10/21/10 QIC 710 Lecture 12

Schmidt decomposition

Impossibility of bit commitment

General quantum operations, POVMs, Stinespring dilations

Coin-flipping and bit commitment

- possible based on computational assumptions (one-way permutations)
  a guaranteed noisy channel
  special relativity [Kent, quant-ph/9906103]
- motivation: rochambeau
  secure computation, ...

last time: BB84 bit commitment protocol, not secure
(Alice can change her commitment by keeping a purification of the mixed states sent)

Schmidt decomposition (for bipartite pure states only)

Theorem: Let $|\psi\rangle$ be a pure state in $\mathcal{H}_A \otimes \mathcal{H}_B$, $k = \dim \mathcal{H}_A$, $L = \dim \mathcal{H}_B$.
Then there exist orthonormal bases $|e_1\rangle, \ldots, |e_k\rangle$ for $\mathcal{H}_A$
$|f_1\rangle, \ldots, |f_L\rangle$ for $\mathcal{H}_B$

and reals $\lambda_i \geq 0$ such that

$$|\psi\rangle = \sum_{i=1}^{\min(k,L)} \sqrt{\lambda_i}\, |e_i\rangle \otimes |f_i\rangle .$$

Proof: $|\psi\rangle = \sum_{ij} \alpha_{ij} |i\rangle \otimes |j\rangle = \sum_i |i\rangle \otimes |\tilde{i}\rangle$, $|\tilde{i}\rangle = \sum_j \alpha_{ij} |j\rangle$

Choose a basis so that ρ_A is diagonal

$$\rho_A = \sum_{ij} |i\rangle\langle j| \cdot \mathrm{Tr}\left(|\tilde{i}\rangle\langle\tilde{j}|\right)$$

$$\vdots$$

$$\langle \tilde{j} | \tilde{i} \rangle$$

$$\Rightarrow \langle \tilde{j} | \tilde{i} \rangle = 0 \text{ for } i \neq j$$

$$\Rightarrow |\psi\rangle = \sum_i |i\rangle \otimes |\tilde{i}\rangle \quad \checkmark \qquad \square$$

$$\Rightarrow \rho_A = \sum_i \lambda_i |e_i\rangle\langle e_i| \;, \quad \rho_B = \sum_i \lambda_i |f_i\rangle\langle f_i|$$

have the same eigenvalues (non-zero)

Def: $\mathrm{Rank}(\rho_A) = \mathrm{Rank}(\rho_B) :=$ Schmidt number
a (fragile) entanglement measure (for pure states)

Corollary: Let $|\phi\rangle, |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, $\rho = |\phi\rangle\langle\phi|$, $\sigma = |\psi\rangle\langle\psi|$.
Then $\rho_B = \sigma_B \iff \exists\, U_A$ so $(U_A \otimes \mathbb{1})|\phi\rangle = |\psi\rangle$.

Proof: Starting with a basis $|f_1\rangle, \ldots |f_L\rangle$ so ρ_B is diagonal,

$$|\phi\rangle = \sum \sqrt{\lambda_i}\, |e_i\rangle \otimes |f_i\rangle$$

$$|\psi\rangle = \sum \sqrt{\lambda_i}\, |e_i'\rangle \otimes |f_i\rangle$$

$$\Rightarrow U_A = \sum_i |e_i'\rangle\langle e_i| \qquad \square$$

Corollary: Perfect bit commitment is impossible (think about it).

$$\begin{array}{ccc} |\phi^0\rangle_{AB} & \not\simeq & |\phi^1\rangle_{AB} \\ \downarrow & & \downarrow \\ \rho_B & = & \sigma_B \end{array} \Rightarrow A \text{ is not committed.}$$

Def: A quantum state is a matrix ρ that is
- positive semi-definite (and Hermitian)
- with trace 1.

ρ is pure, i.e. $\rho = |\psi\rangle\langle\psi|$ (rank-one) $\iff \mathrm{Tr}\,\rho^2 = 1$.

unitary evolution: $\rho \mapsto U\rho U^\dagger$

measurement: $\rho \longrightarrow \frac{\Pi\rho\Pi}{\mathrm{Tr}\,\Pi\rho}$ with prob. $\mathrm{Tr}\,\Pi\rho$.

