Introduction to Quantum Information Processing

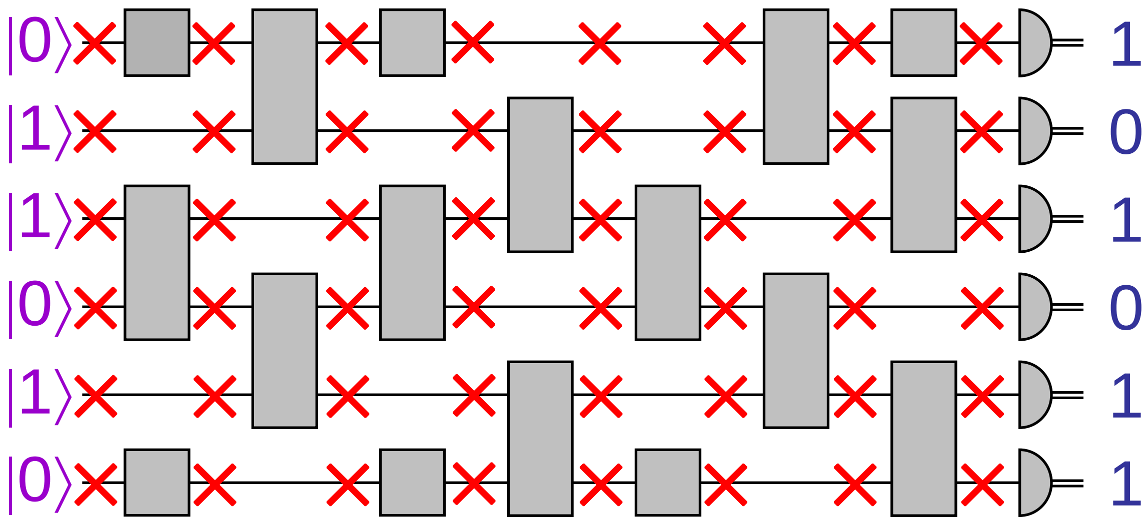
CS 667 / PH 767 / CO 681 / AM 871

Lecture 22 (2009)

Richard Cleve
DC 2117
cleve@cs.uwaterloo.ca

Brief remarks about fault-tolerant computing

A simple error model



At each qubit there is an ✕ error per unit of time, that denotes the following noise:

$$\begin{cases} I & \text{with probability } 1-\varepsilon \\ X & \text{with probability } \varepsilon/3 \\ Y & \text{with probability } \varepsilon/3 \\ Z & \text{with probability } \varepsilon/3 \end{cases}$$

Threshold theorem

If ε is very small then this is okay — a computation of size* less than $1/(10\varepsilon)$ will still succeed most of the time

But, for every constant value of ε, the size of the maximum computation possible is constant

Threshold theorem: There is a fixed constant $\varepsilon_0 > 0$ such that any computation of size T can be translated into one of size $O(T \log^c(T))$ that is robust against the error model with parameter ε_0

(The proof is omitted here)

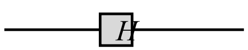
* where size = (# qubits)x(# time steps)

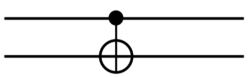
Comments about the threshold theorem

Idea is to use a quantum error-correcting code at the start and then perform all the gates ***on the encoded data***

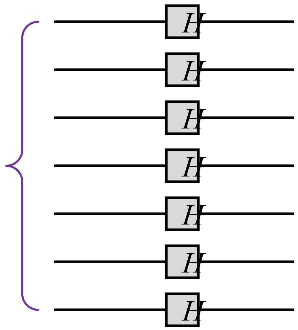
At regular intervals, an error-correction procedure is performed, very carefully, since these operations are also subject to errors!

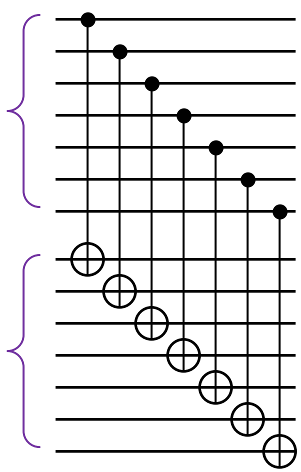
The 7-qubit CSS code has some nice properties that enable some (not all) gates to be directly peformed on the encoded data: H and $CNOT$ gates act "transversally" in the sense that:





