Introduction to Quantum Information Processing

QIC 710 / CS 678 / PH 767 / CO 681 / AM 871

Lectures 9–11 (2013)

Richard Cleve

DC 2117 / QNC 3129

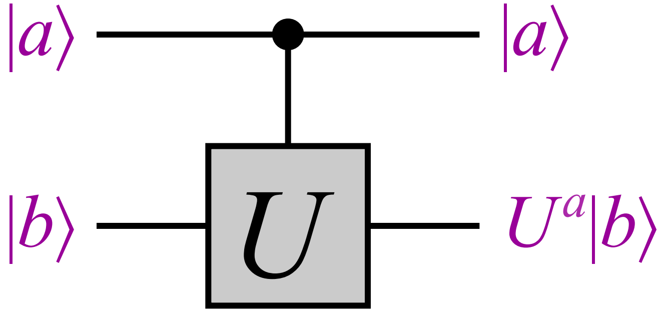
cleve@cs.uwaterloo.ca

Continuation of:

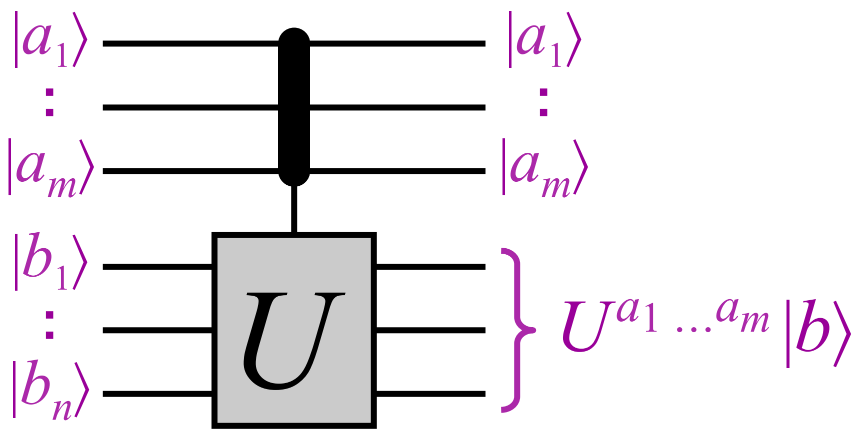
Eigenvalue estimation problem

(a.k.a. phase estimation)

Generalized controlled-U gates



$$\begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix}$$



$$\begin{bmatrix} I & 0 & 0 & \cdots & 0 \\ 0 & U & 0 & \cdots & 0 \\ 0 & 0 & U^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & U^{2^m-1} \end{bmatrix}$$

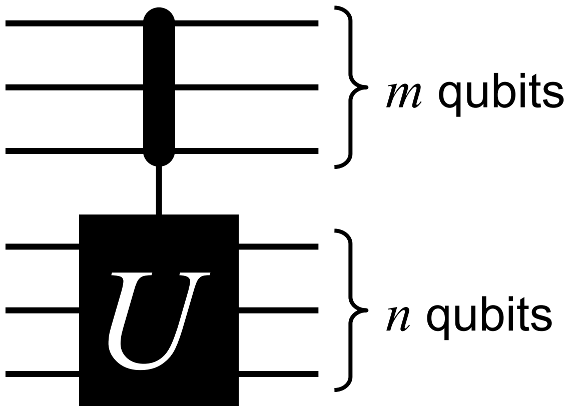
Example: $|1101\rangle|0101\rangle \rightarrow |1101\rangle U^{1101}|0101\rangle$

Eigenvalue estimation problem

U is a unitary operation on n qubits

$|\psi\rangle$ is an eigenvector of U, with eigenvalue $e^{2\pi i\phi}$
$(0 \leq \phi < 1)$

Input: black-box for

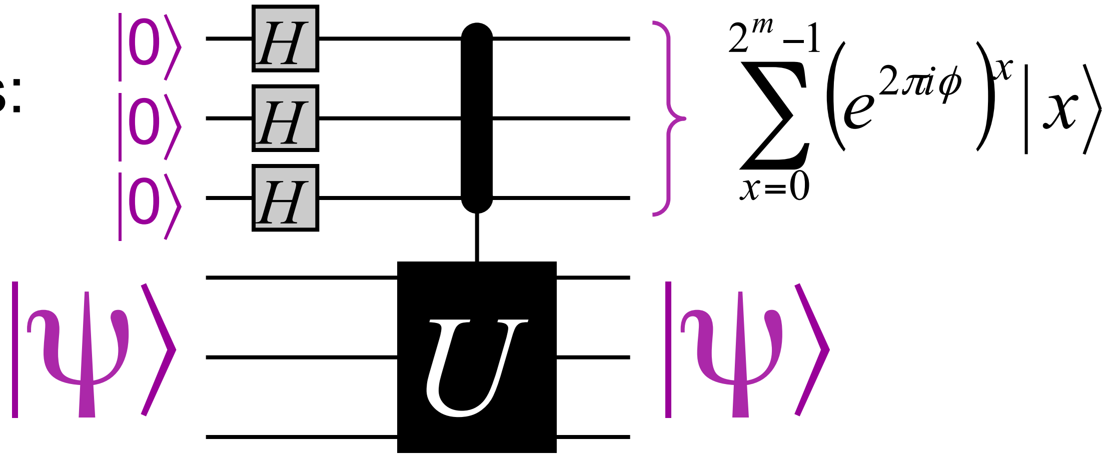


and a copy of $|\psi\rangle$

Output: ϕ (m-bit approximation)

Algorithm for eigenvalue estimation (1)

Starts off as:



$|00 \ldots 0\rangle|\psi\rangle$

$\boxed{|a\rangle|b\rangle \rightarrow |a\rangle U^a|b\rangle}$

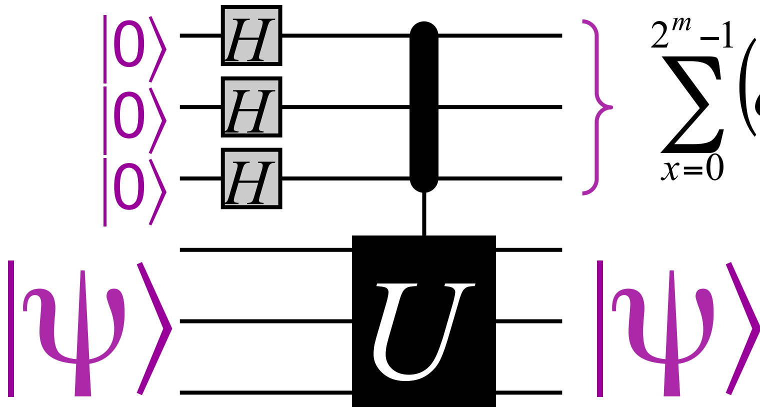
$\rightarrow (|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \ldots (|0\rangle + |1\rangle)|\psi\rangle$

$= (|000\rangle + |001\rangle + |010\rangle + |011\rangle + \ldots + |111\rangle)|\psi\rangle$

$= (|0\rangle + |1\rangle + |2\rangle + |3\rangle + \ldots + |2^m - 1\rangle)|\psi\rangle$

$\rightarrow (|0\rangle + e^{2\pi i\phi}|1\rangle + (e^{2\pi i\phi})^2|2\rangle + (e^{2\pi i\phi})^3|3\rangle + \ldots + (e^{2\pi i\phi})^{2^m-1}|2^m-1\rangle)|\psi\rangle$

Algorithm for eigenvalue estimation (2)



