

量子拜占庭协议中的纠缠态探测

武霞, 贾恒越, 朱建明

(中央财经大学信息学院, 北京 100081)

摘要: 在分布式计算系统中, 拜占庭协议是解决其容错问题的一种实用方法。拜占庭问题有一种演变形式, 称之为检测的拜占庭协议。这类协议在经典世界中无法解决容错问题, 但在量子系统中利用纠缠态却可以。GBKCW 协议是一种典型的量子检测拜占庭协议。针对 GBKCW 协议中数据列表的生成和分发部分, 利用量子纠缠态的确定性, 探测了参与者共享的量子态, 以抵御针对 GBKCW 的截获重发攻击。

关键词: 检测的拜占庭协议; GBKCW 协议; 量子系统; 纠缠态的确定性

中图分类号: TP309.7

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00110

Entangled state testing in the quantum Byzantine agreement

WU Xia, JIA Heng-yue, ZHU Jian-ming

(School of Information, Central University of Finance and Economics, Beijing 100081, China)

Abstract: In distributed computing, Byzantine agreement is a practical method to solve its fault-tolerance problem. There is a variation of the Byzantine agreement which is called detectable Byzantine agreement. This kind of protocol is unsolvable by classical means, but can be solved using quantum resources—quantum entangled states. A typical quantum detectable Byzantine agreement is the GBKCW protocol. The part with the generation and distribution of the lists in the GBKCW protocol was dealt with. In order to keep the GBKCW protocol from the intercept-and-resend strategy, the property of the determination of entangled states were employed to test the sharing state between the parties.

Key words: detectable Byzantine agreement, GBKCW protocol, quantum system, determination of entangled states

1 引言

在分布式计算系统中, 只有每一个组件都协调合作, 整个系统才能正常运行。但现实生活中, 分布式系统的某些组件出现问题的情况难以避免, 如有问题的组件可能发送无效或错误的信息给系统中其他的组件。如果这种情况发生, 那么将威胁系统的正常运作。而拜占庭协议^[1,2]就是一种

种解决分布式系统容错问题的实用的方法。

详细地说, 最简单的拜占庭问题具体可被描述如下^[3]。有 3 路拜占庭军队, 分散驻扎于敌军城外, 其中每一支军队都有一个将军, 称他们为 A、B、C。将军们彼此之间可以通信来传递消息, 他们想通过传递消息来达成一致的行动计划, 即攻击或撤退。指挥官将军 A 决定了一个计划, 并且将他的计划发送给了 B 和 C, 接下来 B 和 C 交换他

收稿日期: 2016-09-24; 修回日期: 2016-10-09。通信作者: 武霞, wuxiaqingdao@163.com

基金项目: 国家自然科学基金资助项目 (No.61309029, No.U1509214, No.61272398); 中央财经大学青年教师发展基金资助项目 (No.QJJ1633)

Foundation Items: The National Natural Science Foundation of China (No.61309029, No.U1509214, No.61272398), The Young Teachers Development Fund of Central University of Finance and Economics (No.QJJ1633)

们手中收到的消息, 来保证行动计划的一致性。然而在他们中可能有将军已经被敌军收买, 变成了叛徒 (包括指挥官 A), 他试图阻止所有诚实的将军们达成一致的行动计划。拜占庭问题是指设计满足下面 2 个条件的协议: 1) 所有诚实的将军们执行同一个计划; 2) 如果指挥官将军 A 是诚实的, 那么所有诚实的将军都遵守 A 所制定的行动计划。

3 个将军的拜占庭问题是无解的^[4, 5], 除非将军们事先分享某些合适的私人数据。即每个将军必须拥有不为其他将军所知的数字列表, 但这个数字列表还要与其他将军的数字列表有适当的关联关系。因此解决拜占庭问题可以简化为解决生成和安全分发这些列表的问题。然而, 无论在经典世界还是量子世界中, 都没有方法来保证所需要的数字列表分发成功。然而 3 个将军的拜占庭问题可以产生一类演化问题, 称之为检测的拜占庭协议或者检测广播^[3, 6-14], 这种条件放松后的拜占庭协议, 利用经典方法无法解决, 但是利用量子资源——量子纠缠态却可以。在检测的拜占庭协议中, 条件 1) 和 2) 放松为: 1') 所有诚实的将军要么执行相同的计划, 要么终止行动; 2') 如果 A 是诚实的, 那么每个诚实的将军要么遵守 A 所制定的计划, 要么终止行动。而达成这个协议, 所依赖的就是量子世界所独有的性质。

众所周知, 量子力学是 20 世纪物理学中最伟大的进展之一^[15, 16], 它能够解释许多经典物理所不能解释的现象^[17]。量子系统中, 存在一种被我们所熟知的量子态, 即量子纠缠态^[18]。量子力学不同于经典物理, 最神奇的特征就是量子纠缠, 纠缠反映了量子理论的本质。而与经典信息论中的信息资源截然不同, 纠缠是一种崭新的量子资源, 一些利用经典手段所不能实现的任务却可以利用纠缠来实现。因此利用量子纠缠可以实现许多令人惊叹的应用, 如单向量子计算^[19, 20]、量子密钥分发^[21, 22]、量子隐形传态^[23]。本文介绍的检测拜占庭协议, 也是量子纠缠态的一次非常完美的应用。

一般的量子检测的拜占庭协议包括 2 个部分。第一部分主要给 3 个将军生成和分配数据列表, 在这一部分中主要利用的就是量子纠缠态特殊的性质。这一部分最重要的是检测纠缠态, 即