are equivalent to

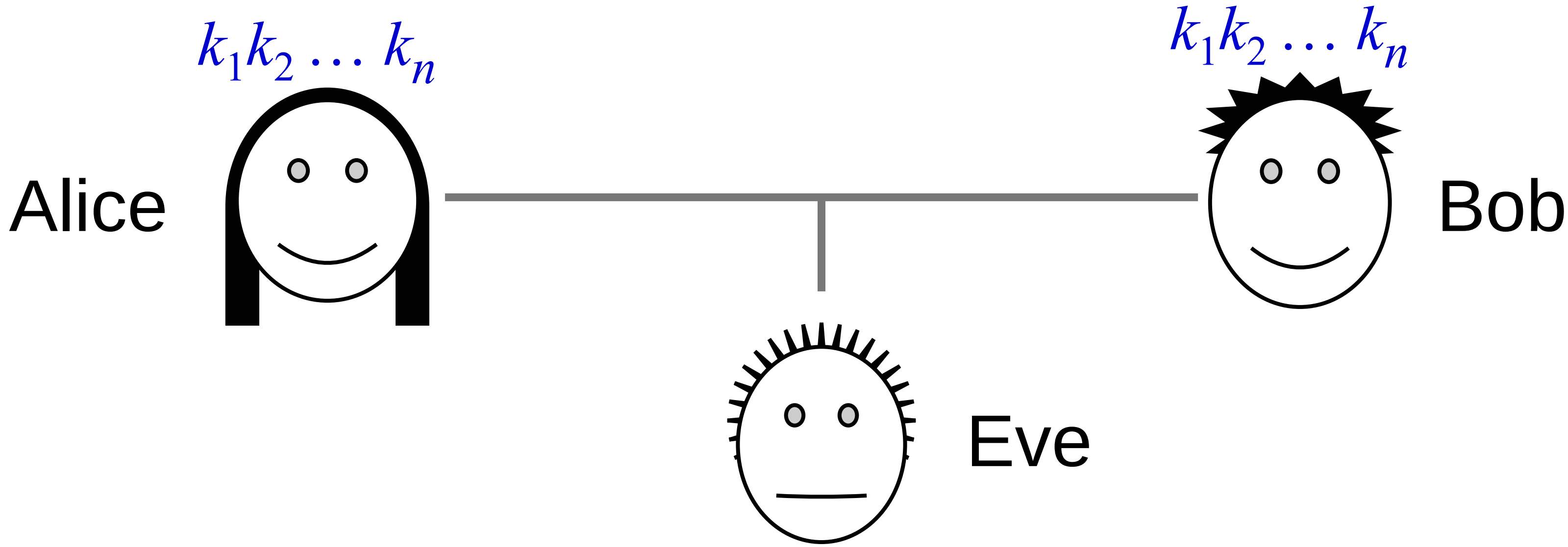




Also, codes applied recursively become stronger

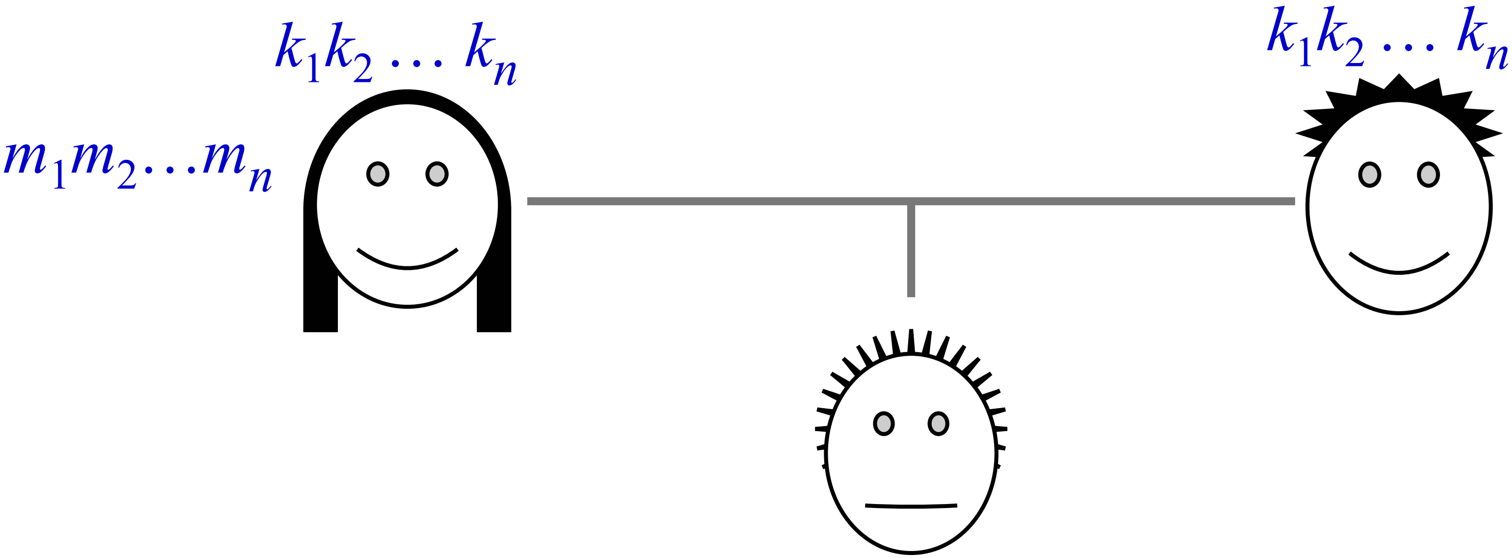
Quantum key distribution

Private communication



- Suppose Alice and Bob would like to communicate privately in the presence of an eavesdropper Eve
- A provably secure (classical) scheme exists for this, called the ***one-time pad***
- The one-time pad requires Alice & Bob to share a ***secret key***: $k \in \{0,1\}^n$, uniformly distributed (secret from Eve)

Private communication



One-time pad protocol:

- Alice sends $c = m \oplus k$ to Bob
- Bob receives computes $c \oplus k$, which is $(m \oplus k) \oplus k = m$

This is secure because, what Eve sees is c, and c is uniformly distributed, regardless of what m is

Key distribution scenario

- For security, Alice and Bob must never reuse the key bits
  - E.g., if Alice encrypts both m and m' using the same key k then Eve can deduce $m \oplus m' = c \oplus c'$
- Problem: how do they distribute the secret key bits in the first place?
  - Presumably, there is some trusted preprocessing stage where this is set up (say, where Alice and Bob get together, or where they use a trusted third party)
- **Key distribution problem:** set up a large number of secret key bits

