QCQI

This class

1. Intro to QI
2. QECC
3. QIT
4. q algorithms
5. complexity
6. physics

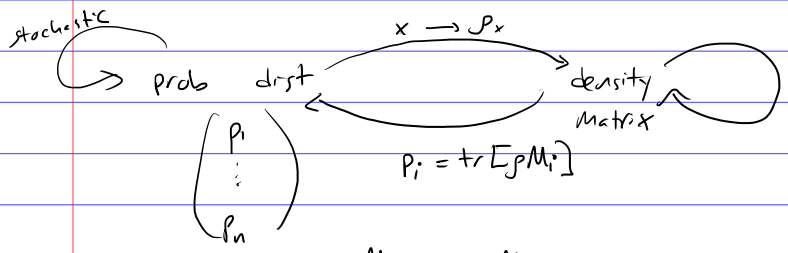
Why?

- Building and using a QC
- Using QI for tasks like sensing & control
- understanding QI in nature

States and operations

	deterministic	random
States		
classical	$[d]$	$p \in \mathbb{R}^d$, $p \geq 0$, $\|p\|_1 = 1$
quantum	$\|\psi\rangle \in \mathbb{C}^d$, $\langle\psi\|\psi\rangle = 1$	$\rho \in \mathbb{C}^{d \times d}$, $\rho \geq 0$, $\mathrm{tr}\,\rho = 1$
operations	$f: [d] \to [d]$	$T \in \mathbb{R}^{d \times d}$ stochastic
	$U(d)$	q. operations / channels / TPCP maps

we can also map between distributions and states



q. operations $\rho \to \mathcal{N}(\rho)$

$M_1 + \cdots + M_n = I$

$M_i \geq 0$

Examples

$\mathcal{N}(\rho) = U\rho U^\dagger$ dephasing

$\mathcal{N}(\rho_{AB}) = \mathrm{tr}_B[\rho_{AB}]$ depolarizing

$\mathcal{N}(\rho) = \rho \otimes \sigma$ amp. damping

$\mathcal{N}(\rho) = V\rho V^\dagger$ V isometry

$\mathcal{N}(\rho) = \sum_i p_i \mathcal{N}_i(\rho)$

$\mathcal{N}(\rho) = \sigma$

$\mathcal{N}(\rho) = \sum \mathrm{tr}[\rho M_i]\,\sigma_i$

"measure-and-prepare"

Three ways to characterize q. operations

1) physical (Stinespring)
2) algebraic (Kraus)
3) axiomatic (TPCP)

(1) "one equation to rule them all"

$$\frac{d}{dt}|\Psi_{universe}\rangle = \frac{-iH}{\hbar}|\Psi_{universe}\rangle$$

- everything is unitary
- partial trace is subjective

possible operations within this picture

$\rho \to \rho \otimes \sigma$ suffices to use $\rho \to \rho \otimes |0\rangle\langle 0|$

$\rho \to U\rho U^\dagger$

$U(\rho \otimes |0\rangle\langle 0|)U^\dagger = V\rho V^\dagger$ for an isometry $V = U(I \otimes |0\rangle)$

$\rho_{SE} \to tr_E \rho$

$$N(\rho_S) = tr_E\, V\rho V^\dagger \qquad V: S \to S\otimes E$$

or $V: A \to B \otimes E$

(2)

$V: A \to B \otimes E$

means $V = \sum_e V_e \otimes |e\rangle$ where $\{|e\rangle\}$ is an o.n. basis for E

$V_e \in L(A, B)$ = lin. operators from $A \to B$

$$N(\rho) = tr_E \sum_{e_1,e_2} V_{e_1}\rho V_{e_2}^\dagger \otimes |e_1\rangle\langle e_2|$$

$$\boxed{N(\rho) = \sum_e V_e \rho V_e^\dagger}$$

Kraus decomposition or OSR

$\{V_e\}$ are Kraus operators operator-sum representation

$$V = \begin{pmatrix} V_1 \\ \hline V_2 \\ \hline \vdots \\ \hline V_{d_E} \end{pmatrix}$$

V_i is $d_B \times d_A$

constraints?