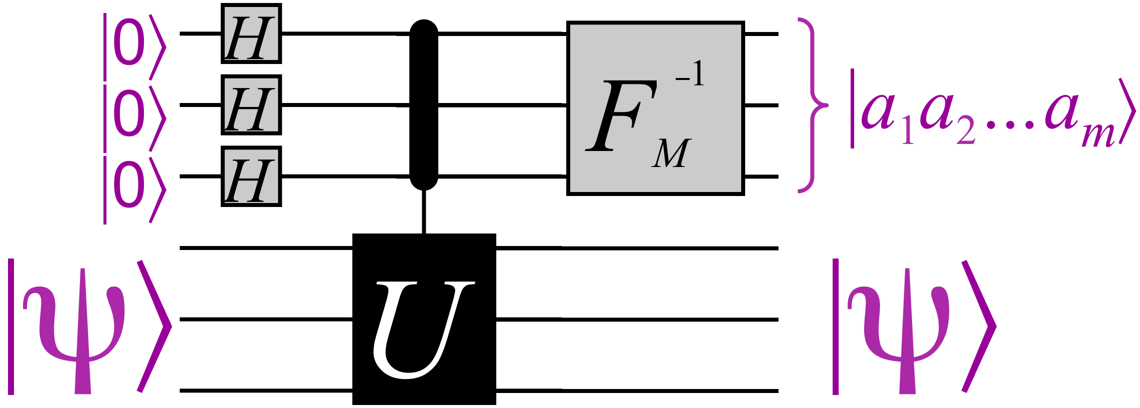
$$\sum_{x=0}^{2^m-1}\left(e^{2\pi i\phi}\right)^x|x\rangle$$

Recall that $$F_M|a_1a_2\ldots a_m\rangle=\sum_{x=0}^{2^m-1}\left(e^{2\pi i(0.a_1a_2\ldots a_m)}\right)^x|x\rangle$$

$$F_M^{-1}=\frac{1}{\sqrt{M}}\begin{bmatrix}1 & 1 & 1 & 1 & \cdots & 1\\ 1 & \omega^{-1} & \omega^{-2} & \omega^{-3} & \cdots & \omega^{-(M-1)}\\ 1 & \omega^{-2} & \omega^{-4} & \omega^{-6} & \cdots & \omega^{-2(M-1)}\\ 1 & \omega^{-3} & \omega^{-6} & \omega^{-9} & \cdots & \omega^{-3(M-1)}\\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & \omega^{-(M-1)} & \omega^{-2(M-1)} & \omega^{-3(M-1)} & \cdots & \omega^{-(M-1)^2}\end{bmatrix}$$

Therefore, when $\phi = 0.a_1a_2\ldots a_m$ applying the ***inverse*** of F_M yields ϕ (digits)

Algorithm for eigenvalue estimation (3)



If $\phi = 0.a_1 a_2 \ldots a_m$ then the above procedure yields $|a_1 a_2 \ldots a_m\rangle$ (from which ϕ can be deduced exactly)

But what ϕ if is not of this nice form?

Example: $\phi = ⅓ = 0.0101010101010101\ldots$

Algorithm for eigenvalue estimation (4)

What if ϕ is not of the nice form $\phi = 0.a_1 a_2 \ldots a_m$?

Example: $\phi = ⅓ = 0.\underline{0101010101}010101\ldots$

Let's calculate what the previously-described procedure does:

Let $a/2^m = 0.a_1 a_2 \ldots a_m$ be an m-bit approximation of ϕ, in the sense that $\phi = a/2^m + \delta$, where $|\delta| \leq 1/2^{m+1}$

$$\left(F_M\right)^{-1} \sum_{x=0}^{2^m-1} \left(e^{2\pi i \phi}\right)^x |x\rangle = \frac{1}{2^m} \sum_{y=0}^{2^m-1} \sum_{x=0}^{2^m-1} e^{-2\pi i x y / 2^m} e^{2\pi i \phi x} |y\rangle$$

$$= \frac{1}{2^m} \sum_{y=0}^{2^m-1} \sum_{x=0}^{2^m-1} e^{-2\pi i x y / 2^m} e^{2\pi i \left(\frac{a}{2^m} + \delta\right) x} |y\rangle$$

What is the amplitude of $|a_1 a_2 \ldots a_m\rangle$?

$$= \frac{1}{2^m} \sum_{y=0}^{2^m-1} \sum_{x=0}^{2^m-1} e^{2\pi i (a-y) x / 2^m} e^{2\pi i \delta x} |y\rangle$$

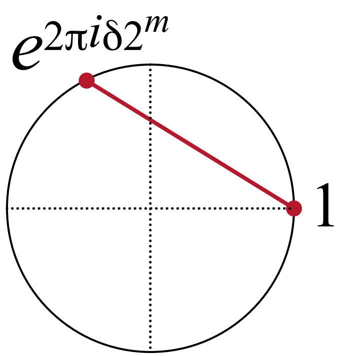
Algorithm for eigenvalue estimation (5)

State is: $\dfrac{1}{2^m}\displaystyle\sum_{y=0}^{2^m-1}\sum_{x=0}^{2^m-1} e^{2\pi i(a-y)x/2^m} e^{2\pi i\delta x}|y\rangle$

geometric series!

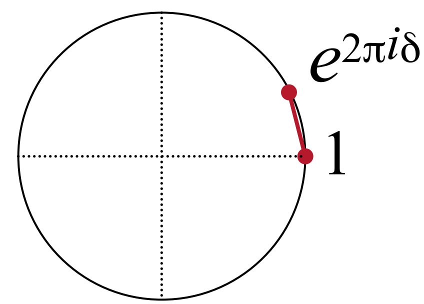
The amplitude of $|y\rangle$, for $y = a$ is $\dfrac{1}{2^m}\displaystyle\sum_{x=0}^{2^m-1} e^{2\pi i\delta x} = \dfrac{1}{2^m}\dfrac{1-\left(e^{2\pi i\delta}\right)^{2^m}}{1-e^{2\pi i\delta}}$

Numerator:



lower bounded by
$2\pi\delta 2^m(2/\pi) > 4\delta 2^m$

Denominator:



