含至多四个参与者的量子秘密共享方案的最优信息率

宋 云[1],李志慧[1],李永明[2]
(1.陕西师范大学数学与信息科学学院,陕西西安 710062;2.陕西师范大学计算机科学学院,陕西西安 710062)

摘 要: 信息率是衡量量子秘密共享方案性能的一个重要指标.在本文中,我们利用超图的相关理论刻画了量子存取结构.然后,利用超图和量子存取结构间的关系给出了参与者人数至多为 4 的所有 13 个量子存取结构,并基于量子信息论研究了其最优信息率及所对应的完善的量子秘密共享方案.对其中的 5 种存取结构的最优信息率的准确值进行了计算,并讨论了达到此信息率的方案的具体构造;对余下的 8 种存取结构的最优信息率的上界进行了计算.

关键词: 信息率; 量子秘密共享; 量子存取结构; 超图; 量子熵
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2014)10-1951-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.10.013

The Optimal Information Rate of Quantum-Secret-Sharing Schemes Based on at Most Four Participants

SONG Yun[1], LI Zhi-hui[1], LI Yong-ming[2]
(1. *College of Mathematics and Information Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*;
2. *College of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*)

Abstract: The information rate is an important metric of the performance of a quantum-secret-sharing scheme. In this paper, we characterize the quantum access structures by means of the theory of hypergraph. Furthermore, we derive the optimal information rate and the construction of perfect quantum-secret-sharing schemes corresponding to the quantum access structures with at most four players which are given in terms of the relationship between certain access structures and hypergraphs. The exact values for the optimal information rate in 5 of the 13 access structures are computed and the relevant construction of perfect secret sharing schemes is discussed. At the same time, the upper bounds for the information rate of other 8 quantum access structures are computed.

Key words: information rate; quantum-secret-sharing scheme; quantum access structures; hypergraph; quantum entropy

1 引言

量子秘密共享方案是参与者利用量子资源共享一个秘密(经典或量子)的密码协议.对于经典或量子态的秘密,参与者集合中只有那些事先授权的子集中的参与者,利用他们持有的依据秘密所分配的份额量子态(共享)才能恢复秘密,这些子集组成的集合称为存取结构,其中的子集叫授权子集.如果一个授权子集的任意真子集均不能恢复秘密,称这个授权子集为极小授权子集,极小授权子集组成的集合称作极小存取结构[1,2].1999 年,Hillery 等人[1]利用 GHZ 三重态提出了第一个量子秘密共享方案,首次将秘密共享引入到量子密码领域,此后各类量子秘密共享方案层出不穷,相关研究在理论和实验上均取得了诸多重要的成果[3~12].

量子秘密共享方案的效率可以由信息率来衡量.信息率可以认为是秘密份额大小与最长共享的大小之比.由于大的份额将会破坏协议的安全性,并影响方案的存储复杂性和通信复杂性,所以设计信息率较高的量子秘密共享方案具有重要的意义.目前,与量子秘密共享方案信息率相关的两个重要问题分别是:如何构造实现给定存取结构的高效的量子秘密共享方案以及寻找所有实现给定存取结构的方案的最优信息率[12].就有关如何得到给定存取结构的最优信息率这个问题,文献[3,4]针对一般存取结构给出了相应的量子秘密共享方案的构造,这些方案间接地提供了所研究的存取结构的最优信息率下界.文献[12]研究了一类特殊存取结构的信息率的上界,并指出其份额大小至少是秘密的 $O(n/\log_2 n)$ 倍.但有关针对基于含较少参与者集合上的所有可能的量子存取结构的最优信息率的计算问题仍然有待讨论.而在现实生活中,考虑实现具有较少参与者的存取结构的秘密共享方案,又是很必要的,如导弹的控制与发射,遗嘱的生效等均是需要较少人参与的秘密管理.

收稿日期:2013-03-29;修回日期:2014-04-08;责任编辑:李勇锋
基金项目:国家自然科学基金(No.61373150);陕西省科学技术研究发展计划工业攻关项目(No.2013k0611)

本文讨论了含至多四个参与者的所有量子存取结构的最优信息率.在一个量子秘密共享方案中,如果任意非授权子集均得不到秘密的任何信息,就称该方案是完善的.一个完善的量子秘密共享方案的共享大小至少等于秘密大小[3].由此可知,一个完善的量子秘密共享方案的信息率的上界为 1,当信息率等于 1 时,称该方案是理想的.然而,对于任意给定的存取结构,不会总是存在实现该存取结构的理想的方案,此时,我们希望求得其所有方案的信息率上界.文中所研究的量子秘密共享方案均是完善的,且其所共享的秘密是量子态.我们借助超图的有关思想刻画了量子存取结构,并依据相关结论给出全部 13 个所要研究的存取结构.然后,利用量子熵的相关理论,对其中 5 个存取结构的最优信息率能达到 1 的情况,构造出对应的理想的方案;对余下的 8 个存取结构,利用存取结构的纯化这一方法讨论了其最优信息率的上界并给出相应的证明.

