 Deutsch 算法[25]。

Deutsch 算法是这样的：对于一个布尔函数 $f(x)$ ， $x=0$ 或者 1 ，输入任意的单比特 x ，其结果只有 0 或 1 。那么我们可以将函数根据输入和结果进行这样的分类：常数函数（Constant Function） $f(0)=f(1)$ ，和平衡函数（Balanced Function） $f(0)\neq f(1)$ 。假设我们有一个黑盒子能实现如上的函数 $f(x)$ ，但我们不知道它是常数函数和平衡函数中的哪一种。假设这个黑盒子执行一次运算需要 1 小时，在经典情况下，我们可以通过分别计算 $f(0)$ 和 $f(1)$ ，花费两小时才能判断出 $f(x)$ 是那类函数。但是在量子情况下，事情变得不同，我们可以只用一次计算，也就是只需花费 1 小时的时间就能判断出来 $f(x)$ 属于哪一类。

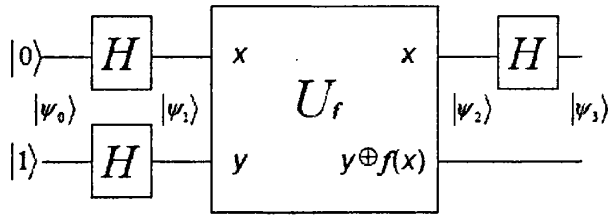


图 3.1 Deutsch 算法示意图

图 (3.1) 给出了 Deutsch 算法的示意图，H 是 Hadamard 门，它可以实现这样的变换：

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (3-1)$$

我们简要的说明一下 Deutsch 算法原理和证明[25]。输入态为

$$|\psi_0\rangle = |01\rangle \quad (3-2)$$

经过 Hadamard 变换以后：

$$|\psi_1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \quad (3-3)$$

将 U_f 作用于 $|\psi_1\rangle$ 后，经过简单的计算，我们可以得到以下两种情况：

$$|\psi_2\rangle = \begin{cases} \pm \frac{|0\rangle + |1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } f(0) = f(1) \\ \pm \frac{|0\rangle - |1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } f(0) \neq f(1). \end{cases} \quad (3-4)$$

最后再对第一个比特进行 Hadamard 变换，我们得到：

$$|\psi_3\rangle = \begin{cases} \pm |0\rangle \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } f(0) = f(1) \\ \pm |1\rangle \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } f(0) \neq f(1). \end{cases} \quad (3-5)$$

这个表达式可以简化为：

$$|\psi_3\rangle = \pm |f(0) \oplus f(1)\rangle \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad (3-6)$$

最后我们只对第一比特进行测量（第二个比特状态一样），我们就可以得出这样的结论——如果第一个比特是 0，那么 $f(0) = f(1)$ ；如果第一个比特是 1，则 $f(0) \neq f(1)$ 。这就表明，使用量子态作为输入，我们可以通过一次 $f(x)$ 的演化，得到函数 $f(x)$ 的更多的性质—— $f(0) \oplus f(1)$ ，而经典情况下却需要两次 $f(x)$ 的演化。由此可以看出量子算法的速度优势。

Deutsch 算法所解决的问题暗示着人们，量子计算机在解决一些计算问题时，效率有可能远远超过经典计算机。广而言之，目前有三类量子算法优于已知的经典算法。第一，基于傅里叶（Fourier）变换的量子算法。Deutsch 算法，Shor 因子分解算法和离散对数算法都属于这一类；第二类是量子加速搜索算法，量子随机行走算法包括其中，而 Grover 算法最为引人注目；第三类算法是量子仿真，即用计算机模拟量子系统。下面简要介绍一下这三类量子算法。

一、基于 Fourier 变换的量子算法

Fourier 变换是一套非常优美的变换理论，它涉及到有限群特征的一些技巧和思想，在这里暂不讨论。量子算法很多都涉及到某种类型的 Fourier 变换，最基本的 Hadamard 变换也是一类广义 Fourier 变换的特例。而已知的 Shor 因子分解算法和离散对数算法，就是基于 Fourier 变换算法的两个例子。在经典情形下，快速 Fourier 变换花费大约 $N \log(N) = n2^n$ 步来完成 $N = 2^n$ 个数的 Fourier 变换。

在量子计算机上, Fourier 变换可以用约 $\log^2(N) = n^2$ 步完成, 相对于经典情形, 指数量级的节省了计算步数! 利用量子 Fourier 变换, 可以有效求解若干被认为经典计算机无法有效求解的问题。这些问题包括 Deutsch 问题、Shor 的离散对数和因子分解算法。尤其是 Kitaev 发现的 Abel 稳定子问题的一种解决方法和对隐含子群问题的推广[26, 27], 使这个方向的研究达到了高潮。

二、量子搜索算法

量子搜索算法是完全不同类型的算法, 其基本原理由 Grover 发现。量子搜索算法解决如下问题: 给定大小为 N 的搜索空间, 没有关于它结构信息的先验知识, 希望找到这个搜索空间中的满足已知性质的一个元素。在经典情形下, 要找到这个满足性质的元素, 大概需要 N 次操作, 但是量子搜索算法却可以用大概 $\sqrt{N}$ 次操作完成。

量子搜索算法只是提供了二次加速, 不如基于量子 Fourier 变换算法的指数加速令人印象深刻。然而量子搜索算法仍有很大的意义, 因为搜索方面的知识的应用比量子 Fourier 变换解决的问题更广泛。而且采用量子搜索算法对很宽范围的问题都可能有帮助。

三、量子仿真

对于自然界发生的量子力学系统, 经典计算机很难完成模拟。因为描述量子系统需要的复数个数往往随着系统规模的增大指数增长, 即经典计算机存储具有 n 个不同元素的系统的量子状态需要大概 c^n 比特的内存, c 是依赖于被模拟系统细节和模拟精度的常数。而量子计算机则可以用 kn 量子比特进行模拟, k 也是依赖于被模拟系统细节和模拟精度的常数, 这使得量子计算机可以有效的模拟被认为在经典计算机上无法模拟的量子系统。量子系统仿真在许多领域都很重要, 特别是在量子化学中。由于经典计算机在计算能力上的限制, 使得它很难精确模拟哪怕是中等规模的分子, 更不用说在许多重要生物学系统中出现的超大分子了。因此, 获得这类系统的更快和更精确的仿真, 有利于促进量子现象扮演重要角色的其他领域加速发展。

在实验上, Deutsch 算法也已经在很多体系中实现, 例如核磁共振 (NMR) 系统[28-30]、腔 QED[31]、离子阱[32]、高温超导体[33]、原子系综[34]和线性

光学体系[35]。其他算法例如 Shor 算法和 Grover 算法也都在实验上有了很大进展[36-38]。

3.2 量子随机行走的介绍

除了上述提到的几种量子算法，基于量子随机行走的量子算法也吸引了很多科学家的兴趣[6-23]。这样，量子随机行走得到了更为广泛的研究，深入揭示了量子随机行走的本质及其表现，为进一步的理论研究和试验实现奠定了坚实的基础。

首先我们先来简单介绍经典的随机行走。经典随机行走可以分为一维随机行走和多维随机行走，也可以分为离散随机行走和连续随机行走。一维离散随机行走是最为简单的一种。它可以这样来描述：假设有一人，手中拿着一个硬币，他的行动规定在一条直线上，而且每次只能根据丢硬币得到的正反面，决定自己每一步的行走方向。这样，我们就有这么一个问题，经过 t 步以后，他在某一位置的概率是多少？将这一问题数学化，可以变为计算经过 t 步以后，处于位置 x 的概率 P 。假设初始位置为零，通过经典的概率计算，很容易得到：

$$P_t(x) = \frac{1}{2^t} C_t^{\frac{t+x}{2}}, \quad (3-7)$$

其中 $C_t^{\frac{t+x}{2}}$ 表示组合数，当 $t+x$ 是奇数时， $P_t(x)$ 等于 0。表格 I 给出了前 5 步的概率分布。

t	x										
	-5	-4	-3	-2	-1	0	1	2	3	4	5
0						1					
1					1/2	0	1/2				
2				1/4	0	1/2	0	1/4			
3			1/8	0	3/8	0	3/8	0	1/8		
4		1/16	0	1/4	0	3/8	0	1/4	0	1/16	
5	1/32	0	5/32	0	5/16	0	5/16	0	5/32	0	1/32

表格 I 经典随机行走的概率分布

这种概率分布可以用经典的五点梅花图 (Galton's Board) 来描述，如图 (3.2)。我们可以看出经典随机行走的特点就是概率分布中心对称。对于连续的随机行走，其概率分布也是呈对称分布。但是量子随机行走，情况则有所不同。对应于

经典一维随机行走，我们介绍一下量子一位随机行走的概念和结果。

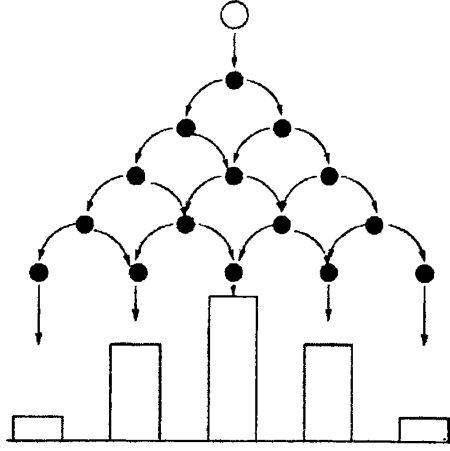


图 3.2 Galton's Board

量子情形与经典情形不同之处在于量子比特的与经典比特的差别。经典的随机行走，硬币的状态只有正（ $\uparrow$ ）和反（ $\downarrow$ ），但是如果将这个硬币变成一个量子硬币，那么它的状态则可以处于 $\uparrow$ 和 $\downarrow$ 的叠加态 $\alpha|\uparrow\rangle + \beta|\downarrow\rangle$ ，如果这个量子硬币出现正反的几率相等，则 $\alpha = \beta = \frac{\sqrt{2}}{2}$ 。这时候，量子随机行走的过程就可以用量子态的演化来描述，需要计算概率时，再对量子态进行测量。如此将会得到与经典完全不同的概率分布。在量子理论中，可以用 Hadamard 变换 $\hat{H}$ 实现掷量子硬币的过程，而平移算符则可以用 $\exp(i\hat{p}\hat{\sigma}_z)$ 来表示，其中 $\hat{p}$ 为动量算符， $\hat{\sigma}_z$ 为泡利-z (pauli-z) 算符。所以对于量子行走，其演化算符可以表示为：

$$\hat{U} = e^{i\hat{p}\hat{\sigma}_z} \hat{H} \quad (3-8)$$

假设初态为 $|\psi_{in}\rangle$ ，则经过 t 步演化以后，末态 $|\psi_t\rangle$ 可以表示为：

$$|\psi_t\rangle = (e^{i\hat{p}\hat{\sigma}_z} \hat{H})^t |\psi_{in}\rangle. \quad (3-9)$$

如果初态为 $|\psi_{in}\rangle = |\downarrow\rangle \otimes |0\rangle$ ，表示初始状态位于位置 0，且量子硬币的态为 $|\downarrow\rangle$ ，那么我们可以计算出 3 步以后的状态：

$$|\psi_{in}\rangle \xrightarrow{U} \frac{1}{\sqrt{2}} (|\uparrow\rangle \otimes |1\rangle - |\downarrow\rangle \otimes |-1\rangle)$$

$$\begin{aligned} &\xrightarrow{U} \frac{1}{2}[(|\uparrow\rangle \otimes |2\rangle + (|\downarrow\rangle - |\uparrow\rangle) \otimes |0\rangle) + |\downarrow\rangle \otimes |-2\rangle] \\ &\xrightarrow{U} \frac{1}{2\sqrt{2}}(|\uparrow\rangle \otimes |3\rangle + |\downarrow\rangle \otimes |1\rangle + |\uparrow\rangle \otimes |-1\rangle - 2|\downarrow\rangle \otimes |-1\rangle - |\downarrow\rangle \otimes |-3\rangle). \end{aligned} \quad (3-10)$$

我们可以通过这个计算过程，得到每一步处于各个位置的概率，见表格 II。

t	x										
	-5	-4	-3	-2	-1	0	1	2	3	4	5
0						1					
1					1/2	0	1/2				
2				1/4	0	1/2	0	1/4			
3			1/8	0	5/8	0	1/8	0	1/8		
4		1/16	0	5/8	0	1/8	0	1/8	0	1/16	
5	1/32	0	17/32	0	1/8	0	1/8	0	5/32	0	1/32

表格 II 量子随机行走的概率分布

对照表格 I，我们可以很容易的看出，前两步概率与经典随机行走相同，但是从第三步开始，量子随机行走的概率分布变得与经典不同。图（3.3）给出了在这种初态下，100 步以后的概率分布图。在奇数位置的概率都为 0，偶数位置

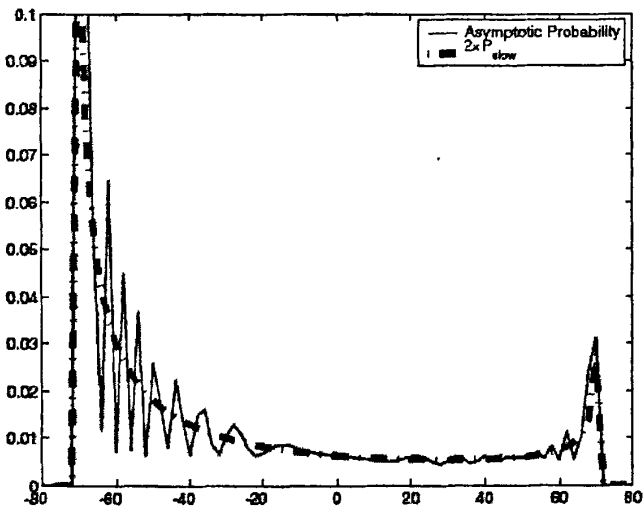


图 3.3 100 步后量子随机行走的概率分布

则有概率存在。虚线给出了一个整体的概率分布曲线，很显然，这种概率分布有明显的向左偏移，与经典的对称高斯分布完全不同。量子随机行走的概率分布与初始状态密切相关，不同的初始态，概率分布也不相同。假设初始状态不是上面假设的 $|\downarrow\rangle \otimes |0\rangle$ ，而是 $|\uparrow\rangle \otimes |0\rangle$ ，那么概率分则向右偏移。

离散一维量子随机行走是最基本，也是最重要的一种。可以将其推广到非对称量子硬币或者连续高维体系，这些都将会引出很多有意义的工作，也为提出

新的量子算法提供了更坚实的基础。

3.3 一维量子随机行走的实验实现

自从量子随机行走的概念提出以后，很多的科学家和科研小组对其进行了理论和实验上的研究。在理论方面，深入讨论了各种量子随机行走的性质和本质。在实验上，也已经在很多体系中实现了量子随机行走。下面主要介绍一下线性光学方法实现量子随机行走的实验以及我们在实验方面所做的工作[17, 21]。

光学上实现量子随机行走，最简单的想法就是用光子的两个正交偏振态作为量子硬币正反面，用光子的空间位置（路径）表示光子的行走坐标。Binh Do 在 2005 年利用这种思路，第一次在实验上利用线性光学方法实现了量子随机行走 [17]。光路图如(3.4)所示，主要元件是 Half-wave plate（半波片）和 PBS Cube（偏振分束器）。以光子偏振态作为量子硬币（qubit），Hadamard 变换可以用半波片实现，然后再利用偏振分束器实现不同偏振态光子处于不同的路径。这样经过