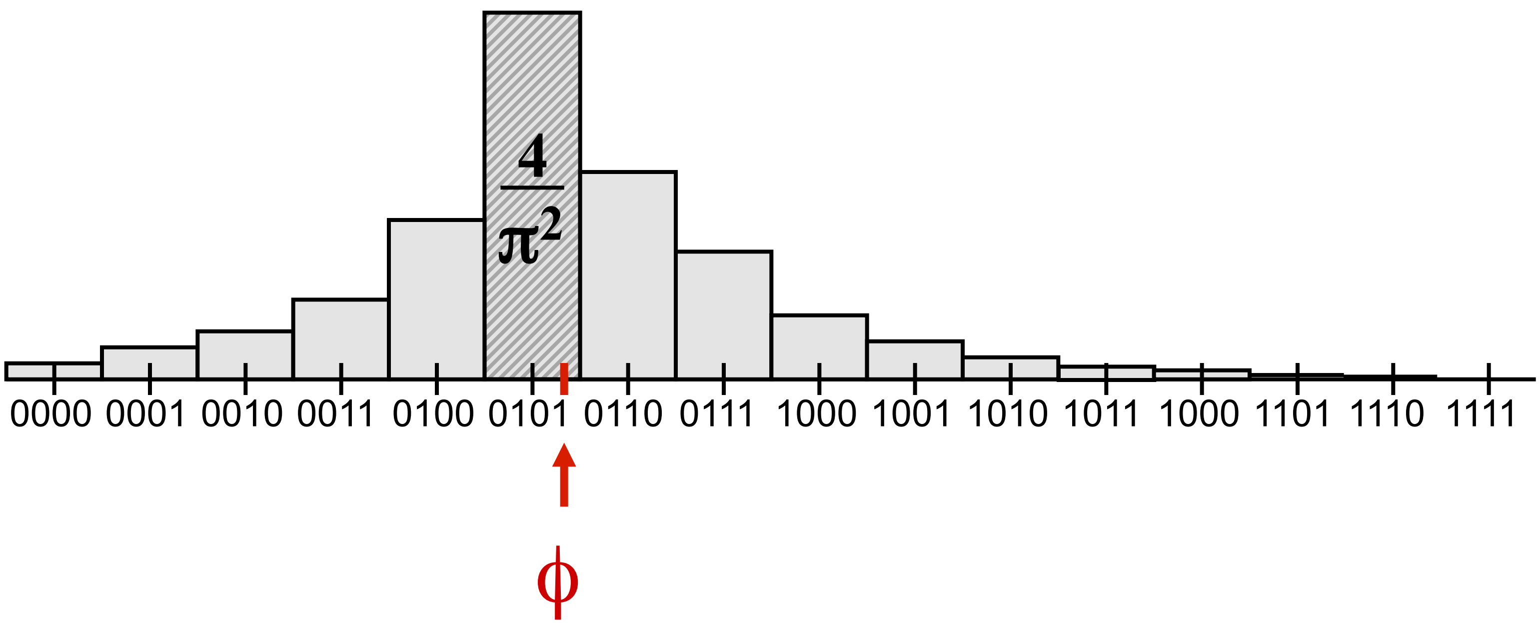
upper bounded by $2\pi\delta$

Therefore, the absolute value of the amplitude of $|y\rangle$ is at least the quotient of $(1/2^m)$(numerator/denominator), which is $2/\pi$

Algorithm for eigenvalue estimation (6)

Therefore, the probability of measuring an m-bit approximation of ϕ is always at least $4/\pi^2 \approx 0.4$

For example, when $\phi = ⅓ = 0.\underline{0101}0101010101\ldots$, the outcome probabilities look roughly like this:



Order-finding via eigenvalue estimation

Order-finding problem

Let m be an n-bit integer

Def: $\mathbf{Z}_m^* = \{x \in \{1,2,\ldots, m-1\} : \gcd(x,m) = 1\}$ (a group)

Def: $\mathrm{ord}_m(a)$ is the minimum $r > 0$ such that $a^r = 1 \pmod m$

Order-finding problem: given a and m, find $\mathrm{ord}_m(a)$

Example: $\mathbf{Z}_{21}^* = \{1,2,4,5,8,10,11,13,16,17,19,20\}$

The powers of 10 are: $1, 10, 16, 13, 4, 19, 1, 10, 16, \ldots$

Therefore, $\mathrm{ord}_{21}(10) = 6$

Note: no ***classical*** polynomial-time algorithm is known for this problem (turns out that it's as hard as factoring)

Order-finding algorithm (1)

Define: U (an operation on m qubits) as: $U|y\rangle = |ay \bmod M\rangle$

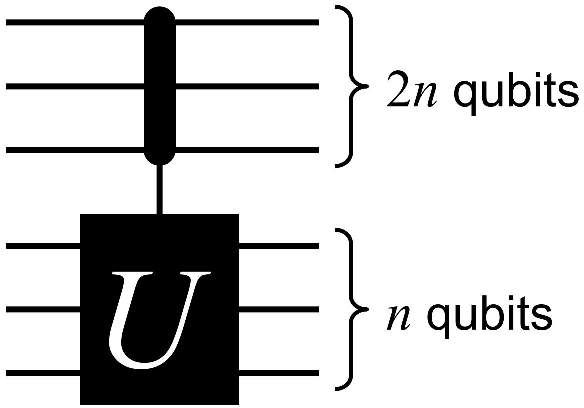
Define: $$|\psi_1\rangle = \sum_{j=0}^{r-1} e^{-2\pi i(1/r)j} \left|a^j \bmod m\right\rangle$$

Then $$U|\psi_1\rangle = \sum_{j=0}^{r-1} e^{-2\pi i(1/r)j} \left|a^{j+1} \bmod m\right\rangle$$

$$= \sum_{j=0}^{r-1} e^{2\pi i(1/r)} e^{-2\pi i(1/r)(j+1)} \left|a^{j+1} \bmod m\right\rangle$$

$$= e^{2\pi i(1/r)} |\psi_1\rangle$$

Order-finding algorithm (2)



corresponds to the mapping:
$|x\rangle|y\rangle \rightarrow |x\rangle|a^x y \bmod m\rangle$

Moreover, this mapping can be implemented with roughly $O(n^2)$ gates

The phase estimation algorithm yields a $2n$-bit estimate of $1/r$

From this, a good estimate of r can be calculated by taking the reciprocal, and rounding off to the nearest integer

Exercise: why are $2n$ bits necessary and sufficient for this?

Problem: how do we construct state $|\psi_1\rangle$ to begin with?

Bypassing the need for $|\psi_1\rangle$ (1)

Let $$|\psi_1\rangle = \sum_{j=0}^{r-1} e^{-2\pi i(1/r)j} |a^j \bmod m\rangle$$

$$|\psi_2\rangle = \sum_{j=0}^{r-1} e^{-2\pi i(2/r)j} |a^j \bmod m\rangle$$

$$\vdots$$

$$|\psi_k\rangle = \sum_{j=0}^{r-1} e^{-2\pi i(k/r)j} |a^j \bmod m\rangle$$

$$\vdots$$

$$|\psi_r\rangle = \sum_{j=0}^{r-1} e^{-2\pi i(r/r)j} |a^j \bmod m\rangle$$

Any one of these could be used in the previous procedure, to yield an estimate of k/r, from which r can be extracted

What if k is chosen randomly and kept secret?

Bypassing the need for $|\psi_1\rangle$ (2)

What if k is chosen randomly and kept secret?

Can ***still*** uniquely determine k and r, from a $2n$-bit estimate of k/r, provided they have no common factors, using the ***continued fractions algorithm****

Note: If k and r have a common factor, it is impossible because, for example, $2/3$ and $17/51$ are indistinguishable

So this is fine as long as k and r are relatively prime …

* For a discussion of the *continued fractions algorithm*, please see Appendix A4.4 in [Nielsen & Chuang]

To be continued

Introduction to Quantum Information Processing

QIC 710 / CS 678 / PH 767 / CO 681 / AM 871

Lecture 10 (2013)

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

Contunuation of:

Order-finding via eigenvalue estimation

Order-finding problem

Let m be an n-bit integer

Def: $\mathbf{Z}_m{}^* = \{x \in \{1,2,\ldots, m-1\} : \gcd(x,m) = 1\}$ (a group)

Def: $\mathrm{ord}_m(a)$ is the minimum $r > 0$ such that $a^r = 1 \pmod m$

Order-finding problem: given a and m, find $\mathrm{ord}_m(a)$

Example: $\mathbf{Z}_{21}{}^* = \{1,2,4,5,8,10,11,13,16,17,19,20\}$

The powers of 10 are: $1, 10, 16, 13, 4, 19, 1, 10, 16, \ldots$

Therefore, $\mathrm{ord}_{21}(10) = 6$

Note: no ***classical*** polynomial-time algorithm is known for this problem (turns out that it's as hard as factoring)