2 预备知识

2.1 量子信息论

首先给出本文用到的一些有关量子信息的知识.

定义 1[13] 设有一个量子系统 A,且 ρ_A 是 A 的 m 阶密度矩阵,则量子系统 A 的量子熵定义为

$$S(\rho) = -\mathrm{Tr}(\rho_A \log_2 \rho_A) = -\sum_{1\leqslant j\leqslant m} \lambda_j \log_2 \lambda_j \quad (1)$$

其中,$\lambda_1,\cdots,\lambda_m$ 是 ρ_A 的特征值.

定义 2[13] 设 A 和 B 是两个量子系统,用 $I(A:B)$ 表示 A 和 B 间的互信息,则有

$$I(A:B) = S(A) + S(B) - S(A,B) \quad (2)$$

特别地,$I(A:B)=0$ 当且仅当复合系统 AB 所处的态是一个直积态,即 $\rho^{AB} = \rho^A \otimes \rho^B$.

文中需要对复合量子系统进行分析,而约化密度算子是重要的工具[13],因此以下我们对这一概念进行叙述.

定义 3[13] 设 A 和 B 是两个量子系统,其复合量子态由密度算子 ρ^{AB} 描述,针对系统 A 的约化密度算子定义为 $\rho^A = tr_B(\rho^{AB})$,其中 tr_B 是一个算子映射,称为在系统 B 上的偏迹.偏迹定义为

$$\mathrm{tr}_B(|a_1\rangle\langle a_2|)\otimes(|b_1\rangle\langle b_2|) = \langle b_2|b_1\rangle|a_1\rangle\langle a_2| \quad (3)$$

其中,$|a_1\rangle$和$|a_2\rangle$是状态空间 A 中的两个向量,$|b_1\rangle$和$|b_2\rangle$是状态空间 B 中的两个向量.

以下给出几个比较重要的不等式:

(ⅰ)量子熵的次可加性

$$S(A,B) \leqslant S(A) + S(B) \quad (4)$$

(ⅱ)Araki-Lieb 不等式

$$S(A,B) \geq |S(A) - S(B)| \quad (5)$$

其中,$|\cdot|$表示绝对值.

(ⅲ)熵的强次可加性不等式为:

$$S(A,C) + S(B,C) \geq S(A,B,C) + S(C) \quad (6)$$

2.2 量子秘密共享方案的信息率

文献[5]提出了一个量子秘密共享方案的信息论模型.由于在本文中我们会利用这个模型,下面给出这一方案模型的描述.

一个系统 A 的 Hilbert 空间记为 H_A.令 S 是参与者共享的秘密,且令 H_S 是相应 Hilbert 空间.设 $\rho_S = \sum_{i\in F_q} \alpha_i |i\rangle\langle i|$,其中 F_q 是有限域,利用辅助系统 R 可将秘密 S 纯化为纯态 $|RS\rangle \in H_R \otimes H_S$,故有 $S(R) = S(S)$.设 $P = \{1,2,\cdots,n\}$ 为参与者集合.量子秘密共享方案中参与者份额的分发是由一个完全正映射 Λ 给出

$$\Lambda : H_{RS} \to H_R \otimes H_P \quad (7)$$

Λ 满足对每一个授权集 $A \subseteq P$,存在一个恢复秘密的映射 $I_R \otimes R_A : H_R \otimes H_A \to H_{RS}$,使得 $\rho_{RA} \to |RS\rangle\langle RS|$.

定义 4[5] 设 P 是参与者集合,Γ 是 P 上的一个存取结构,S 是秘密量子态.则一个量子秘密共享方案的信息率定义为 $\varepsilon = \dfrac{S(S)}{\max_{X\in P} S(X)}$.

定义 5 设 P 是参与者集合,Γ 是 P 上的一个存取结构,S 是秘密量子态.则存取结构 Γ 的最优信息率定义为 $\varepsilon^* = \sup\{\varepsilon\}$.

引理 1[5] 实现存取结构 Γ 的完善量子秘密共享方案满足:

(ⅰ)对于所有的 $A \in \Gamma$

$$I(A:R) = I(A:S) = 2S(S) \quad (8)$$

(ⅱ)对于所有的 $A \notin \Gamma$

$$I(A:R) = I(A:S) = 0 \quad (9)$$

3 量子存取结构与超图

一个存取结构如果能由一个量子秘密共享方案实现,则这个存取结构就是量子存取结构.在参与者共享一个秘密量子态时,为了满足不可克隆原理,一个存取结构是量子存取结构当且仅当其中的任意两个授权集都有交集[3].为了通过研究超图与量子存取结构间的关系来刻画量子存取结构,首先引入超图的相关理论.