V isometry means $V^\dagger V = I = \sum_{e_1} V_{e_1}^\dagger \otimes \langle e_1| \sum_{e_2} V_{e_2} \otimes |e_2\rangle = \sum_e V_e^\dagger V_e$

(*) $\boxed{\sum_e V_e^\dagger V_e = I}$ Kraus operator conditions.

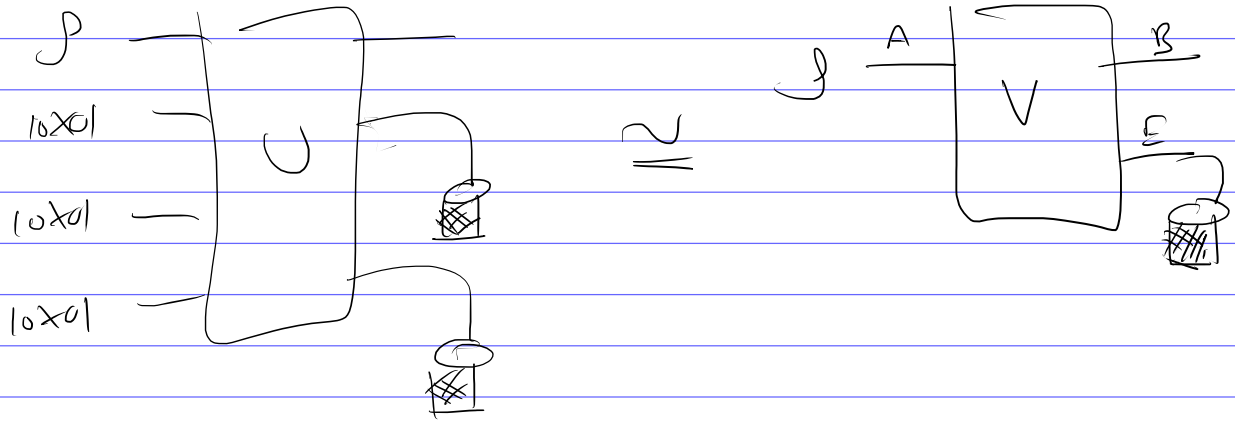
conversely if $\{V_e\}$ satisfies (*) then $V = \sum_e V_e \otimes |k\rangle$ is an isometry and N is a physical map

examples 1) unitary

2) measurement $\{M_i\} \to V = \sum_i |i\rangle\otimes M_i$

$\mathrm{tr}_E V\rho V^\dagger = \sum_i \mathrm{tr}[M_i\rho]\,|i\rangle\langle i|$

compositions?



or OSR $\rho \to \sum_e V_e \rho V_e^\dagger \to \sum_{e,f} W_f V_e \rho V_e^\dagger W_f^\dagger$ $= (W_f V_e)^\dagger$

TPCP maps

V vector space

$\rho \in L(V) = L(V,V)$

$N \in L(L(V)) = L(L(V), L(V))$

i.e. N is linear, and Hermiticity preserving

1. TP $\mathrm{tr}\, N(\rho) = \mathrm{tr}\,\rho$
2. CP $\rho \geq 0 \Rightarrow N(\rho) \geq 0$ and $(N\otimes \mathrm{id}) \geq 0$

why necessary? $\rho \geq 0 \Rightarrow \rho^T = T(\rho) \geq 0$ but $(T\otimes \mathrm{id})\left(\frac{F}{d}\right) = \frac{F}{d}$

$N(\rho) = \sum_e V_e \rho V_e^\dagger$ $\mathrm{tr}\, N(\rho) = \mathrm{tr}\,\rho \underbrace{\sum_e V_e^\dagger V_e}_{I}$