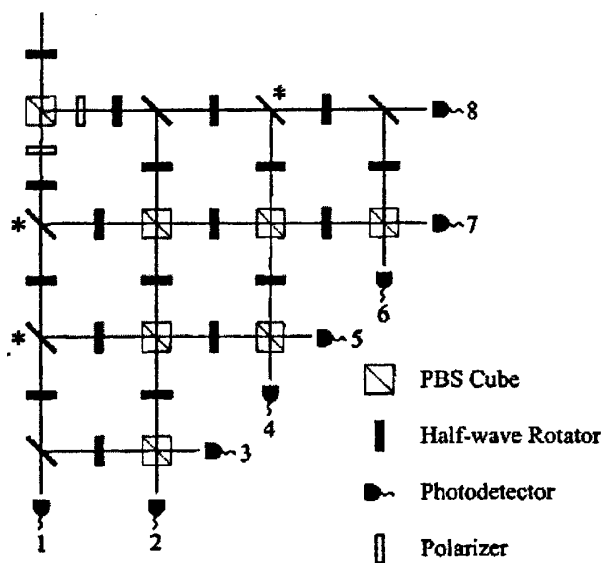


图 3.4 光子偏振态实现量子随机行走

变换，可以根据最后 8 个探测器的结果，判断随机行走的结果。图中加“*”的位置表示存在压电陶瓷微控制器。图（3.5）给出了他们的实验结果，他们通过调节第一块半波片，实现不同的量子态输入，给出了六组情况的实验结果。而且

重复四次得到了几乎相同的实验数据，来展示其光路稳定性。

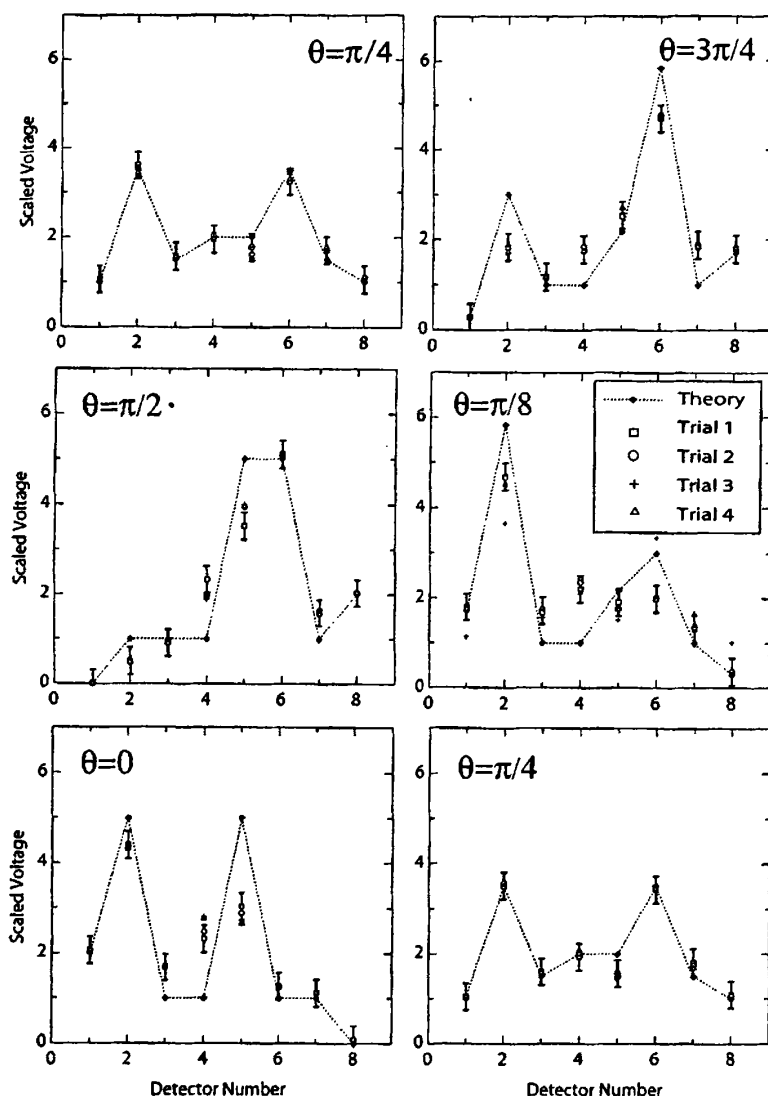


图 3.5 光子偏振态实现量子随机行走方案试验结果

这种方虽然很直观，但是耗用元件多，占用空间大，使其可扩展性受到很大限制。波片和偏振分束器的大量使用，也会导致实验误差的增大。从图（3.5）的实验结果可以看出，数据和理论预言吻合并不是很好，有些点相差比较大。

第二章我们已经介绍了光子轨道角动量（OAM）的一些基本知识。我们知道，光子可以携带不同的轨道角动量，而且这些轨道角动量构成了一组无限维的正交基矢。邹旭波教授等人根据光子轨道角动量的这一性质，提出了使用光子轨道角动量作为量子随机行走空间的设想[18]。我们小组经过努力，在实验上成功

地实现了这一方案[21]。下面简要介绍一下我们的工作。

理论方面，我们选择光子的上下路径比特为 qubit，光子的轨道角动量为行走空间。选择 $|\downarrow\rangle \otimes |0\rangle$ 作为输入态，经过 3 步量子随机行走，便可以获得与经典完全不同的概率分布，推导过程同上。这里 $|\downarrow\rangle$ 表示光子开始处于下路径， $|0\rangle$ 表示光子开始处于 LG_0^0 模式，也就是通常的高斯光束。光子的上下路径比特为 qubit，其 Hadamard 变换可以用 50/50 能量分束镜来实现，这样相当于实现了所谓的量子硬币。而光子轨道角动量的改变可以用我们前面提到的计算全息片（computer generated holograms）来完成。实验光路图见图（3.6）。我们在上路径摆放使光子轨道角动量+1 的计算全息片，下路径摆放-1 的计算全息片，实现了根据不同量子硬币结果选择相应行走方向的目的。我们知道，光子轨道角动量与光传播时的波前旋转方向有关，我们可以定义延光传播方向看，右旋为正，左旋为负。那么光在传播过程中，经过一次反射，其旋转方向将会发生改变，即轨道角动量正负发生改变。普通的能量分束器依靠反射和透射对光进行分束，这对于普通的高斯光束（ LG_0^0 模）没有影响，但是对于高阶模式，则会出现模式的反转。然而我们实验中希望能量分束器只对路径比特进行作用而不改变光子的轨道角动量态，所以我们设计了如图（3.7）的轨道角动量能量分束器。在普通能量分束镜的一个输入端口和另一个输出端口加上一个反射镜，便可以实现尽对光束能量分束，而不影响光束模式的轨道角动量能量分束器。

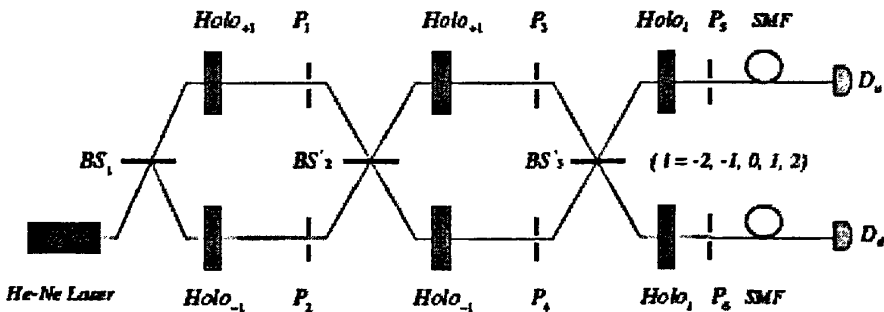


图 3.6 光子轨道角动量空间上的一维量子随机行走

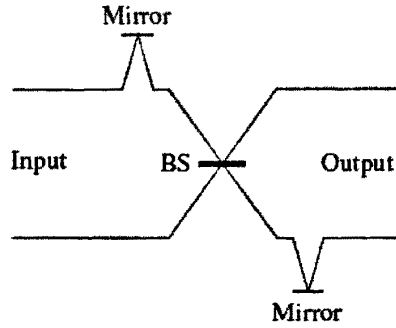


图 3.7 轨道角动量分束器的实现

我们在实验上实现了步数为 3 的量子随机行走，整个实验装置如图 (3.6) 所示。因为量子随机行走过程只与输入态的二阶相关性有关，所以我们可以用相干光作为光源，理解成大量单光子的集合[39, 40]。实验中我们用 He-Ne 激光器产生波长为 632.8nm 的高斯光 ($|0\rangle$)，输出功率为 4.8mW。从下路径 ($|\downarrow\rangle$) 照射到 50/50 的轨道角动量分束器 (路径比特的 Hadamard 门)。上路光经过计算全息片 ($Holo_{+1}$) 衍射后，用小孔 (P_1) 选择+1 级衍射光，实现了轨道角动量+1 的变换。下路径使用使轨道角动量-1 的计算全息片 ($Holo_{-1}$) 和小孔 (P_2)，实现轨道角动量-1 的变换。这样，就实现了一步的量子行走，通过探测小孔 P_1 、 P_2 后各种光模式的比例，便可得到随机行走的概率分布。重复同样的过程，便可以在小孔 P_3 、 P_4 后得到第二步的概率分布， P_5 、 P_6 后得到第三步的概率分布。探测用到了前面介绍的对高阶模式探测的方法——全息片+单模光纤+探测器。选择不同的全息片，便可以将不同的模式变换到基模，然后用单模光纤进行选择探测。

我们对轨道角动量从-3 到+3 之间的光进行探测，得到不同轨道角动量光的概率分布，如表格 III 所示：

Position (3rd step)	-3	-2	-1	0	1	2	3
Theoretical (%)	12.5	0	62.5	0	12.5	0	12.5
Experimental (%)	12.4±0.3	0.281±0.005	61.4±1.5	0.332±0.007	13.4±0.3	0.136±0.003	12.1±0.3

表格 III 量子随机行走三步后的理论和实验概率分布

因为高阶模式光仍会有一小部分耦合进单模光纤，这就导致了我们的实验结果中那些理论概率为 0 的位置仍有很小的概率值。但是整体而言，数据与理论预言十分

吻合。量子随机行走与经典随机行走之所以不同，其本质在于量子随机行走过程中存在量子态的干涉[14]。在我们的前面的理论分析中可以看出，前两步随机性走不存在态之间的相互干涉，所以他们的概率分布也与经典得完全相同，但是第三步的时候，上路径的 LG_0^0 光与下路径的 LG_0^0 光在 BS_3' 上产生干涉，这样使得后面 1 和 -1 处的光分布概率发生改变，从而表现出与经典的不同。我们注意到结果中，轨道角动量 -1 的位置概率偏小于理论值，轨道角动量 1 的位置稍大于理论值。这正是由于我们实验中 M-Z 干涉仪（Mach-Zehnder）的干涉可见度为 92.6%，并非理想的 100%。

比较前面提到的 Do 等人所做的光学实验，他们的方案随着步数的增加，波片和探测器数量成倍增加，而且占用空间更大。正是由于我们的实验中元件应用极少，而且光路极其简单，所以我们得到了更接近理论值的实验结果。我们实验中用到了计算全息片，受它们模式转换效率的限制（37%），以及区分正一级衍射级所需较长的距离，使得我们的实验很难做到更多步数。但是我们的试验方案却是可以很容易推广到更多步数，因为我们可以选择旋转相位片作为模式转换器。这种器件第二章中曾经提到，它可以以很高的效率实现模式转化，而且占用空间极小。这也为物理集成化实现量子随机行走算法提供了一个有效的方法。

3.4 小结

这一章我们先介绍了量子并行计算和量子算法的分类，然后从理论和实验方面详细介绍了量子随机行走算法。在实验上，我们利用光子轨道角动量所形成的 Hilbert 空间作为量子随机行走的空间，巧妙的实现了一维量子随机行走。我们还讨论了这种方案的可扩展性，为集成化实现量子计算提供了有力的工具。我们可以看出，目前对于量子算法的研究还处于基础阶段，很多问题还需要更深入的研究。包括更多更有效的量子算法，以及量子算法在实验上的实现。尤其是量子算法的物理实现，是一项很值得关注的研究课题。因为量子计算机的理论向传统的计算机概念提出了有趣和重要的挑战，根本在于量子计算的理论模型被认为在实验上是可以实现的。目前已知的各种量子算法，在实验上都已经实现，而且应用于各种物理体系。所以量子计算已经不仅仅只让人们在数学上感到惊奇，而是让人们的日常生活也会变得更加惊奇。

参考文献

- [1] D. Deutsch, Proc. R. Soc. A **400**, 97 (1985).
- [2] P. W. Shor, *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1994), p. 124.
- [3] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
- [4] M. N. Barber and B. W. Ninham, *Random and Restricted Walks: Theory and Applications* (Gordon and Breach, New York, 1970).
- [5] R. A. Dana and M. Jeanblanc, *Financial Markets in Continuous Time* (Springer, Berlin, 2002).
- [6] Y. Aharonov, L. Davidovich, and N. Zagury, Phys. Rev. A **48**, 1687 (1993).
- [7] B. C. Travaglione and G. J. Milburn, Phys. Rev. A **65**, 032310 (2002).
- [8] E. Farhi and S. Gutmann, Phys. Rev. A **58**, 915 (1998).
- [9] A. Ambainis *et al.*, *Proceedings of the 30th Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, New York, 2001), pp. 37–49.
- [10] B. C. Sanders, S. D. Bartlett, B. Tregenna, and P. L. Knight, Phys. Rev. A **67**, 042305 (2003); P. L. Knight, E. Roldan, and J. E. Sipe, Opt. Commun. **227**, 147 (2003); E. Roldán and J. C. Soriano, J. Mod. Opt. **52**, 2649 (2005).
- [11] J. Du, H. Li, X. Xu, M. Shi, J. Wu, X. Zhou, and R. Han, Phys. Rev. A **67**, 042316 (2003).
- [12] C. A. Ryan, M. Laforest, J. C. Boileau, and R. Laflamme, Phys. Rev. A **72**, 062317 (2005).
- [13] W. Dür, R. Raussendorf, V. M. Kendon, and H.-J. Briegel, Phys. Rev. A **66**, 052319 (2002).
- [14] P. L. Knight, E. Roldán, and J. E. Sipe, Phys. Rev. A **68**, 020301(R) (2003).
- [15] Z. Zhao, J. F. Du, H. Li, T. Yang and J. W. Pan, e-print arXiv:quant-ph/0212149.
- [16] H. Jeong, M. Paternostro, and M. S. Kim, Phys. Rev. A **69**, 012310 (2004).
- [17] B. Do, M. L. Stohler, S. Balasubramanian, C. Eash, E. Fischbach, M. A.