3 个将军采取适当的方法, 来确认他们之间分配的量子纠缠态是协议第二部分中所用到的那个态。第二部分是协议的主体部分, 一旦 3 个将军拥有了各自的数字列表, 在协议的第二部分中, 他们利用这些数字列表, 并结合双向经典通信来达成一致行动。

由此可见, 分发和检测量子态在量子检测拜占庭协议中至关重要, 本文提出一种新的检测拜占庭协议中量子态的方法, 即利用量子纠缠态的确定性。

量子纠缠态的确定性问题, 是量子纠缠理论研究中最重要的问题之一^[24-29]。在这个问题中, 人们主要研究量子纠缠态与其子系统的约化密度矩阵之间的关联性质。简而言之, 对几乎所有的量子态, 它们都可以由其约化密度矩阵唯一确定。本文利用三体纠缠态可以由其两体约化密度矩阵所唯一确定的性质, 来讨论 GBKCW 协议第一部分有关量子态探测的问题。

2 准备知识

2.1 拜占庭将军问题

分布式计算的一个基本目标是: 即使在某些分布式进程失败的情况下, 分布式计算依旧能够进行。这要求无故障组件在收到受干扰信息的时候依旧能够达成一个一致性协议。解决这样任务的问题被简称为拜占庭将军问题, 也称为拜占庭协议。拜占庭协议简要描述如下。

有 3 路拜占庭军队包围了一座敌军城市, 每一路军队都由一个将军带领, 分别为 A、B、C。将军只能通过消息进行相互通信 (通过双方认证无错经典信道)。通过消息通信, 将军们必须决定一个一致的计划: 攻击, 用 0 表示; 撤退, 用 1 来表示。指挥官将军 A 决定了一个计划, 并且将他的计划传递给将军 B 和 C, 传递给将军 B 的消息记为 m_{AB} , 传递给将军 C 的消息记为 m_{AC} 。接下来, B 将其消息 m_{BC} 传递给 C 来进行行动计划的沟通, C 也将消息 m_{CB} 传递给将军 B。然而, 其中一个 (有且仅有一个) 将军 (包括 A) 有可能是叛徒, 试图阻止诚实的将军们达成同一个计划。对于诚实的将军 C 来说, 会出现下面 2 种情况。

1) 将军 B 是叛徒。指挥官 A 发给将军 B 和 C 同样的消息, $m_{AB}=m_{AC}=1$ 。B 收到消息后为了干扰将军 C, 他将 A 传来的消息进行了修改, 因此他传递给 C 的消息是 $m_{BC}=0$, 而 C 传递给 B 的消息是正确的, 即 $m_{CB}=m_{AC}=1$ 。在这种情况下, 可以看出将军 C 收到了 2 个互相矛盾的消息, 0 和 1。

2) 指挥官 A 是叛徒, 他发送给 B 的消息为 $m_{AB}=0$, 发送给 C 的是 $m_{AC}=1$ 。因为只能有一个叛徒, 此时将军 B 和 C 都是诚实的, B 把从 A 那里收到的消息发送给 C, $m_{BC}=m_{AB}=0$, C 传递给 B 的消息为 $m_{CB}=m_{AC}=1$ 。在这种情况下, 将军 C 又收到 2 个互相矛盾的消息, 0 和 1。

从上面的分析可以看出, 诚实的将军 C 根据自己手中所掌握的信息, 并不能判断到底 A 是叛徒还是 B 是叛徒。因为无论 A 和 B 哪个将军叛变, 对 C 来说, 得到的是同样的消息集合, 因此 C 无法找出叛徒到底是谁。在经典领域, 达成拜占庭协议允许的故障部件个数 (或叛徒个数) 为

$$t = \left\lfloor \frac{(n-1)}{3} \right\rfloor, \text{ 其中, } n \text{ 为将军的个数。}$$

本文主要讨论拜占庭问题的一类演变问题, 即检测的拜占庭问题, 这个问题在经典领域并没有解决办法, 而在量子领域, 存在利用量子纠缠态设计关联关系来探测拜占庭系统中叛徒的量子方法。为了探测叛徒, 系统可以容许最大数量的故障部件为 $t = \left\lfloor \frac{(n-1)}{2} \right\rfloor$, 其中, n 为将军的总数。

众所周知, 解决拜占庭问题可以简化为解决生成和安全分发数字列表的问题, 而根据量子力学的性质, 人们已经提出了多种生成和安全分发所需数字列表的方法。迄今为止, 这些方法有的基于三体三维单重量子态^[3], 有的基于四量子比特纠缠态^[6, 7, 9], 有的基于 3 个或者 2 个量子密钥分发信道^[12], 有的利用单体三维量子态^[10], 还有的利用 Hardy 争论问题^[11]。Hardy 争论反证了量子关联的一种局域隐变量描述, 它是没有不等式的 Bell 理论的一种形式。

本文主要讨论的是 GBKCW 协议中四量子比特纠缠态的一种新颖的探测方法, 即利用纠缠态的确定性。

2.2 量子纠缠态的确定性

量子纠缠理论主要研究纠缠的数学结构, 及其刻画、操纵和度量。人们试图从很多视角来理解多体量子纠缠态, 其中的一种方法就是将纠缠看成是整个量子态与其子系统之间的关联, 即从部分和整体的角度来看待量子纠缠。人们也称之为量子纠缠态的确定性。

详细地说, 给定多体量子纯态的一部分, 其中, 部分是指子系统的约化密度矩阵, 那么, 从部分中能够获得关于整个量子态什么样的信息? 这就是量子纠缠态的确定性问题。