一个超图 G_H,其中 V 是非空顶点集,E 是超边集,$E = \{E_1,\cdots,E_m\} \subseteq 2^V$.超图 G_H 是连通的如果其任意两个顶点 $u,v \in V$,都存在从 u 到 v 的一条超径.两个超图 $G_{H_1} = (V_1,E_1)$ 与 $G_{H_2} = (V_2,E_2)$ 同构当且仅当在 V_1 与 V_2 及 E_1 与 E_2 之间,各存在一一映射 $\Psi: V_1 \to V_2$ 及 $\Phi: E_1 \to E_2$,且有 $\Phi(E_1) = \Psi(v_{11})\Psi(v_{12})\cdots\Psi(v_{1n})$,对于任何 $E_1 = v_{11}v_{12}\cdots v_{1n}$.本文研究的是连通的非同构的情况.那么,令每个参与者为超图的一个顶点,即 $P = V(G_H)$;每个授权集为超边,即 $\Gamma = E(G_H)$,则每个量子

存取结构 $\Gamma\subseteq 2^P$ 都对应一个超图 G_H,这时将 P 上的量子存取结构 Γ 称为超图存取结构,记为 $\Gamma(G_H)$.首先介绍与量子存取结构有重要联系的两类超图,即超星和超圈.

定义 6[14]　超图 $G_H=(V,E)$称为超星,如果其满足以下两个条件:

(ⅰ) $A=\bigcap_{E_i\in E}E_i\neq\varnothing$.

(ⅱ) $\forall\, i,\exists\, v\in V$ 使 $v\in E_i$ 且 $v\notin E_j$,对所有 $j\neq i$.

定义 7[14]　超图 $G_H=(V,E)$称为超圈,如果其满足以下条件:在 E 中存在一个超边序列$(E_0,\cdots,E_{m-1})$使 $E_i\cap E_{(i+1)\bmod m}\neq\varnothing$ $(i=0,1,\cdots,m-1)$且对任意的 i,有 $E_i\cap E_j=\varnothing$ 如果 $j\notin\{(i-1)\bmod m,i,(i+1)\bmod m\}$.

定义 8　令 $G_H=(V,E)$是一个超图.如果 $V'\subseteq V$ 且 $E'\subseteq 2^{V'}\cap E$,则 $G'_H=(V',E')$是 G_H 的一个子超图.

定义 9　令 $G_H=(V,E)$是一个超图且 $W\subseteq V$.如果其子超图 $G'_H=(V',E')$满足 $V'=V\setminus W$ 且 $E'=2^{V'}\cap E$,则 G'_H 是 G_H 的一个 W-诱导子图.

我们将子超图中不含超圈的这类超图记为超树.

定理 1　设 $A\subseteq 2^P$.如果 A 对应的超图 $G_{H_A}=(V_A,E_A)$是超树,则 A 是一个量子存取结构当且仅当 G_{H_A} 是一个超星.

证明　充分性:如果 G_{H_A} 是一个超星,则由定义 6 知,$\bigcap_{E_i\in E}E_i\neq\varnothing$,即 A 中任意两个授权集都有交集,故 A 是量子存取结构.

必要性:如果 A 对应的超图 $G_{H_A}=(V_A,E_A)$是超树,且 A 是一个量子存取结构.假设 G_{H_A} 不是一个超星,即对某个 i,$\forall\, v\in V$ 且 $v\in E_i$,必存在一个 E_j,使 $v\in E_j(j\neq i)$,不难验证这将导致有三边会形成一个超圈.如 $V_A=\{v_1,v_2,v_3,v_4,v_5\}$,$E_1=\{v_1,v_2\}$,$E_2=\{v_1,v_3,v_5\}$,$E_3=\{v_2,v_4,v_5\}$,$E_1,E_2,E_3$ 是一个超圈,这与 G_{H_A} 是超树矛盾.　证毕

定理 2　设 $A\subseteq 2^P$.如果 A 对应的超图 $G_{H_A}=(V_A,E_A)$不是超树,则 A 是一个量子存取结构当且仅当 G_{H_A} 中任意三边形成的子超图均是超圈.

