讲　座

量子信息讲座续讲
第四讲　量子对策论*

张永生　　李传锋　　郭光灿

(中国科学技术大学物理系　量子通信与量子计算开放实验室　合肥　230026)

摘　要　　量子对策论是量子信息学的新兴分支,是经典对策论与量子信息学两门学科的交叉学科.由于引入了量子力学中的量子叠加性和纠缠态,量子对策得出了与经典对策迥然不同的结果.

关键词　　量子对策论,量子信息论,对策论

QUANTUM　GAME　THEORY

ZHANG Yong-Sheng　　LI Chuan-Feng　　GUO Guang-Can

(*Laboratory of Quantum Communication & Quantum Computation, Department of Physics, University of Science & Technology of China, Hefei* 230026)

Abstract　　Quantum game theory is a new branch of the quantum information theory. It develops as the combination of the classical game theory and the quantum information theory. Because superposition and entanglement are introduced from quantum mechanics, the quantum game theory will get many new results, which are very different with the classical counterparts.

Key words　　quantum game theory, quantum information theory, game theory

1　对策量子化

在自然界和人类社会中,存在着大量的具有对抗或竞争性质的现象.对策论(game theory)亦称博弈论,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,这门具有悠久历史的学科直到本世纪初才作为数学的一个重要分支被系统地研究,其奠基之作就是J.von Neumann和O.Morgenstern合著的《博弈论和经济行为》.由于这门学科研究的现象与人们的政治、经济、军事活动以及生物进化、生态竞争等有着密切联系,所以引起越来越广泛的注意[1,2].

从抽象的意义上讲,对策论研究的是对抗或竞争各方采取某些策略,去最大化或最小化某些特定的函数.物理学家受到量子信息其他领域如量子计算、量子密码的启发,很自然地要考虑:如果对策拓展到量子领域,即允许存在策略的线性叠加和纠缠,会得出什么结果.J.Eisert, M.Wilkens和M.Lewenstein指出[3]:将对策量子化有以下几个重要意义.首先,目前被广泛应用的经典对策论是建立在经典概率论基础上的,如果将此基础扩展到量子概率(幅),应当会出现一些有趣的现象.再者,对策量子化很可能会有助于研究基因竞争,即分子层次上的竞争现象.还有,量子通信及量子密码就可以作为一种量子对策来研究:通信的各方与窃听者对抗,对抗双方可以采用量子及经典策略.另外,对策量子化还可以带来一些有趣的小游戏[4].

我们将分别通过介绍目前已经量子化的几个例子,来看一下量子对策的内容、方法及一些结果.

2　PQ翻硬币问题[5]

代号为P和Q的两个人进行这样一个游戏:P

* 　国家自然科学基金资助项目
2000-06-16收到

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(见表1).表1 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1中的数字表示 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(H表示正面朝上,T表示反面朝上,下同)所以这一局 P 赢.

表1

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

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[2],任何一个有限策略的零和对策,总存在概率解,即混合策略.在 PQ 翻硬币问题中,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收益期望值.

本游戏的主人公之一 P 用概率论分析得到以上结果后,发现这游戏还算公平,就答应与 Q 玩这一游戏,可是结果每次都输,原因何在?

其中奥妙就在于 Q 没有按上面的分析每次混合使用策略 N, F.在经典情况下,硬币状态集为$\{H, T\}$,Q 可采取混合策略 $\frac{1}{2}\begin{vmatrix}1 & 1\\1 & 1\end{vmatrix}\begin{vmatrix}H\\T\end{vmatrix}$,即无论硬币处于 H 还是 T 状态,都以 1/2 的概率翻或者不翻.在量子领域,硬币状态集为$\{|H\rangle, |T\rangle\}$,Q 就可以使用量子策略,即把这两种策略叠加起来,使用 $\frac{1}{\sqrt{2}}\begin{vmatrix}1 & 1\\1 & -1\end{vmatrix}\begin{vmatrix}|H\rangle\\|T\rangle\end{vmatrix}$ 策略.这样就把硬币从$|H\rangle$态变为叠加态 $\frac{1}{\sqrt{2}}\left|\,|H\rangle+|T\rangle\right|$,无论 P 翻($|H\rangle$变为$|T\rangle$,$|T\rangle$变为$|H\rangle$)还是不翻,硬币还是保持这一状态不变.然后,Q 再使用一次 $\frac{1}{\sqrt{2}}\begin{vmatrix}1 & 1\\1 & -1\end{vmatrix}$ 策略,硬币状态就变为$|H\rangle$,所以 Q 必赢无疑.