在量子纠缠态的确定性问题中, 想要计算一个给定的 n 体量子态 $|\psi\rangle$, 到底可以被其几体约化密度矩阵的集合所唯一确定。给定一个 n 体量子态 $|\psi\rangle$, 很容易可以求出它的任意约化密度矩阵, 不妨设 $|\psi\rangle$ 的所有约化密度矩阵的集合为 R , 但是如果已知的是约化密度矩阵的子集 $R' \subset R$, 那么是不是还有其他的量子态 $|\psi'\rangle$, 其相应约化密度矩阵集合跟 R' 一致? 如果存在这样其他的量子态, 那么称 $|\psi\rangle$ 不能被 R' 所唯一确定; 反之, 则称 $|\psi\rangle$ 由 R' 所唯一确定, 并且 R' 称为 $|\psi\rangle$ 的确定集。

由于这个问题的解决与探究纠缠有密切的关系, 因此近 10 年来获得了很多关注, 并且取得了一些很好的结论。

对 GBKCW 协议中所描述的 3 个将军的量子检测拜占庭协议, 至关重要的一步是 3 个将军探测他们之间共享的到底是不是某个特定的四粒子纠缠态。而通过将军之间彼此将其拥有的量子比特传递给对方, 然后检测手中所具有的新的二体量子态, 最后与四粒子纠缠态相应二体量子态进行对比的方法, 提供一种新颖的量子态探测方式。在这之前, 需要首先回忆 GBKCW 协议中探测的拜占庭协议的第二部分, 然后再分析协议第一部分中纠缠态的探测问题。

3 检测的拜占庭协议

拜占庭问题已经被证明是不可解决的问题, 除非每个将军都有不被其他将军所知的数字列表, 并且自己拥有的数字列表与其他将军手中的列表之间有合适的关联关系。因此, 解决拜占庭问题可以简化为解决生成和安全分发这些列表的

问题。利用量子协议就能检测分发的安全性, 然而, 一旦有了攻击, 就没有可用的秘密列表, 并且整个通信必须终止。在这种情况下, 拜占庭协议有一种演变形式, 称之为检测的拜占庭或检测广播。在检测的拜占庭协议中, 需要满足下面 2 个新的条件: 1') 所有诚实的将军要么执行相同的计划, 要么终止行动; 2') 如果 A 是诚实的, 那么每个诚实的将军要么遵守 A 所指定的计划, 要么终止行动。这个协议在经典世界是不能完成的, 在量子领域却可以。而达成这个协议, 所依赖的就是量子世界所独有的性质。

GBK CW 协议中, 检测的拜占庭协议分为 2 个部分。第一部分的目标是利用一种特殊的四量子比特纠缠态的相关性质, 生成并且分发 3 个数据列表, 其中, A 手中的列表记为 l_A , B、C 手中的数据列表分别为 l_B 和 l_C 。一旦将军们手中有这些列表, 在协议的第二部分, 他们利用这些列表和双向经典通信来完成协议, 达成一致的计划或检测出说谎者。

详细地说, 列表 l_A 、 l_B 和 l_C 具有下面的性质。

性质 1 3 个列表长度相等。 l_A 中的元素是集合 $\{0, 1, 2\}$ 的任意一个元素。 l_B 和 l_C 的元素在比特 0, 1 中任意选取。

性质 2 在这些列表的第 j 位, 具有下面的关联关系: 000 (即 $l_{Aj} = 0, l_{Bj} = 0, l_{Cj} = 0$)、111 或等概率的 201 或 210。

性质 3 除了能从自己的列表中根据性质 1 和性质 2 所推断出的, 每个将军都不知道其他将军的列表内容。

例如, 如果将军 A 发现自己手中第 j 位的元素是 0, 即 $l_{Aj} = 0$, 那么根据 3 个将军之间列表的性质, 他可以推断出将军 B、C 相应位置上的元素也必定是 0。而如果 $l_{Aj} = 2$, 此时他推断不出 B、C 位置上的元素。对于将军 B 来说, 如果他发现 $l_{Bj} = 0$, 那么他只能推断出 $l_{Aj} = 0$ 或 $l_{Aj} = 2$, 而 l_{Cj} 等于 0 或 1。即此时他也无法判断别的将军手中的粒子是几。

为了简化协议第二部分的讨论, 本文只站在 C 的角度来分析, 因为 B 和 C 的角色是完全对称的, 因此本文对于将军 C 出现的情况, 完全适用于 B, 反之亦然。

协议部分如下。

1) 当指挥官 A 发送消息 m_{AB} (0 或 1) 时, 随之一起发送的还包括其他的数据, 这个数据必须与消息本身有关, 并且只为 A 所知。为了达成这个目的, A 同样发送一个数据列表 l_{AB} 给 B, 这个列表中包含 l_A 中出现比特 m_{AB} 的所有位置。之后如果 A 诚实, 他会遵守自己发送的计划。

举例来说, 假设

$$l_A = \{2, 0, 0, 1, 1, 2, 0, 1, 0, 2, 2\}$$

$$l_B = \{0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1\}$$

$$l_C = \{1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1\}$$

A 要发送消息 0。如果指挥官 A 诚实, 那么他会发送 $m_{AB} = m_{AC} = 0$, 同时发送 $l_{AB} = l_{AC} = \{2, 3, 8, 10\}$ 。

当 B 收到 m_{AB} 和 l_{AB} , 只会产生 2 个结果。

①若 l_{AB} 的长度合适 (根据性质 1, 可知 l_{AB} 长度大约是数据列表 l_A 的 $\frac{1}{3}$), 并且 m_{AB} 、 l_{AB} 和 l_B 确实满足性质 2, 那么此时称数据 (即 m_{AB} 、 l_{AB} 和 l_B) 一致。如果数据一致, 那么 B 将服从计划 m_{AB} , 除非在协议的下一步 2) 中, 将军 C 使他相信 A 是叛徒。