证明　因为 A 对应的超图 $G_{H_A}=(V_A,E_A)$不是超树,即 G_{H_A} 中含有超圈子图.如果 G_{H_A} 中任意三边形成的子超图均是超圈,根据定义 7,G_{H_A} 中任意两边形成的子超图均是超星,即满足 A 中任意两个授权集交集非空.故 A 是一个量子存取结构.反过来,如果 A 是一个量子存取结构,则 G_{H_A} 中任意两边形成的子超图均为超星.设 $E_A=\{E_1,\cdots,E_n\}$,不妨设所取三边为 E_1,E_2,E_3,则有 $E_1\cap E_2\neq\varnothing$,$E_2\cap E_3\neq\varnothing$,$E_3\cap E_1\neq\varnothing$,那么,$E_1,E_2,E_3$ 所形成的子超图是超圈.　证毕

利用上述定理可确定出本文所要研究的参与者人数不超过 4 的所有非同构的量子存取结构,见表 1.

表 1　参与者人数不超过 4 的所有量子存取结构的 ε^*

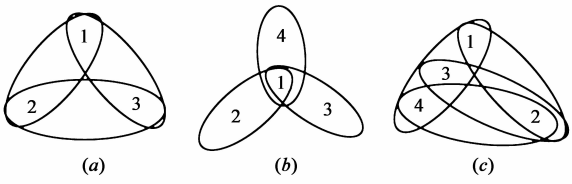
编号	参与人数	量子存取结构	ε^*
1.	2	$\{\{P_1,P_2\}\}$	1
2.	3	$\{\{P_1,P_2\},\{P_2,P_3\}\}$	$\leqslant 3/4$
3.	3	$\{\{P_1,P_2,P_3\}\}$	1
4.	3	$\{\{P_1,P_2\},\{P_2,P_3\},\{P_1,P_3\}\}$	1
5.	4	$\{\{P_1,P_2\},\{P_1,P_3\},\{P_1,P_4\}\}$	$\leqslant 2/3$
6.	4	$\{\{P_1,P_2,P_3\},\{P_1,P_4\}\}$	$\leqslant 2/3$
7.	4	$\{\{P_1,P_3,P_4\},\{P_1,P_2\},\{P_2,P_3\}\}$	$\leqslant 2/3$
8.	4	$\{\{P_1,P_3,P_4\},\{P_1,P_2\},\{P_2,P_3\},\{P_2,P_4\}\}$	$\leqslant 3/4$
9.	4	$\{\{P_1,P_2,P_3\},\{P_1,P_2,P_4\}\}$	$\leqslant 1$
10.	4	$\{\{P_1,P_2,P_3\},\{P_1,P_2,P_4\},\{P_3,P_4\}\}$	$\leqslant 1$
11.	4	$\{\{P_1,P_2,P_3\},\{P_1,P_2,P_4\},\{P_1,P_3,P_4\}\}$	$\leqslant 1$
12.	4	$\{\{P_1,P_2,P_3\},\{P_1,P_2,P_4\},\{P_1,P_3,P_4\},\{P_2,P_3,P_4\}\}$	1
13.	4	$\{\{P_1,P_2,P_3,P_4\}\}$	1

例 1　表 1 中的 #3, #4, #8 的量子存取结构对应的超图分别为图(*a*)、(*b*)、(*c*).

易看出,超图(*a*)是一个三边超圈;超图(*b*)是一个超星;超图(*c*)是一个任意三边均为超圈的非超树.

4　量子秘密共享方案的最优信息率

在本节中我们首先对完善的量子秘密共享方案进行一个新的刻画.然后,基于这一完善性定义,证明了完善的量子秘密共享方案的信息率的上界是 1.本节主



要是计算在第三节中所得到的参与者不超过 4 的量子存取结构的最优信息率,对于信息率为 1 情形,构造出相应的理想的方案.所有结果将列在表 1 中.

定理 3 令 P 是参与者集合,Γ 是 P 上的存取结构,S 是秘密量子态.一个实现存取结构 Γ 的量子秘密共享方案是完善的,如果以下两个条件成立:

(ⅰ)对于任何参与者的授权子集 $A\subseteq P$,

$$S(S|A) = -S(S).$$

(ⅱ)对于任何参与者的非授权子集 $A\subseteq P$,

$$S(S|A) = S(S).$$

证明 对于任何子集 A,利用式(2)互信息的定义有 $I(A:S) = S(A) + S(S) - S(A,S)$ (10)

由引理 1 知,当 $A\in\Gamma$ 时,$I(A:S) = 2S(S)$,代入式(10)得,$S(S|A) = -S(S)$.当 $A\notin\Gamma$ 时,$I(A:S) = 0$,代入式(10),$S(S|A) = S(S)$. 证毕

与经典的秘密共享方案类似,定理 3 中的(ⅰ)称为重构性要求,(ⅱ)称为安全性要求.本文研究的均是完善的量子秘密共享方案.

定理 4 对于实现一个存取结构的任何完善的量子秘密共享方案,都有 $\varepsilon\leqslant 1$.