- Fischbach, A. Mills, and B. Zwickl, J. Opt. Soc. Am. B **22**, 499 (2005).
- [18] X. B. Zou, Y. L. Dong, and G. C. Guo, New J. Phys. **8**, 81 (2006).
- [19] Z.-Y. Ma, K. Burnett, M. B. d'Arcy, and S. A. Gardiner, Phys. Rev. A **73**, 013401 (2006).
- [20] V. Kendon and M. Kendon, Philos. Trans. R. Soc. London, Ser. A **364**, 3407 (2006).
- [21] P. Zhang, X.-F. Ren, X.-B. Zou, B.-H. Liu, Y.-F. Huang, and G.-C. Guo, Phys. Rev. A **75**, 052310 (2007).
- [22] A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman, *Proceedings of the 35th ACM Symposium on Theory of Computing (STOC 2003)* (Association for Computing Machinery, New York, 2003), pp. 59–68; see also e-print arXiv:quant-ph/0209131.
- [23] N. Shenvi, J. Kempe, and K. Birgitta Whaley, Phys. Rev. A **67**, 052307 (2003)
- [24] D. Deutsch, and R. Josa, Proc. R. Soc. A **439**, 553 (1992).
- [25] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
- [26] A. Y. Kitaev, Russ. Math. Surv., **52** (6): 1191-1249 (1997).
- [27] A. Y. Kitaev, Annals of Physics, **298**, 210-226 (2003).
- [28] N. Linden, H. Barjat and R. Freeman, Chem. Phys. Lett. **296**, 61-67 (1998).
- [29] J. Kim, J. S. Lee, S. Lee and C. Cheong, Phys. Rev. A **62**, 022312 (2000).
- [30] K. Dorai, Arvind and A. Kumar, Phys. Rev. A **61**, 042306 (2000).
- [31] S. B. Zheng, Phys. Rev. A **70**, 034301 (2004).
- [32] S. Gulde, M. Riebe, G. P. T. Lancaster, C. Becher, J. Eschner, H. Haffner, F. Schmidt-Kaler, I. L. Chuang and R. Blatt, Nature (London), **421**, 48-50 (2003).
- [33] J. Siewert and R. Fazio, J. of Mod. Opt., **49**, 1245-1254 (2002).
- [34] S. Dasgupta, A. Biswas and G. S. Agarwal, Phys. Rev. A **71**, 012333 (2005).
- [35] A. N. de Oliveira, S. P. Walborn and C. H. Monken, J. Opt. B: Quantum Semiclass. Opt. **7**, 288–292 (2005).
- [36] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood and I. L. Chuang, Nature (London), **414**, 883-887 (2001).

- [37] V. L. Ermakov and B. M. Fung, Phys. Rev. A **66**, 042310 (2002).
- [38] K. A. Brickman, P. C. Haljan, P. J. Lee, M. Acton, L. Deslauriers and C. Monroe, Phys. Rev. A **72**, 050306 (2005).
- [39] M. Mohseni, J. S. Lundeen, K. J. Resch, and A. M. Steinberg, Phys. Rev. Lett. **91**, 187903 (2003).
- [40] P. J. Mosley, S. Croke, I. A. Walmsley, and S. M. Barnett, Phys. Rev. Lett. **97**, 193601 (2006).

第四章 量子博弈

博弈论亦称对策论,作为运筹学中的一个重要分支,就是研究具有对抗性或竞争性质的数学理论和方法。早在两千多年前的中国古代,就已经有了“田忌赛马”这样的对策研究的例子。不过,经典对策论直到本世纪初才成为数学的一个重要分支被系统地研究,其奠基之作就是 von Neumann 和 Morgenstern 合著的《博弈论和经济行为》。

从物理的观点来看,博弈论和信息论有着内在的联系,在博弈过程中存在信息的交流,如参与人把自己的决策传递给他人或仲裁者,因此博弈过程本质上是一个信息处理过程。量子信息学是物理学的新兴学科,其实质是信息是物理的。量子信息学中的许多问题都可以看成博弈过程。例如,量子密码通信中,窃听过程可以认为是窃听者与信息发送者之间的博弈,量子克隆可以认为是物理学家与自然界的一个两人博弈,而量子算法则可看作是量子玩家与经典玩家之间的博弈[1]等等,所以博弈论的量子化有助于量子信息的研究。而博弈论的基础是概率论,将量子概率引入到博弈论中,为研究量子基本理论提供了一个新的手段。博弈论与量子理论的结合,形成了一门新的交叉科学,这就是量子博弈论。

4.1 量子博弈论简介

量子博弈论开始于 Meyer,他在研究零和便士博弈(又称 PQ 翻硬币问题)时指出将策略空间拓展到量子可以使参与人获得更多利益[2]。接着 Eisert 等人将量子纠缠引入到“囚徒困境”中,找到了不同于经典博弈的均衡并解决了经典模型中存在的困境[3]。Goldenberg 等人又提出了量子赌博理论[4],从而更加丰富了量子博弈,从此量子博弈论迅速地发展起来[5-11]。

4.1.1 PQ 翻硬币问题

代号为 P 和 Q 的两个人进行这样一个游戏:分别用 H、T 表示硬币的正面和反面,P 把一枚正面朝上的硬币放进一个盒子里,然后他和 Q 二人按 Q, P,

Q 的顺序去操作，即翻或不翻这枚硬币，但是不能看这枚硬币的状态（即朝上还是朝下）；当最后打开盒子时，如果正面朝上，Q 赢，否则 P 赢。

这是一个二人零和游戏，可以用下面的支付矩阵来分析：

	NN	NF	FN	FF
N	-1	1	1	-1
F	1	-1	-1	1

表格 I 二人零和游戏的支付矩阵

表格 I 的两行表示 P 的两种策略，四列表示 Q 的四种策略；F 表示翻，N 表示不翻；表格里的数字表示 P 的收益，1 表示 P 赢而 Q 输，-1 表示 P 输 Q 赢。例如，第一行第二列，表示 Q 第一次不翻而第二次翻，P 不翻；这样硬币的状态就先后为：H，H，H，T，所以这一局 P 赢。

像这一个对策游戏没有一个确定性的策略解，任何一方使用一个确定策略（或称为单纯策略），另一方就可以使用相应策略使其必输无疑。但是，von Neumann 已经证明，任何一个有限策略的零和对策，总存在概率解，即混合策略[12]。像这一游戏，其平衡解就是：P 分别以 1/2 的概率使用其两种策略 N，F；而 Q 分别以 1/4 的概率使用其四种策略 NN，NF，FN，FF 或者说每次都以 1/2 的概率使用 N，F 两种策略。在此情况下，双方的收益的期望值都为 0，并且在一方采取平衡解时，另一方无法通过改变其使用的概率来提高其期望值。

假设 P 只具备经典力学知识，而 Q 具有丰富的量子力学和经典力学知识，这也就说，在对硬币进行操作时，P 只能使用纯经典的翻转或者不翻转策略，而 Q 则可以使用量子力学所允许的任何么正操作。这样将会存在着使 Q 每次都获胜的方法。我们引入 Dirac 记号来表示一些量子态：如果我们用 $|H\rangle$ 表示硬币正面朝上的（量子）态，而 $|T\rangle$ 表示硬币反面朝上的（量子）态，那么一般而言，这个（量子的）硬币将可以处于这两个态的任意线性叠加态上。在这个博弈中，硬币的初始状态是 $|H\rangle$ ，然后紧接着 Q 对着硬币进行操作。Q 只要通过一个特定的么正操作将硬币的态改变到这样一个叠加态 $|H\rangle + |T\rangle$ 上，他就可以确定性的每次都获胜。因为 P 始终是一个经典的博弈者，他不会使用量子策略，不论 P 翻转或者不翻转这个硬币，这个硬币的态始终保持在 $|H\rangle + |T\rangle$ 这一叠加态上；等到 P 完成了他的那一步，Q 只要实施另一个相应的么正操作便可以把硬币的状态还

原至 $|H\rangle$ 上，这也就是为什么 P 每一次都输的原因[2]。量子“囚徒困境”

“囚徒困境”是经典博弈论中的一个极富代表性的一个著名例子。这个例子的创造本身就奠定了非合作博弈论的理论基础，并且它可以作为实际生活中许多现象的一个抽象概括。

经典“囚徒困境”讲的是两个嫌疑犯（Alice 和 Bob）作案后被警察抓住，被分别关在不同的屋子里审讯。他们每个人都有两种选择（策略）：坦白（Defect，策略 D）和抵赖（Cooperate，策略 C）。警察告诉他们：如果两人都坦白，各判刑 3 年（收益均为 1）；如果两个都抵赖，因证据不足，各判刑 1 年（收益均为 3）。如果其中一人坦白，另一人抵赖，坦白地放出去（收益为 5），抵赖的判刑 5 年（收益为 0）。两个人的目的都是尽可能的是自己的收益最大化。在这个博弈中，坦白（D）是占优策略（dominant strategy），也就是说，不论对方的选择是什么，个人的最优选择是坦白。比如说，如果 Bob 抵赖，Alice 坦白的話被放出来，抵赖的话被判 1 年；如果 Bob 坦白，Alice 坦白的話被判 3 年，抵赖的话被判 5 年。下表给出了他们的支付矩阵，括号内是他们的收益。

	Bob: C	Bob: D
Alice: C	(3, 3)	(0, 5)
Alice: D	(5, 0)	(1, 1)

表格 II “囚徒困境”问题的收益表

在这个模型中我们假设参与人是理性的，他们的目的是通过选择自己的策略来最大化自己的收益，而且并不会考虑自己的选择对其他人的影响。我们首先从 Alice 的角度来考虑她可能选择的策略，当 Bob 选择沉默 C 时，显然 Alice 选择坦白 D 就比选择沉默 C 的获利要多两个单位，所以理性的 Alice 会选择坦白 D；当 Bob 选择坦白 D 时，同样的 Alice 选择坦白 D 就比选择沉默 C 的获利要多一个单位，所以理性的 Alice 还是会选择坦白 D。由此可见，无论 Bob 的选择是什么，对 Alice 而言选择坦白 D 的获利都比选择沉默 C 要多，所以理性的 Alice 会选择坦白 D。同样的，若我们从 Bob 的角度来看，理性的 Bob 也会做出坦白 D 的选择。总之，在他们不能相互交流信息的情况下，对其中任何一个人而言，无论对方选择是怎样的，理性的参与者都会各自独立的选择坦白 D。此时，Alice 和 Bob 的策略组合构成了一个均衡点，这个均衡点在经济学上被称为 Nash 均衡

[13]。Nash 均衡指的是这样一种策略组合，这种策略组合由所有参与人的最优策略组成，也就是说，在给定别人的策略的情况下，没有任何单个参与人有积极性选择其他策略，从而没有人愿意打破这种均衡[14]。这个选择对他们个人来说都是最佳的，但是对他们集体而言却并非如此。很显然从他们集体的角度来看，如果两个人同时选择沉默 C，每人都可以获得 3 个单位的利益，这显然要比两人都选择坦白 D 的结果要好得多。由此可见最符合个体理性的选择，并不一定是集体的理性选择。囚徒困境反映的就是个人理性与集体理性的矛盾[15]。

1999 年 Eisert 等人将囚徒困境量子化[3]，图（4.1）是他们提出的量子化物理模型。这个模型包含每个参与人都十分清楚的三个部分：(1)存在一个产生两量子比特的发生器，使每个参与人拥有一个量子比特；(2)存在一些物理操作仪器，使参与人能根据自己的策略操纵自己的量子比特；(3)有物理测量装置，可从输出的两量子比特态中决定参与人的支付。

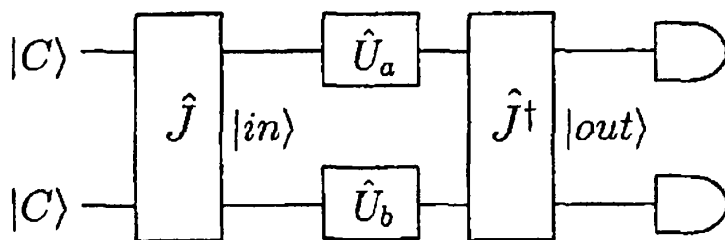


图 4.1 囚徒困境的量子化模型

其量子化的具体过程如下：将经典策略 C 和 D 的可能结果对应为一个 qubit 系统的基矢，分别记为 $|C\rangle$ 和 $|D\rangle$ 。两个参与者，就需要提供两个 qubit，两人的经典结果对应的态为 $|CC\rangle$ 、 $|CD\rangle$ 、 $|DC\rangle$ 和 $|DD\rangle$ ，其中第一项代表 Alice 的量子比特，第二项代表 Bob 的量子比特，这四个态相互正交，构成一个四维的 Hilbert 空间。每一时刻，博弈的态都在这个四维空间中演化。

博弈的初态由幺正算符作用于 $|CC\rangle$ 产生，记为 $|in\rangle$ ， $|in\rangle = \hat{J}|CC\rangle$ ，算符 $\hat{J}$ 是一个引入量子力学纠缠特性的幺正算符。Alice 和 Bob 的策略分别用幺正算符 $\hat{U}_a$ 和 $\hat{U}_b$ 表示， $\hat{U}_a$ 和 $\hat{U}_b$ 属于策略空间 S 。由于在囚徒困境中 Alice 和 Bob 不能相互交流信息，并且各自独立地选择自己的策略，因此 $\hat{U}_a$ 和 $\hat{U}_b$ 应分别作用在他们各

自的量子比特上。Alice 和 Bob 的策略实施之后，博弈的状态变为 $(\hat{U}_a \otimes \hat{U}_b) \hat{J} |CC\rangle$ 。最后 Alice 和 Bob 的量子比特被送入到测量装置中，这个测量装置由一个实行 $\hat{J}$ 逆操作的两量子位门 $\hat{J}^+$ 和其后的一对 Stern-Gerlach 型探测器组成。每个探测器都有两个通道，用参数 σ 标记， $\sigma = C, D$ 。两量子比特经过 $\hat{J}^+$ 门后，博弈的末态 $|out\rangle = \hat{J}^+ (\hat{U}_a \otimes \hat{U}_b) \hat{J} |CC\rangle$ 。接下来的测量会将博弈的末态以一定的概率塌缩到 $|CC\rangle$ 、 $|CD\rangle$ 、 $|DC\rangle$ 和 $|DD\rangle$ 中的一个上，两个参与人的收益仍然同经典的支付矩阵。例如 $\sigma\sigma' = CD$ ，两人的收益为 $(0, 5)$ ，而量子力学的概率性说明参与人的收益应该是期望值，因此定义 Alice 和 Bob 的期望收益分别为 $\$_a$ 和 $\$_b$ ，

$$\$ _a = rP_{CC} + tP_{DC} + sP_{CD} + pP_{DD}, \quad (4-1)$$

$$\$ _b = rP_{CC} + tP_{DC} + sP_{CD} + pP_{DD}, \quad (4-2)$$

这里 $P_{\sigma\sigma'} = |\langle\sigma\sigma'|out\rangle|^2$ ，参数 $r=3$ 、 $t=5$ 、 $s=0$ 、 $p=1$ 对应于参与人的四种收益。

Alice 和 Bob 的策略空间 S 是 2×2 酉群的某个子集，若将其现在 2×2 ，由 θ 和 φ 两参数描述的么正矩阵集合上，具体形式如下：

$$\hat{U}(\theta, \varphi) = \begin{pmatrix} e^{i\varphi} \cos \frac{\theta}{2} & \sin \frac{\theta}{2} \\ -\sin \frac{\theta}{2} & e^{-i\varphi} \cos \frac{\theta}{2} \end{pmatrix}, \quad (4-3)$$