Order-finding algorithm (1)

Define: U (an operation on m qubits) as: $U|y\rangle = |ay \bmod M\rangle$

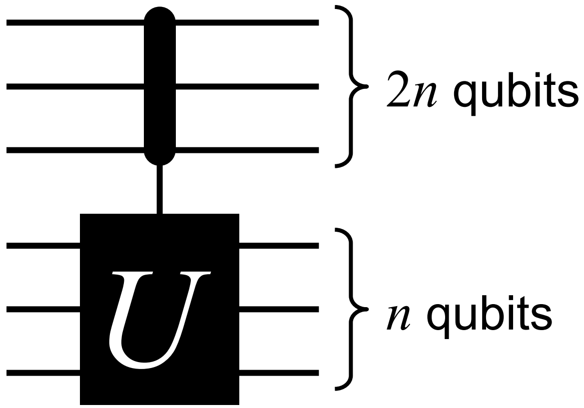
Define: $$|\psi_1\rangle = \sum_{j=0}^{r-1} e^{-2\pi i(1/r)j} |a^j \bmod m\rangle$$

Then $$U|\psi_1\rangle = \sum_{j=0}^{r-1} e^{-2\pi i(1/r)j} |a^{j+1} \bmod m\rangle$$

$$= \sum_{j=0}^{r-1} e^{2\pi i(1/r)} e^{-2\pi i(1/r)(j+1)} |a^{j+1} \bmod m\rangle$$

$$= e^{2\pi i(1/r)} |\psi_1\rangle$$

Order-finding algorithm (2)



corresponds to the mapping:
$|x\rangle|y\rangle \rightarrow |x\rangle|a^x y \bmod m\rangle$

Moreover, this mapping can be implemented with roughly $O(n^2)$ gates

The phase estimation algorithm yields a $2n$-bit estimate of $1/r$

From this, a good estimate of r can be calculated by taking the reciprocal, and rounding off to the nearest integer

Exercise: why are $2n$ bits necessary and sufficient for this?

Problem: how do we construct state $|\psi_1\rangle$ to begin with?

Bypassing the need for $|\psi_1\rangle$ (1)

Let
$$|\psi_1\rangle = \sum_{j=0}^{r-1} e^{-2\pi i (1/r) j} |a^j \bmod m\rangle$$

$$|\psi_2\rangle = \sum_{j=0}^{r-1} e^{-2\pi i (2/r) j} |a^j \bmod m\rangle$$

$$\vdots$$

$$|\psi_k\rangle = \sum_{j=0}^{r-1} e^{-2\pi i (k/r) j} |a^j \bmod m\rangle$$

$$\vdots$$

$$|\psi_r\rangle = \sum_{j=0}^{r-1} e^{-2\pi i (r/r) j} |a^j \bmod m\rangle$$

Any one of these could be used in the previous procedure, to yield an estimate of k/r, from which r can be extracted

What if k is chosen randomly and kept secret?

Bypassing the need for $|\psi_1\rangle$ (2)

What if k is chosen randomly and kept secret?

Can ***still*** uniquely determine k and r, from a $2n$-bit estimate of k/r, provided they have no common factors, using the ***continued fractions algorithm****

Note: If k and r have a common factor, it is impossible because, for example, $2/3$ and $17/51$ are indistinguishable

So this is fine as long as k and r are relatively prime …

* For a discussion of the *continued fractions algorithm*, please see Appendix A4.4 in [Nielsen & Chuang]

Bypassing the need for $|\psi_1\rangle$ (3)

What is the probability that k and r are relatively prime?

Recall that k is randomly chosen from $\{1,\ldots,r\}$
The probability that this occurs is $\phi(r)/r$, where ϕ is ***Euler's totient function***

It is known that $\phi(r) = \Omega(r/\log\log r)$, which implies that the above probability is at least $\Omega(1/\log\log r) = \Omega(1/\log n)$

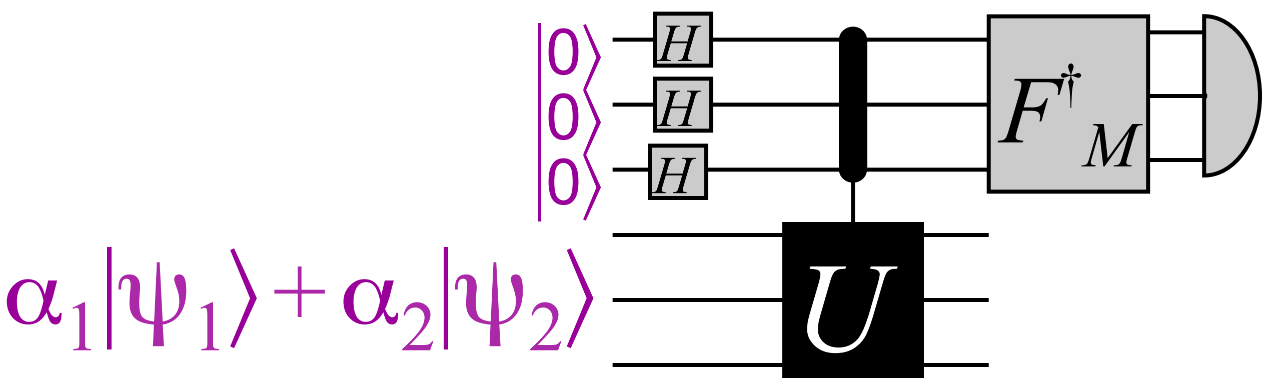
Therefore, the success probability is at least $\Omega(1/\log n)$

Is this good enough? Yes, because it means that the success probability can be amplified to any constant < 1 by repeating $O(\log n)$ times (so still polynomial in n)

But we'd still need to generate a random $|\psi_k\rangle$ here …

Bypassing the need for $|\psi_1\rangle$ (4)

Returning to the phase estimation problem, suppose that $|\psi_1\rangle$ and $|\psi_2\rangle$ have respective eigenvalues $e^{2\pi i\phi_1}$ and $e^{2\pi i\phi_2}$, and that $\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle$ is used in place of an eigenvector:



What will the outcome be?

It will be an estimate of $\begin{cases} \phi_1 \text{ with probability } |\alpha_1|^2 \\ \phi_2 \text{ with probability } |\alpha_2|^2 \end{cases}$

Showing this is left as an exercise; related questions in Assignment #3

Bypassing the need for $|\psi_1\rangle$ (5)

