研究快讯

量子态的概率克隆和认证*

段路明　郭光灿

(中国科学技术大学物理系及非线性中心　合肥　230026)

摘　要　随机地选自一组非正交的量子态不可能通过幺正过程精确克隆.但是如果把幺正演化和选择性测量过程结合起来,则可以以一定的概率精确地克隆上述输入态.文章简述了概率克隆研究的最新进展,并指出它和量子态认证之间的密切联系.

关键词　概率量子克隆,量子态认证,幺正-坍缩过程

PROBABILISTIC CLONING AND IDENTIFICATION OF QUANTUM STATES

Duan Luming　Guo Guangcan

(*Physics Department and Nonlinear Science Center, University of Science and Technology of China, Hefei* 230026)

Abstract　Nonorthogonal quantum states cannot be faithfully cloned by a unitary evolution. However, a combination of the unitary evolution together with a measurement can yield faithful copies of nonorthogonal input states, with a postselection of the measurement results. We trace recent advances in the field of probabilistic quantum cloning, and point out its close connection with the problem of identification of a set of states.

Key words　probabilistic quantum cloning, identification of quantum states, unitary-reduction process

“克隆”一词现在已家喻户晓,而量子克隆指的是通过一定的物理过程,产生未知输入态的两份或多份复制(输入量子态在此过程中被破坏).量子克隆在新兴的量子信息论中具有重要应用[1],例如它可应用于量子密码的接收和窃听.量子力学中有一个很基本的定理,即量子态不可克隆定理[2],该定理有着两个不同的版本.早在1982年,Wootters 和 Zurek 就首次提出量子态不可克隆定理,其含义是指,一个完全未知的量子态不可能通过任何量子过程精确克隆(精确克隆指输出是输入态的两份或多份精确复制),这里的量子过程既包括幺正演化,也包括了任意的测量[2].该定理的证明基于量子力学的线性和克隆过程之间的矛盾.后来,随着量子信息论的发展,人们感兴趣的量子态往往不再是完全未知的,而是已知它随机地选自一个确定的态集合$\{|\psi_1\rangle,|\psi_2\rangle,\cdots,|\psi_n\rangle\}$.在这种情况下,量子态是否可以精确克隆呢?在1986年,Yuen 首先考虑了这个问题,他发现,当量子过程限定为幺正演化时,一个随机选自确定态集合的量子态被精确克隆的充要条件是该集合中所有量子态相互之间正交[3].这一定理遗留下这样一个问题,如果我们的克隆机器

* 国家自然科学基金资助项目

1998-11-23 收到初稿,1999-03-08 修回

不限定为幺正演化,它是否能够精确克隆一个从非正交态集合中随机选出的量子态呢?我们最先考虑了这个问题,并发现,幺正演化和选择性测量过程结合起来,确实可以以一定的概率产生从非正交集合中随机选出的输入态的精确复制[4].这里,概率克隆的含义是指,我们的测量结果可分为两类,一类结果为"成功",另一类结果为"失败",当测量结果为"成功"时,我们就确知该过程已产生了输入态的精确复制态,反之,若测量结果为"失败",机器的输出态就不是输入态的复制态,我们抛弃该输出态.我们要求机器成功地克隆输入态的概率大于零,并希望它尽可能大.

这里有必要强调一下概率克隆和近来文献中研究得较多的非精确克隆之间的区别[5,6].实际上,概率克隆和非精确克隆可以看作是量子态不可克隆定理朝两个不同方向的发展.既然从一组非正交态中随机选出的态不可能通过幺正演化精确克隆,那么在非精确克隆中,人们就放松要求,允许输入态和输出态之间存在差别,但希望该差别尽可能小.因此,一个用于非精确克隆的机器对于每个输入态都能产生输出,但是对从非正交态集合随机选出的量子态,其输出与输入之间总存在差别.与此不同的是,概率克隆机的输出一定是输入态的精确复制态,但对于非正交态,有时候机器没有输出(对应于测量结果为"失败"的情况).

我们的主要结果包括在下面的四条定理中[7].

定理1:设$|\ \Psi_i\rangle$随机地选自一个已知的确定态集合$\{|\ \Psi_1\rangle,|\ \Psi_2\rangle,\cdots,|\ \Psi_n\rangle\}$,则$|\ \Psi_i\rangle$可以以大于零的概率精确克隆的充要条件为$|\ \Psi_1\rangle,|\ \Psi_2\rangle,\cdots,|\ \Psi_n\rangle$线性无关.

这条定理说明线性无关性刻画了能被概率克隆的量子态集合的特征,正如在原来的量子态不可克隆定理中,正交性刻画了能被幺正克隆的量子态集合的特征.对于不同的输入态,概率克隆成功的概率可以不同.我们希望概率克隆成功的概率尽可能大,最大的成功概率由下面的一条定理决定.

定理2:量子态$|\ \Psi_1\rangle,|\ \Psi_2\rangle,\cdots,|\ \Psi_n\rangle$可以分别以概率$\eta_1,\eta_2,\cdots,\eta_n$精确克隆的充要条件为$n\times n$的矩阵$X^{(1)}-\sqrt{\Gamma}X^{(2)}\sqrt{\Gamma}$半正定.

定理2中,$\Gamma=\mathrm{diag}(\eta_1,\eta_2,\cdots,\eta_n)$是个$n\times n$的对角矩阵,称为概率克隆机的效率矩阵.$n\times n$的矩阵$X^{(m)}$称为$m$阶内积矩阵,它的$(i,j)$矩阵元为$\langle\Psi_i|\ \Psi_j\rangle^m$,$X^{(1)}$,$X^{(2)}$分别对应于$m=1,2$的情形.矩阵$X^{(1)}-\sqrt{\Gamma}X^{(2)}\sqrt{\Gamma}$的半正定性给出了成功概率$\eta_1,\eta_2,\cdots,\eta_n$的一组不等式,这组不等式决定了最佳的成功概率.

以上考虑的概率克隆实际上指的是$1\to2$的克隆,亦即,对于随机选择的输入态,克隆机产生输入态的两份精确复制(原态毁坏).类似地,我们也可以考虑$1\to m$甚至$1\to\infty$的概率克隆.一个$1\to m$的概率克隆机以一定的概率产生输入态的m份精确复制.显然,m越大,复制的份数越多,我们就能得到未知输入态更多的信息,$m=\infty$意味着该输入态已被完全确定.我们发现概率克隆与量子态的认证之间有着密切的联系.量子态的认证指的是这样一种测量[8]:对于n种可能的输入态,该测量有着$n+1$种可能的测量结果$1,2,\cdots,n+1$.其中测量结果为$i(i=1,2,\cdots,n)$,表示可以唯一地确定输入态为$|\ \Psi_i\rangle$;若测量结果为$n+1$,则表示我们不能确定输入态是n种可能态中的哪一个,此时认证测量失败.我们希望认证成功的概率尽可能大.量子态认证在量子密码术中有着重要应用[9].量子态的认证与$1\to\infty$的概率克隆可按如下方式联系起来:一方面,如果我们得到了输入态的无穷份复制,则我们可以唯一地确定该量子态;另一方面,如果我们确定了输入态是n种可能态中的哪一个,我们当然可以精确复制它无穷多份.通过这种联系,我们给出了对n种可能的量子态进行认证所能达到的最大成功概率.下面的两条定理描述了$1\to m$的概率克隆和量子态的认证.

定理3:量子态$|\ \Psi_1\rangle,|\ \Psi_2\rangle,\cdots,|\ \Psi_n\rangle$可以

(下转第606页)