$\rho = WW^\dagger$ $N(\rho) = \sum_e V_e W W^\dagger V_e^\dagger \geq 0$

Different channel pictures are based on idea of purifications

$\forall\, \rho_A$ $\exists$ purification $\psi_{AB} = |\psi\rangle\langle\psi|$ s.t. $\psi_A := \mathrm{tr}_B[\psi] = \rho_A$

recall

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

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

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

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

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

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

$\text{eig}(\rho)$ determines D

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

V is arbitrary

$|\psi\rangle = \sum_{ij} C_{ij} |i\rangle \otimes |j\rangle \qquad (A\otimes B)|\psi\rangle = \sum_{ijkl} A_{ki} C_{ij} B^T_{je} |k\rangle|l\rangle = \text{vec}(ACB^T)$

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

$\Updownarrow$

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

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

$\Rightarrow \quad |\psi\rangle = \text{vec}(C_1) \qquad C_1 = U_1 D_1 V_1^\dagger \qquad W$ can remove $V_1^\dagger, V_2^\dagger$

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

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

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

$U_1 R = U_2$ 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 $(I\otimes W)|\gamma\rangle = |\psi\rangle$

info theoretic crypto

Oko

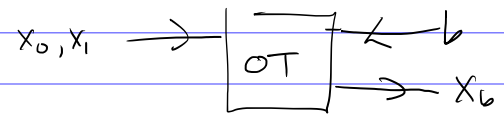
coin-flipping : output random bit with $Pr[1] = p \approx 1/2$

NO strong $p \approx 1/2$

YES 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

No 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 $\Rightarrow$ $\rho_0^B = \rho_1^B$

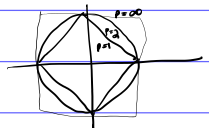
$\Rightarrow$ not binding

Metrics on states and prob. distributions

Norms $\|\cdot\|$ satisfying
1) $\|cv\| = |c| \cdot \|v\|$ for $c \in \mathbb{C}$
2) $\|v+w\| \leq \|v\| + \|w\|$
3) $\|v\| = 0 \iff v = 0$

$\|v\|^2 = \langle v, v \rangle$? only for 2-norm

L_p $\quad x \in \mathbb{C}^d$ $\quad \|x\|_{L_p} = \|x\|_p = \left(\sum_{i=1}^{d} |x_i|^p \right)^{1/p}$



L_1 $\sum_i |x_i|$
L_2 Euclidean
L_∞ $\max_i |x_i|$

S_p = Schatten-p $\quad \|X\|_{S_p} = \|X\|_p = \|\text{svals}(X)\|_{L_p}$

$\|X\|_{S_1} = \text{tr}\sqrt{X^\dagger X} = \text{tr}|X|$ if X is normal
$\|X\|_{S_\infty}$ = op. norm = biggest sval $= \|X\|$

unit sphere / ball	$S(\ )$, $B(\ )$	
pure state QM	$S(L_2)$	L_p and L_q dual if $\frac{1}{p} + \frac{1}{q} = 1$
probability dists	$S(L_1) \cap \mathbb{R}^d_+$	S_p & S_q " " "
density matrices	$S(S_1) \cap$ psd	e.g. $1, \infty$
measurement ops	$B(S_\infty)$	$2, 2$

Comparing prob dists

total variation distance

$$T(p,q) = \frac{1}{2}\|p-q\|_1 = \max_{\|x\|_\infty \leq 1} \frac{1}{2}\langle p-q, x \rangle = \max_{S \subseteq [d]} |p(S) - q(S)|$$

fidelity

$$\langle \sqrt{p}, \sqrt{q} \rangle = \sum_x \sqrt{p(x)q(x)} =: F(p,q)$$

$1 - F \leq T \leq \sqrt{2(1-F)}$

$F(p_1 \otimes p_2, q_1 \otimes q_2) = F(p_1, q_1)\, F(p_2, q_2)$

$\Rightarrow 1 - T(p^{\otimes n}, q^{\otimes n}) \sim e^{-cn}$

7. states

pure states $\| |\alpha\rangle - |\beta\rangle \|_2 = \sqrt{2(1 - \mathrm{Re}\langle\alpha|\beta\rangle)}$