并给定了 θ 和 φ 的变化范围， $0 \leq \theta \leq \pi$ ， $0 \leq \varphi \leq \pi/2$ 。沉默策略 $\hat{C} \equiv \hat{U}(0,0) = \hat{I}$ ，坦白策略 $\hat{D} \equiv \hat{U}(\pi,0) = i\sigma_y$ 。为了使量子博弈包含经典博弈，即当参与人使用策略 C 和 D 时，博弈不能出现与经典博弈相悖的性质；且无量子纠缠时，博弈依然是经典博弈，需要引入量子纠缠的 $\hat{J}$ 门满足

$$[\hat{J}, \hat{D} \otimes \hat{D}] = 0, \quad [\hat{J}, \hat{D} \otimes \hat{C}] = 0, \quad [\hat{J}, \hat{C} \otimes \hat{D}] = 0, \quad (4-4)$$

$\hat{J}$ 的形式为

$$(4-5)$$

其中的参数 γ 表征了博弈初态的纠缠度，它的取值从 0 (博弈初态不纠缠) 到 $\pi/2$ (博弈初态为最大纠缠态)。

4.1.3 量子赌博

假设这么一个经典游戏：Alice 往一个盒子里丢一个硬币，那么理论上硬币出现正面和反面的几率相等，然后将这个盒子送给 Bob；当 Bob 打开这个盒子，如果发现正面朝上，则 Bob 赢（简单起见，假设赢一个硬币），否则 Bob 输一个硬币。在经典情况下，Bob 无法验证 Alice 是否作弊，即是否完全随机的放入硬币，尤其在对弈次数比较少的情况下。所以这种远程的公平博弈因为双方的互相不信任，将无法实行。但是这一游戏量子化后可以做到这一点。量子化后的这一游戏框架如下[4]：Alice 有两个盒子 A 和 B 用来放一个粒子。粒子在 A 盒子或 B 盒子的状态分别用 $|a\rangle$ 和 $|b\rangle$ 来表示。Alice 把粒子制备到某个态上，然后将盒子 B 发送给 Bob。在下列两种情况下 Bob 赢：（1）、如果 Bob 发现粒子在 B 盒子里，同时 Alice 检查确信粒子不在 A 盒子里，则 Bob 赢得一个硬币；（2）、Bob 没有在 B 盒子中发现粒子，他要求 Alice 把 A 盒子发送过来，检验到 Alice

制备的态不是事先约定好的初始态： $|\varphi_0\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$ ，如果不是，那么 Alice

就要付给 Bob R 个硬币。其它情况下，Alice 赢，Bob 付给 Alice 一个硬币。

Alice 的策略就是将粒子制备到 $|\varphi_0\rangle$ 态上，即粒子处在盒子 A、B 的均等叠加态上，测量后在两个盒子发现粒子的几率相等可以确保其收益期望值不低于 0。当然也可以将粒子制备在偏离 $|\varphi_0\rangle$ 的态： $|\varphi_1\rangle = \alpha|a\rangle + \beta|b\rangle$ 上， $\alpha > \beta$ 。这样就有可能多赢，也有可能被 Bob 发现作弊从而受罚损失 R 硬币。

Bob 的策略是收到 B 盒子后并不立即测量粒子是否在 B 盒子里，而是先做一个变换：

$$|b\rangle \rightarrow \sqrt{1-\eta}|b\rangle + \sqrt{\eta}|b'\rangle, \quad (4-6)$$

这里 $|b\rangle$ 和 $|b'\rangle$ 正交，就好像把粒子在 B 盒子里的态不破坏的分成两部分，在这里劈裂参数为 η 。在完成态的劈裂操作后，Bob 作态 $|b\rangle$ 的投影测量，即查看盒子 B

里有没有 Alice 放置的粒子。如果 Bob 发现了粒子，Bob 赢了这一局。否则 Bob 向 Alice 索要 A 盒子用来检验：他可以用 A 盒子和留下来的 $|b'\rangle$ 做联合测量，即验证粒子是否处在期望的末态上，就可以以一定的概率判断出 Alice 是否作弊。接下来将详细介绍我们在实验上实现这一量子赌博机的方案和结果

4.2 量子赌博机的光学实现

我们在 4.1.3 中简要介绍了量子赌博机的原理，下面我们将详细介绍一下量子赌博中博弈论的体现和我们的光学实验方案。

前面已经说明了 Alice 和 Bob 的可选择方案，现在我们来讨论一下他们的获益情况。如果 Alice 采取 $|\varphi_0\rangle$ 作为输入态的方案，可以很明显地看出 Alice 的收益 $G_A \geq 0$ ，而 Bob 的收益 $G_B \leq 0$ 。因为，如果 Bob 采取直接打开 B 盒子的方案，那么他将以 0.5 的概率赢得 1 硬币或者输掉 1 硬币（他不能欺骗 Alice，因为 Alice 可以用 A 盒子验证）。如果他选择验证 Alice 的初态是否是他们约定好的 $|\varphi_0\rangle$ ，那么他肯定失败而输掉 1 硬币。所以说，不管 Bob 采取那种方案，结果都是 $G_B \leq 0$ ， $G_A \geq 0$ 。

在这种情况下，我们可以证明，存在一个合适的劈裂参数 $\eta = \tilde{\eta}$ ，可以保证 Bob 的收益 $G_B \geq \delta$ 。假设 Bob 打开 B 盒子并发现粒子的概率为 P_b 。如果没有发现粒子，他将检验初态。他赢得 R 硬币的概率为 $(1 - P_b)P_D$ ，其中 P_D 为检验初始态的成功概率。所以他输掉一个硬币的概率为 $(1 - P_b)(1 - P_D)$ 。我们可以得到 Bob 的收益为：

$$G_B = P_b + (1 - P_b)[P_D R - (1 - P_D)]. \quad (4-7)$$

如果劈裂参数为 η ，我们可以计算出当 Bob 没有在 B 中发现粒子后，所期望的末态为：

$$|\varphi_2\rangle = \sqrt{\frac{1}{1+\eta}}|a\rangle + \sqrt{\frac{\eta}{1+\eta}}|b'\rangle. \quad (4-8)$$

然而 Alice 的目的则是要尽可能的减少 Bob 的收益, 她可以采取非 $|\varphi_0\rangle$ 的输入态来达到这个目的。假设她以 $|\varphi'_0\rangle$ 态输入:

$$|\varphi'_0\rangle = \sqrt{\frac{1}{2} + \varepsilon}|a\rangle + \sqrt{\frac{1}{2} - \varepsilon}|b\rangle. \quad (4-9)$$

此时 Bob 的劈裂 $|b\rangle$ 后得到的态为:

$$|\varphi'_1\rangle = \sqrt{\frac{1}{2} + \varepsilon}|a\rangle + \sqrt{\frac{1}{2} - \varepsilon}(\sqrt{1-\eta}|b\rangle + \sqrt{\eta}|b'\rangle). \quad (4-10)$$

此时,

$$P_b = \|\langle b|\varphi'_1\rangle\|^2 = (\frac{1}{2} - \varepsilon)(1 - \eta). \quad (4-11)$$

当 Bob 没有在 B 中发现粒子, 此时 $|\varphi'_1\rangle$ 将塌缩为 $|\varphi'_2\rangle$,

$$|\varphi'_2\rangle = \frac{\sqrt{1+2\varepsilon}|a\rangle + \sqrt{\eta(1-2\varepsilon)}|b'\rangle}{\sqrt{1+2\varepsilon + \eta(1-2\varepsilon)}}. \quad (4-12)$$

这样, 我们就可以得到 Bob 的检验末态成功, 赢得 R 硬币的概率为:

$$P_D = 1 - \|\langle \varphi_2|\varphi'_2\rangle\|^2 = \frac{2\eta(1 - \sqrt{1-4\varepsilon^2})}{(1+\eta)^2 + 2\varepsilon(1-\eta^2)}. \quad (4-13)$$

根据这些结果, 我们得到 Bob 的收益为:

$$G_B = -\frac{1}{1+\eta}[2\varepsilon(1-\eta^2) + \eta(\eta + \sqrt{1-4\varepsilon^2}) - \eta(1-\sqrt{1-4\varepsilon^2})R]. \quad (4-14)$$

为了计算 Bob 的最小收益 δ , 我们假设 Bob 采用了最优化的策略, 同时 Alice 采用了使 Bob 收益变小的最优策略。这两个策略表现在参数 η 和 ε 上:

$$\delta(R) = \max_{\eta}[\min_{\varepsilon} G_B(R, \eta, \varepsilon)]. \quad (4-15)$$

经过极值计算, Bob 的最优劈裂参数

$$\tilde{\eta} = \sqrt{R+2 - \sqrt{(R+2)^2 - 1}}. \quad (4-16)$$

特别的, 当 $R \gg 1$ 时, 结果可以简化为:

$$\delta \approx -\sqrt{\frac{2}{R}}, \quad \tilde{\eta} \approx \sqrt{\frac{1}{2R}}. \quad (4-17)$$

根据这些理论计算, 我们设计了一个光学实现量子赌博机的方案, 并且得

到了比较好的结果[16]。

在实验上，我们光子作为 Alice 方的粒子，光子的两个偏振态（水平偏振和竖直偏振）作为两个盒子 A 和 B。Alice 可以将光子制备到偏振叠加态上，然后将光子发送给 Bob，假设 Bob 发现光子处于水平偏振，那么他就赢得 1 硬币，否则，他将验证光子的末态，由于单光子态无法 100%区分，所以 Bob 将或赢得 R 硬币，或输掉 1 硬币。出于这种思想，我们实验上成功地实现了量子赌博机，其光路图如下（图 4.2）。

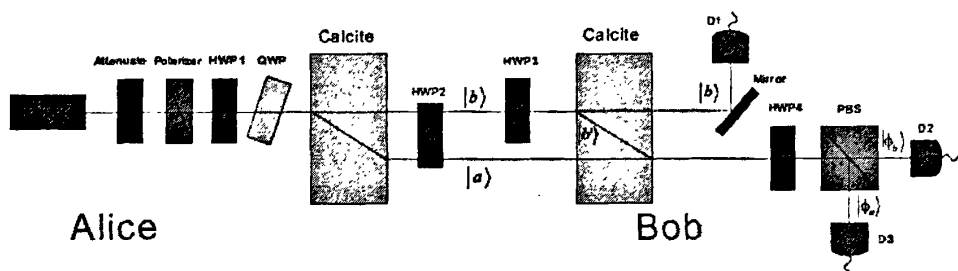


图 4.2 量子赌博机的实验实现

图 4.2 中，光源为普通的 He-Ne 激光器（波长 632.8nm），经过一个衰减器（Attenuate）衰减到单光子量级。起偏器（Polarizer）将光子态制备到单一偏振态，然后经过一个半波片（HWP1），输入态就被制备到 $|\varphi'_0\rangle$ 。通过调节 HWP1 的度数，可以改变输入态的参数 ε ，即，实现了 Alice 的博弈策略。然后 Alice 将这个光子态分两路经（A 和 B 盒子的传输路径）送给 Bob，此处我们用了方解石晶体（Calcite）作为偏振分束器，上路径传送 B 盒子，下路径传送 A 盒子。图中 HWP2（@22.5°）的作用是根据实验的要求，将两路径的偏振态发生交换。这样，Bob 通过调节 HWP3 实现劈裂操作，通过改变半波片的角度改变劈裂参数 η 。最后，劈裂后的 B 盒子直接通过偏振分束器，进行检验有无光子，另一部分则与 A 盒子一起实现末态的检验。半波片 HWP4 和偏振分束器 PBS 组成了末态的投影测量。D1、D2 和 D3 分别是单光子探测器。

我们实验中，通过调节 HWP1 改变 ε ，通过调节 HWP3 改变 η ，最后通过改变 HWP4 实现末态的检验。整个光路的核心部分是由两块双折射晶体组成的 M-Z 干涉仪[17]。众所周知，M-Z 干涉仪是一种相位敏感的干涉仪，其稳定性很难长时间保持。这种由两块双折射晶体组成干涉仪，只要两块晶体切割类型和尺寸相

同，由于整个干涉仪只用到两个光学架，且环境引起的相位变化对于干涉两臂的影响相同，所以干涉可以很稳定的保持。正是由于这种长时间的稳定干涉，使得实验上能够有充足的时间测量数据，也使得实验结果更具有说服力。

我们实验上选取了 5 个不同的 ε ，对应每个 ε ，选取了 8 个不同的 η ，将 Bob 赢得一个硬币，赢得 R 个硬币，和输掉一个硬币的概率绘成曲线，更好的说明的互相之间的博弈特性。通过 Bob 的收益曲线，可以更加清楚地看到 Bob 的最优参数选择 $\tilde{\eta}$ 。

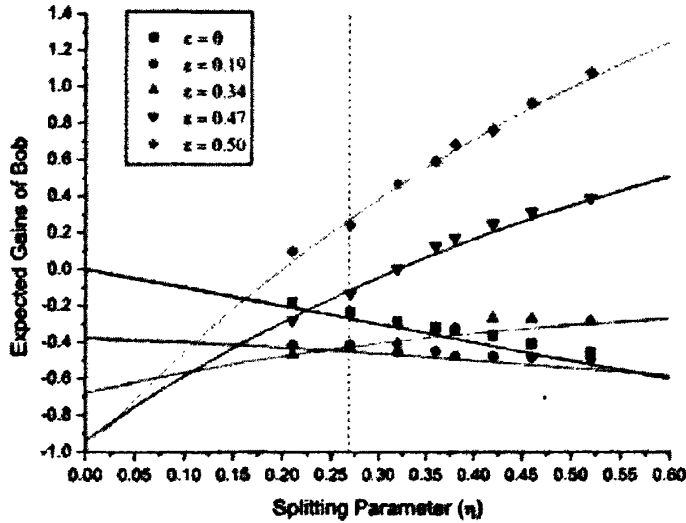


图 4.3 Bob 的收益曲线

实验数据如图 4.3 和 4.4 所示，图中的实线为理论预言曲线，数据点为实验所测几率。图 4.3 给出了 Bob 的收益曲线，虚线标出了在 $R=5$ 时的最优参数 $\tilde{\eta}(R=5) \approx 0.27$ 。图 4.4 为三个探测器测得光子的探测几率。从图中可以看出，实验结果与理论预言十分吻合。

光学方法具有很多优点。最明显的就是光学方法的退相干很低。而且我们在利用双折射晶体实现 M-Z 干涉仪，有效的降低了环境的影响，增加了干涉仪的稳定性。实验上成功实现量子博弈，误差必须控制在 $\sqrt{2/R^3}$ 以内[4]。我们实验的干涉可见度为 98%，即误差为 1/100，这种情况下，可以实现的量子博弈的 R 指在 27.1 以内。所以我们在干涉可见度 98% 下，实现的 $R=5$ 的量子赌博机是完全可以的。