例如, 将军 B 收到 $m_{AB} = 0$, $l_{AB} = \{2, 3, 8, 10\}$, 他首先发现 l_{AB} 的长度合适, 为 4。接下来检查 l_B 中的比特在位置 l_{AB} 上确实都为 0, 此时数据一致。

②若 m_{AB} 、 l_{AB} 和 l_B 不一致, 那么 B 确认 A 是叛徒。B 将不采取任何行动, 直到在协议的下一步与 C 达成一致的计划。

例如, B 收到 $m_{AB} = 0$, $l_{AB} = \{2, 3, 7, 10\}$, 此时数据不一致。因为 A 在位置 7 不可能为 0。

2) B 将自己收到的数据传递给 C。消息 m_{BC} 不仅可以为 0 或者 1, 还可以为 “ $\perp$ ”, 表示 “我收到了不一致的数据”。而如果 B 收到的消息为 0 或者 1, 他发送给 C 其他的数据来表明 $m_{BC} = m_{AB}$ 。为了这个目的, B 同样发送一个列表 l_{BC} 给 C, 并且声称这与从 A 处收到的 l_{AB} 一样。

当 C 收到来自 B 的 m_{BC} 、 l_{BC} 或者 “ $\perp$ ”, 他手头早已收到来自 A 的 m_{AC} 和 l_{AC} 。接下来, 罗列在 C 手中的信息到底会出现多少种可能。

对于来自 A 的信息, 只有 2 种可能情况。

①A₁: m_{AC} 、 l_{AC} 、 l_C 一致。

②A₂: m_{AC} 、 l_{AC} 、 l_C 不一致, 即 “ $\perp$ ”。

对于来自 B 的信息,有以下 4 种情况。

①B₁: m_{BC} 、 l_{BC} 、 l_C 一致,且 $m_{BC} = m_{AC}$ 。

②B₂: m_{BC} 、 l_{BC} 、 l_C 一致,且 $m_{BC} \neq m_{AC}$ 。

③B₃: “ $\perp$ ”,即 B 告诉 C,他已经知道 A 是叛徒。

④B₄: m_{BC} 、 l_{BC} 、 l_C 不一致。

下面对以上情况进行排列组合。

如果 C 手中的信息是 A₁B₁,此时没有叛徒,3 个将军达成了相同的行动计划, C 服从计划 $m_{AC} = m_{BC}$ 。

如果 C 手中的信息是 A₁B₂,那么 C 可以断定指挥官 A 是叛徒,他只需执行事先与 B 商定好的行动计划。这是因为 A 是唯一能够发送一致数据给 B 和 C 的人。

如果 C 手中的信息是 A₁B₃,那么 C 服从计划 m_{AC} 。在这种情况下, B 并没有任何办法说服 C,他从 A 处确实收到了不一致的信息。

如果 C 手中的信息是 A₁B₄,那么 C 确认 B 为叛徒,他执行计划 m_{AC} 。这是因为 C 没有收到“ $\perp$ ”,这说明在 B 手中 m_{AB} 、 l_{AB} 和 l_B 一致。如果 B 诚实,他必定发送 $m_{BC} = m_{AB}$, $l_{BC} = l_{AB}$ 到 C 处,此时 m_{BC} 、 l_{BC} 、 l_C 必定也一致。

如果 C 手中的信息是 A₂B₁ 或 A₂B₂,此时 A 是叛徒,他们服从计划 m_{BC} 。

如果 C 手中的信息是 A₂B₃,那么 B 和 C 都知道 A 是叛徒,他们只需执行事先定好的计划。

C 手中的信息是 A₂B₄ 这种情况,是不可能出现的。

这就是 GBKCW 协议的第二部分。而要执行这个协议的前提,就是数据列表的分发。在 GBKCW 协议中,给出了数据列表的生成和分发方法,但是存在很严重的漏洞,并且很快被 Gao 等^[6]利用截获一重发攻击所击破。在 GBKCW 协议给出的数据列表的分发方法中,利用截获重发攻击,叛徒能够控制接下来协议的整个第二部分,他可以达到完美的欺骗,而不被另外 2 个将军所察觉。

4 利用态的确定性方法探测纠缠态

在 GBKCW 协议的第一部分,是生成和分发具有性质 1、性质 2、性质 3 的数据列表。他所做的步骤是:首先有一个粒子源 S 制备并分发一类特殊的四量子比特纠缠态 $|\psi\rangle_{abcd}$,前 2 个粒子给将军 A,后 2 个粒子分别给 B 和 C;之后 A、B、

C 在 4 个粒子上分别做投影测量,如果都用相同的基进行测量,那么测量结果之间展现了性质 1、性质 2、性质 3 所需要的完美的关联关系;最后,3 个将军检测他们的测量结果是否展现了所要求的关联关系。

但这个协议有一个很大的漏洞。Gao 等^[6]提出,利用截获一重发攻击,不诚实的将军只需派 2 个手下截获一测量并重新将粒子源 S 发送给另外 2 个将军的粒子,那么不诚实的将军就很容易控制协议的第二部分。他可以在第二部分中的拜占庭协议中,很容易地达成完美欺骗,并且不为另外 2 个诚实的将军所察觉。

可以看到,叛徒能够这样做的根本原因是,2 个诚实的将军并不知道从粒子源 S 手中收到的粒子已经被进行了操作,他们以为自己手中拿到的粒子依旧是 $|\psi\rangle_{abcd}$ 中的粒子,而不知道中途已经被测量并重发过,即已经发生了改变。