证明 令 A,B 是参与者集合中任意两个子集 $A,B\notin\Gamma$,$A\cup B\in\Gamma$,则根据定理 3(ⅰ)知,

$$S(S|A,B) = -S(S),$$

则 $S(A,B) - S(S,A,B) = S(S)$.

对 $S(S,A,B)$ 应用 Araki-Lieb 不等式,得

$$S(S)\leqslant S(A,B) - |S(S,A) - S(B)| \quad (11)$$

由于 $A\notin\Gamma$,则有 $S(S|A) = S(S)$,即

$$S(S,A) = S(S) + S(A) \quad (12)$$

(1)当 $S(S,A) - S(B)\geq 0$ 时,式(11)可化为 $S(S)\leqslant S(A,B) - S(S,A) + S(B)$.由式(12)有 $S(B)\geq S(S)$,又由定义 4 可得 $\varepsilon\leqslant 1$.

(2)当 $S(S,A) - S(B) < 0$ 时,由式(12)得 $\frac{S(S)}{S(B)} < 1 - \frac{S(A)}{S(B)}$,由于 $S(B) > S(A)$,由定义 4 可得 $\varepsilon < 1$. 证毕

根据定理 4 的证明过程的(2),可得以下推论:

推论 1 令 P 是参与者集合,Γ 是 P 上的存取结构,S 是秘密量子态.对于一个实现存取结构 Γ 的完善量子秘密共享方案,如果存在一个非授权子集 B,有 $S(B) - S(A) > S(S)$,其中非授权集 A 满足 $A\cup B\in\Gamma$,则该量子秘密共享方案是非理想的.

以下给出有关参与者人数至多为 4 的量子存取结构的最优信息率.我们已将参与者人数为 2、3、4 的非同构的共 13 个量子存取结构列于表 1 中,表中的 ε^* 列表示了实现每个存取结构的所有方案中信息率的最大值.基于超图 G_H 的存取结构的最优信息率记为 $\varepsilon^*(\Gamma(G_H))$.设 G_H' 是 G_H 的 W – 诱导子图,则由定义 9 易知,如果存在一个实现 $\Gamma(G_H)$ 的量子秘密共享方案,该方案也可实现 $\Gamma(G_H')$,所以有下面的引理:

引理 2 令 $G_H = (V,E)$ 是一个超图,$W\subseteq V$ 且令 G_H' 是 G_H 的 W – 诱导子图.则 $\varepsilon^*(\Gamma(G_H))\leqslant\varepsilon^*(\Gamma(G_H'))$.

定理 5 假设 $\Gamma(G_H)$ 是一个参与者人数至多为 4 的量子存取结构,如果 $\Gamma(G_H)$ 同构与表 1 中 #1, #3, #4, #12, #13 中的任何一个,则有 $\varepsilon^*(\Gamma(G_H)) = 1$.

证明 此定理的证明就是理想的量子秘密共享方案的构造过程,证明分为两部分:

(1)对于 #1 和 #4,由于 #1 是 #4 的 $\{3\}$ – 诱导子图,由引理 2 可知,只需构造实现 #4 对应的 $\Gamma(G_H) = \{\{P_1,P_2\},\{P_2,P_3\},\{P_1,P_3\}\}$ 的理想方案.根据 2.2 介绍的方案模型,有如下方案[5].

设秘密量子态 S 是一个三维 Hilbert 空间的量子态,且 $\rho_S = 1/3\sum_{i=0}^{2}|i\rangle\langle i|$.为了进行共享分发,定义一个保距映射 $U_S:\mathbb{C}^3\to\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^3$

$$U_S:\alpha|0\rangle+\beta|1\rangle+\gamma|2\rangle\to\alpha(|000\rangle+|111\rangle+|222\rangle)+\beta(|012\rangle+|120\rangle+|201\rangle)+\gamma(|021\rangle+|102\rangle+|210\rangle).$$

由 U_S 可诱导出一个完全正映射 $\Lambda = I_{\otimes}U_S$.由于 S 是一个完全混合态,可利用辅助系统 R 将其纯化,即 $|RS\rangle = 1/\sqrt{3}\sum_{i=0}^{2}|i\rangle_{\otimes}|i\rangle$.令 $A = P$,则共享分发规则如下,

$$|RA\rangle = (I_{\otimes}U_S)|RS\rangle = \frac{1}{3}(|0000\rangle+|0111\rangle+|0222\rangle+|1012\rangle+|1120\rangle+|1201\rangle+|2021\rangle+|2102\rangle+|2210\rangle) \quad (13)$$

秘密恢复过程如下:

如对于前两个参与者,第一个参与者将其份额与第二个参与者的模 3 求和后作为第二个参与者份额位置上的向量,而后第二个参与者将此向量与第一个参与者份额模 3 求和作为第一个参与者份额位置上的向量,此时可得量子态 $(\alpha|0\rangle+\beta|1\rangle+\gamma|2\rangle)(|00\rangle+|12\rangle+|21\rangle)$.

