Introduction to Quantum Information Processing

QIC 710 / CS 768 / PH 767 / CO 681 / AM 871

Lecture 23 (2013)

Richard Cleve
DC 2117 / QNC 3129
cleve@cs.uwaterloo.ca

Schmidt decomposition

Schmidt decomposition

Theorem:

Let $|\psi\rangle$ be ***any*** bipartite quantum state:

$$|\psi\rangle = \sum_{a=1}^{m}\sum_{b=1}^{n} \alpha_{a,b}|a\rangle\otimes|b\rangle$$ (where we can assume $n \le m$)

Then there exist orthonormal states
$|\mu_1\rangle, |\mu_2\rangle, \ldots, |\mu_n\rangle$ and $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_n\rangle$ such that

- $|\psi\rangle = \sum_{c=1}^{n} \sqrt{p_c}\,|\mu_c\rangle\otimes|\varphi_c\rangle$
- $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_n\rangle$ are the eigenvectors of $\mathrm{Tr}_1|\psi\rangle\langle\psi|$

Schmidt decomposition: proof (1)

The density matrix for state $|\psi\rangle$ is given by $|\psi\rangle\langle\psi|$

Tracing out the first system, we obtain the density matrix of the second system, $\rho = \mathrm{Tr}_1|\psi\rangle\langle\psi|$

Since ρ is a density matrix, we can express $\rho = \sum_{c=1}^{n} p_c |\varphi_c\rangle\langle\varphi_c|$,
where $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_n\rangle$ are orthonormal eigenvectors of ρ

Now, returning to $|\psi\rangle$, we can express $|\psi\rangle = \sum_{c=1}^{n} |\nu_c\rangle \otimes |\varphi_c\rangle$,
where $|\nu_1\rangle, |\nu_2\rangle, \ldots, |\nu_n\rangle$ are ***just some arbitrary vectors*** (not necessarily valid quantum states; for example, they might not have unit length, and we cannot presume they're orthogonal)

Schmidt decomposition: proof (2)

Claim: $\langle \nu_c | \nu_{c'} \rangle = \begin{cases} p_c & \text{if } c = c' \\ 0 & \text{if } c \neq c' \end{cases}$

Proof of Claim: Compute the partial trace Tr_1 of $|\psi\rangle\langle\psi|$ from

$$|\psi\rangle\langle\psi| = \left(\sum_{c=1}^{n} |\nu_c\rangle \otimes |\varphi_c\rangle \right) \left(\sum_{c'=1}^{n} \langle \nu_{c'}| \otimes \langle \varphi_{c'}| \right) = \sum_{c=1}^{n} \sum_{c'=1}^{n} |\nu_c\rangle\langle\nu_{c'}| \otimes |\varphi_c\rangle\langle\varphi_{c'}|$$

Note that: $\mathrm{Tr}_1(A \otimes B) = \mathrm{Tr}(A) \cdot B$ Example: $\mathrm{Tr}_1(\rho \otimes \sigma) = \sigma$

$$\mathrm{Tr}_1 \left(\sum_{c=1}^{n} \sum_{c'=1}^{n} |\nu_c\rangle\langle\nu_{c'}| \otimes |\varphi_c\rangle\langle\varphi_{c'}| \right) = \sum_{c=1}^{n} \sum_{c'=1}^{n} \mathrm{Tr}\left(|\nu_c\rangle\langle\nu_{c'}| \right) |\varphi_c\rangle\langle\varphi_{c'}| \quad \text{(linearity)}$$

$$= \sum_{c=1}^{n} \sum_{c'=1}^{n} \langle \nu_{c'} | \nu_c \rangle |\varphi_c\rangle\langle\varphi_{c'}|$$

Since $\sum_{c=1}^{n} \sum_{c'=1}^{n} \langle \nu_{c'} | \nu_c \rangle \otimes |\varphi_c\rangle\langle\varphi_{c'}| = \sum_{c=1}^{n} p_c |\varphi_c\rangle\langle\varphi_c|$ the claim follows

