量子情報科学ウィンタースクール
量子秘密分散法

小川朋宏

電気通信大学 大学院情報システム学研究科

2010 年 2 月 27 日

What is Quantum Secret Sharing Schemes ?

○ Classical Secret Sharing Schemes (SSS)

- (k, n)-threshold SSS (Shamir 1979, Blakley 1979)
- (k, L, n)-threshold ramp SSS (Yamamoto 1985, Blakley-Meadows 1985)

○ Quantum Secret Sharing Schemes (QSSS)

to encode classical messages (bit) into quantum states
to encode quantum states (qbit) into quantum states

○ What for ?

- outputs of quantum computer
- outputs of expensive apparatus
- quantum key in cryptography with quantum algorithm

Literature on QSSS

- (k, n)-threshold QSSS (Cleve-Gottesman-Lo, 1999)
- Coding efficiency of perfect QSSS (Gottesman, 2000)
- Information theoretical treatment (Imai et al., 2003) based on coherent information and reference system

Our Goal

- Information theoretical treatment based on reversibility and Holevo Information
- Coding efficiency of ramp QSSS and optimal construction

Quantum Secret Sharing Schemes (QSSS)

○ $\mathcal{S}(\mathcal{H})$: totality of density operators on $\mathcal{H}$

$\mathcal{H}$: Hilbert space

ρ : original state $\in \mathcal{S}(\mathcal{H})$

$\Downarrow$ W_N : encoder into shares $N = \{1, 2, \ldots, n\}$

$\mathcal{H}_N = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$

$W_N(\rho)$: entangled state

partial trace for a subset $X \subseteq N$

$\mathcal{H}_X = \bigotimes_{i \in X} \mathcal{H}_i$

$W_X(\rho) = \mathrm{Tr}_{N \setminus X} \cdot W_N(\rho)$

$W_X(\rho)$ reproduces ρ or not ?

Authorized and Unauthorized Sets

$$\rho \in \mathcal{S}(\mathcal{H}) \xrightarrow{\boxed{W_N}\ \text{encoder}} W_N(\rho) \xrightarrow{\boxed{\mathrm{Tr}_{N\setminus X}}\ \text{partial trace}} W_X(\rho)$$

- subset $X \subseteq N$ $\quad W_X = \mathrm{Tr}_{N\setminus X} \cdot W_N$

- $\boxed{X \text{ : authorized}}$

  $\overset{\text{def}}{\Longleftrightarrow}$ $W_X(\rho)$ can reproduce ρ for $\forall \rho \in \mathcal{S}(\mathcal{H})$

- $\boxed{X \text{ : unauthorized}}$

  $\overset{\text{def}}{\Longleftrightarrow}$ $W_X(\rho)$ has no information about $\rho \in \mathcal{S}(\mathcal{H})$ for $\forall \rho$

- $\boxed{X \text{ : intermediate}}$ $\overset{\text{def}}{\Longleftrightarrow}$ otherwise

Perfect Schemes and Ramp Schems

$$\rho \in \mathcal{S}(\mathcal{H}) \Rightarrow \boxed{W_N} \Rightarrow W_N(\rho) \Rightarrow \boxed{\mathrm{Tr}_{N \setminus X}} \Rightarrow W_X(\rho)$$

- $\boxed{\text{QSSS } W_N \text{ : perfect scheme}}$

$\stackrel{\text{def}}{\Longleftrightarrow}$ X is either authorized or unauthorized for $\forall X \subseteq N$

- $\boxed{\text{QSSS } W_N \text{ : ramp scheme}}$

$\stackrel{\text{def}}{\Longleftrightarrow}$ otherwise

Reversibility of Quantum Operations

- quantum operation

$$\rho \in \mathcal{S}(\mathcal{H}) \longrightarrow \boxed{\mathcal{E}} \longrightarrow \mathcal{E}(\rho)$$

$\left\{ \begin{array}{l} \text{trace preserving} \\ \text{completely positive} \\ \text{affine map} \end{array} \right.$

- subset $\mathcal{S} \subseteq \mathcal{S}(\mathcal{H})$

- $\mathcal{E}$: reversible w.r.t. $\mathcal{S}$

$\overset{\text{def}}{\Longleftrightarrow}$ $\exists \mathcal{R}$ such that

$$\forall \rho \in \mathcal{S} \quad \longrightarrow \boxed{\mathcal{E}} \longrightarrow \mathcal{E}(\rho) \longrightarrow \boxed{\mathcal{R}} \longrightarrow \mathcal{R}\mathcal{E}(\rho) = \rho$$