PQ 翻硬币问题是一个很简单的问题.但是许多重要问题都与此类似,例如著名的 Grover 算法[6].Grover 算法的任务是要在一个规模假设为 N 的大型数据库里搜寻某个指定的记录.不妨把数据库与搜寻者看作对弈双方,数据库随机放置了一个记录,搜寻者如果用经典方法搜寻,平均要搜索 $N/2$ 次,而利用量子策略,即利用叠加性和幺正变换,则平均用 $\sqrt{N}$ 这一量级的搜索次数.

经过分析,D.A.Meyer 提出并证明了以下三个定理[5].

定理一:在二人零和对策中的对弈者,使用最优量子策略的收益期望值不低于使用最优经典混合策略的收益期望值(证明:因为经典混合策略都可以找到一个量子策略来表示).

定理二:二人零和对策中并不一定存在双方都采用单纯量子策略的平衡点.

定理三:二人零和对策中总存在双方均采取混合(或单纯)量子策略的平衡点.

3 量子博弈

第二个例子是 L.Goldenberg 等提出的量子博弈[4].赌博中有这样一个常见的游戏:艾丽丝随机地往两个盒子中的一个放一枚硬币(放进两个盒子的几率相等).鲍博选中一个盒子,当鲍博打开这个盒子,如果有硬币,鲍博赢(简单起见,假设赢一个硬币),否则鲍博输一个硬币.但是在经典情况下,鲍博不易检验艾丽丝是否按几率 $\frac{1}{2}:\frac{1}{2}$ 往盒子里放硬币,尤其在对弈次数较少的时候.但是这一游戏量子化后可以做到这一点,而且还可以进行远程对弈.

量子化后的这一游戏框架如下:艾丽丝有两个盒子 A 和 B 用来放一个粒子.粒子在 A 盒子或 B 盒子的状态用$|a\rangle$及$|b\rangle$来表示.艾丽丝把粒子制备到某个态上,然后将盒子 B 发送给鲍博.在下列两种情况下鲍博赢:(1)如果他发现粒子在 B 盒子里,艾丽丝检查确信粒子不在 A 盒子里,付给鲍博一个硬币;(2)鲍博要求艾丽丝把 A 盒子发送过来,检验到艾丽丝最初制备的态不是 $|\Phi_0\rangle=\frac{1}{\sqrt{2}}(|a\rangle+|b\rangle)$,那么艾丽丝就要付给鲍博 R(R 为两人事先约定的数值)个硬币.其他情况下,艾丽丝赢,鲍博付给艾

丽丝一个硬币.

艾丽丝的策略就是将粒子制备到$|\Phi_0\rangle$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,艾丽丝就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$|\Phi_0\rangle$的态$|\Phi_1\rangle = \alpha|a\rangle + \beta|b\rangle$上,这样就有可能被鲍博发现从而受罚损失$R$个硬币.

鲍博的策略是收到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:

$$|b\rangle = \sqrt{1-\eta}|b\rangle + \sqrt{\eta}|b'\rangle, \qquad (1)$$

这里$|b\rangle$,$|b'\rangle$正交.这就好像把粒子在B盒子的态不破坏地分成两部分,在这里分裂参数η依赖于惩罚参数R.在完成态分裂操作后,鲍博做态$|b\rangle$的投影测量,即查看盒子B里有没有艾丽丝放置的粒子.如果鲍博发现了粒子,鲍博赢了这一局.否则,鲍博向艾丽丝索要A盒子用来检验:他可以用A盒子和留下来的$|b'\rangle$来做联合测量,即看一下粒子是否处在$|a\rangle + \sqrt{\eta}|b'\rangle$态(忽略归一化因子)上,就可以以一定的概率判断出艾丽丝是否作弊.