Key distribution based on computational hardness

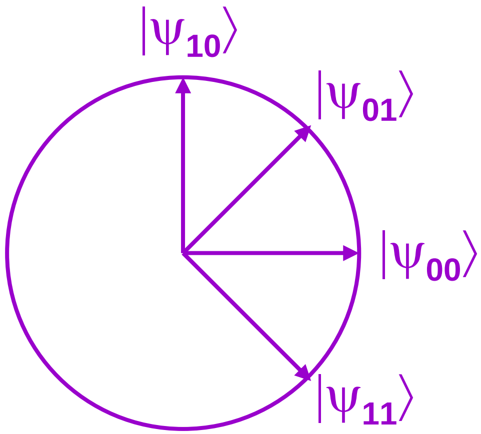
- The **RSA** protocol can be used for key distribution:
  - Alice chooses a random key, encrypts it using Bob's ***public key***, and sends it to Bob
  - Bob decrypts Alice's message using his ***secret (private) key***
- The security of **RSA** is based on the presumed computational difficulty of factoring integers
- More abstractly, a key distribution protocol can be based on any ***trapdoor one-way function***
- Most such schemes are breakable by quantum computers

Quantum key distribution (QKD)

- A protocol that enables Alice and Bob to set up a secure* secret key, provided that they have:
  - A ***quantum channel***, where Eve can read and modify messages
  - An ***authenticated classical channel***, where Eve can read messages, but cannot tamper with them (the authenticated classical channel can be simulated by Alice and Bob having a ***very short*** classical secret key)
- There are several protocols for QKD, and the first one proposed is called "**BB84**" [Bennett & Brassard, 1984]:
  - BB84 is "easy to implement" physically, but "difficult" to prove secure
  - [Mayers, 1996]: first true security proof (quite complicated)
  - [Shor & Preskill, 2000]: "simple" proof of security