General quantum operations: observed dynamics are <u>not</u> always unitary

Def: A general quantum operation (completely positive trace-preserving map) is a mapping

$$\rho \longmapsto \sum_k A_k \rho A_k^\dagger$$

where the matrices A_k satisfy

$$\sum_k A_k^\dagger A_k = \mathbb{1}$$

(Kraus operators)

Example 1: Unitary evolution $\rho \mapsto U\rho U^\dagger$

Example 2: Full decoherence (dephasing) of a qubit

$$A_0 = |0\rangle\langle 0|, \quad A_1 = |1\rangle\langle 1|$$

$$\rho = \begin{pmatrix} a & b \\ b^* & 1-a \end{pmatrix} \longmapsto \begin{pmatrix} a & 0 \\ 0 & 1-a \end{pmatrix}$$

Example 3: Partial dephasing

$$A_0 = \sqrt{1-p}\,\mathbb{1}, \quad A_1 = \sqrt{p}\,|0\rangle\langle 0|, \quad A_2 = \sqrt{p}\,|1\rangle\langle 1|$$

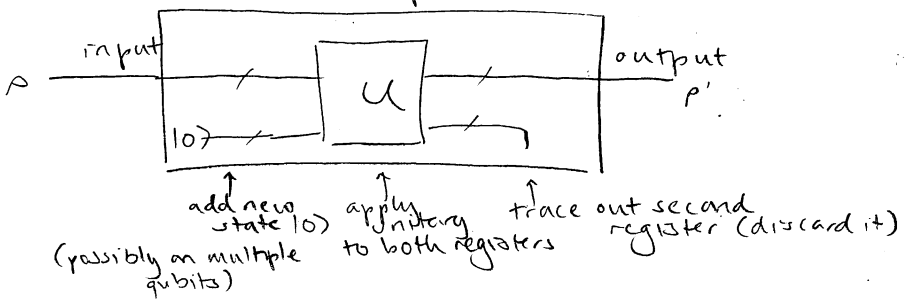
$$\rho = \begin{pmatrix} a & b \\ b^* & 1-a \end{pmatrix} \longmapsto \begin{pmatrix} a & (1-p)b \\ (1-p)b^* & 1-a \end{pmatrix}$$

time until $p = \frac{1}{e}$ known as T_2 or spin-spin relaxation time

(more examples later)

Note: The output is a density matrix.

"Derivation": Consider the procedure



We have

$$\rho' = \mathrm{Tr}_B\left[U(\rho_A \otimes |0\rangle\langle 0|_B)U^\dagger\right]$$

$$= \sum_k (\mathbb{1}\otimes\langle k|)\left[U(\rho_A\otimes|0\rangle\langle 0|_B)U^\dagger\right](\mathbb{1}\otimes|k\rangle)$$

$$= \sum_k \underbrace{\left[(\mathbb{1}\otimes\langle k|)U(\mathbb{1}\otimes|0\rangle)\right]}_{A_k} \rho \underbrace{\left[(\mathbb{1}\otimes\langle 0|)U^\dagger(\mathbb{1}\otimes|k\rangle)\right]}_{A_k^\dagger}$$

$$= \sum_k A_k \rho A_k^\dagger$$

and $\sum_k A_k^\dagger A_k = \sum_k (\mathbb{1}\otimes\langle 0|)U(\mathbb{1}\otimes|k\rangle)(\mathbb{1}\otimes\langle k|)U^\dagger(\mathbb{1}\otimes|0\rangle)$

$$= {}_B\langle 0|U\underbrace{\left(\sum_k |k\rangle\langle k|_B\right)}_{\mathbb{1}}U^\dagger|0\rangle_B$$

$$= {}_B\langle 0|UU^\dagger|0\rangle_B$$

$$= \mathbb{1}_A \quad \checkmark$$

Observe: Different basis choices give different Kraus rep's for same operator.

(and in fact only different basis choices do) Conversely, any quantum operation can be implemented in this manner. (Stinespring dilation)

Proof:

Given $\{A_k\}_1^m$ Kraus operators satisfying $\sum_k A_k^\dagger A_k = \mathbb{1}_{\mathcal{H}}$.

Define U on $\mathcal{H}\otimes\mathbb{C}^m$ by

$$U(|\psi\rangle\otimes|0\rangle) = \sum_k A_k|\psi\rangle\otimes|k\rangle$$

note: Inner products are preserved

$$(\langle\varphi|\otimes\langle 0|)U^\dagger U(|\psi\rangle\otimes|0\rangle)$$

$$= \left(\sum_{k'}\langle\varphi|A_{k'}^\dagger\otimes\langle k'|\right)\left(\sum_k A_k|\psi\rangle\otimes|k\rangle\right)$$

$$= \sum_k \langle\varphi|A_k^\dagger A_k|\psi\rangle = \langle\varphi|\psi\rangle$$

so U can be extended to a full unitary.

Moreover,

$$\mathrm{Tr}_B\left(U|\psi\rangle\langle\psi|\otimes|0\rangle\langle 0|U^\dagger\right) = \sum_k A_k|\psi\rangle\langle\psi|A_k^\dagger \quad \checkmark \quad \square$$

-allows for simulation of arbitrary quantum operations