这一量子化结果在实验上如果用一般的粒子(如原子及离子)来实现是比较困难的事情.我们课题组发现如果利用光子,在现有技术下完全能够实现.我们的实验方案是利用光子经过分束器的路径来代表A,B两个盒子,利用光子的偏振来区别$|b\rangle$,$|b'\rangle$.而且(1)式中的变换即光子偏振的旋转,以及光子偏振或路径态的测量都比较容易实现.具体实验方案及结果见文献[7].

4 量子“囚徒怪圈”

第三个例子是两量子比特的对策,称作量子“囚徒怪圈”.在经典对策“囚徒怪圈”中的两个局中人(假设为艾丽丝和鲍博)面临着这样的局面:艾丽丝与鲍博这两个囚徒被抓起来,如果双方合作,都不向司法部门提供对方的犯罪证据,司法部门会因为证据较少各判他们三年有期徒刑;如果双方对抗,都向司法部门提供对方的犯罪证据,双方会都被判五年;若一方提供对方的证据而另一方不提供对方的证据,提供方立功被判一年,另一方被判七年.这一对局可以用表2中的数值表示(数值大表明被判刑时间短,即收益大,数值小则被判刑时间长,收益小).

在这张策略-收益表格中,括号内前面的数值为艾丽丝的收益而后者为鲍博的收益.从表2可以看出,对任何参加者来说,无论对方采用什么策略,

表2

		Bob(鲍博)	
		C(合作)	D(对抗)
Alice (艾丽丝)	C(合作)	(3,3)	(0,5)
	D(对抗)	(5,0)	(1,1)

自己采用D(对抗)策略要比C(合作)策略好,即主动提供对方犯罪证据要比顽抗好.这样双方就找到了平衡点D:D.我们从表2还可以看出,如果艾丽丝双方能够合作,其结果要比双方对抗更为有利,但是在双方都独立地追求自己的最大利益的情况下,却得到比较差的结果D:D,这就是所谓囚徒怪圈.

量子化后的这一模型将策略C,D用量子比特$|C\rangle$,$|D\rangle$表示,模型见图1.

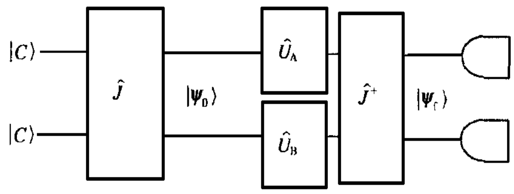

图1 “囚徒怪圈”量子化模型

对弈的初态为$|\Phi_0\rangle = \hat{J}|CC\rangle$($\hat{J}$是一个特定的幺正变换).接着艾丽丝和鲍博分别对分给自己的那一部分态做局域幺正变换.然后系统再做一次反变换$\hat{J}^+$,输出态即为$|\Phi_f\rangle = \hat{J}^+ |\hat{U}_A \otimes \hat{U}_B| \hat{J}|CC\rangle$.最后对末态做$|C\rangle$,$|D\rangle$正交测量,收益取决于测量结果,例如,艾丽丝的收益期望值即为

$$\$_A = rP_{CC} + pP_{DD} + tP_{DC} + sP_{CD}, \qquad (2)$$

这里$P_{\sigma\sigma'}$即测量得到$\sigma\sigma'$的概率.在文献[3]的第一篇文章中,该文作者分析了当艾丽丝和鲍博的幺正变换限制为如下的形式

$$\hat{U}(\theta,\phi) = \begin{vmatrix} e^{i\phi}\cos\theta/2 & \sin\theta/2 \\ -\sin\theta/2 & e^{-i\phi}\cos\theta/2 \end{vmatrix} \qquad (3)$$

时,双方存在平衡策略:$\hat{Q} = \hat{U}(0,\pi/2)$.双方均采取平衡策略时,收益都为3.参考文献[3]中后面的文章对一般幺正变换作了进一步探讨,发现不存在单纯量子策略构成的平衡点,双方都要采用混合量子策略.在以上两种情况下,双方的收益期望值都优于经典对策平衡点处的收益(1,1).

5 结语

目前已经提出的量子对策模型主要是以上三

(下转第731页)