Schmidt decomposition: proof (3)

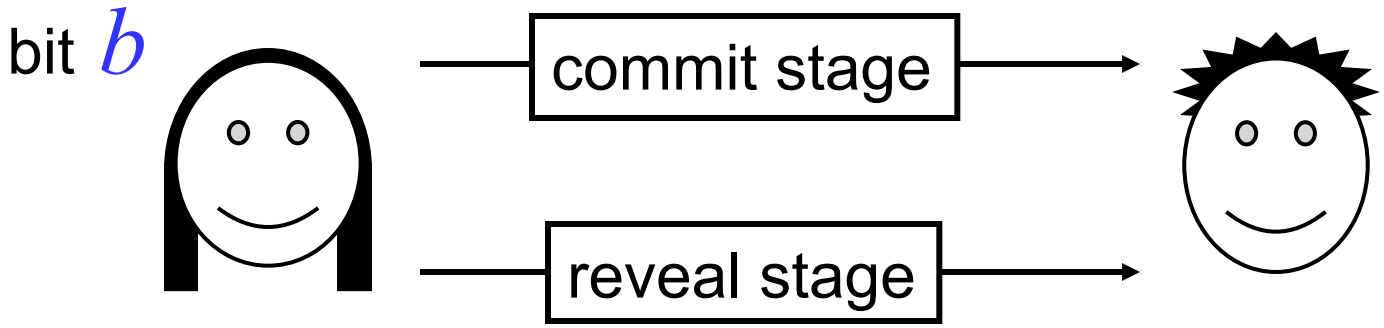
Normalize the $|\nu_c\rangle$ by setting $|\mu_c\rangle = \frac{1}{\sqrt{p_c}}|\nu_c\rangle$

Then $\langle\mu_c|\mu_{c'}\rangle = \begin{cases} 1 & \text{if } c = c' \\ 0 & \text{if } c \neq c' \end{cases}$

and $|\psi\rangle = \sum_{c=1}^{n} \sqrt{p_c}\,|\mu_c\rangle \otimes |\varphi_c\rangle$

The story of bit commitment

Bit-commitment



- Alice has a bit b that she wants to ***commit*** to Bob:
- After the ***commit*** stage, Bob should know nothing about b, but Alice should not be able to change her mind
- After the ***reveal*** stage, either:
  - Bob should learn b and accept its value, or
  - Bob should reject Alice's reveal message, if she deviates from the protocol

Simple physical implementation

- **Commit:** Alice writes b down on a piece of paper, locks it in a safe, sends the safe to Bob, but keeps the key
- **Reveal:** Alice sends the key to Bob, who then opens the safe
- Desirable properties:
  - **Binding:** Alice cannot change b after **commit**
  - **Concealing:** Bob learns nothing about b until **reveal**

Question: why should anyone care about bit-commitment?

Answer: it is a useful primitive operation for other protocols, such as coin-flipping, and "zero-knowledge proof systems"

Complexity-theoretic implementation

Based on a ***one-way function**** $f: \{0,1\}^n \rightarrow \{0,1\}^n$ and a ***hard-predicate*** $h: \{0,1\}^n \rightarrow \{0,1\}$ for f

Commit: Alice picks a random $x \in \{0,1\}^n$, sets $y = f(x)$ and $c = b \oplus h(x)$ and then sends y and c to Bob

Reveal: Alice sends x to Bob, who verifies that $y = f(x)$ and then sets $b = c \oplus h(x)$

This is (i) perfectly binding and (ii) computationally concealing, based on the hardness of predicate h

* should be one-to-one

Quantum implementation

- Inspired by the success of QKD, one can try to use the properties of quantum mechanical systems to design an information-theoretically secure bit-commitment scheme
- One simple idea:
  - To **commit** to **0**, Alice sends a random sequence from $\{|0\rangle, |1\rangle\}$
  - To **commit** to **1**, Alice sends a random sequence from $\{|+\rangle, |-\rangle\}$
  - Bob measures each qubit received in a random basis
  - To **reveal**, Alice tells Bob exactly which states she sent in the commitment stage (by sending its index 00, 01, 10, or 11), and Bob checks for consistency with his measurement results
- A paper appeared in 1993 proposing a quantum bit-commitment scheme and a proof of security