为了抵抗这种攻击,可以在将军们收到 S 发来的粒子后、做投影测量之前,加上额外的一步,即探测 3 个将军之间的态依旧是 $|\psi\rangle_{abcd}$,没有被进行任何破坏。为了达到这个目的,利用量子纠缠态的确定性方法。

在本协议中,用到的四量子比特纠缠态 $|\psi\rangle_{abcd}$ 为

$$|\psi\rangle_{abcd} = \frac{1}{2\sqrt{3}}(2|0011\rangle + 2|1100\rangle - |0101\rangle - |0110\rangle - |1001\rangle - |1010\rangle)_{abcd} \quad (1)$$

为了介绍探测 $|\psi\rangle_{abcd}$ 的方法,首先来看一下 $|\psi\rangle_{abcd}$ 的确定集。

4.1 四量子纠缠态的确定集

本节主要证明 $|\psi\rangle_{abcd}$ 可以由其任意的 2 个两体约化密度矩阵所唯一确定。

在给出定理之前,先介绍密度矩阵的一些性质。如果 n 量子比特密度矩阵 $\rho_M = (r_{ij})_{n \times n}$,那么有下面的性质成立。

① $r_{ii} \geq 0, \forall i$ 。

②如果某个 $r_{kk} = 0$,那么 $r_{ik} = r_{kj} = 0, \forall i, j$ 。

③ $r_{ii}r_{jj} \geq |r_{ij}|^2, \forall i, j$ 。

④ ρ_M 所有的主子式的行列式值都是非负的。

定理 1 量子态 $|\psi\rangle_{abcd}$,在任意的量子态(纯态或者混合态)中,由其两体约化密度矩阵集合

$\{\rho_{\psi}^{abc}, \rho_{\psi}^{cd}\}$ 所唯一确定。

证明 根据约化密度矩阵的计算公式, 由 $|\psi\rangle_{abcd}$ 的表达式, 很容易得出

$$\rho_{\psi}^{abc} = \frac{1}{12} (4|001\rangle\langle 001| - 2|001\rangle\langle 010| - 2|001\rangle\langle 100| + |010\rangle\langle 010| - 2|010\rangle\langle 001| + |010\rangle\langle 100| + |011\rangle\langle 011| - 2|011\rangle\langle 110| + |011\rangle\langle 101| + |100\rangle\langle 100| - 2|100\rangle\langle 001| + |100\rangle\langle 010| + |101\rangle\langle 101| - 2|101\rangle\langle 110| + |101\rangle\langle 011| + 4|110\rangle\langle 110| - 2|110\rangle\langle 011| - 2|110\rangle\langle 101|) \quad (2)$$

$$\rho_{\psi}^{cd} = \frac{1}{6} (2|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + 2|11\rangle\langle 11| + |01\rangle\langle 10| + |10\rangle\langle 01|) \quad (3)$$

只需证明: 对任意一个四粒子量子态 (可能是混合态, 也可能是纯态)

$$\begin{aligned} \rho_M &= \sum_{i_a, \dots, j_d=0}^1 r_{(i_a i_b i_c i_d)(j_a j_b j_c j_d)} |i_a i_b i_c i_d\rangle\langle j_a j_b j_c j_d| \\ &= \sum_{i, j=0}^{15} r_{ij} |i\rangle\langle j| \end{aligned} \quad (4)$$

如果有 $\rho_M^{abc} = \rho_{\psi}^{abc}$, $\rho_M^{cd} = \rho_{\psi}^{cd}$, 那么 $\rho_M = |\psi\rangle\langle\psi|_{abcd}$ 。

式(4)中第一个等式是密度矩阵的通俗写法, 但为了接下来表达方便, 本文将其在第二个等式中用十进制数进行了重新表示, 如量子态 $|\psi\rangle_{abcd}$ 的十进制表示为

$$|\psi\rangle_{abcd} = \frac{1}{2\sqrt{3}} (2|3\rangle + 2|12\rangle - |5\rangle - |6\rangle - |9\rangle - |10\rangle)$$

这 2 种表示方法完全等价。

利用约化密度矩阵的计算方法, 可以得出约化密度矩阵 ρ_M^{cd} 中 $|i_c i_d\rangle\langle j_c j_d|$ 位置上的元素为

$$\begin{aligned} &r_{(0_a 0_b i_c i_d)(0_a 0_b j_c j_d)} + r_{(0_a 1_b i_c i_d)(0_a 1_b j_c j_d)} + \\ &r_{(1_a 0_b i_c i_d)(1_a 0_b j_c j_d)} + r_{(1_a 1_b i_c i_d)(1_a 1_b j_c j_d)} \end{aligned} \quad (5)$$

例如, ρ_M^{cd} 中 $|01_d\rangle\langle 10_d|$ 项的系数为

$$\begin{aligned} &r_{(0001)(0010)} + r_{(0101)(0110)} + r_{(1001)(1010)} + r_{(1101)(1110)} \\ &= r_{1,2} + r_{5,6} + r_{9,10} + r_{13,14} \end{aligned}$$

而约化密度矩阵 ρ_M^{abc} 中 $|i_a i_b i_c\rangle\langle j_a j_b j_c|$ 位置上的元素为

$$r_{(i_a i_b i_c 0_d)(j_a j_b j_c 0_d)} + r_{(i_a i_b i_c 1_d)(j_a j_b j_c 1_d)} \quad (6)$$