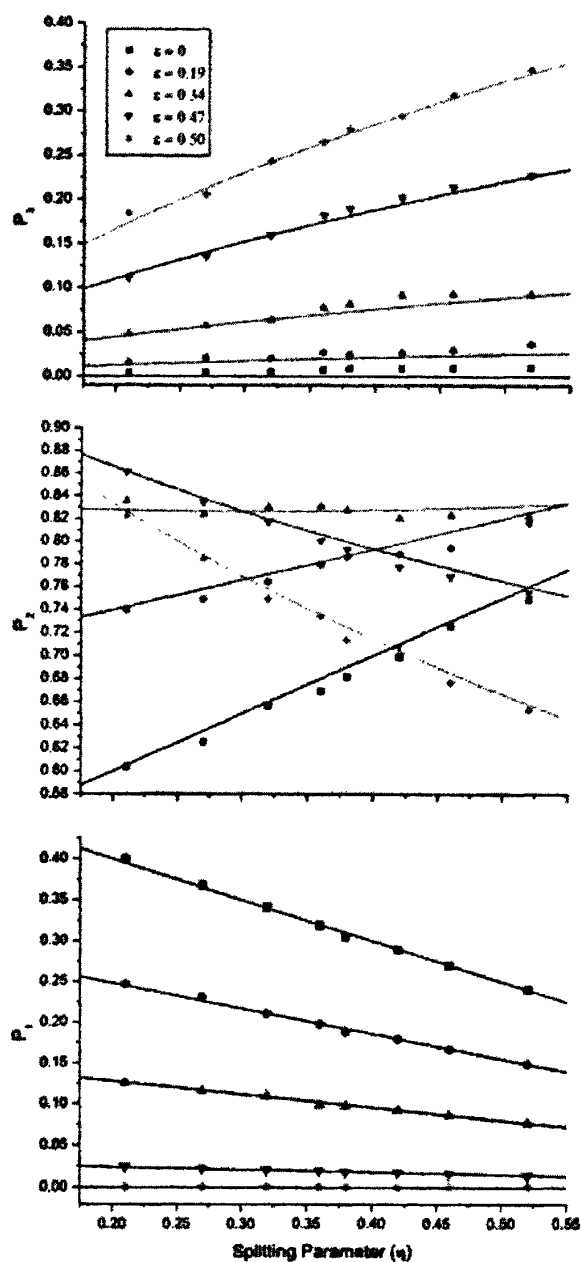


图 4.4 三个探测器的探测概率曲线

量子赌博机也可以看作是一种远程博弈[18,19]。因为博弈的双方可以相距很远, Alice 可以将制备好的量子态传送给 Bob, 通过最后的经典信息决定博弈的结果。这也使得两体的远程量子安全密钥分配变为可能, 为更进一步的研究奠定了基础[20-23]。

4.3 小结

本章主要介绍量子博弈的相关知识，介绍了三种著名的量子博弈问题：PQ 翻硬币问题、量子“囚徒困境”问题和量子赌博机问题。重点介绍了量子赌博机的原理及我们利用光学方法进行的物理实验。我们在实验上利用线性光学元件，利用光子的路径和偏振信息，实现了 $R=5$ 的量子赌博机。我们使用两块双折射晶体作为偏振分束器，实现了 M-Z 干涉仪的长时间稳定，解决了因为 M-Z 干涉仪不稳定引起的实验计数困难，更增加了实验的说服力。实验中，我们选择 5 组不同的数据，对理论预言进行了验证，更加直观地得到了两体之间博弈的关系，也很容易的看出了博弈双方使得自己获益不小于某一值时，应该采取的策略。

参考文献

- [1] S. C. Benjamin and P. M. Hayden, Phys. Rev. A **64**, 030301 (2001).
- [2] D. A. Meyer, Phys. Rev. Lett. **82**, 1052 (1999).
- [3] J. Eisert, M. Wilkens and M. Lewenstein, Phys. Rev. Lett. **83**, 3077 (1999).
- [4] L. Goldenberg, . Vaidman and S. Wiesner, Phys. Rev. Lett. **82**, 16 (1999).
- [5] A. Iqbal and A. H. Toor, Phys. Lett. A **280**, 249 (2001).
- [6] Y.-J. Han, Y.-S. Zhang and G.-C. Guo, Phys. Lett. A **295**, 61 (2002).
- [7] Y. M. Ma, G. L. Long, *et al.*, Phys. Lett. A **301**, 117 (2002).
- [8] A. Iqbal and A. H. Toor, Phys. Lett. A **293**, 103 (2002).
- [9] E. W. Piotrowski and J. Sladkowski, Physica A **312**, 208 (2002).
- [10] E. W. Piotrowski and J. Sladkowski. Physica A **318**, 505 (2003).
- [11] X. F. Liu and C. P. Sun, Commun. Theor. Phys. **41**, 553 (2004).
- [12] J. Von Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, 1955).
- [13] J. F. Nash and Proc. Natl. Acad. Sci. U.S.A. **36**, 48 (1950).
- [14] 曾谨言, 龙桂鲁等, 量子力学新进展(第三辑)。北京: 北京大学出版社 (2003).
- [15] 张维迎, 博弈论与信息经济学。上海: 上海人民出版社 (1996).
- [16] P. Zhang, Y.-S. Zhang, Y.-F. Huang, L. Peng, C.-F. Li and G.-C. Guo, Euro. Phys. Lett. **82**, 30002 (2008).
- [17] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph and D. Branning, Nature (London) **426** 264 (2003).
- [18] J. Du, H. Li, X. Xu, M. Shi, J. Wu, X. Zhou and R. Han, Phys. Rev. Lett. **88**, 137902 (2002).
- [19] R. Prevedel, A. Stefanov, P. Walther and A. Zeilinger, New J. of Phys. **9** 205 (2007).
- [20] R. B. Myerson, *Game Theory: An Analysis of Conflict* (MIT Press, Cambridge, 1991).
- [21] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smonlin, J. Crypto **5**, 3 (1992).

[22] K. Shimizu and N. Imoto, Phys. Rev. A **66**, 052316 (2002).

[23] W-Y Hwang, Phys. Rev. Lett. **91** 057901 (2003).

第五章 量子么正操作的完美区分

人们生活的世界丰富多彩，绚丽多姿，根本原因在于物质所表现出来的多样性，不同性。在经典世界中，不同的事物原则上都是可以完全区分的。而且这种可区分的性质，影响着人们生活的各个方面，像基因辨别，指纹识别，密码验证等等。在量子世界中，量子态的区分和么正操作的区分，同样有着重要的意义。经典事物的这种可区分性质在于我们可以对事物重复测量，获取事物的各方面信息。但是在量子世界中，情况变得不尽相同。量子态的不可克隆定理[1,2]和量子测量理论[3]告诉我们，量子态不能够精确的被复制。所以对于未知的量子态，我们无法获得它足够多的拷贝来完成所有信息的获取。人们在研究量子态局域操作可区分性方面做出了大量的工作，也取得了很大的进展。量子么正操作的区分同样有着重要的意义[4]，但是又不同于量子态的区分。本章主要介绍有关量子么正操作区分的一些基本内容和我们在实验上的一些工作。

5.1 量子态和量子么正操作的区分

量子态的区分是量子信息中的基本问题。实际上正是由于非正交态的不可完全区分性，才保证了量子密码方案的安全。态区分的研究历史可以上溯到上世纪七、八十年代，最早的讨论主要集中在纯态的情况，讨论利用各种手段实现区分的效果是其核心问题。这其中，有两种方案是值得关注的。一种是叫做最小错误区分(Minimum-error discrimination) [3, 5-9]，在该方案中，测量操作每次都要求给出区分的结果，虽然它并不能保证每次的结果都是正确的，这种方案的好坏是用最小错误 PE 来衡量的。对于两混态的最小错误区分，解析的结果可以给出来，但是，对于更多输入态的情况，求解解析解非常困难；不过对于一些特殊情形，例如，输入态等概率分布并且满足一定的对称性，解析结果也是可以写出来的。第二种比较受关注的区分方案就是明确区分(Unambiguous discrimination) [10-15]。这种区分不保证每次都能给出结果，但是，一旦给出结果，则一定是正确的，这也是其命名明确(Unambiguous)的原因。

在量子信息中，非正交量子态不可区分已成为共识，然而，这一结论对量

子操作却并不成立,有结论表明,么正操作是可以确切识别的[16-18]。在原则上,任何一个可逆量子操作都可以局域地识别开来,尽管这些量子操作是作用在多个客体上,并具有纠缠能力。这一结论也使得我们了解到,尽管量子态的许多特性与经典世界中的很多观念大不相同,但是量子操作似乎表现出更多的经典性,故而许多已有的关于量子态的结论不能简单的移植到量子操作上。

但是,量子操作和量子态有着密切的联系。实际上,在许多问题的研究中,它们对应问题本身不同的描述方式,可以提供同一问题的不同研究思路。一个最明显的例子就是量子力学中的薛定谔表象和海森堡表象,前者对应量子态的演化方程,通过求解微分方程,可以得到所考察系统的具体性质;后者直接从体系的算符演化着手,利用算符之间的对易关系,同样可以得到同一问题的解。一般地,为了问题研究的方便,可以选择不同的表象,有助于对问题的理解。

在量子态的区分中,由于量子力学的测量塌缩假说,输入量子态在被测量以后状态发生改变,从而不能再作进一步的操作。然而对于量子操作而言,这种情况是一般是不存在的,对输出态上的测量不会影响到操作仪器的状态。原则上,只要我们需要,操作仪器可以使用无穷次。量子操作的这些特性使得在区分问题的讨论上和量子态大为不同,特别是在么正操作的完美区分上,这一差别更为明显。研究显示,对任意两个不同的么正操作,不论它们是否正交,我们总可以通过并行运行该操作有限次的方法[16,17]或者串行加入辅助么正操作的方法[18]将它们完美区分。这和量子态的区分很不一样,一般的,对非正交的两输入态,任意有限份拷贝都不足以让我们完成完美的区分。

下面我们将介绍量子么正操作完美区分的两种方法,并且说明我们在实验上所取得的结果。

5.2 量子么正操作的完美区分

么正操作完美区分描述的是这样一个问题:对于两个量子电路,只知道它们分别能实现量子么正变换 U 和 V ,但是不知道 U 操作对应于那一块线路, V 操作对应于那一块电路。或者说,给定一个量子电路,只知道它能实现 U 或者 V 操作,目标是实现 100% 概率的正确判断确认该操作是 U 还是 V 。这里,有一个前提假设,量子操作可以有有限份拷贝。有一些简单的想法,比如给定一个输入

态 $|\varphi_{in}\rangle$ ，让它经过未知量子电路进行演化，通过判断演化后末态 $|\varphi_{out}\rangle$ 来确定该电路实现的操作是 U 还是 V 。很明显，能否实现量子操作的完美区分归结于对末态 $|\varphi_{out}\rangle_U$ 和 $|\varphi_{out}\rangle_V$ 的完美区分。由量子态的区分可以知道，非正交态无法实现完美区分，所以，实现量子么正操作的完美区分，目标必须是找到合适的方法和输入态，使得末态 $|\varphi_{out}\rangle_U$ 和 $|\varphi_{out}\rangle_V$ 正交。

5.2.1 并行方案

在 2001 年，A. Acin 和 G. Mauro D'Ariano 等人几乎同时独立的提出了利用纠缠态，实现量子么正操作完美区分的方法[16-17]。他们利用适当的纠缠态 $|\varphi_{in}\rangle$ 作为输入态，并行的实施 N 次有限操作，便可以实现 $|\varphi_{out}\rangle_U$ 和 $|\varphi_{out}\rangle_V$ 的正交，达到量子么正操作的完美区分，下面我们详细介绍一下并行方案。

首先，我们简要介绍一下态区分一些基本知识。假设有两个态 ρ_1 和 ρ_2 （这里用密度矩阵来表示态）同属于一个 Hilbert 空间。那么这两个态的相似程度或者叫做保真度 F 可以表示为：

$$\sqrt{F(\rho_1, \rho_2)} = \min_{M_i} \sum_i \sqrt{\text{tr}(M_i \rho_1) \text{tr}(M_i \rho_2)}. \quad (5-1)$$

这里 M_i 是 POVM (Positive Operator Valued Measure) 算子[19]。对于一位投影子， $\rho = |\psi\rangle\langle\psi|$ ，Wootters 证明[20](5-1)式可以简化为：

$$F(\psi_1, \psi_2) = \left| \langle \psi_1 | \psi_2 \rangle \right|^2. \quad (5-2)$$

对于混态，(5-1)式可以变为[21,22]：

$$\sqrt{F(\rho_1, \rho_2)} = \text{tr} \sqrt{\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}}. \quad (5-3)$$

这里用保真度 F 很好的刻画了两个态的可区分程度（相似度）。将这一思想推广到单比特么正操作（单比特门操作或者 $SU(2)$ 变换）我们也可以得到相似的结论。

假设 $U_1, U_2 \in SU(2)$ ，我们讨论这两个么正操作的可区分程度，可以同样引入么正操作的保真度概念。我们知道，对于任意的 $U \in SU(2)$ ，可以将其展开为以下形式：

$$U = \cos \alpha + i \sin \alpha \vec{n}(\theta, \phi) \cdot \vec{\sigma} = e^{i \alpha \vec{n}(\theta, \phi) \cdot \vec{\sigma}}, \quad (5-4)$$

其中 θ , ϕ 和 α 是 Bloch 球上的 3 个标准极化角[23]。它的谱分解可以写为:

$$U = e^{i\alpha} |u\rangle\langle u| + e^{-i\alpha} |u^\perp\rangle\langle u^\perp|, \quad (5-5)$$

$|u\rangle$ 和 $|u^\perp\rangle$ 属于 $\vec{n}(\theta, \phi) \cdot \vec{\sigma}$ 的本征矢量, 它们的本征值为 ± 1 。对于任意的两比特纠缠态, $|\psi\rangle \in C^2 \otimes C^2$, 我们希望找到合适的态使得 U_1 和 U_2 的可区分性最大, 也就是说使得末态 $(U_i \otimes 1|\psi\rangle, i=1,2)$ 的可区分性最大。这样我们可以定义单比特么正操作的保真度为:

$$F(U_1, U_2) = \min_{|\psi\rangle} |\langle \psi | (U_1^\dagger \otimes 1)(U_2 \otimes 1) | \psi \rangle|^2. \quad (5-6)$$

因为么正操作只作用在第一个量子比特上, 所以我们可以通过 $\rho_A = \text{tr}_B(|\psi\rangle\langle\psi|)$ 简化上式:

$$\min_{\rho_A} |\text{tr}(\rho_A U)|^2 = \min_{\vec{s}} \frac{1}{2} |\text{tr}[(1 + \vec{s} \cdot \vec{\sigma})U]|^2. \quad (5-7)$$

这里 $\vec{s}$ 是 ρ_A 的 Bloch 矢量, $U = U_1^\dagger U_2$ 。通过(5-4)式可以计算出最小值。我们可以得到, 当 $|\psi\rangle$ 是最大纠缠态时, U_1 和 U_2 具有最大的可区分性, 此时它们的保真度变为:

$$F(U_1, U_2) = \frac{|\text{tr}(U_1^\dagger U_2)|^2}{4}. \quad (5-8)$$

事实上, 我们总可以找到一个依赖于 U 的最优 $|\psi\rangle$, 使得两么正操作最大的区分。

对于单比特么正操作来说, 最大纠缠态就是最优的 $|\psi\rangle$ 。

现在考虑这样一种情况, 么正操作可以有 N 份拷贝, $U_1, U_2 \in SU(2)$, 输入态 $|\psi\rangle$ 经过 N 次并行操作后, 使得 $U_1^{\otimes N}$ 和 $U_2^{\otimes N}$ 的可区分性最大, 即实现完美区分。在这种情形下输入态 $|\psi\rangle$ 依赖于 N , 而 N 则依赖于 $U = U_1^\dagger U_2$ 。对 U 进行式(5-5)的谱分解, $0 \leq \alpha \leq \pi/2$ 。 $U^{\otimes N}$ 的本征值为 $\{e^{\pm iN\alpha}, e^{\pm i(N-2)\alpha}, \dots, e^{\pm i(N \bmod 2)\alpha}\}$, 当 N 是偶数 (奇数) 时, $(N \bmod 2)$ 等于 1 (0), 本征态可以用相应的 $|u\rangle$ 和 $|u^\perp\rangle$ 表示。接