Along similar lines, the state $\frac{1}{\sqrt{r}}\sum_{k=1}^{r}|\psi_k\rangle$

yields results equivalent to choosing a $|\psi_k\rangle$ at random

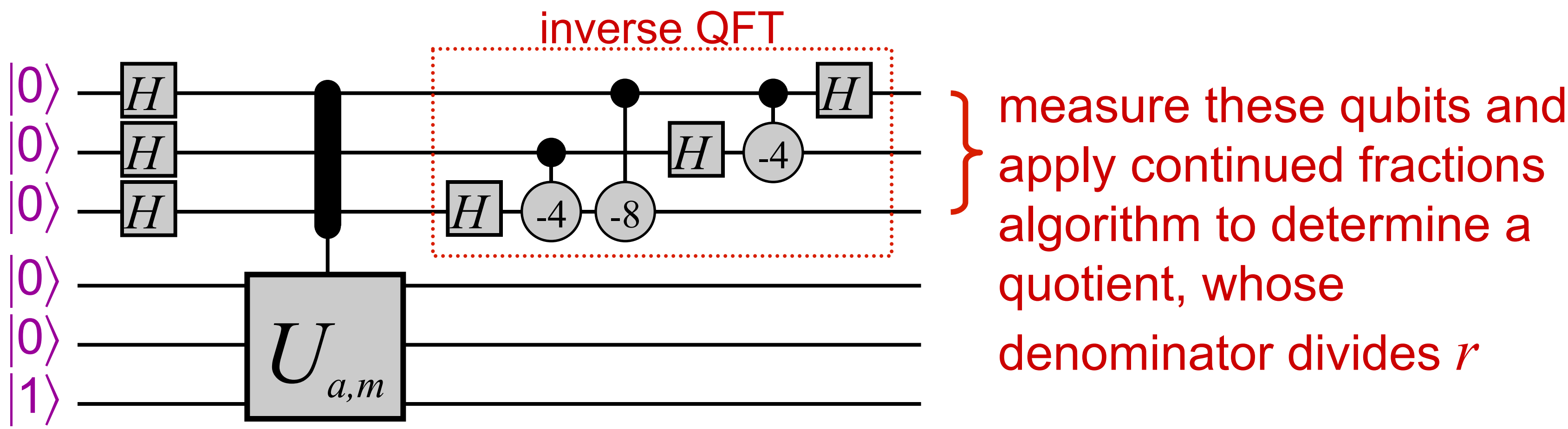
Is it hard to construct the state $\frac{1}{\sqrt{r}}\sum_{k=1}^{r}|\psi_k\rangle$?

In fact, ***this*** is something that is easy, since

$$\frac{1}{\sqrt{r}}\sum_{k=1}^{r}|\psi_k\rangle = \frac{1}{\sqrt{r}}\sum_{k=1}^{r}\sum_{j=0}^{r-1} e^{-2\pi i(k/r)j}\left|a^j \bmod m\right\rangle = |1\rangle$$

This is how the previous requirement for $|\psi_1\rangle$ is bypassed

Quantum algorithm for order-finding



$$U_{a,m}|y\rangle = |ay \bmod m\rangle$$

Number of gates for $\Omega(1/\log n)$ success probability is: $O(n^2 \log n \operatorname{loglog} n)$

For ***constant*** success probability, repeat $O(\log n)$ times and take the smallest resulting r such that $a^r = 1 \pmod m$

Reduction from factoring to order-finding

The integer factorization problem

Input: m (n-bit integer; we can assume it is composite)

Output: p, q (each greater than 1) such that $pq = m$

Note 1: no efficient (polynomial-time) classical algorithm is known for this problem

Note 2: given any efficient algorithm for the above, we can recursively apply it to fully factor m into primes* efficiently

* A polynomial-time ***classical*** algorithm for ***primality testing*** exists

Factoring prime-powers

There is a straightforward ***classical*** algorithm for factoring numbers of the form $m = p^k$, for some prime p

What is this algorithm?

Therefore, the interesting remaining case is where m has at least two distinct prime factors

Numbers other than prime-powers

Proposed quantum algorithm (repeatedly do):

1. randomly choose $a \in \{2, 3, \ldots, m-1\}$
2. compute $g = \gcd(a, m)$
3. **if** $g > 1$ **then**

   output g, m/g

   else

   compute $r = \mathrm{ord}_m(a)$ (quantum part)

   if r is even **then**

   compute $x = a^{r/2} - 1 \bmod m$

   compute $h = \gcd(x, m)$

   if $h > 1$ **then** output h, m/h

Analysis:

we have $m \mid a^r - 1$

so $m \mid (a^{r/2}+1)(a^{r/2}-1)$

thus, either $m \mid a^{r/2} + 1$

or $\gcd(a^{r/2} + 1, m)$

is a nontrivial factor of m

It can be shown that at least half of the $a \in \{2, 3, \ldots, m-1\}$ are have order even and result in $\gcd(a^{r/2} + 1, m)$ being a nontrivial factor of m

New topic:
Density matrices and operations on them

More state distinguishing problems

More state distinguishing problems

Which of these states are distinguishable? Divide them into equivalence classes:

1. $|0\rangle + |1\rangle$
2. $-|0\rangle - |1\rangle$
3. $\begin{cases} |0\rangle \text{ with prob. } \tfrac{1}{2} \\ |1\rangle \text{ with prob. } \tfrac{1}{2} \end{cases}$
4. $\begin{cases} |0\rangle + |1\rangle & \text{with prob. } \tfrac{1}{2} \\ |0\rangle - |1\rangle & \text{with prob. } \tfrac{1}{2} \end{cases}$
5. $\begin{cases} |0\rangle & \text{with prob. } \tfrac{1}{2} \\ |0\rangle + |1\rangle & \text{with prob. } \tfrac{1}{2} \end{cases}$
6. $\begin{cases} |0\rangle & \text{with prob. } \tfrac{1}{4} \\ |1\rangle & \text{with prob. } \tfrac{1}{4} \\ |0\rangle + |1\rangle & \text{with prob. } \tfrac{1}{4} \\ |0\rangle - |1\rangle & \text{with prob. } \tfrac{1}{4} \end{cases}$
7. The first qubit of $|01\rangle - |10\rangle$

This is a probabilistic mixed state

Answers later on ...

Density matrix formalism

Density matrices (1)

Until now, we've represented quantum states as ***vectors*** (e.g. $|\psi\rangle$, and all such states are called ***pure states***)

An alternative way of representing quantum states is in terms of ***density matrices*** (a.k.a. ***density operators***)

The density matrix of a pure state $|\psi\rangle$ is the matrix $\rho = |\psi\rangle\langle\psi|$

Example: the density matrix of $\alpha|0\rangle + \beta|1\rangle$ is

$$\rho = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \begin{bmatrix} \alpha^* & \beta^* \end{bmatrix} = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix}$$

Density matrices (2)

How do quantum operations work using density matrices?

Effect of a unitary operation on a density matrix:
applying U to ρ yields $U\rho U^\dagger$

(this is because the modified state is $U|\psi\rangle\langle\psi|U^\dagger$)

Effect of a measurement on a density matrix:
measuring state ρ with respect to the basis $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_d\rangle$,
yields the kth outcome with probability $\langle\varphi_k|\rho|\varphi_k\rangle$

(this is because $\langle\varphi_k|\rho|\varphi_k\rangle = \langle\varphi_k|\psi\rangle\langle\psi|\varphi_k\rangle = |\langle\varphi_k|\psi\rangle|^2$)

—and the state collapses to $|\varphi_k\rangle\langle\varphi_k|$

Density matrices (3)

A probability distribution on pure states is called a ***mixed state***:

$((|\psi_1\rangle, p_1), (|\psi_2\rangle, p_2), \ldots, (|\psi_d\rangle, p_d))$

The ***density matrix*** associated with such a mixed state is:

$$\rho = \sum_{k=1}^{d} p_k |\psi_k\rangle\langle\psi_k|$$

Example: the density matrix for $((|0\rangle, ½), (|1\rangle, ½))$ is:

$$\frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Question: what is the density matrix of

$((|0\rangle + |1\rangle, ½), (|0\rangle - |1\rangle, ½))$?

Density matrices (4)

How do quantum operations work for these ***mixed*** states?

Effect of a unitary operation on a density matrix:

applying U to ρ ***still*** yields $U\rho U^\dagger$

This is because the modified state is:

$$\sum_{k=1}^{d} p_k U|\psi_k\rangle\langle\psi_k|U^t = U\left(\sum_{k=1}^{d} p_k|\psi_k\rangle\langle\psi_k|\right)U^t = U\rho U^t$$

Effect of a measurement on a density matrix:

measuring state ρ with respect to the basis $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_d\rangle$,

still yields the k^{th} outcome with probability $\langle\varphi_k|\rho|\varphi_k\rangle$

Why?