如 ρ_M^{abc} 中 $|0_a 0_b 1_c\rangle\langle 1_a 0_b 1_c|$ 位置上的元素为

$$r_{(0010)(1010)} + r_{(0011)(1011)} = r_{2,10} + r_{3,11}$$

由于 $\rho_M^{abc} = \rho_{\psi}^{abc}$, 可以得到 ρ_M^{abc} 对角线上的元素为

$$\begin{cases} r_{0,0} + r_{1,1} = 0 \\ r_{2,2} + r_{3,3} = \frac{1}{3} \\ r_{4,4} + r_{5,5} = \frac{1}{12} \\ r_{6,6} + r_{7,7} = \frac{1}{12} \\ r_{8,8} + r_{9,9} = \frac{1}{12} \\ r_{10,10} + r_{11,11} = \frac{1}{12} \\ r_{12,12} + r_{13,13} = \frac{1}{3} \\ r_{14,14} + r_{15,15} = 0 \end{cases} \quad (7)$$

由 $r_{ii} \geq 0$ 可得, $r_{0,0} = r_{1,1} = r_{14,14} = r_{15,15} = 0$ 。

接下来不妨看 ρ_M^{cd} 中 $|00\rangle\langle 00|, |11\rangle\langle 11|, |01\rangle\langle 01|, |10\rangle\langle 10|, |01\rangle\langle 10|$ 位置上的系数, 由于 $\rho_M^{cd} = \rho_{\psi}^{cd}$, 因此利用式(5)可以得出

$$\begin{cases} r_{0,0} + r_{4,4} + r_{8,8} + r_{12,12} = \frac{1}{3} \\ r_{3,3} + r_{7,7} + r_{11,11} + r_{15,15} = \frac{1}{3} \\ r_{1,1} + r_{5,5} + r_{9,9} + r_{13,13} = \frac{1}{6} \\ r_{2,2} + r_{6,6} + r_{10,10} + r_{14,14} = \frac{1}{6} \\ r_{1,2} + r_{5,6} + r_{9,10} + r_{13,14} = \frac{1}{6} \end{cases} \quad (8)$$

利用密度矩阵的性质③, 式(8)中最后的公式可变换为

$$\begin{aligned} &\frac{1}{6} = r_{1,2} + r_{5,6} + r_{9,10} + r_{13,14} \\ &\leq |r_{1,2}| + |r_{5,6}| + |r_{9,10}| + |r_{13,14}| \\ &\leq \sqrt{r_{1,1}r_{2,2}} + \sqrt{r_{5,5}r_{6,6}} + \sqrt{r_{9,9}r_{10,10}} + \sqrt{r_{13,13}r_{14,14}} \\ &\leq \sqrt{(r_{1,1} + r_{5,5} + r_{9,9} + r_{13,13})(r_{2,2} + r_{6,6} + r_{10,10} + r_{14,14})} \\ &= \frac{1}{6} \end{aligned} \quad (9)$$

由此可以看出, 式(9)中所有的不等式都应该是等式, 因此

$$\sqrt{r_{1,1}r_{2,2}} + \sqrt{r_{5,5}r_{6,6}} + \sqrt{r_{9,9}r_{10,10}} + \sqrt{r_{13,13}r_{14,14}} = \sqrt{(r_{1,1}+r_{5,5}+r_{9,9}+r_{13,13})(r_{2,2}+r_{6,6}+r_{10,10}+r_{14,14})} \quad (10)$$

对式(10)进行化简, 可以得出

$$\begin{cases} r_{1,1}r_{6,6}=r_{2,2}r_{5,5} \\ r_{1,1}r_{10,10}=r_{2,2}r_{9,9} \\ r_{1,1}r_{14,14}=r_{2,2}r_{13,13} \\ r_{5,5}r_{10,10}=r_{6,6}r_{9,9} \\ r_{5,5}r_{14,14}=r_{6,6}r_{13,13} \\ r_{9,9}r_{14,14}=r_{10,10}r_{13,13} \end{cases} \quad (11)$$

因为 $r_{11}=0$, 所以从式(11)中可以得出: $r_{2,2}=0$ 或者 $r_{5,5}=r_{9,9}=r_{13,13}=0$ 。而后面的情况不可能成立。这是因为如果 $r_{5,5}=r_{9,9}=r_{13,13}=0$, 那么就有 $r_{1,1}+r_{5,5}+r_{9,9}+r_{13,13}=0$, 这与式(8)中的第3个等式矛盾, 因此可以得到 $r_{2,2}=0$ 。同理因为 $r_{14,14}=0$, 可得 $r_{13,13}=0$ 。将这些结果代入式(7)和式(8)中, 可以得到 ρ_M 中的对角线元素为

$$\begin{cases} r_{0,0}=r_{1,1}=r_{2,2}=r_{4,4}=r_{7,7}=r_{8,8}=r_{11,11}=r_{13,13}=r_{14,14}=r_{15,15}=0 \\ r_{5,5}=r_{6,6}=r_{9,9}=r_{10,10}=\frac{1}{12} \\ r_{3,3}=r_{12,12}=\frac{1}{3} \end{cases} \quad (12)$$

由密度矩阵的性质②可以得到: 对任意 $i' \in \{0,1,2,4,7,8,11,13,14\}$ 和任意 j , 都有 $r_{ij}=r_{ji'}=0$ 。接下来, 只需证明对于任意 $i, j \in \{3,5,6,9,10,12\}$, 都有 r_{ij} 等于 $|\psi\rangle\langle\psi|_{abcd}$ 中 $|i\rangle\langle j|$ 项的系数。