下来就是找到复合体系 AB 的合适 $|\psi\rangle \in C^{2^N} \otimes C^{2^N}$ ，使得 $\langle\psi|U^{\otimes N} \otimes I|\psi\rangle$ 最小。

用 u_i^N 和 $|u_i^N\rangle$ 表示 U 的本征值和本征态，定义 $\gamma \equiv \text{tr}_B(|\psi\rangle\langle\psi|)$ ，则可以写成：

$$\langle\psi|U^{\otimes N} \otimes I|\psi\rangle^2 = \left| \sum_i \lambda_i u_i^N \right|^2, \quad (5-9)$$

这里 $\lambda_i \equiv \langle u_i^N | \gamma | u_i^N \rangle$ 为正数满足 $\sum_i \lambda_i = 1$ 。现在很容易证明，当 $N\alpha \geq \pi/2$ ，则(5-9)

式为 0，即达到了完美区分。可以看出 $N_{\min}$ 满足：

$$N_{\min} = \left\lceil \frac{\pi}{2\alpha} \right\rceil, \quad (5-10)$$

其中 $\lceil x \rceil$ 表示大于 x 的最小整数。在这种情况下，可分态 $|\psi\rangle \equiv |\psi^S\rangle \otimes |0\rangle$ ， $|\psi^S\rangle$ 为：

$$|\psi^S\rangle = \sqrt{q}(|u_{+N}\rangle + |u_{-N}\rangle) + \sqrt{\frac{1}{2} - q}(|u_{+}\rangle + |u_{-}\rangle), \quad (5-11)$$

$u_{\pm N}$ 和 $u_{\pm}$ 是本征态，对应的本征值为 $e^{\pm i N_{\min} \alpha}$ 和 $e^{\pm i (N_{\min} \bmod 2) \alpha}$ ，并且

$$q = \frac{\cos[(N_{\min} \bmod 2)\alpha]}{2\{\cos[(N_{\min} \bmod 2)\alpha] - \cos(N_{\min} \alpha)\}}. \quad (5-12)$$

这些条件的实现，将会使得 $N_{\min}$ 份拷贝的两个么正变换实现完美区分，也就是末态 $|\psi_i^S\rangle \equiv U_i^{\otimes N_{\min}} |\psi^S\rangle$ 正交。我们可以看出，除非 $U=1$ ，也就是 $U_1=U_2$ ，N 总是有限的一个整数。

最后，将这种方法推广到任意维度 (d 维)，即 $U_1, U_2 \in SU(d)$ ，此时， $|\psi\rangle \in C^d \otimes C^d$ 。同样的推导，我们可以得到：

$$F(U_1, U_2) = \cos^2 \alpha = \cos^2 [\min(\delta, \pi/2)]. \quad (5-13)$$

定义 2δ 为包含所有 u_i 的最小弧长。这样，我们仍然可以找到依赖于 U 的最优输入态，使得在有限次作用么正操作后，实现末态的正交。

并行方案的示意图如图(5.1)A 中所示，O 为未知量子电路， $|\psi_i\rangle$ 和 $|\psi_o\rangle$ 分别表示初态和末态，并行方案的目标就是经过并行的 N 次 O 操作后，末态 $|\psi_o\rangle_1$ 和 $|\psi_o\rangle_2$ 正交。

5.2.2 串行方案

在 2001 年提出并行方案以后，一种普遍的观点就是，认为量子纠缠的核心作用，才使得么正操作的区分成为现实。因为我们知道，在并行方案中，输入态是依赖于 U 的纠缠态，最后得到的也是两个正交的纠缠态。最近，清华大学段润尧博士等人发现了一种不需要纠缠，仍然可以实现么正操作完美分的方案 [18]，又称作串行方案，引起大家的关注。

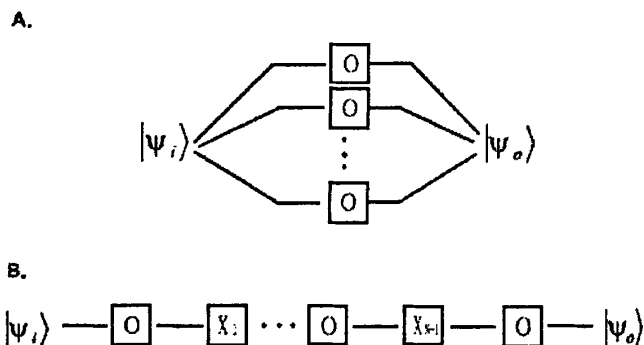


图 5.1 并行方案和串行方案示意图

串行方案的描述如下：给定一个量子线路，它可能实现了 U 或者 V 的么正操作， $U, V \in SU(d)$ 。我们将此电路作用于一个已知的初态 $|\psi\rangle$ ，然后根据结果是 $U|\psi\rangle$ 还是 $V|\psi\rangle$ 来判断此未知电路。如果 $U|\psi\rangle$ 和 $V|\psi\rangle$ 是正交态，则实现了完美区分，否则，我们再在次系统上作用一个辅助么正操作 $X_1 \in SU(d)$ ，然后第二次作用未知电路。这样系统变为 $UX_1U|\psi\rangle$ 或者 $VX_1V|\psi\rangle$ ，再次判断这两个态是否正交，如果正交，则实现完美区分，否则，重复刚才的步骤。经过 N 步以后，末态变为 $|\psi_U\rangle = UX_{N-1}U \cdots X_1U|\psi\rangle$ 或 $|\psi_V\rangle = VX_{N-1}V \cdots X_1V|\psi\rangle$ ，幸运的是，在有限的 N 步内，总是存在合适的输入态 $|\psi\rangle$ 和辅助么正操作 $X_1, \dots, X_{N-1} \in SU(d)$ ，使得末态 $|\psi_U\rangle$ 和 $|\psi_V\rangle$ 正交。

串行方案的示意图如图(5.1)B 所示，图中 U 表示 U 或者 V 。在详细证明串行方案之前，我们先来定义一些量。用 $\mathcal{H}_d$ 来表示 d 维 Hilbert 空间，符号 $U(d)$ 表示作用在这个 d 维 Hilbert 空间上的一组么正算符。一般情况下，我们可以根据

上下文确定空间维度，故而省略 d 。对于一个么正算符 U ，用 $\Theta(U)$ 表示包含 U 的所有本征值的最小弧度。显然， $\Theta(U) = \Theta(U^*)$ ，对于任意的 $X \in U$ ， $\Theta(U) = \Theta(XUX^*)$ 。

根据上面的这些定义，串行方案可以描述为： U 和 V 为两个不同的么正操作，令 $N = \left\lceil \frac{\pi}{\Theta(U^*V)} \right\rceil$ 。那么存在 $X_1, \dots, X_{N-1} \in U$ 和 $|\psi\rangle \in \mathcal{H}$ ，使得：

$$UX_{N-1} \dots UX_1 U |\psi\rangle \perp VX_{N-1} \dots VX_1 V |\psi\rangle. \quad (5-14)$$

证明如下：

为了简单，假设要区分的两个么正操作为 U 和单位操作 I 。此时问题可以简化为：存在 $X \in U$ ，使得 $\Theta(X^*UXU^{N-1}) \geq \pi$ ，即存在 $|\psi\rangle \in \mathcal{H}$ ，使得 $X|\psi\rangle$ 和 $UXU^{N-1}|\psi\rangle$ 正交。

首先考虑二维情形 ($d=2$)，由谱分解的理论，我们可以将任意一个么正操作写成对角形式—— $\text{diag}(e^{i\theta}, 1)$ ，其中 $\theta = \Theta(U) \in (0, \pi]$ 。如果 $\theta = \pi$ ，那么令 $N=1$ ， $X=I$ ，很容易发现两个末态是正交的。否则，令

$$X = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}, \quad (5-15)$$

为一个实的旋转操作，这里 $0 \leq \alpha \leq \pi/2$ 。由于要满足 $\Theta(X^*UXU^{N-1}) \geq \pi$ ，所以我们得到这个方程： $\text{tr}(X^*UXU^{N-1}) = 0$ ，展开以后变为：

$$\cos^2 \alpha e^{iN\theta} + \sin^2 \alpha e^{i(N-1)\theta} + \sin^2 \alpha e^{i\theta} + \cos^2 \alpha = 0. \quad (5-16)$$

注意到 $(N-1)\theta < \pi \leq N\theta$ ，求解可得到：

$$\alpha = \tan^{-1} \sqrt{\frac{\cos(N\theta/2)}{\cos((N-2)\theta/2)}}. \quad (5-17)$$

然后，对于上面的 α ，令 $X^*UXU^{N-1} = e^{i\beta}|\varphi_1\rangle\langle\varphi_1| - e^{i\beta}|\varphi_2\rangle\langle\varphi_2|$ 是一种特殊的谱分解，那么选择输入态

$$|\psi\rangle = (|\varphi_1\rangle + |\varphi_2\rangle) / \sqrt{2}, \quad (5-19)$$

可以很容易的得到

$$\langle \psi | X^* U X U^{N-1} | \psi \rangle = 0. \quad (5-20)$$

当 $d > 2$ 时, 我们可以继续将 U 表示为 $\text{diag}(e^{i\theta_1}, e^{i\theta_2}, \dots, e^{i\theta_d})$, $0 \leq \theta_k \leq \Theta(U) < \pi$ 。假设 $\theta_1 = \Theta(U)$, $\theta_2 = 0$, 由 $d=2$ 时的结论可以知道, 存在 $X_{11} \in \mathbb{U}(2)$, $|\psi'\rangle \in \mathbb{C}_2$, 使得 $\langle \psi' | X_{11}^* U_{11} X_{11} U_{11}^{N-1} | \psi' \rangle = 0$, 这里 $U_{11} = \text{diag}(e^{i\theta_1}, 1)$ 。只要令 $X = X_{11} \oplus I_{d-2}$ 和 $|\psi\rangle = |\psi'\rangle \oplus 0_{d-2}$, 便可以得到 $d > 2$ 的结果。

最后, 推广到更一般的 U 和 V 。这时, 令 U 和 N 分别表示 U^*V 和 $\left\lceil \frac{\pi}{\Theta(U^*V)} \right\rceil$,

这样一般情形便可以转化到上面所讨论的特殊情形, 相当于区分 U^*V 和 I 。由上面的结论可知, 存在 $X \in \mathbb{U}$, $|\psi'\rangle \in \mathbb{C}_N$, 使得 $X|\psi'\rangle$ 和 $U^*VX(U^*V)^{N-1}|\psi'\rangle$ 正交。令 $X_1 = X_2 = \dots = X_{N-2} = U^*$, $X_{N-1} = XU^*$, $|\psi\rangle = |\psi'\rangle$, 则可以得到一般情形的结果。

至此, 我们完成了对串行方案的全部证明。可以明显地看出, 串行方案中, 输入态是单粒子 qudit 态, 并非并行方案中所用到的纠缠态。这样很大程度的降低了态制备的难度, 也降低了最终末态正交性测量的难度。因为我们知道, 对于单粒子多比特态, 使用正交投影测量便可以很容易的实现区分, 而多体纠缠态则需要非局域测量才能达到正交性的验证。

5.3 量子么正操作完美区分的实验实现

如上一节末尾所提到的, 由于并行算法在实验上的难度, 从 2001 年理论证明到现在, 并未发现有实验上的证明。2007 年串行方案的提出, 使得量子么正操作区分在实验上变得容易实现。单比特量子么正操作 (量子门) 在量子计算中有着极为重要的作用, 并且在实验上, 可以很容易的通过两块四分之一波片和一块半波片实现所有的单比特量子么正操作[24, 25]。而对于多比特门, 即使是最为基础的 C-NOT 门, 实验上实现起来也极为的复杂[26-30]。所以我们在实验上选择了两组单比特么正操作作为待区分的量子电路, 使用并行和串行方法进行了

实验验证，并且比较了两种法的优劣之处[31]。

5.3.1 并行方案的实验实现

根据前面并行方案的理论推导，我们在实验上选择两组单比特么正操作进行了区分，下面介绍实验的有关内容。

在实验中，我们选择了以下两组么正操作进行区分：

$$(A). U_1 = \begin{pmatrix} e^{i\frac{2}{3}\pi} & 0 \\ 0 & 1 \end{pmatrix} \quad \text{和} \quad V_1 = \begin{pmatrix} e^{i\frac{1}{6}\pi} & 0 \\ 0 & 1 \end{pmatrix}$$

$$(B). U_2 = \begin{pmatrix} e^{i\frac{2}{3}\pi} & 0 \\ 0 & 1 \end{pmatrix} \quad \text{和} \quad V_2 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

可以很容易的计算出对于 A, B 两组, $N = \left\lceil \frac{\pi}{\Theta(U^*V)} \right\rceil = 2$ 。A 组中的两个操作由于其 $\Theta(U_1^*V_1) = \pi/2$ ，所以对应的输入态比较特殊，因此 B 组中选择了更为一般的两个操作， $\Theta(U_2^*V_2) = 2\pi/3$ 。虽然 V_2 是单位操作，但是由前一节中的证明可以得知，并不影响其一般性。在这里，考虑到并行方案中多粒子纠缠的难度，我们选择了 $N=2$ ，也就是说，以两粒子纠缠态作为输入态，鉴别末态的正交性。

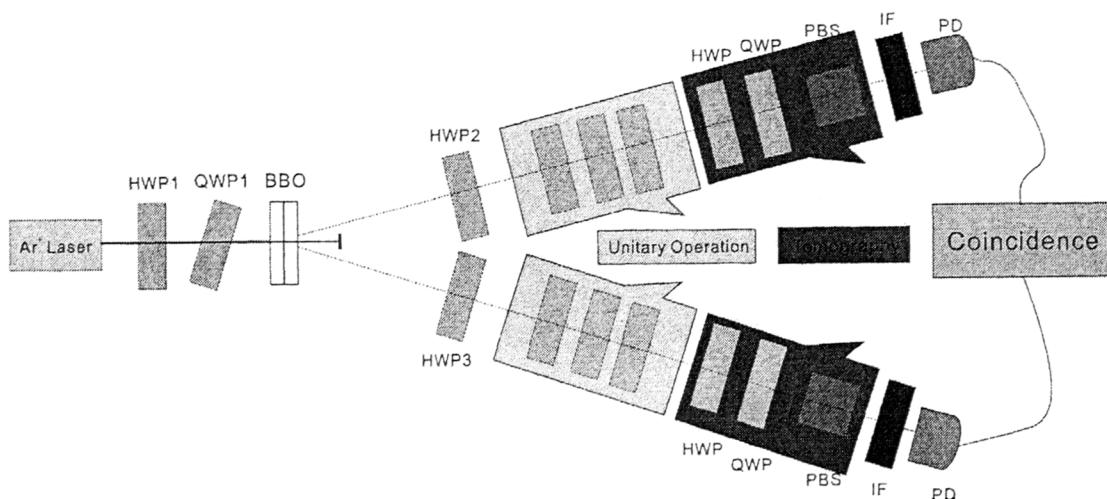


图 5.2 并行方案实现么正操作的完美区分

实验光路如图 5.2 所示。氩离子激光器泵浦 I 型 BBO 晶体产生偏振纠缠的双光子[32]，作为实验的光源。光子纠缠态由三个半波片 HWP1、HWP2 和 HWP3 进行制备，四分之一波片 QWP1 用来补偿双光子对之间的相位。么正操作由两