Recap: density matrices

Quantum operations in terms of density matrices:

- Applying U to ρ yields $U\rho U^{\dagger}$

- Measuring state ρ with respect to the basis $|\varphi_1\rangle$, $|\varphi_2\rangle$,…, $|\varphi_d\rangle$, yields: k^{th} outcome with probability $\langle\varphi_k|\rho|\varphi_k\rangle$
  —and causes the state to collapse to $|\varphi_k\rangle\langle\varphi_k|$

Since these are expressible in terms of density matrices alone (independent of any specific probabilistic mixtures), states with identical density matrices are ***operationally indistinguishable***

Return to state distinguishing problems …

State distinguishing problems (1)

The ***density matrix*** of the mixed state

$((|\psi_1\rangle, p_1), (|\psi_2\rangle, p_2), \ldots, (|\psi_d\rangle, p_d))$ is: $\rho = \sum_{k=1}^{d} p_k |\psi_k\rangle\langle\psi_k|$

Examples (from earlier in lecture):

1. & 2. $|0\rangle + |1\rangle$ and $-|0\rangle - |1\rangle$ both have $\rho = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$

3. $\begin{cases} |0\rangle \text{ with prob. } ½ \\ |1\rangle \text{ with prob. } ½ \end{cases}$

4. $\begin{cases} |0\rangle + |1\rangle \text{ with prob. } ½ \\ |0\rangle - |1\rangle \text{ with prob. } ½ \end{cases}$

6. $\begin{cases} |0\rangle \text{ with prob. } ¼ \\ |1\rangle \text{ with prob. } ¼ \\ |0\rangle + |1\rangle \text{ with prob. } ¼ \\ |0\rangle - |1\rangle \text{ with prob. } ¼ \end{cases}$

(3, 4, 6): $\rho = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

State distinguishing problems (2)

Examples (continued):

5. $\begin{cases} |0\rangle & \text{with prob. ½} \\ |0\rangle + |1\rangle & \text{with prob. ½} \end{cases}$

has: $$\rho = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} = \begin{bmatrix} 3/4 & 1/2 \\ 1/2 & 1/4 \end{bmatrix}$$

7. The first qubit of $|01\rangle - |10\rangle$ **...? (later)**

Introduction to Quantum Information Processing
QIC 710 / CS 678 / PH 767 / CO 681 / AM 871

Lecture 11 (2013)

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

Characterizing density matrices

$$\boxed{\rho = \sum_{k=1}^{d} p_k |\psi_k\rangle\langle\psi_k|}$$

Three properties of ρ :

- $\text{Tr}\rho = 1$ $(\text{Tr}M = M_{11} + M_{22} + \ldots + M_{dd})$
- $\rho = \rho^\dagger$ (i.e. ρ is *Hermitian)*
- $\langle\varphi|\rho|\varphi\rangle \geq 0$, for all states $|\varphi\rangle$ (i.e. ρ is *positive semidefinite*)

Moreover, for ***any*** matrix ρ satisfying the above properties, there exists a probabilistic mixture whose density matrix is ρ

Exercise: show this

Taxonomy of various normal matrices

Normal matrices

Definition: A matrix M is ***normal*** if $M^\dagger M = MM^\dagger$

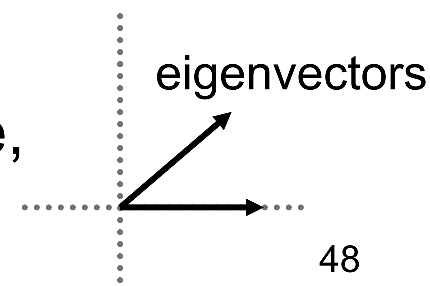
Theorem: M is normal iff there exists a unitary U such that $M = U^\dagger D U$, where D is diagonal (i.e. unitarily diagonalizable)

$$D = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_d \end{bmatrix}$$

Examples of ***ab***normal matrices:

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ is not even diagonalizable

$\begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$ is diagonalizable, but not unitarily



Unitary and Hermitian matrices

Normal:
$$M = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_d \end{bmatrix}$$
with respect to ***some*** orthonormal basis

Unitary: $M^\dagger M = I$ which implies $|\lambda_k|^2 = 1$, for all k

Hermitian: $M = M^\dagger$ which implies $\lambda_k \in \mathbf{R}$, for all k

Question: which matrices are both unitary ***and*** Hermitian?

Answer: reflections ($\lambda_k \in \{+1,-1\}$, for all k)

Positive semidefinite

Positive semidefinite: Hermitian and $\lambda_k \geq 0$, for all k

Theorem: M is positive semidefinite iff M is Hermitian and, for all $|\varphi\rangle$, $\langle\varphi|M|\varphi\rangle \geq 0$

(**Positive *definite***: $\lambda_k > 0$, for all k)

Projectors and density matrices

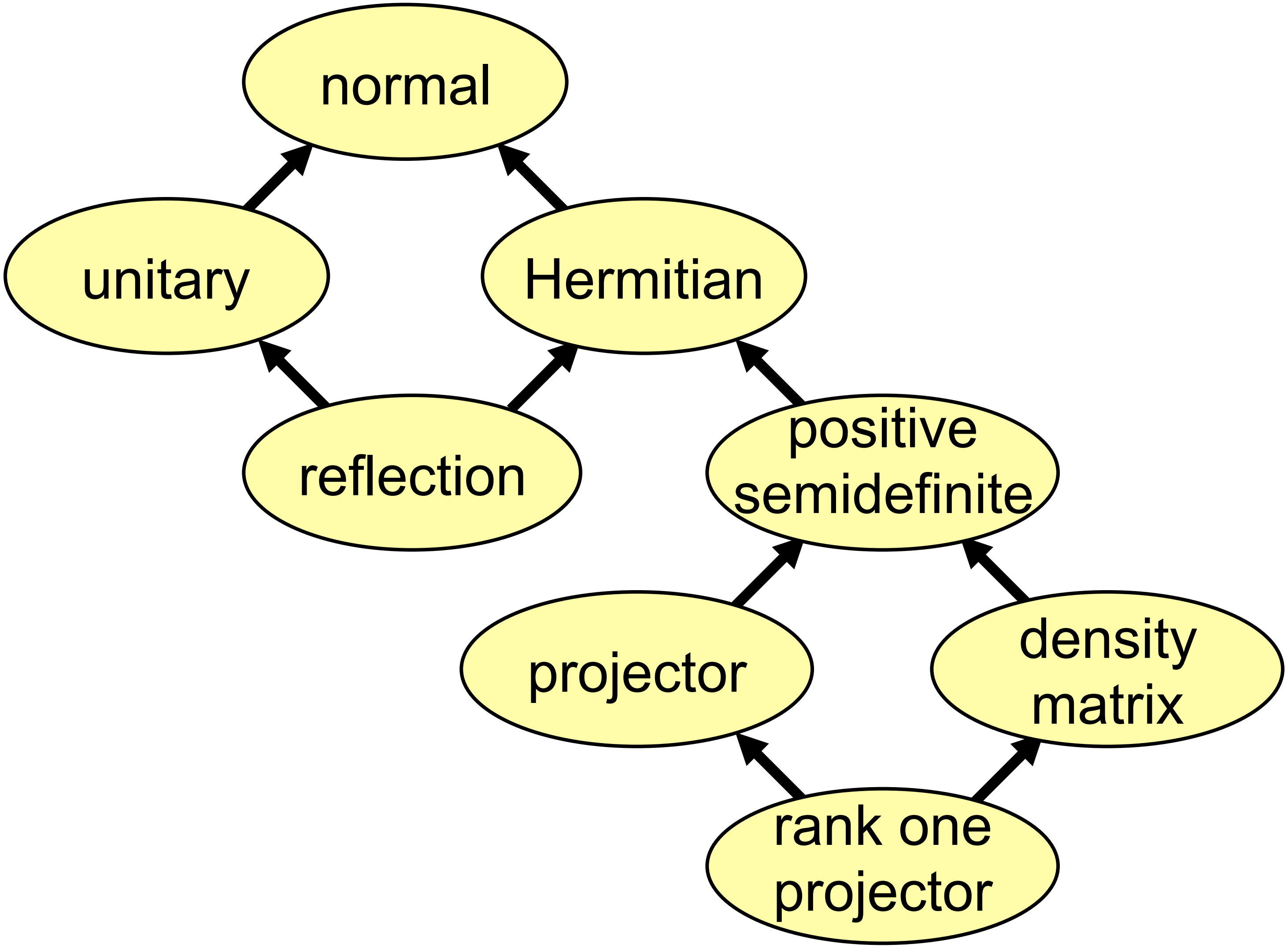
Projector: Hermitian and $M^2 = M$, which implies that M is positive semidefinite and $\lambda_k \in \{0,1\}$, for all k