下面我们证明方案的完善性和理想性.

完善性:由引理 1 及式(13)知,

(ⅰ)当 $A\in\Gamma$,不妨设 $A = \{1,2\}$,根据式(3)得

$$\rho^{\mathscr{C}_{1,2}}=\frac{1}{9}(|00\rangle\langle 00|+|11\rangle\langle 11|+|22\rangle\langle 22|+|01\rangle\langle 01|+|12\rangle\langle 12|+|20\rangle\langle 20|+|02\rangle\langle 02|+|10\rangle\langle 10|+|21\rangle\langle 21|)$$

以及 $\rho^{\mathscr{C}_3}=\frac{1}{3}(|0\rangle\langle 0|+|1\rangle\langle 1|+|2\rangle\langle 2|)$,

其中 $\rho^{\mathscr{C}_{1,2}}$和 $\rho^{\mathscr{C}_3}$分别表示三个参与者集合$\{1,2,3\}$中前两个参与者的份额所在联合系统 $\mathscr{C}_{1,2}$的约化密度算子和第三个参与者的份额所在系统 $\mathscr{C}_3$ 的约化密度算子. 由上述计算过程易知,系统 $\mathscr{C}_{1,2}$和 $\mathscr{C}_3$ 均处于最大纠缠态,故 $S(\mathscr{C}_{1,2})=\log_2 9=2\log_2 3$且 $S(R,\mathscr{C}_{1,2})=S(\mathscr{C}_3)=\log_2 3$. 又 $\rho_S=1/3\sum_{i=0}^{2}|i\rangle\langle i|$,则 $S(R)=S(S)=\log_2 3$. 因此,$I(\mathscr{C}_{1,2}:R)=2S(S)=2\log_2 3$,即满足完善性中的重构性要求.

(ⅱ)当 $A\notin\Gamma$,不妨设 $A=\{1\}$,根据式(3)得

$\rho^{R\mathscr{C}_1}=\frac{1}{3}I_3\otimes\frac{1}{3}I_3$,其中 I_3 表示 3 阶单位阵. 因此,$I(\mathscr{C}_1:R)=0$,即满足完善性中的安全性要求.

理想性:因为 $S(\mathscr{C}_1)=S(\mathscr{C}_2)=S(\mathscr{C}_3)=\log_2 3$,由定义 4 知,$\varepsilon=\frac{S(S)}{\max_{X\in P}S(X)}=1$,即 $\varepsilon^*=1$.

(2)对于 #3 和 #12,由于它们分别是(3,5)门限量子存取结构的$\{4,5\}$ – 诱导子图和$\{5\}$ – 诱导子图,所以根据引理 2,构造出实现(3,5)门限量子存取结构的理想方案即可. 根据 2.2 介绍的方案模型,我们可构造如下方案.

设秘密量子态 S 是一个三维 Hilbert 空间的量子态,且 $\rho_S=1/3\sum_{i=0}^{2}|i\rangle\langle i|$,为了进行共享分发,定义一个保距映射 $U_S:\mathbb{C}^3\to\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^3$

$$\begin{aligned}U_S:\alpha|0\rangle+\beta|1\rangle+\gamma|2\rangle\to&\alpha(|01201\rangle+|11111\rangle+|00000\rangle+|12012\rangle+|22222\rangle+|21021\rangle+|20120\rangle+|10210\rangle+|02102\rangle)+\beta(|02002\rangle+|12212\rangle+|01101\rangle+|10110\rangle+|20020\rangle+|21221\rangle+|22122\rangle+|00200\rangle+|11011\rangle)+\gamma(|00100\rangle+|10010\rangle+|21121\rangle+|22022\rangle+|01001\rangle+|02202\rangle+|11211\rangle+|20220\rangle+|12101\rangle).\end{aligned}$$

由 U_S 可诱导出一个完全正映射 $\Lambda=I\otimes U_S$. 由于 S 是一个完全混合态,可利用辅助系统 R 将其纯化,即 $|RS\rangle=1/\sqrt{3}\sum_{i=0}^{2}|i\rangle\otimes|i\rangle$. 令 $A=P$,则共享分发规则如下,

$$\begin{aligned}|RA\rangle=&(I\otimes U_S)|RS\rangle\\=&\frac{1}{\sqrt{27}}(|001201\rangle+|011111\rangle+|000000\rangle+|012012\rangle+|022222\rangle+|021021\rangle+|020120\rangle+|010210\rangle+|002102\rangle+|102002\rangle+|112212\rangle+|101101\rangle+|110110\rangle+|120020\rangle+|121221\rangle+|122122\rangle+|100200\rangle+|111011\rangle+|200100\rangle+|210010\rangle+|221121\rangle+|222022\rangle+|201001\rangle+|202202\rangle+|211211\rangle+|220220\rangle+|212101\rangle)\end{aligned}\tag{14}$$

秘密恢复过程与 #3 类似,下面证明此方案的完善性和理想性.