- $\mathcal{E}$: vanishing w.r.t. $\mathcal{S}$

$\overset{\text{def}}{\Longleftrightarrow}$ $\exists \rho_0$ such that

$$\forall \rho \in \mathcal{S} \quad \longrightarrow \boxed{\mathcal{E}} \longrightarrow \mathcal{E}(\rho) = \rho_0$$

Quantum Relative Entropy

- $D(\rho||\sigma) \overset{\mathrm{def}}{=} \mathrm{Tr}[\rho(\log\rho - \log\sigma)]$
- monotonicity

$$\rho \xrightarrow{\mathcal{E}} \mathcal{E}(\rho)$$
$$\sigma \xrightarrow{\mathcal{E}} \mathcal{E}(\sigma)$$

$$D(\rho||\sigma) \quad \geq \quad D(\mathcal{E}(\rho)||\mathcal{E}(\sigma))$$

Theorem (Petz, 1986)

The following conditions are equivalent.

1. $\mathcal{E}$ is reversible w.r.t. $\{\rho, \sigma\}$
2. $D(\rho||\sigma) = D(\mathcal{E}(\rho)||\mathcal{E}(\sigma))$

Holevo Information

- $\mathcal{E}$: quantum operation
- μ : probability measure on $\mathcal{S} \subseteq \mathcal{S}(\mathcal{H})$

$$\mathrm{E}_\mu[\,\cdot\,] \stackrel{\mathrm{def}}{=} \int_{\mathcal{S}} \cdot \, \mu(\mathrm{d}\rho) \qquad \sigma_\mu \stackrel{\mathrm{def}}{=} \mathrm{E}_\mu[\rho]$$

- $\boxed{\text{Holevo Information for } \mathcal{E} \text{ and } \mu}$

$$I(\mu;\mathcal{E}) \stackrel{\mathrm{def}}{=} \mathrm{E}_\mu[D(\mathcal{E}(\rho)||\mathcal{E}(\sigma_\mu))]$$

- also written as

$$I(\mu;\mathcal{E}) = H(\mathcal{E}(\sigma_\mu)) - \mathrm{E}_\mu[H(\mathcal{E}(\rho))]$$

$$H(\rho) \stackrel{\mathrm{def}}{=} -\mathrm{Tr}[\rho \log \rho] \text{ : von Neumann entropy}$$

Holevo Information and Reversibility

- $\mathcal{P}_+(\mathcal{S})$: set of probability measures on $\mathcal{S} \subseteq \mathcal{S}(\mathcal{H})$
- $\mu \in \mathcal{P}_+(\mathcal{S})$
- monotonicity $I(\mu;\mathcal{I}) \geq I(\mu;\mathcal{E})$ ($\mathcal{I}$: identity)

Theorem 1

The following conditions are equivalent.

1. $\mathcal{E}$ is reversible (resp. vanishing) w.r.t. $\mathcal{S}$
2. $\forall \mu \in \mathcal{P}_+(\mathcal{S})$, $I(\mu;\mathcal{E}) = I(\mu;\mathcal{I})$ (resp. $= 0$)
3. $\exists \mu \in \mathcal{P}_+(\mathcal{S})$, $I(\mu;\mathcal{E}) = I(\mu;\mathcal{I})$ (resp. $= 0$)

- cf. Schumacher and Nielsen, 1996

Authorized (Unauthorized) Condition for Shares

- $\mathcal{E} = W_X \quad \mathcal{S} = \mathcal{S}_1(\mathcal{H})$: set of pure states
- reversibility w.r.t. $\mathcal{S}(\mathcal{H}) \Longleftrightarrow$ reversibility w.r.t. $\mathcal{S}_1(\mathcal{H})$
- Holevo information for $\mu \in \mathcal{P}_+(\mathcal{S}_1(\mathcal{H}))$

$$I(\mu;\mathcal{I}) = H(\sigma_\mu) - \mathrm{E}_\mu[H(\rho)] \quad \geq \quad I(\mu;W_X)$$

0 for pure state

Theorem 2

The following conditions are equivalent.