Density matrix: positive semidefinite and Tr $M = 1$, so $\sum_{k=1}^{d} \lambda_k = 1$

Question: which matrices are both projectors ***and*** density matrices?

Answer: rank-1 projectors ($\lambda_k = 1$ if $k = j$; otherwise $\lambda_k = 0$)

Taxonomy of normal matrices



Bloch sphere for qubits

Bloch sphere for qubits (1)

Consider the set of all 2x2 density matrices ρ

They have a nice representation in terms of the ***Pauli matrices***:

$$\sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Note that these matrices—combined with I—form a ***basis*** for the vector space of all 2x2 matrices

We will express density matrices ρ in this basis

Note that the coefficient of I is ½, since X, Y, Y are traceless

Bloch sphere for qubits (2)

We will express $\rho = \dfrac{I + c_x X + c_y Y + c_z Z}{2}$

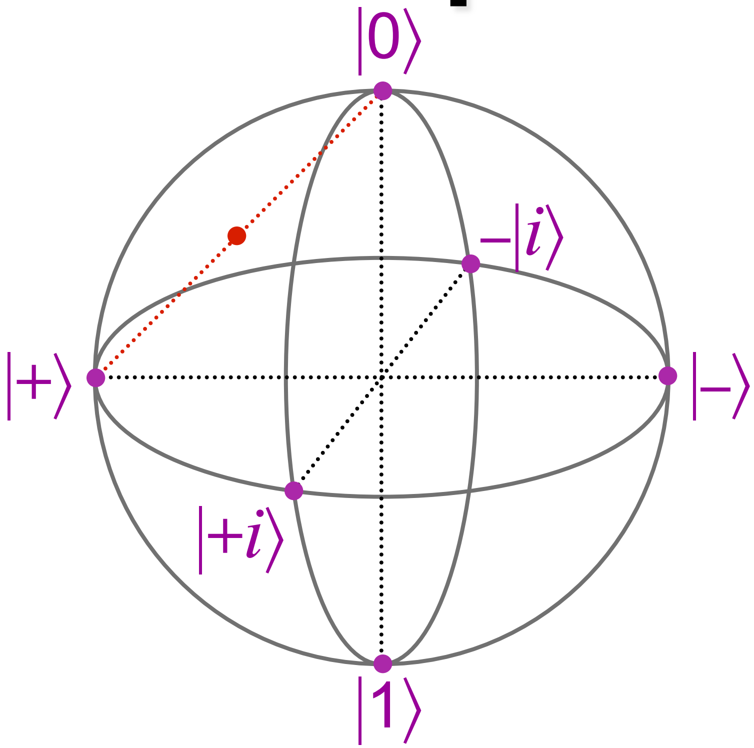
First consider the case of pure states $|\psi\rangle\langle\psi|$, where, without loss of generality, $|\psi\rangle = \cos(\theta)|0\rangle + e^{2i\phi}\sin(\theta)|1\rangle$ $(\theta, \phi \in \mathbf{R})$

$$\rho = \begin{bmatrix} \cos^2\theta & e^{-i2\varphi}\cos\theta\sin\theta \\ e^{i2\varphi}\cos\theta\sin\theta & \sin^2\theta \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1+\cos(2\theta) & e^{-i2\varphi}\sin(2\theta) \\ e^{i2\varphi}\sin(2\theta) & 1-\cos(2\theta) \end{bmatrix}$$

Therefore $c_z = \cos(2\theta)$, $c_x = \cos(2\phi)\sin(2\theta)$, $c_y = \sin(2\phi)\sin(2\theta)$

These are ***polar coordinates*** of a unit vector $(c_x, c_y, c_z) \in \mathbf{R}^3$

Bloch sphere for qubits (3)



$|+\rangle = |0\rangle + |1\rangle$

$|-\rangle = |0\rangle - |1\rangle$

$|+i\rangle = |0\rangle + i|1\rangle$

$|-i\rangle = |0\rangle - i|1\rangle$

Note that ***orthogonal*** corresponds to ***antipodal*** here

Pure states are on the surface, and mixed states are inside (being weighted averages of pure states)

Distinguishing mixed states

Distinguishing mixed states (1)

What's the best distinguishing strategy between these two mixed states?

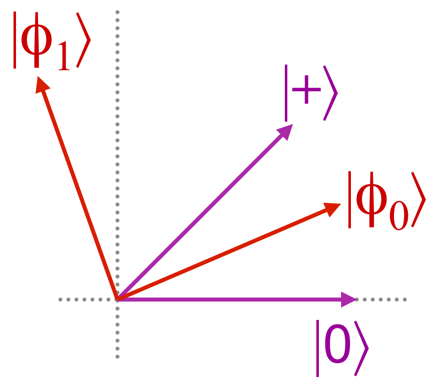
$$\begin{cases} |0\rangle & \text{with prob. } 1/2 \\ |0\rangle + |1\rangle & \text{with prob. } 1/2 \end{cases}$$

$$\rho_1 = \begin{bmatrix} 3/4 & 1/2 \\ 1/2 & 1/4 \end{bmatrix}$$

$$\begin{cases} |0\rangle & \text{with prob. } 1/2 \\ |1\rangle & \text{with prob. } 1/2 \end{cases}$$

$$\rho_2 = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

ρ_1 also arises from this orthogonal mixture:



… as does ρ_2 from:

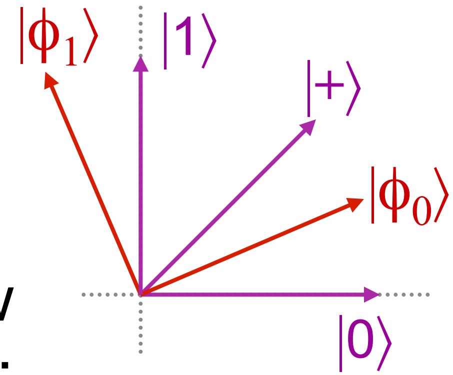
$$\begin{cases} |\phi_0\rangle & \text{with prob. } \cos^2(\pi/8) \\ |\phi_1\rangle & \text{with prob. } \sin^2(\pi/8) \end{cases}$$

$$\begin{cases} |\phi_0\rangle & \text{with prob. } 1/2 \\ |\phi_1\rangle & \text{with prob. } 1/2 \end{cases}$$

Distinguishing mixed states (2)

We've effectively found an orthonormal basis $|\phi_0\rangle$, $|\phi_1\rangle$ in which both density matrices are diagonal:

$$\rho_2' = \begin{bmatrix} \cos^2(\pi/8) & 0 \\ 0 & \sin^2(\pi/8) \end{bmatrix} \qquad \rho_1' = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$



Rotating $|\phi_0\rangle$, $|\phi_1\rangle$ to $|0\rangle$, $|1\rangle$ the scenario can now be examined using classical probability theory:

Distinguish between two ***classical*** coins, whose probabilities of "heads" are $\cos^2(\pi/8)$ and ½ respectively (details: exercise)

Question: what do we do if we aren't so lucky to get two density matrices that are simultaneously diagonalizable?