块 QWP 和一块 HWP 组成（具体的波片角度见表 5.1），分别作用在两个光子上，实现并行的操作。我们选择量子态层析技术（quantum state tomography）对末态进行分析[33,34]，通过末态的密度矩阵判断其正交性。

具体的，对于 A 组的两个么正操作，由公式(5-11 和(5-12)以得到输入态为最大纠缠态：

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle). \quad (5-21)$$

对于 B 组的么正操作，其输入态为：

$$|\psi_2\rangle = \frac{1}{\sqrt{3}}(|HH\rangle + |VV\rangle) + \frac{1}{\sqrt{6}}(|HV\rangle + |VH\rangle). \quad (5-22)$$

为了使实验更具有说服力，我们测量了输入态的保真度（定义见(5-3)式），分别为 $F(\rho_{\psi_1}) = 0.989$ ， $F(\rho_{\psi_2}) = 0.982$ 。对三个么正操作也做了过程 tomography 测量 [35-38]，并计算了其相对于理论矩阵的平均保真度 [39,40]，其中 $F(U_1) = F(U_2) = 0.985$ ， $F(V_1) = 0.975$ 。从这保真度的数据可以看出，不管是输入态，还是么正操作，都还比较理想。

对于 A 组的情形，先制备最大纠缠态最为输入态——式(5-21)。当实验光路中放入 U_1 操作时，通过对末态的量子层析，得到末态的密度矩阵，计算次密度矩阵和理论密度矩阵的保真度，得到 $F(\rho_{U_1}) = 0.985$ ，同样的方法，得到放入 V_1 后的末态保真度为 $F(\rho_{V_1}) = 0.983$ 。然后计算这两个末态的保真度 $F(\rho_{U_1}, \rho_{V_1}) = 0.014$ 。由此可以看出当分别放入 U_1 或 V_1 时，所得到的末态是正交的（保真度越接近 1，说明两个态越相似；保真度越接近于 0，说明两个态趋向于正交）。

对于 B 组的情形，输入态为式(5-21)的非最大纠缠态形式。此时放入 U_2 操作或者去掉 U_2 操作（ $V_2 = I$ ），分别得到两个末态，保真度分别为： $F(\rho_{U_2}) = 0.956$ ， $F(\rho_{V_2}) = F(\rho_{\psi_2}) = 0.982$ 。它们的正交性表示为 $F(\rho_{U_2}, \rho_{V_2}) = F(\rho_{U_2}, \rho_{\psi_2}) = 0.009$ 。

可以看到，选择适当的纠缠态（依赖于 U^*V ）作为输入态，经过 $N=2$ 平行

演化以后，我们得到了两个正交的输出态，从而在实验上实现么正操作的完美区分。

5.3.2 串行方案的实验实现

由前面的讨论可知，并行方案和串行方案需要最少的 N 相同， $N = \left\lceil \frac{\pi}{\Theta(U^\dagger V)} \right\rceil$ 。但是对于并行方案， N 个么正操作并行的作用在（每个 qudit 作用一次） N 粒子纠缠态上；而串行方案则是分为 N 步串行的作用在单粒子 qudit 态上。

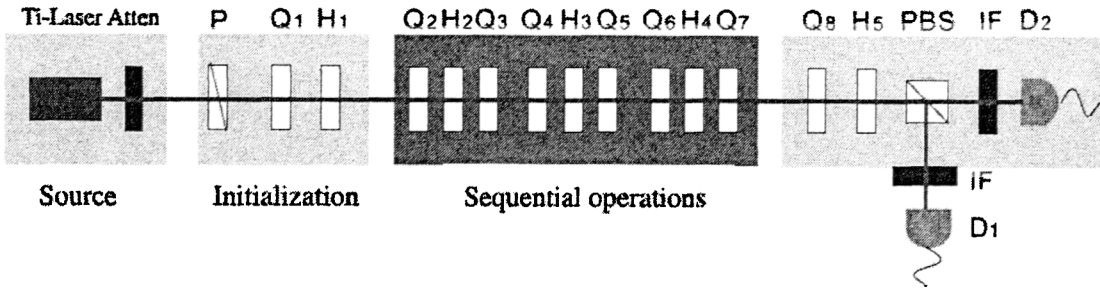


图 5.3 串行方案实现么正操作完美区分光路图

首先，计算 A、B 两种情形的输入态。根据式(5-19)，可以得到 A、B 两组的输入态分别为：

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \quad (5-23)$$

$$|\psi_2\rangle = (0.151 + 0.262i)|H\rangle + 0.953|V\rangle \quad (5-24)$$

然后，根据式公式(5-15)和(5-17)计算辅助么正操作 X 。对于 A 组可以得到：

$$X_1 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (5-25)$$

B 组的辅助么正操作为：

$$X_2 = \frac{1}{\sqrt{3}} \begin{pmatrix} \sqrt{2} & -1 \\ 1 & \sqrt{2} \end{pmatrix} \quad (5-26)$$

得到输入态和辅助么正操作后，便可以根据图 5.3 的光路图实现单比特么正操作的完美区分。具体过程是：钛宝石激光器经过衰减器，衰减到单光子量级，作为单光子源。初态的制备由起偏器（P）、 $\lambda/4$ 波片（ Q_1 ）和半波片（ H_1 ）完

成。紧接着是串行的么正操作序列，对于我们所选择的两组么正操作，由于 $N=2$ ，所以串行么正操作序列为 UXU 。最后，对末态进行正交投影测量， Q_8 、 H_5 和 PBS 组成了测量投影基。

	input		U(V)			X			U(V)			measurement	
	Q_1	H_1	Q_2	H_2	Q_3	Q_4	H_3	Q_6	Q_8	H_4	Q_7	Q_8	H_5
U_1	0	22.5	45	15	45	0	0	0	45	15	45	45	37.5
V_1	0	22.5	45	37.5	45	0	0	0	45	37.5	45	45	37.5
U_2	-15	42.4	45	15	45	27.4	45	62.6	45	15	45	45	15
V_2	-15	42.4	0	0	0	27.4	45	62.6	0	0	0	45	15

表格 I 串行方案中所有波片的角度设置（单位：degree）

根据输入态和辅助么正操作，可以决定投影基的选择。实验中，对于 A 组，我们选择的投影基为 $|\psi_b\rangle_1 = \frac{1}{\sqrt{2}}(-e^{\frac{\pi}{3}i}|H\rangle + |V\rangle)$ ，这样，当末态是 $|\psi_b\rangle_1$ 时，只有探测器 D_1 能探测到光子， D_2 探测不到光子。当末态是 $|\psi_b\rangle_1$ 的正交态时，情况相反；对于 B 组，投影基为 $|\psi_b\rangle_2 = \frac{1}{\sqrt{2}}(e^{-\frac{\pi}{6}i}|H\rangle + |V\rangle)$ ，同样当末态是 $|\psi_b\rangle_2$ 时，光子只能到达探测器 D_1 ，当同样当末态是 $|\psi_b\rangle_2$ 的正交态，光子只能到达 D_2 。从初态的制备，到投影测量，所有的波片角度列在表格 I 中。

根据上面的分析，当光路中波片角度分别按照表格 I 中的设定时，我们得到了两个探测器的计数值与待区分么正操作的关系，如图 5.4。串行方案中，我们选择了正交投影测量，直接判断末态的正交性，而并非并行方案中的量子态 tomography，然后再根据末态的密度矩阵计算保真度来衡量末态的正交性。原因是对于单光子态，正交投影测量很容易实现，这也正是串行方案相对于并行方案简单的原因之一。

图 5.4 中，(a)、(b)、(c)和(d)的区分成功概率分别为 98.0%、98.1%、98.3%和 98.4%。实验误差主要来源于波片角度的精度（0.2 度），因为从初态制备到末态探测，整个过程都是用波片实现的。由于误差的存在，使得区分成功概率小于 100%，但是这不同于其它的非完美区分，因为非完美区分即使在理论上也不可能在有限次内得到 100%的区分。

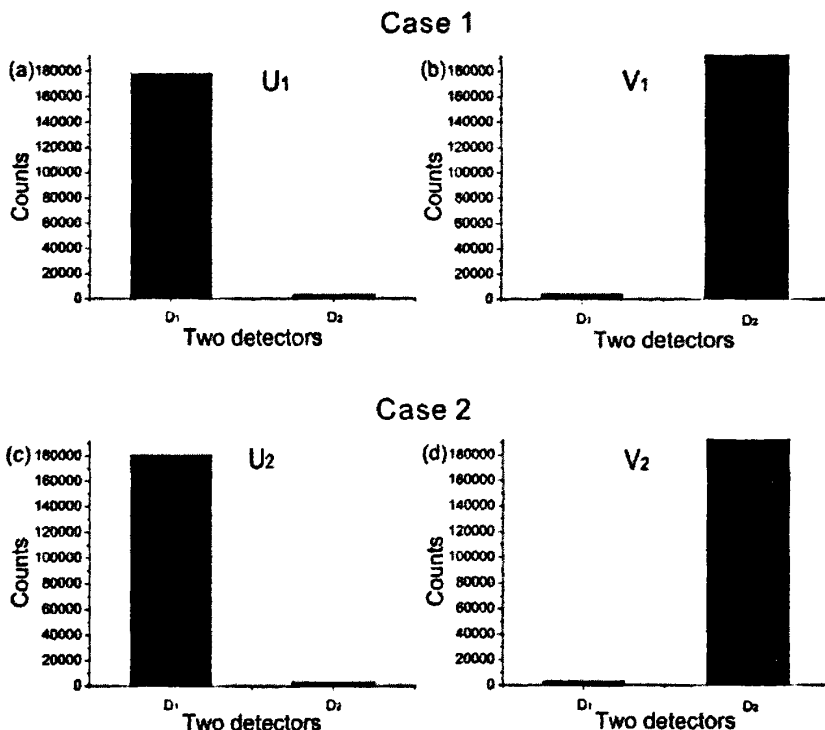


图 5.4 串行方案实验结果

5.3.3 两种方案的比较

以上，我们分别使用并行方案和串行方案在实验上实现了对未知么正操作（U 和 V）的完美区分，这两种方案都是建立在有限次么正操作基础上概率 100% 的区分。它们所需最少的么正操作数都为 $N = \left\lceil \frac{\pi}{\Theta(U^*V)} \right\rceil$ 。但是两种方案的实验难度却不尽相同。

在实验的难易程度方面，串行方案表现出了优越性。首先，初态的要求串行方案比较简单。并行方案需要 N 粒子纠缠态最为输入态，而串行方案则需要单粒子多比特态作为初态，比特数与么正操作的维度有关，与 N 无关。可以发现，即使是对于单比特么正操作，当 $N = \left\lceil \frac{\pi}{\Theta(U^*V)} \right\rceil$ 比较大时，输入态的制备将成为一个难题。而串行方案则不受影响，因为只要是区分单比特么正操作，它的输入态永远是单粒子 qubit 态，即使对于区分多比特么正操作，输入态仍是单粒子 qudit 态。从我们的实验中也能看出两种方案在 $N=2$ 时的初态情况，串行方案

相对简单。其次，末态的探测串行方案也相对于并行方案容易。串行方案的末态仍然是单粒子 qudit 态，因此可以用正交投影测量简单的完成。但是并行方案，由于末态是 N 粒子纠缠态，所以探测要用到多粒子联合测量。而且由于实验噪声的影响，并行方案的最终输入态一般都是混合纠缠态，而混合纠缠态一般无法用 LOCC 获得精确分辨，但串行方案则不受影响。由此可以看出，串行方案更适合于实验实施，并且在 N 比较大的时候体现出来巨大的优势。

但是，串行方案也有其相对于并行方案的不足之处。首先，串行方案需要构造两种辅助操作， X 和 U^* ，并且要实施 $N-1$ 次辅助操作，这使得误差的引入和实验的不确定度增加。其次，串行方案需要串行的实施 N 次未知么正操作和 $N-1$ 次辅助操作，这使得其区分速度（完成区分所需要的时间）相对于并行操作变慢，因为并行操作只需要一步便可完成。可以这样辩证的去理解这个问题，即并行方案耗费了纠缠资源换来了时间上的节约，而串行方案则是牺牲了时间，节约了纠缠资源。

两种方案各有优缺点，我们可以根据实际的需要，将两种方案结合起来，变成混合方案（图 5.5），从而实现区分时间和纠缠消耗的折中[18]。这种混合方

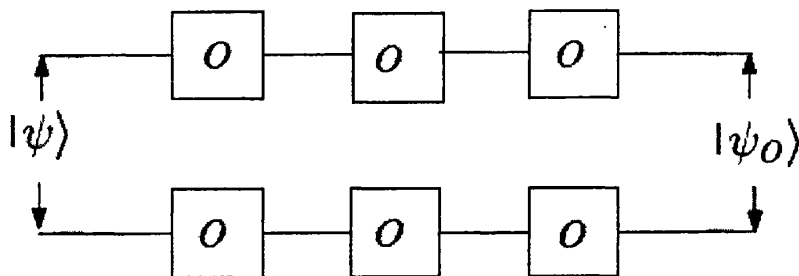


图 5.5 混合方案示意图

案所需要的最少么正操作数量仍是 $N = \left\lceil \frac{\pi}{\Theta(U^*V)} \right\rceil$ ，只是同时引入了纠缠输入和辅助操作，可以适当的减少区分时间，同时也降低纠缠资源的耗费。

5.4 小结

本章开始介绍了量子态区分和么正操作区分的基本理论，并引入么正操作完美区分的概念，介绍了两种完美区分么正操作的方案——并行方案和串行方

案。实验上，我们利用光子偏振比特，两种方法分别实现单比特么正操作的完美区分，得到了和理论相符的实验结果。同时，根据实验的结果分析了两种方案的优缺点，并且讨论向更高维、更多步数推广的一些问题。总体说来，串行方案在目前的实验条件下，是一种比较简单的完美区么正操作的可用方案。

参考文献

- [1] W. K. Wootters and W. H. Zurek, *Nature* (London) **299**, 802 (1982).
- [2] L.-M. Duan and G.-C. Guo, *Phys. Rev. Lett.* **80**, 4999 (1998).
- [3] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
- [4] A. M. Childs, J. Preskill and J. Renes, *J. Mod. Opt.* **47**, 155 (2000).
- [5] H.P Yuen, R.S. Kennedy and M. Lax, *IEEE Trans. Inf. Theory* **21**, 125 (1975).
- [6] M. Ban, K. Kurokawa, R. Momose and O. Hirota, *Int. J. Theor. Phys.* **55**, 22 (1997).
- [7] M. Sasaki, K. Kato, M. Izutsu and O. Hirota, *Phys. Rev. A* **58**, 146 (1998).
- [8] S.M. Barnett, *Phys. Rev. A* **64**, 030303 (2001).
- [9] U. Herzog and J.A. Bergou, *Phys. Rev. A* **70**, 022302 (2004).
- [10] I.D. Ivanovic, *Phys. Lett. A* **123**, 257 (1987).
- [11] D. Dieks, *Phys. Lett. A* **126**, 303 (1988).
- [12] A. Peres, *Phys. Lett. A* **128**, 19 (1988).
- [13] G. Jaeger and A. Shimony, *Phys. Lett. A* **197**, 83 (1995).
- [14] A. Chefles, *Phys. Lett. A* **239**, 339 (1998).
- [15] A. Chefles and S. M. Barnett, *Phys. Lett. A* **250**, 223 (1998).
- [16] A. Acin, *Phys. Rev. Lett.* **87** 177901 (2001).
- [17] G. M. D'Ariano, P. Lo Presti, and M. G. A. Paris, *Phys. Rev. Lett.* **87**, 270404 (2001).
- [18] R. Duan, Y. Feng, and M. Ying, *Phys. Rev. Lett.* **98**, 100503 (2007).
- [19] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000)
- [20] W. K. Wootters, *Phys. Rev. D* **23**, 357 (1981).
- [21] S. L. Braunstein and C. M. Caves, *Phys. Rev. Lett.* **72**, 3439 (1994).
- [22] C. A. Fuchs, *Ph.D. thesis* (University of New Mexico, 1995), quant-ph/9601020.
- [23] J. F. Cornwell, *Group Theory in Physics* (Academic, London, 1984), pp. 44–91.
- [24] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum and P. H. Eberhard, *Phys. Rev.*