1. X is authorized (resp. unauthorized)
2. $\forall\mu \in \mathcal{P}_+(\mathcal{S}_1(\mathcal{H}))$, $I(\mu;W_X) = H(\sigma_\mu)$ (resp. $= 0$)
3. $\exists\mu \in \mathcal{P}_+(\mathcal{S}_1(\mathcal{H}))$, $I(\mu;W_X) = H(\sigma_\mu)$ (resp. $= 0$)

Coding Efficiency of Perfect QSSS

Theorem 3 (cf. Imai et al. 2003)

$$\forall X \subseteq N \qquad \forall \mu \in \mathcal{P}_+(\mathcal{S}_1(\mathcal{H}))$$

$$H(\sigma_\mu) \leq H(W_X(\sigma_\mu))$$

μ : invariant measure on $\mathcal{S}_1(\mathcal{H})$

(uniform distribution on pure states)

$$\Longrightarrow \quad \sigma_\mu = I/\dim \mathcal{H}$$

Corollary 1 (Gottesman 2000)

$$\forall i \in N \qquad \dim \mathcal{H} \leq \dim \mathcal{H}_i$$

Proof of Theorem 3 (1)

- For $X \subseteq N$ $\quad \exists Y$: unauthorized $\Longrightarrow$ $I(\mu; W_Y) = 0$

  $X \cup Y$: authorized $\Longrightarrow$ $I(\mu; W_{XY}) = H(\sigma_\mu)$

- $H(\sigma_\mu) = I(\mu; W_{XY}) - I(\mu; W_Y)$

$$= H(W_{XY}(\sigma_\mu)) - \mathrm{E}_\mu[H(W_{XY}(\rho))] - H(W_Y(\sigma_\mu)) + \mathrm{E}_\mu[H(W_Y(\rho))]$$

$$\leq H(W_X(\sigma_\mu)) - \mathrm{E}_\mu[H_\rho(W_X|W_Y)]$$

- subadditivity

$$H(W_{XY}(\sigma_\mu)) \leq H(W_X(\sigma_\mu)) + H(W_Y(\sigma_\mu))$$

- conditional entropy

$$H_\rho(W_X|W_Y) \stackrel{\mathrm{def}}{=} H(W_{XY}(\rho)) - H(W_Y(\rho))$$

Proof of Theorem 3 (2)

- Y : unauthorized $\quad$ $X \cup Y$: authorized

$$H(\sigma_\mu) \leq H(W_X(\sigma_\mu)) - \mathrm{E}_\mu[H_\rho(W_X|W_Y)]$$

- classical case : $H_\rho(W_X|W_Y) \geq 0$

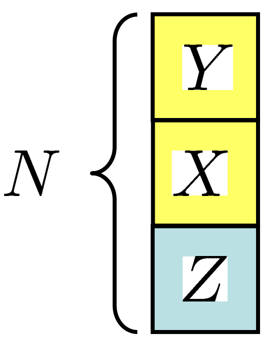
- quantum case : $\cancel{H_\rho(W_X|W_Y) \geq 0}$

Proof of Theorem 3 (3)

- ρ : pure state $\Longrightarrow$ $W_N(\rho)$: pure state
  ($\because$ Steinspring dilation, called pure state scheme)
- $X \cap Y = \emptyset$

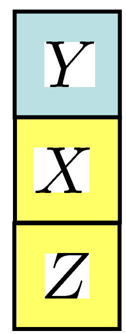
$$\boxed{Z \stackrel{\mathrm{def}}{=} N \backslash X \cup Y}$$

- no cloning theorem



$X \cup Y$: authorized
$\Downarrow$
Z : unauthorized

- no deleting theorem



Y : unauthorized
$\Downarrow$
$X \cup Z$: authorized

- Z has the same property as Y !

Proof of Theorem 3 (4)

$$\begin{cases} Y : H(\sigma_\mu) \le H(W_X(\sigma_\mu)) - \mathrm{E}_\mu[H_\rho(W_X|W_Y)] \\ Z : H(\sigma_\mu) \le H(W_X(\sigma_\mu)) - \mathrm{E}_\mu[H_\rho(W_X|W_Z)] \end{cases}$$

$$\Downarrow$$

$$H(\sigma_\mu) \le H(W_X(\sigma_\mu)) - \frac{1}{2}\{\mathrm{E}_\mu[H_\rho(W_X|W_Y)] + \mathrm{E}_\mu[H_\rho(W_X|W_Z)]\}$$

0 for pure state scheme

$$= H(W_X(\sigma_\mu))$$