完善性:由引理 1 及式(14)知,

(ⅰ)当 $A\in\Gamma$,不妨设 $A=\{1,2,3\}$,根据式(3)得 $\rho^{\mathscr{A}_{1,2,3}}=\frac{I_{27\times 27}}{27}$,且

$$\rho^{\mathscr{A}_{4,5}}=\frac{1}{9}(|00\rangle\langle 00|+|11\rangle\langle 11|+|22\rangle\langle 22|+|01\rangle\langle 01|+|12\rangle\langle 12|+|20\rangle\langle 20|+|02\rangle\langle 02|+|10\rangle\langle 10|+|21\rangle\langle 21|).$$

由上述计算过程易知,系统 $\mathscr{A}_{1,2,3}$和 $\mathscr{A}_{4,5}$均处于最大纠缠态,故 $S(\mathscr{A}_{1,2,3})=\log_2 27=3\log_2 3$. 且 $S(R,\mathscr{A}_{1,2,3})=S(\mathscr{A}_{4,5})=\log_2 9=2\log_2 3$. 又 $\rho_S=1/3\sum_{i=0}^{2}|i\rangle\langle i|$,则 $S(R)=S(S)=\log_2 3$.

因此,$I(\mathscr{A}_{1,2,3}:R)=2S(S)=2\log_2 3$,即满足完善性中的重构性要求.

(ⅱ)当 $A\notin\Gamma$,不妨设 $A=\{1,2\}$,根据式(3)得 $\rho^{R\mathscr{A}_{1,2}}=\frac{1}{3}I_3\otimes\frac{1}{3}I_9$,其中 I_3 表示 3 阶单位阵. 因此,$I(\mathscr{A}_{1,2}:R)=0$,即满足完善性中的安全性要求.

理想性:因为 $S(\mathscr{A}_i)=\log_2 3(1\leqslant i\leqslant 5)$,由定义 4 知,$\varepsilon=\frac{S(S)}{\max_{X\in P}S(X)}=1$,即 $\varepsilon^*=1$.

#13 相关结论可采用类似方法证明. 证毕

以下讨论 #2, #5, #6, #7, #8 的最优信息率的上界. 为了得到相关结论,首先引入存取结构的纯化这一概念.

定义 10[5]　设 Γ 是 $P=\{1,2,\cdots,n\}$上的存取结构,$\overline{\Gamma}$ 是 $P'=\{1,2,\cdots,n,n+1\}$上的存取结构. 如果满足 $\overline{\Gamma}=\Gamma\cup\{A\cup\{n+1\}|A\notin\Gamma,P\setminus A\notin\Gamma\}$,则称 $\overline{\Gamma}$ 为 Γ 的纯化.

引理 3　令 A,B 是任意两个授权集且 $A\cap B$ 是非授权集,则有

$$S(A)+S(B)\geq S(A\cup B)+S(A\cap B)+2S(S)\tag{15}$$

证明　由定理 3 知,若 $A,B\in\Gamma$,则

$$S(A)=S(A\cup S)+S(S),S(B)=S(B\cup S)+S(S)\tag{16}$$

故有 $S(A)+S(B)=S(A\cup B)+S(B\cup S)+2S(S)$,

由强次可加性知,

$$S(A)+S(B)\geq S(A\cup B\cup S)+S((A\cap B)\cup S)+2S(S),$$

再由定理 3 得

$$S(A)+S(B)\geq S(A\cup B)+S(A\cap B)+2S(S).$$ 证毕

定理 6　假设 $\Gamma(G_H)$是一个参与者人数至多为 4

的量子存取结构,如果 $\Gamma(G_H)$同构与表 1 中 #2, #8 中的任何一个,则有 $\varepsilon^*(\Gamma(G_H))\leqslant 3/4$.