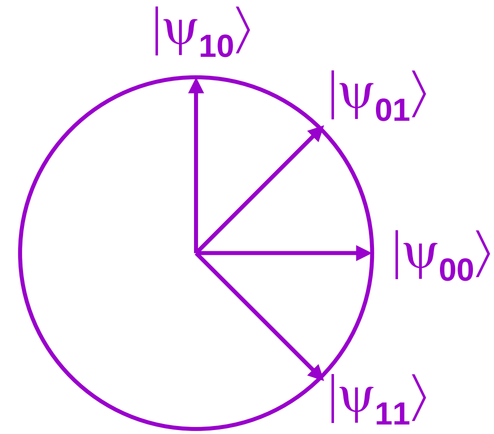
∗ Information-theoretic security

BB84



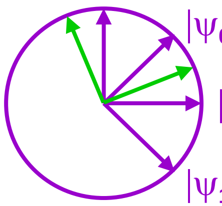
- First, define: $|\psi_{00}\rangle = |0\rangle$
  $|\psi_{10}\rangle = |1\rangle$
  $|\psi_{11}\rangle = |-\rangle = |0\rangle - |1\rangle$
  $|\psi_{01}\rangle = |+\rangle = |0\rangle + |1\rangle$
- Alice begins with two random n-bit strings $a, b \in \{0,1\}^n$
- Alice sends the state $|\psi\rangle = |\psi_{a_1 b_1}\rangle|\psi_{a_2 b_2}\rangle \dots |\psi_{a_n b_n}\rangle$ to Bob
- **Note:** Eve may see these qubits (and tamper wth them)
- After receiving $|\psi\rangle$, Bob randomly chooses $b' \in \{0,1\}^n$ and measures each qubit as follows:
  - If $b'_i = 0$ then measure qubit in basis $\{|0\rangle, |1\rangle\}$, yielding outcome a'_i
  - If $b'_i = 1$ then measure qubit in basis $\{|+\rangle, |-\rangle\}$, yielding outcome a'_i

BB84



- **Note:**
  - If $b'_i = b_i$ then $a'_i = a_i$
  - If $b'_i \neq b_i$ then $\Pr[a'_i = a_i] = ½$
- Bob informs Alice when he has performed his measurements (using the public channel)
- Next, Alice reveals b and Bob reveals b' over the public channel
- They discard the cases where $b'_i \neq b_i$ and they will use the ***remaining bits*** of a and a' to produce the key
- **Note:**
  - If Eve did not disturb the qubits then the key can be just a (= a')
  - The ***interesting*** case is where Eve may tamper with $|\psi\rangle$ while it is sent from Alice to Bob

BB84



- **Intuition:**
  - Eve cannot acquire information about $|\psi\rangle$ without disturbing it, which will cause ***some*** of the bits of a and a' to disagree
  - It can be proven* that: the more information Eve acquires about a, the more bit positions of a and a' will be different
- From Alice and Bob's remaining bits, a and a' (where the positions where $b'_i \neq b_i$ have already been discarded):
  - They take a random subset and reveal them in order to estimate the fraction of bits where a and a' disagree
  - If this fraction is not too high then they proceed to distill a key from the bits of a and a' that are left over (around $n/4$ bits)

* To prove this rigorously is nontrivial

BB84

- If the error rate between a and a' is below some threshold (around 11%) then Alice and Bob can produce a good key using techniques from classical cryptography:
  - **Information reconciliation** (“distributed error correction”)**:** to produce shorter a and a' such that (i) $a = a'$, and (ii) Eve doesn’t acquire much information about a and a' in the process
  - **Privacy amplification:** to produce shorter a and a' such that Eve’s information about a and a' is very small

- There are already commercially available implementations of BB84, though assessing their true security is a subtle matter (since their physical mechanisms are not ideal)

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 $n \leq m$)

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 (I)

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 (II)

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

Schmidt decomposition: proof (III)

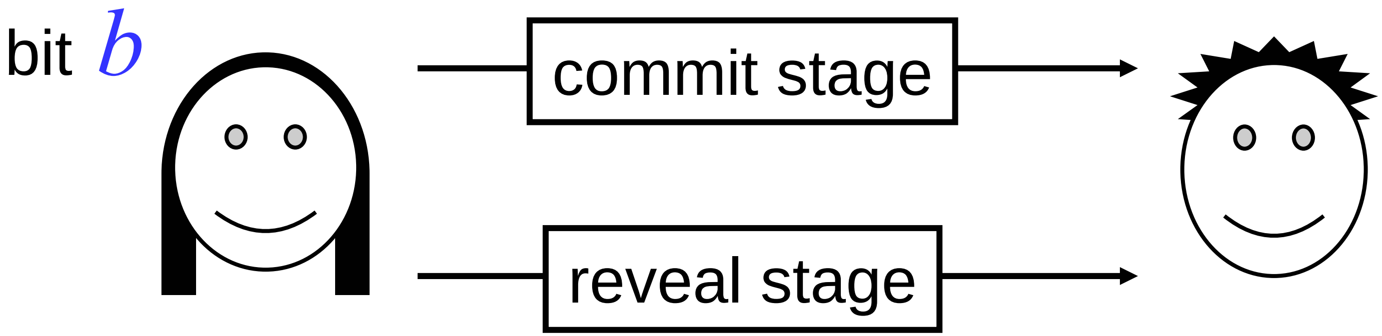
Normalize the $|\nu_c\rangle$ by setting $|\mu_c\rangle = \frac{1}{\sqrt{p_c}}|\nu_c\rangle$

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

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

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

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

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 $c = 1,2,\ldots,n$ $\blacksquare$

- 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 $|\psi_1\rangle$)