Impossibility proof (I)

- Not only was the 1993 scheme shown to be insecure, but it was later shown that ***no such scheme can exist!***
- To understand the impossibility proof, recall the ***Schmidt decomposition:***

Let $|\psi\rangle$ be any bipartite quantum state:

$$|\psi\rangle = \sum_{a=1}^{n}\sum_{b=1}^{n} \alpha_{a,b}|a\rangle|b\rangle$$

Then there exist orthonormal states

$|\mu_1\rangle, |\mu_2\rangle, \ldots, |\mu_n\rangle$ and $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_n\rangle$ such that

$$|\psi\rangle = \sum_{c=1}^{n} \beta_c |\mu_c\rangle|\phi_c\rangle$$

Eigenvectors of $\mathrm{Tr}_1|\psi\rangle\langle\psi|$

[Mayers '96][Lo & Chau '96]

Impossibility proof (II)

- **Corollary:** if $|\psi_0\rangle$, $|\psi_1\rangle$ are two bipartite states such that $\mathrm{Tr}_1|\psi_0\rangle\langle\psi_0| = \mathrm{Tr}_1|\psi_1\rangle\langle\psi_1|$ then there exists a unitary U (acting on the first register) such that $(U\otimes I)|\psi_0\rangle = |\psi_1\rangle$
- **Proof:**

$$|\psi_0\rangle = \sum_{c=1}^{n} \beta_c |\mu_c\rangle|\phi_c\rangle \quad \text{and} \quad |\psi_1\rangle = \sum_{c=1}^{n} \beta_c |\mu'_c\rangle|\phi_c\rangle$$

We can define U so that $U|\mu_c\rangle = |\mu'_c\rangle$ for $c = 1,2,\ldots,n$ ∎

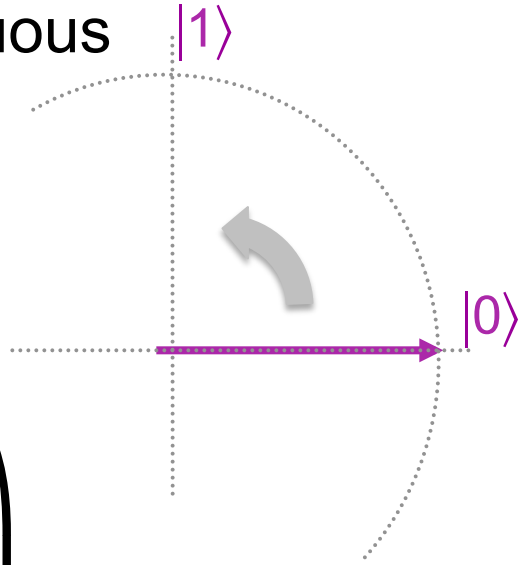
- Protocol can be "purified" so that Alice's commit states are $|\psi_0\rangle$ & $|\psi_1\rangle$ (where she sends the second register to Bob)
- By applying U to her register, Alice can change her commitment from $b = 0$ to $b = 1$ (by changing $|\psi_0\rangle$ to $|\psi_1\rangle$)

Continuous-time evolution

(very briefly)

Continuous-time evolution

Although we've expressed quantum operations in discrete terms, in real physical systems, the evolution is continuous



Let H be any ***Hermitian*** matrix and $t \in \mathbf{R}$

Then e^{iHt} is ***unitary*** — why?

H is called a ***Hamiltonian***

$$H = U^\dagger D U, \text{ where } D = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_d \end{pmatrix}$$

$$e^{iHt} = U^\dagger e^{iDt} U = U^\dagger \begin{pmatrix} e^{i\lambda_1 t} & & \\ & \ddots & \\ & & e^{i\lambda_d t} \end{pmatrix} U \quad \text{(unitary)}$$