根据 $\rho_M^{abc}=\rho_\psi^{abc}$, 可以得到 ρ_M^{abc} 非对角线上的元素为

$$\begin{cases} r_{3,5}=-\frac{1}{6} \\ r_{3,9}=-\frac{1}{6} \\ r_{5,9}=\frac{1}{12} \\ r_{6,10}=\frac{1}{12} \\ r_{6,12}=-\frac{1}{6} \\ r_{10,12}=-\frac{1}{6} \end{cases} \quad (13)$$

由式(9)得

$$r_{5,6}+r_{9,10}=|r_{5,6}|+|r_{9,10}|=\sqrt{r_{5,5}r_{6,6}}+\sqrt{r_{9,9}r_{10,10}}=\frac{1}{6}$$

因此又可以得到 $r_{5,6}=r_{9,10}=\frac{1}{12}$ 。

本文的证明还没有结束, 因为到这一步为止, 还有很多非对角元的值是未知的, 如 $r_{3,6}, r_{3,10}, \dots, r_{9,12}$ 等非对角元, 迄今为止仍然没有出现。下面以求 $r_{3,6}$ 为例, 说明这一类非对角元的求解方法。在这里, 本文利用密度矩阵的性质④, 考虑 ρ_M 中第3、5、6行和列组成的主子式

$$\begin{bmatrix} \frac{1}{3} & -\frac{1}{6} & r_{3,6} \\ -\frac{1}{6} & \frac{1}{12} & \frac{1}{12} \\ \bar{r}_{3,6} & \frac{1}{12} & \frac{1}{12} \end{bmatrix}$$

这个主子式的行列式值是非负的, 此时有

$$-\left|r_{3,6}+\frac{1}{6}\right|^2 \geq 0, \text{ 因此可以得到 } r_{3,6}=-\frac{1}{6}。 \text{ 这与 } |\psi\rangle\langle\psi|_{abcd} |3\rangle\langle 6| \text{ 项的系数相等。}$$

以此类推, 可以得到, 对于任意 $i, j \in \{3,5,6,9,10,12\}$, 都有 r_{ij} 等于 $|\psi\rangle\langle\psi|_{abcd}$ 中 $|i\rangle\langle j|$ 项的系数, 所以 $\rho_M=|\psi\rangle\langle\psi|_{abcd}$ 。

证毕。

需要注意的是, 因为粒子 c 和粒子 d 的角色完全相同, 所以很容易看出 $\rho_\psi^{abc}=\rho_\psi^{abd}$ 。

对于下面的定理2, 证明方法与定理1完全类似, 在此不再赘述。

定理2 量子态 $|\psi\rangle_{abcd}$, 在任意的量子态(纯态或者混合态)中, 由其两体约化密度矩阵集合 $\{\rho_\psi^{abc}, \rho_\psi^{abd}\}$ 唯一确定。

4.2 四粒子纠缠态的探测

在这一步中, 本文将 GBKCW 协议的第一部分协议过程进行一些补充, 这个补充就是关于 $|\psi\rangle_{abcd}$ 态的探测, 以确保他们在收到光子源发送的光子之后, 他们之间的态并没有被破坏, 即没有被截获并操作。

1) 信源 S 制备很多 $|\psi\rangle_{abcd}$ 态, 对每个态, 他发送2个粒子给 A, 剩下的一个给 B, 一个给 C。

2) A 检测自己手中的粒子在

$$\frac{1}{6}(2|00\rangle\langle 00| + 2|11\rangle\langle 11| + |01\rangle\langle 01| + |10\rangle\langle 10| + |01\rangle\langle 10| + |10\rangle\langle 01|)$$

态上, 而 B 和 C 检测他们手中的粒子在最大混合态上。如果成功, 继续下一步。

3) 他们 3 个分别将自己手中粒子的样本发送给另外 2 个将军, 那么对将军 A 来说, 他手中有 2 个三粒子态。他探测这 2 个态是否相等, 并且都为 ρ_{ψ}^{abc} 。如果成功, 根据定理 2, 他可以确定 3 个将军之间分享的确实是量子态 $|\psi\rangle_{abcd}$, 并且记为 1, 否则记为 0。对于将军 B, 他检测手中的二粒子态和三粒子态分别为 ρ_{ψ}^{cd} 、 ρ_{ψ}^{abc} , 如果检测成功, 根据定理 1, 他确定 3 个人之间分享的是 $|\psi\rangle_{abcd}$, 对于将军 C, 与 B 完全等价。

4) 每个将军把自己手中的探测结果发送给另外 2 个将军。对于诚实的将军来说, 如果他手中的结果是 1, 而他收到的消息中有 0, 那么发送消息 0 的将军必定是叛徒。同理, 如果他手中结果是 0, 而他收到的消息中有 1, 那么发送 1 的将军必定是叛徒。

5) 如果 3 个将军手中都是 1, 并且收到的消息也都是 1, 那么他们可以进行接下来的步骤, 即数据列表的生成。

从以上可以看出, 通过加入量子态的检测步骤, 将军之间能够确定他们之间分享是正确的、没有被干扰过的量子态 $|\psi\rangle_{abcd}$ 。而使这一步成功的基本因素, 就是三体量子态 $|\psi\rangle_{abcd}$ 由其任意的 2 个两体约化密度矩阵所唯一确定的性质。这是量子纠缠态确定性的一个巧妙的应用。

5 结束语

纠缠作为一种崭新的量子资源, 可以实现很多经典无法实现的任务。它是量子信息处理主要的研究和应用对象。纠缠最为人所知的应用就是量子密码和能够有效分解大数的 Shor 算法。本文主要研究拜占庭问题的一种演变形式, 即检测的拜占庭协议问题。这一类拜占庭问题被证明在经典世界中是无法解决的, 但是利用量子方法却可以。