General quantum operations

General quantum operations (1)

Also known as:
"quantum channels"
"completely positive trace preserving maps",
"admissible operations"

Let $A_1, A_2, \ldots, A_m$ be matrices satisfying $\sum_{j=1}^{m} A_j^\dagger A_j = I$

Then the mapping $\rho \mapsto \sum_{j=1}^{m} A_j \rho A_j^\dagger$ is a general quantum op

Note: $A_1, A_2, \ldots, A_m$ do not have to be square matrices

Example 1 (unitary op): applying U to ρ yields $U\rho U^\dagger$

General quantum operations (2)

Example 2 (decoherence): let $A_0 = |0\rangle\langle 0|$ and $A_1 = |1\rangle\langle 1|$

This quantum op maps ρ to $|0\rangle\langle 0|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1|$

For $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,
$$\begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix} \mapsto \begin{bmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{bmatrix}$$

Corresponds to measuring ρ "without looking at the outcome"

After looking at the outcome, ρ becomes $\begin{cases} |0\rangle\langle 0| & \text{with prob. } |\alpha|^2 \\ |1\rangle\langle 1| & \text{with prob. } |\beta|^2 \end{cases}$

General quantum operations (3)

Example 3 (discarding the second of two qubits):

Let $A_0 = I \otimes \langle 0| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ and $A_1 = I \otimes \langle 1| = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

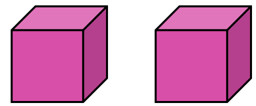
States of the form $\rho \otimes \sigma$ (product states) become ρ

State $\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}\langle 00| + \frac{1}{\sqrt{2}}\langle 11|\right)$ becomes $\frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Note 1: it's the same density matrix as for $((½, |0\rangle), (½, |1\rangle))$

Note 2: the operation is called the ***partial trace*** $\mathrm{Tr}_2\, \rho$

More about the partial trace

Two quantum registers  in states σ and μ (resp.) are ***independent*** when the combined system is in state $\rho = \sigma \otimes \mu$

If the 2nd register is discarded, state of the 1st register remains σ

In general, the state of a two-register system may not be of the form $\sigma \otimes \mu$ (it may contain ***entanglement*** or ***correlations***)

The ***partial trace*** Tr_2 gives the effective state of the first register

For d-dimensional registers, Tr_2 is defined with respect to the operators $A_k = I \otimes \langle \phi_k |$, where $|\phi_0\rangle, |\phi_1\rangle, \ldots, |\phi_{d-1}\rangle$ can be any orthonormal basis

The **partial trace** $\mathrm{Tr}_2 \rho$, can also be characterized as the unique linear operator satisfying the identity $\mathrm{Tr}_2(\sigma \otimes \mu) = \sigma$

Partial trace continued

For 2-qubit systems, the partial trace is explicitly

$$\mathrm{Tr}_2 \begin{bmatrix} \rho_{00,00} & \rho_{00,01} & \rho_{00,10} & \rho_{00,11} \\ \rho_{01,00} & \rho_{01,01} & \rho_{01,10} & \rho_{01,11} \\ \rho_{10,00} & \rho_{10,01} & \rho_{10,10} & \rho_{10,11} \\ \rho_{11,00} & \rho_{11,01} & \rho_{11,10} & \rho_{11,11} \end{bmatrix} = \begin{bmatrix} \rho_{00,00} + \rho_{01,01} & \rho_{00,10} + \rho_{01,11} \\ \rho_{10,00} + \rho_{11,01} & \rho_{10,10} + \rho_{11,11} \end{bmatrix}$$

and

$$\mathrm{Tr}_1 \begin{bmatrix} \rho_{00,00} & \rho_{00,01} & \rho_{00,10} & \rho_{00,11} \\ \rho_{01,00} & \rho_{01,01} & \rho_{01,10} & \rho_{01,11} \\ \rho_{10,00} & \rho_{10,01} & \rho_{10,10} & \rho_{10,11} \\ \rho_{11,00} & \rho_{11,01} & \rho_{11,10} & \rho_{11,11} \end{bmatrix} = \begin{bmatrix} \rho_{00,00} + \rho_{10,10} & \rho_{00,01} + \rho_{10,11} \\ \rho_{01,00} + \rho_{11,10} & \rho_{01,01} + \rho_{11,11} \end{bmatrix}$$

General quantum operations (4)

Example 4 (adding an extra qubit):

Just one operator $A_0 = I \otimes |0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$

States of the form ρ become $\rho \otimes |0\rangle\langle 0|$

More generally, to add a register in state $|\phi\rangle$, use the operator $A_0 = I \otimes |\phi\rangle$

POVM measurements

(POVM = Positive Operator Valued Measure)

POVM measurements (1)

Let $A_1, A_2, \ldots, A_m$ be matrices satisfying $\sum_{j=1}^{m} A_j^\dagger A_j = I$

Corresponding ***POVM measurement*** is a stochastic operation on ρ that, with probability $\mathrm{Tr}\left(A_j \rho A_j^\dagger\right)$, produces outcome:

$$\begin{cases} j & \text{(classical information)} \\ \dfrac{A_j \rho A_j^\dagger}{\mathrm{Tr}\left(A_j \rho A_j^\dagger\right)} & \text{(the collapsed quantum state)} \end{cases}$$

Example 1: $A_j = |\phi_j\rangle\langle\phi_j|$ (orthogonal projectors)

This reduces to our previously defined measurements …

POVM measurements (2)

When $A_j = |\phi_j\rangle\langle\phi_j|$ are orthogonal projectors and $\rho = |\psi\rangle\langle\psi|$,

$$\begin{aligned}\mathrm{Tr}\left(A_j \rho A_j^\dagger\right) &= \mathrm{Tr}|\phi_j\rangle\langle\phi_j|\psi\rangle\langle\psi|\phi_j\rangle\langle\phi_j| \\ &= \langle\phi_j|\psi\rangle\langle\psi|\phi_j\rangle\langle\phi_j|\phi_j\rangle \\ &= |\langle\phi_j|\psi\rangle|^2\end{aligned}$$

Moreover, $$\frac{A_j \rho A_j^\dagger}{\mathrm{Tr}\left(A_j \rho A_j^\dagger\right)} = \frac{|\varphi_j\rangle\langle\varphi_j|\psi\rangle\langle\psi|\varphi_j\rangle\langle\varphi_j|}{\left|\langle\varphi_j|\psi\rangle\right|^2} = |\varphi_j\rangle\langle\varphi_j|$$