- A **60**, R773 (1999).
- [25] B. G. Englert, C. Kurtsiefer, and H. Weinfurter, *Phys. Rev. A* **63**, 032303 (2001).
- [26] J.L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, *Nature* (London) **426**, 264 (2003).
- [27] T. B. Pittman, M. J. Fitch, B. C. Jacobs, and J. D. Franson, *Phys. Rev. A* **68**, 032316 (2003).
- [28] S. Gasparoni, J.-W. Pan, P. Walther, T. Rudolph and A. Zeilinger, *Phys. Rev. Lett.* **92**, 020504 (2004).
- [29] M. Fiorentino and F N. C. Wong, *Phys. Rev. Lett.* **93**, 070502 (2004).
- [30] Z. Zhao, A.-N. Zhang, Y.-A. Chen, H. Zhang, J.-F. Du, T. Yang, and J.-W. Pan, *Phys. Rev. Lett.* **94**, 030501 (2005).
- [31] P. Zhang, L. Peng, Z.-W. Wang, X.-F. Ren, B.-H. Liu, Y.-F. Huang and G.-C. Guo, Submitted.
- [32] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, *Phys. Rev. A* **64**, 052312 (2001).
- [33] U. Leonhardt, *Phys. Rev. Lett.* **74**, 4101 (1995).
- [34] U. Leonhardt, *Phys. Rev. A* **53**, 2998 (1996).
- [35] J. F. Poyatos, J. I. Cirac and P. Zoller, *Phys. Rev. Lett.* **78**, 390 (1997).
- [36] I. L. Chuang and M. A Nielsen, *J. Mod. Opt.* **44**, 2455 (1997).
- [37] A. M. Childs, I. L. Chuang and D. W. Leung, *Phys. Rev. A* **64**, 012314 (2001).
- [38] M. W. Mitchell C. W. Ellenor, S. Schneider, and A. M. Steinberg, *Phys. Rev. Lett.* **91**, 120402 (2003).
- [39] J. B. Altepeter et al., *Phys. Rev. Lett.* **90**, 193601 (2003).
- [40] Z.-W. Wang, Y.-S. Zhang, Y.-F. Huang, X.-F. Ren, and G.-C. Guo, *Phys. Rev. A* **75**, 044304 (2007).

第六章 总结与展望

量子信息科学是一门交叉学科，是经典信息学和量子力学相结合的产物。它的最大特点是一量子态作为信息载体，量子态演化作为信息的传输，量子态测量作为信息的探测。由于量子力学的规律不同于经典物理，这就导致量子信息过程具备了许多经典信息过程所没有的特性。科学家们利用这些特性，发现了量子保密通信技术、量子并行加速算法和量子密码学。这些理论和技术的诞生，为未来的信息科学技术勾画出了一幅迷人的蓝图。

单光子多比特体系是线性光学方法研究量子信息问题的基本内容之一。常见编码光子比特的有光子偏振、光子空间动量和光子轨道角动量，而光子空间动量和光子角动量可以用来编码高维体系 (qudit)。单光子多比特体系可以用来很好的研究量子态的叠加性质，也是向多体、高维推广的基础。我们在实验上利用单光子多比特体系，研究了量子随机行走算法，量子博弈问题和单比特量子态操作完美区分。

计算全息片是目前应用最为广泛的产生高阶模式激光的器件。我们掌握了计算全息片的制作工艺，经过长期实践摸索，已经能够得到衍射效率 40%左右的计算全息片，达到了国际水平。基于这种全息片，我们巧妙的应用了光子轨道角动量的高维特性，在实验上实现了光子在轨道角动量空间的随机行走。这种方案实现的量子随机行走，能够很大程度的减少光学元件随行走步数增加而增多的速度，有利于实现更多步数的随机行走。

在量子赌博机的实验中，我们巧妙的应用了两块双折射晶体作为干涉的两个偏振分束器，实现了 Mach-Zehnder (M-Z) 干涉仪的无反馈长时间稳定。由于双折射晶体的天然特性，使得 M-Z 干涉仪只需用到两块双折射晶体和一块半波片便可以实现。我们实验上测得这种 M-Z 干涉仪的稳定时间可以长达 1 小时左右，这种长时间的稳定为我们测量量子赌博的多种方案输入提供了保证。在实验上，我们选择了 5 组方案的输入，

每一组输入使用 8 组方案进行探测，用实验数据证明的量子赌博中两体博弈的最佳方案。

量子么正操作的完美区分在理论上已经取得了巨大的突破，实验上，由于两比特甚至多比特门的实验难度，我们选择了单比特么正操作进行区分。单比特么正操作在光学体系中可以用一组波片（两个 $\lambda/4$ 波片中间夹一半波片）实现。我们在实验上分别采用了并行区分方案和串行区分方案对两组么正操作进行了区分，实验上证明了这两种方案的正确性和可行性。并通过实验的具体情况对两种方案进行了比较，讨论了推广么正操作完美区分的实验设想。

单光子多比特体系是光学系统研究量子信息过程的基础，可以通过多比特系统实现量子的控制非门、量子 Deutsch 算法等更为复杂的问题，也可以作为研究多比特高维度问题、多光子纠缠研究的出发点。这里面仍然存在的很多问题需要我们去探索研究。

附录

计算全息片的制作

计算全息片在研究光的高阶模式和光子轨道角动量中有着广泛的应用。其制作方法有很多种。下面我们介绍一种既经济简单，又具有较高效率的全息片制作工艺。主要过程如下：

1. 计算全息片透射函数，即光栅条纹函数。

透射函数的理论计算方法在第二章中已经介绍，实际制作中，需要将此函数编写成应用绘图程序。我们使用 Delphi 语言编写能产生高像素（ 4096×2732 ）图像的透射函数软件，将各种全息片透射条纹图片通过此程序生成。整个程序就是在生成一个全息片条纹的灰度图，条纹周期和像素大小可以通过程序来控制。

2. 将计算得到的图片记录在照相底片上。

有了通过程序产生的全息片条纹灰度图，通过刻录仪器（Agfa Slide Writer； $35\text{mm} \times 23\text{mm}$ 面积上 4096×2732 像素）将图片的信息记录在照相底片上。照相底片的最佳选择是 Kodak Ektachrome Professional 100 彩色反转底片。另外一种常见的方法是用激光投影条纹花样到照相底片上，这种方法和使用 Slide Writer 相比，缺点是操作麻烦，而且投影出来的条纹灰度与实际的相反。

3. 将照相底片上的信息转移到全息干板上

照相底片上的信息是条纹的灰度图，而真正要得到的光栅则是根据灰度获得立体的光栅条纹。一种简单得的方法便是用全息干板获得光栅。我们使用的全息干板是由 Edmund Scientific 公司生产的，光源使用白光源。曝光时间根据光源的情况确定，但是需要精确控制曝光时间，因为这个环节对全息片的衍射效率影响最大。接下来要对曝光的全息干板进行显影定影和漂白，这三个环节也直接影响到全息片的衍射效率。通过 J. Arlt 等人的经验以及我们多次的实验测试，全息光栅的制作流程和各种溶液的配方列在下方：

制作过程：

- | | |
|-----------------|---|
| 1 曝光 | $2500 - 3000 \mu\text{J} / \text{cm}^2$ |
| 2 坚膜 (Hardener) | 6min |

3 冲洗(水)	1-2min
4 显影 (VRP)	4-5min
5 冲洗(水)	1-2min
6 漂白 (PBU—Amidol)	5-8min
7 冲洗(水)	1-2min
8 停显 (Stop Bath)	2min
9 冲洗(水)	1-2min
10 定影 (Wetting agent)	1min
11 干燥	

配方:

Hardener

福尔马林 (Formalin 37 %)	10ml
溴化钾 (Potassium Bromide)	2g
碳酸钠 (Sodium Carbonate)	5g
水	to 1L

VRP

亚硫酸钠 (Sodium Sulphite)	194g
对苯二酚 (Hydroquinone)	25g
氢氧化钾 (Potassium Hydroxide)	22g
菲尼酮 (Methyl Phenidone)	1.5g
溴化钾 (Potassium Bromide)	20g
偏硼酸钾 (Potassium Metaborate)	140g
苯并三唑 (1,2,3-Benzotriazole)	0.1g
水	to 1L

PBU-Amidol

过硫酸钾 (<i>Potassium Persulphate</i>)	10g
柠檬酸 (<i>Citric Acid</i>)	50g
溴化铜 (<i>Cupric Bromide</i>)	1.0g
溴化钾 (<i>Potassium Bromide</i>)	20g
亚米多尔 (<i>Amidol</i>)	1.0g
水	to 1L

Stop Bath

醋酸 (<i>Acetic Acid</i>)	20g
水	to 1L

整个过程，控制温度稳定保持在 20 度非常的关键。

通过以上的过程，全息干板上便记录了计算所得全息光栅的立体透射条纹，这时候当一束高斯光束正入射在其中心分叉位置，全息光栅后面的衍射正一级便出现设计所需的高阶模式光。我们使用 He-Ne 激光器 (632.8nm) 对全息片的衍射效率进行了测定，正一级最高衍射效率可达 40%。虽然理论的效率可以到达 100%，但是通过全息照相技术获得的光栅不可能达到这样的理论值，40%的衍射效率已经是这种方法目前国际报道的最好效率。

在读期间发表的学术论文与取得的研究成果

已发表论文:

- [1] **Pei Zhang**, Xi-Feng Ren, Xu-Bo Zou, Bi-Heng Liu, Yun-Feng Huang and Guang-Can Guo, *Demonstration of one-dimensional quantum random walks using orbital angular momentum of photons*. **Phys. Rev. A**, **75**, 052310 (2007).
- [2] **Pei Zhang**, Yong-Sheng Zhang, Yun-Feng Huang, Liang Peng, Chuan-Feng Li and Guang-Can Guo, *Optical Realization of Quantum Gambling Machine*. **Euro. Phys. Lett.** **82**, 30002 (2008).
- [3] Xi-Feng Ren, Guo-Ping Guo, **Pei Zhang**, Yun-Feng Huang, Zhi-Wei Wang and Guang-Can Guo, *Removal of surface plasmon eigenmodes degeneracy*, **Appl. Phys. B** **89**, 257–260 (2007).
- [4] Guo-Yong Xiang, Yun-Feng Huang, Fang-Wen Sun, **Pei Zhang**, Ze-Yu Ou and Guang-Can Guo, *Demonstration of Temporal Distinguishability in a Four-Photon State and a Six-Photon State*, **Phys. Rev. Lett.** **97**, 023604 (2006).
- [5] Zhi-Wei Wang, Jian Li, Yun-Feng Huang, Yong-Sheng Zhang, Xi-Feng Ren, **Pei Zhang** and Guang-Can Guo, *Linear Optical Implementation of a Quantum Network for Quantum Estimation*, **Phys. Lett. A** **372**, 106-109 (2008).

待发表论文:

- [1] **Pei Zhang**, Liang Peng, Zhi-Wei Wang, Bi-Heng Liu, Yun-Feng Huang, Xi-Feng Ren and Guang-Can Guo, *Linear-Optical Implementation of Perfect Discrimination between Single-bit Unitary Operations*, **Submitted**;
- [2] **Pei Zhang**, Zhi-Wei Wang, Yun-Feng Huang, Bi-Heng Liu, Xi-Feng Ren and Guang-Can Guo, *Linear-Optical Implementation of Quantum Deutsch's Algorithm*, **in preparing**;
- [3] Xi-Feng Ren, **Pei Zhang**, Guo-Ping Guo, Yun-Feng Huang, Zhi-Wei Wang and Guang-Can Guo, *Properties of subwavelength hole arrays consisting of rectangular holes*, **Accepted by Appl. Phys. B**;
- [4] Xi-Feng Ren, Guo-Ping Guo, **Pei Zhang**, Yun-Feng Huang, Zhi-Wei Wang and

Guang-Can Guo, *Remote control of surface plasmon assisted transmission*,
Submitted;

- [5] Xi-Feng Ren, Guo-Ping Guo, Yun-Feng Huang, Zhi-Wei Wang, **Pei Zhang** and
Guang-Can Guo, *Interference of surface plasmon polaritions controlled by the
phase of incident light*, **Accepted by Appl. Phys. Lett.**

致 谢

在论文完成之际，谨向我的导师——郭光灿教授表示由衷的感谢。郭老师五年来对我工作上的悉心指导和生活上的关心帮助，使我得以顺利完成这篇论文。导师渊博的学识、敏锐的物理直觉、富有创新的科研思想以及善于抓住问题的物理本质的做法无不给我留下了深刻的印象，使我终身受益。此外，导师善于引导学生选择研究课题，却从不强制，在学术讨论中常常鼓励学生的创新想法，这种作风也使我受益非浅。在生活方面，导师也给予我极大的关心和帮助，在此再一次向导师表示我衷心的感谢。

我特别感谢黄运锋博士，他指导并帮助我完成了一系列实验工作。他开拓创新、锲而不舍的科研精神，勤勉积极的工作态度，都给我以巨大的启发，也是我学习的榜样。黄运锋博士从课题的讨论到论文的写作和修改都给了我许多具体的指导。在此向李剑博士表示衷心的感谢。

我对实验室的邹旭波教授、张永生博士和任希峰博士也表示衷心的感谢。感谢他们在理论和实验工作上给我的巨大帮助和无私的指导。

感谢量子信息重点实验室这个良好的学术团体，她是一个充满良好学术氛围的，互助友爱的集体。感谢五年来在实验室共同学习和生活过的所有老师和同学。他们是：韩正甫老师、李剑老师、周正威老师、郭国平老师、史保森老师、项国勇博士、孙方稳博士、柳必恒博士和研究生：王志伟，龚彦晓，牛孝灵，彭亮，黄建发等，以及实验室其他的博士生和硕士生同学。

在此我还要感谢实验室的叶淮老师、王涛老师和段开敏老师，几位老师在实验室的后勤、行政工作方面提供了热情、周到的工作保障，使得实验工作能够顺利进行。而且在生活方面，几位老师也给予我极大的关心和帮助，在此再次表示感谢。

最后，我要感谢家人、女友以及我所有的朋友对我学业上的大力支持、鼓励和关怀，使我得以顺利完成学业，继续攀登科学高峰。

张沛

二零零八年四月