GBKCW 协议是一类典型的检测的拜占庭协议。为了抵御针对 GBKCW 协议的截获重发攻击, 本文利用了量子纠缠态由其子系统所唯一确定的

性质, 在 GBKCW 协议中数据列表的生成和分发部分, 加入了一个新的探测协议。根据量子态的确定性, 利用本文提出的方法, 可以探测将军们之间共享的是正确的量子纠缠态。这是量子纠缠态的确定性在量子协议中一种全新的应用。本文量子纠缠态由其子系统所唯一确定的性质可以成为一种普遍的探测量子纠缠态的方法。

参考文献:

- [1] FITZI M. Generalized communication and security models in Byzantine agreement[D]. Swiss: Swiss Federal Institute of Technology, 2002.
- [2] CONSIDINE J, FITZI M, FRANKLIN M, et al. Byzantine agreement given partial broadcast[J]. Journal of Cryptology, 2005, 18 (3): 191-217.
- [3] FITZI M, GISIN N, MAURER U. Quantum solution to the Byzantine agreement problem[J]. Phys Rev Lett, 2001, 87 (21).
- [4] PEASE M, SHOSTAK R, LAMPORT L. Reaching agreement in the presence of faults[J]. Journal of the ACM (JACM), 1980, 27(2): 228-234.
- [5] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine generals problem[J]. ACM Transactions on Programming Languages and Systems (TOPLAS), 1982, 4(3): 382-401.
- [6] GAO F, GUO F Z, WEN Q Y, et al. Comment on experimental demonstration of a quantum protocol for Byzantine agreement and liar detection[J]. Phys Rev Lett, 2008, 101 (20).
- [7] GAERTNER S, BOURENNANE M, KURTSIEFER C, et al. Experimental demonstration of a quantum protocol for Byzantine agreement and liar detection[J]. Phys Rev Lett, 2008, 100(7): 67-75..
- [8] CHIEN C H, LIN T S, LU M Y, et al. Quantum circuit and Byzantine Generals problem[C]//The 12th IEEE International Conference on Nanotechnology (IEEE-NANO).2012.
- [9] GAERTNER S, BOURENNANE M, KURTSIEFER C, et al. Addendum to experimental demonstration of a quantum protocol for Byzantine agreement and liar detection[J]. Physics, 2008.
- [10] CABELLO A. Solving the liar detection problem using the four-qubit singlet state[J]. Physical Review A, 2003: 68 (1).
- [11] RAHAMAN R, WIESNIAK M, ZUKOWSKI M. Quantum Byzantine agreement via Hardy correlations and entanglement swapping[J]. Physical Review A, 2015, 92 (4).
- [12] IBLISDIR S, GISIN N. Byzantine agreement with two quantum-key-distribution setups[J]. Physical Review A, 2004, 70 (3).
- [13] BOURENNANE M, CABELLO A, ZUKOWSKI M. Quantum Byzantine agreement with a Single Qutrit[J]. Physics, 2010.
- [14] SAKURAI J J, NAPOLITANO J. Modern quantum mechanics[M]. Addison-Wesley, 2011.
- [15] PEREA A. Quantum theory: concepts and methods[J]. Springer Science & Business Media, 2006.

- [16] HARDY L. Quantum mechanics, local realistic theories, and lorentz-invariant realistic theories[J]. Phys Rev Lett, 1992, 68(20): 2981-2984.
- [17] HORODECKI R, HORODECKI P, HORODECKI M, et al. Quantum entanglement[J]. Reviews of modern physics, 2009, 81(2), 865.
- [18] BRIEGEL H J, BROWNE D E, DUR W, et al. Measurement-based quantum computation[J]. Nature Physics, 2009, 5 (1): 19-26.
- [19] RAUSSENDORF R, BRIEGEL H J. A one-way quantum computer[J]. Physical Review Letters, 2001, 86 (22), 5188.
- [20] SHOR P W, PRESKILL J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters, 2000, 85(2):441.
- [21] CURTY M, LEWENSTEIN M, LUTKENHAUS N. Entanglement as a precondition for secure quantum key distribution[J]. Physical Review Letters, 2004, 92 (21).
- [22] RIGOLIN G. Quantum teleportation of an arbitrary two-qubit state and its relation to multipartite entanglement[J]. Physical Review A, 2005, 72(3): 309-315.
- [23] LINDEN N, POPESCU S, WOOTTERS W. Almost every pure state of three qubits is completely determined by its two-particle reduced density matrices[J]. Physical Review Letters, 2002, 89 (20), 207901.
- [24] LINDEN N, WOOTTERS W. The parts determine the whole in a generic pure quantum state[J]. Physical Review Letters, 2002, 89(27), 131-142.
- [25] JONES N S, LINDEN N. Parts of quantum states[J]. Physical Review A, 2005, 71 (1).
- [26] PARASHAR P, RANA S. N -qubit W states are determined by their bipartite marginals[J]. Physical Review A, 2009, 80 (1).
- [27] WALCK S N, LYONS D W. Only n -qubit greenberger-horne-zeilinger states contain n -partite information[J]. Physical Review A, 2009, 79 (3).
- [28] RANA S, PARASHAR P. Optimal reducibility of all W states equivalent under stochastic local operations and classical communication[J]. Physical Review A, 2011, 84 (5).

作者简介:



武霞 (1987-), 女, 山东临沂人, 中央财经大学讲师, 主要研究方向为量子信息。



贾恒越 (1983-), 女, 内蒙古海拉尔人, 中央财经大学讲师, 主要研究方向为量子信息、量子密码协议设计。



朱建明 (1965-), 男, 山西太原人, 中央财经大学教授、博士生导师, 主要研究方向为信息安全、经济信息分析。