not great. $F(\alpha,\beta) = |\langle\alpha|\beta\rangle|$ avoids phase dependence

mixed states

$$T(\rho,\sigma) = \frac{1}{2}\|\rho-\sigma\|_1 = \max_{0\le M\le I} \mathrm{tr}\, M(\rho-\sigma)$$

properties $T(V\rho V^\dagger, V\sigma V^\dagger) = T(\rho,\sigma)$

$T(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \le T(\rho,\sigma)$ pset

note that saturates $\mathcal{E}(\rho) = \mathrm{tr}(M\rho)\,|0\rangle\langle 0| + \mathrm{tr}((I-M)\rho)\,|1\rangle\langle 1|$ this

fidelity of mixed states

$$F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1 = \mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}$$

pset $1-F \le T \le \sqrt{1-F^2}$ $\quad 0 \le F \le 1$

and $F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \ge F(\rho,\sigma)$ $\quad \arccos F$ is a metric

Uhlmann's thm

$F(\rho,\sigma) = \max |\langle\alpha|\beta\rangle|$ over $|\alpha\rangle_{AB}, |\beta\rangle_{AB}$ s.t. $\alpha_A = \rho, \beta_B = \sigma$

by purification uniqueness, we can assume $|\alpha\rangle$ is fixed

pf $|\phi^\rho\rangle = (\sqrt{\rho}\otimes I)|\Gamma\rangle \quad |\Gamma\rangle = \sum_i |i\rangle\otimes|i\rangle$

$|\alpha\rangle = |\phi^\rho\rangle \quad |\beta\rangle = (I\otimes U)|\phi^\rho\rangle$

$$\text{RHS} = \max_U |\langle\phi^\rho| I\otimes U |\phi^\rho\rangle|$$

$$= \max_U |\langle\Gamma| \underbrace{(\sqrt{\rho}\otimes I)(I\otimes U)(\sqrt{\sigma}\otimes I)}_{\sqrt{\rho}\sqrt{\sigma}\otimes U} |\Gamma\rangle|$$

$$= \max_U |\mathrm{tr}\sqrt{\rho}\sqrt{\sigma}U^T| \overset{\star}{=} \|\sqrt{\rho}\sqrt{\sigma}\|_1 = F$$

Justifying S_1 / S_∞ duality

$A = V D W^\dagger$ $\quad \max_U |\mathrm{tr}\, AU| = |\mathrm{tr}\, D W^\dagger U V|$

$= \sum_i D_{ii} \underbrace{(W^\dagger U V)_{ii}}_{\leq 1} \leq \|A\|_1$

achieved if $W^\dagger U V = I$

No-go for noisy bit commitment

After commit states are $|\psi_0\rangle_{AB}$ or $|\psi_1\rangle_{AB}$

$T(\psi_0^B, \psi_1^B) \leq \epsilon$

$\Rightarrow F(\psi_0^B, \psi_1^B) \geq 1-\epsilon$

$\Rightarrow \exists\, U$ s.t. $F(\underbrace{(U \otimes I)|\psi_0\rangle}_{|\psi_{fake}\rangle}, |\psi_1\rangle) \geq 1-\epsilon$

$T(\psi_{fake}, \psi_1) \leq \sqrt{2\epsilon}$

$T(\text{reveal}(\psi_{fake}), \text{reveal}(\psi_1)) \leq \sqrt{2\epsilon}$

What do T & F measure?

$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ vs $\begin{pmatrix} 1-\epsilon \\ \epsilon \end{pmatrix}$ or $\begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$ vs $\begin{pmatrix} 1/2+\epsilon \\ 1/2-\epsilon \end{pmatrix}$

or $|0\rangle$ vs $\cos\theta|0\rangle + \sin\theta|1\rangle$