8.372 sequel to 8.370, 8.371

Information theory / math foundations

tools norms, randomness, group representations, entropies

applications cryptography, many-body physics, optimization & complexity

Example

purifications, trace distance & fidelity, bit commitment

info theoretic crypto

GKO

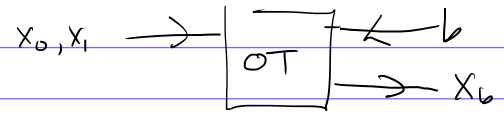
coin-flipping: output random bit with $\Pr[1] = p \approx 1/2$

NO YES strong $p \approx 1/2$

weak Alice can cheat $p \leq \frac{1}{2} + \epsilon$

Bob $p \geq \frac{1}{2} - \epsilon$

oblivious transfer



Bit commitment

Alice has input b.

commit phase

Bob can't guess b (hiding)

reveal phase

Bob outputs b or REJECT (binding)

$\Pr[REJ] \approx 0$ for honest players (valid)

OT > BC > strong coin flipping

Thm info-th. secure q. BC is impossible.

can understand this through purifications

recall

density matrices $D_d = \{\rho \in \mathbb{C}^{d \times d} : \rho \geq 0, \operatorname{tr}\rho = 1\}$

$\rho \geq 0 \Leftrightarrow \rho = C^\dagger C \Leftrightarrow \text{eigs}(\rho) \geq 0 \Leftrightarrow \langle v|\rho|v\rangle \geq 0 \quad \forall |v\rangle$

purifications $|\psi\rangle_{AB} = \sum_{ij} C_{ij} |i\rangle|j\rangle = \text{vec}(C)$ $\psi_A = \sum_{ii'j} C_{ij} C^*_{i'j} |i\rangle\langle i'| = CC^\dagger$

given ρ_A can find $|\psi\rangle_{AB}$ s.t. $\psi_A = \rho_A$

What are the possible purifications?

can understand in terms of SVD

$C = UDV^\dagger$ $\quad D = \mathrm{diag}(\lambda_1, \lambda_2, \dots)$ $\quad \lambda_1 \geq \lambda_2 \geq \dots \geq 0$

$\rho = CC^\dagger = UD^2U^\dagger$

eig (ρ) determines D

U is determined up to UR s.t. $[R, D] = 0$

V is arbitrary

$|\psi\rangle = \sum_{ij} C_{ij} |i\rangle \otimes |j\rangle$ $\quad (A \otimes B)|\psi\rangle = \sum_{ijke} A_{ki} C_{ij} B^T_{je} |k\rangle |e\rangle = \mathrm{vec}(ACB^T)$

Thm given $|\psi\rangle_{AB}$, $|\gamma\rangle_{AB}$ with $\psi_A = \gamma_A$

$\exists$ unitary W s.t. $(I \otimes W)|\psi\rangle = |\gamma\rangle$

pf $\Leftarrow$ $I \otimes W$ doesn't change A Marginal

$\Rightarrow$ $|\psi\rangle = \mathrm{vec}(C_1)$ $\quad C_1 = U_1 D_1 V_1^\dagger$ $\quad W$ can remove $V_1^\dagger, U_2^\dagger$

$|\gamma\rangle = \mathrm{vec}(C_2)$ $\quad C_2 = U_2 D_2 V_2^\dagger$

$C_1 C_1^\dagger = C_2 C_2^\dagger$

$U_1 D_1^2 U_1^\dagger = U_2 D_2^2 U_2^\dagger \Rightarrow D_1 = D_2 =: D$

$U_1 R = U_2$ for some R s.t. $[R, D] = 0$

complete proof on pset

Cor $|\psi\rangle_{AB}, |\gamma\rangle_{AB}$ have $\psi_A = \gamma_A$

$\Updownarrow$

either $\exists$ isometry W s.t. $(I \otimes W)|\psi\rangle = |\gamma\rangle$ or $(I \otimes W)|\gamma\rangle = |\psi\rangle$

ND B.C.

recall channels ① TPCP ② Kraus ③ $\mathcal{N}(\rho) = \sum_k V_k \rho V_k^\dagger$

- purify protocol
- cheaters can access discarded systems

$|\psi_b\rangle_{AB}$ after commit. hiding $\Rightarrow \psi_0^B = \psi_1^B$

$\Rightarrow$ not binding