证明 因为 #2 是 #8 的{4}-诱导子图,由引理 2 知,只需证明对于 #2 定理成立.由于 #2 对应的$\Gamma(G_H)=\{\{P_1,P_2\},\{P_2,P_3\}\}$,则

$\overline{\Gamma(G_H)}=\{\{P_1,P_2\},\{P_2,P_3\},\{P_1,P_3,p\},\{P_2,p\}\}$.由式(15)可知

$$S(1,2)+S(2,3)\geqslant S(1,2,3)+S(2)+2S(S),$$

由次可加性得

$$S(1)+S(2)+S(3)\geqslant S(1,2,3)+2S(S) \tag{17}$$

由式(8)得,若 $A\in\Gamma$,则 $I(A:R)=2S(S)$,即 $S(A)=S(A,R)+S(S)$,所以有

$$S(1,2,3)=S(p)+S(S)\geqslant 2S(S) \tag{18}$$

将式(18)代入式(17)得

$$S(1)+S(2)+S(3)\geqslant 4S(S),$$

因此 $\varepsilon=\dfrac{S(S)}{\max_{X\in P}S(X)}\leqslant\dfrac{S(S)}{4/3S(X)}=\dfrac{3}{4}$. 证毕

定理 7 假设 $\Gamma(G_H)$是一个参与者人数至多为 4 的量子存取结构,如果 $\Gamma(G_H)$同构与表 1 中 #5, #6, #7 中的任何一个,则有 $\varepsilon^*(\Gamma(G_H))\leqslant 2/3$.

证明过程与定理 6 类似.

5 结论

本文针对量子存取结构的最优信息率进行了研究.利用超图相关理论,给出了量子存取结构的另一种刻画.这一刻画不仅可以较快地确定非同构的量子存取结构,而且依据超图的特性更有利于计算实现给定存取结构的量子秘密共享方案的最优信息率.同时,借助量子熵,对量子秘密共享方案的完善性给出了形式上类似经典方案的完善性的定义,并基于此定义证明任意完善的量子秘密共享方案的最优信息率不超过 1.最后,讨论了参与者人数不超过 4 的所有量子存取结构的最优信息率.针对参与者人数更多情况下的方案的最优信息率的计算将是我们今后的研究工作.

参考文献

[1] Hillery M, Buzek V, Berthiaume A. Quantum secret sharing [J]. Phys Rev A, 1999, 59(3): 1829 – 1834.

[2] Cleve R, Gottesman D, Lo H-K. How to share a quantum secret [J]. Phys Rev Lett, 1999, 83: 648 – 651.

[3] Gottesman D. Theory of quantum secret sharing[J]. Phys Rev A, 2000, 61: 042311.

[4] Smith A. Quantum secret sharing for general access structures [DB/OL]. http://arxiv.org/abs/quant-ph/0001087.pdf, 2000 – 01 – 24.

[5] Imai H, Muller-Quade J, Nascimento A, et al. A quantum information theoretical model for quantum secret sharing schemes [J]. Quantum Inf Comput, 2005, 5(1): 69 – 80.

[6] Helwig W, Cui W, et al. Absolute maximal entanglement and quantum secret sharing[J]. Phys Rev A, 2012, 86: 052335.

[7] Du Yu-tao, Bao Wan-su. Multiparty quantum secret sharing scheme based on the phase shift operations[J]. Optics Communications, 2013, 308(1): 159 – 163.

[8] Gao Gan. Improvement of efficient multiparty quantum secret sharing based on bell states and continuous variable operations [J]. International Journal of Theoretical Physics, 2014: 1 – 5.

[9] 周淳,鲍皖苏,付向群.基于态关联性不完美的诱骗态量子密钥分配[J].电子学报,2012,40(10):2015 – 2020.
Zhou Chun, Bao Wan-su, Fu Xiang-qun. Decoy-state quantum key distribution based on state-dependent imperfections[J]. Acta Electronica Sinica, 2012, 40(10): 2015 – 2020. (in Chinese)

[10] Wang Ming-ming, et al. Quantum secret sharing for general access structure based on multiparticle entanglement [J]. Quantum Information Processing, 2014, 13(2): 429 – 443.

[11] Fortescue B, Gour G. Reducing the quantum communication cost of quantum secret Sharing[J]. IEEE Trans Inform Theory, 2012, 58(10): 6659 – 6666.

[12] Sarvepalli P. Bounds on the information rate of quantum-secret-sharing schemes[J]. Phys Rev A, 2011, 83: 042324.

[13] Nielsen M A, Chuang I L. Quantum Computation and Quantum Information[M]. Cambridge, England: Cambridge University, 2000. 410.

[14] Crescenzo G D, Galdi C. Hypergraph decomposition and secret sharing[J]. Discrete Applied Mathematics, 2009, 157(5): 928 – 946.

作者简介

宋 云 女,1987 年生于陕西西安,陕西师范大学数学与信息科学学院博士研究生.研究方向为有限域、密码学.
E-mail: songyun09@163.com

李志慧(通信作者) 女,1966 年生于陕西眉县,陕西师范大学数学与信息科学学院教授,主要研究方向为有限域、代数编码以及密码学方面等.
E-mail: lizhihui@snnu.edu.cn