Introduction to Quantum Information Processing

CS 467 / CS 667
Phys 667 / Phys 767
C&O 481 / C&O 681

Lecture 10 (2008)

Richard Cleve
DC 2117
cleve@cs.uwaterloo.ca

Order-finding via eigenvalue estimation

Order-finding problem

Let M be an m-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

Order-finding algorithm (1)

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

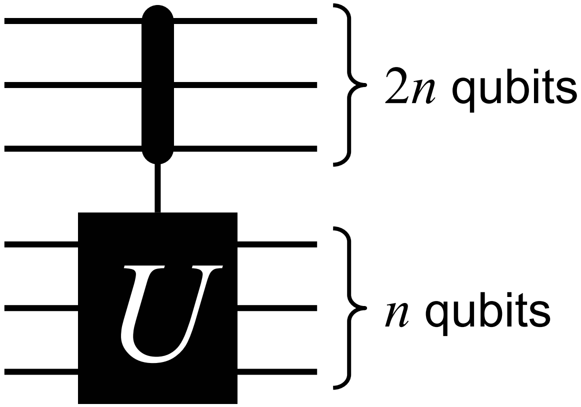
Define: $$|\psi_1\rangle = \sum_{j=0}^{r-1} e^{-2\pi i(1/r)j} \left|a^j \bmod M\right\rangle$$

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

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

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

$$\vdots$$

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

$$\vdots$$

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

Can still uniquely determine k and r, provided they have no common factors (and $O(\log n)$ trials suffice for this)

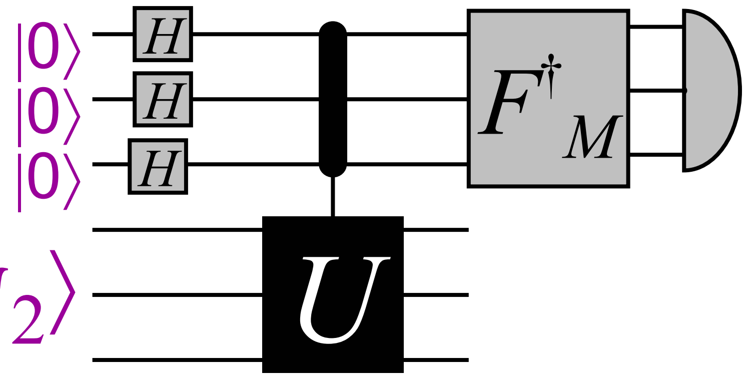
Any one of these could be used in the previous procedure, to yield an estimate of k/r, from which r can be extracted

What if k is chosen randomly and kept secret?

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

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 eigenvalue:

$\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle$



What will the outcome be?

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

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

Using the state

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

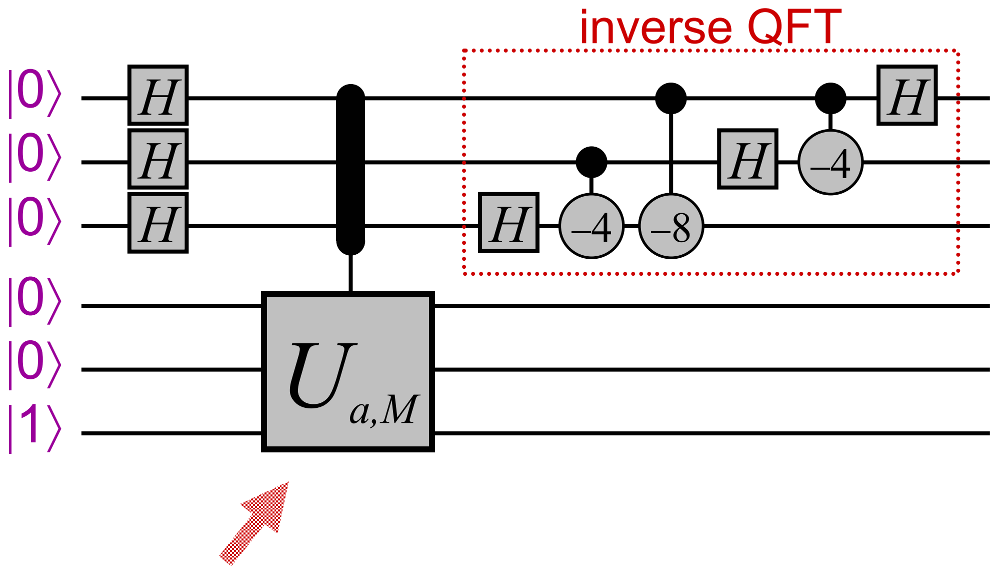
Is it hard to construct the state $\frac{1}{\sqrt{r}}\sum_{k=1}^{r}|\psi_k\rangle$?

In fact, it's 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



measure these qubits and apply continued fractions* algorithm to determine a quotient, whose denominator divides r

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

Number of gates for a constant success probability is:
$O(n^2 \log n \log\log n)$

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

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 $pq = N$

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 $M \,|\, a^r - 1$

so $M \,|\, (a^{r/2}+1)(a^{r/2}-1)$

thus, either $M \,|\, a^{r/2}+1$

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

is a nontrivial factor of M

latter event occurs with probability ≥ ½

Introduction to Quantum Information Processing

CS 467 / CS 667
Phys 667 / Phys 767
C&O 481 / C&O 681

Lecture 11 (2008)

Richard Cleve
DC 2117
cleve@cs.uwaterloo.ca

Universal sets of gates

A universal set of gates (1)

Main Theorem: any unitary operation U acting on k qubits can be decomposed into $O(4^k)$ CNOT and one-qubit gates

Proof sketch (for a slightly worse bound of $O(k^2 4^k)$) **:**

We first show how to simulate a controlled-U, for any one-qubit unitary U

Straightforward to show: every one-qubit unitary matrix can be expressed as a product of the form

$$\begin{bmatrix} e^{i\delta} & 0 \\ 0 & e^{i\delta} \end{bmatrix} \begin{bmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{bmatrix} \begin{bmatrix} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & \cos(\theta/2) \end{bmatrix} \begin{bmatrix} e^{i\beta/2} & 0 \\ 0 & e^{-i\beta/2} \end{bmatrix}$$

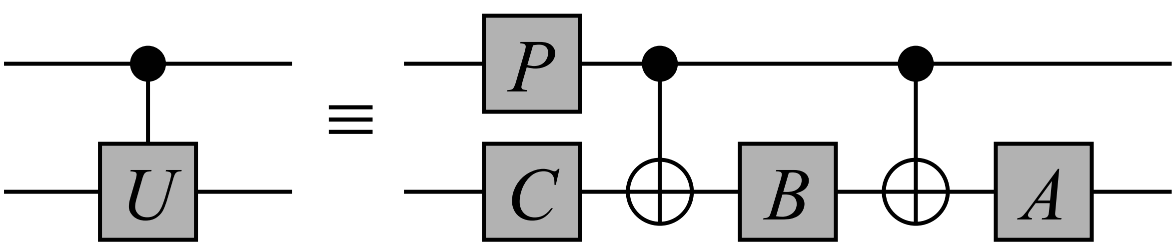
A universal set of gates (2)

This can be used to show that, for every one-qubit unitary U, there exist A, B, C, and λ, such that:

- $A\,B\,C = I$
- $e^{i\lambda}\,A\,X\,B\,X\,C = U$, where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Exercise: show how this follows

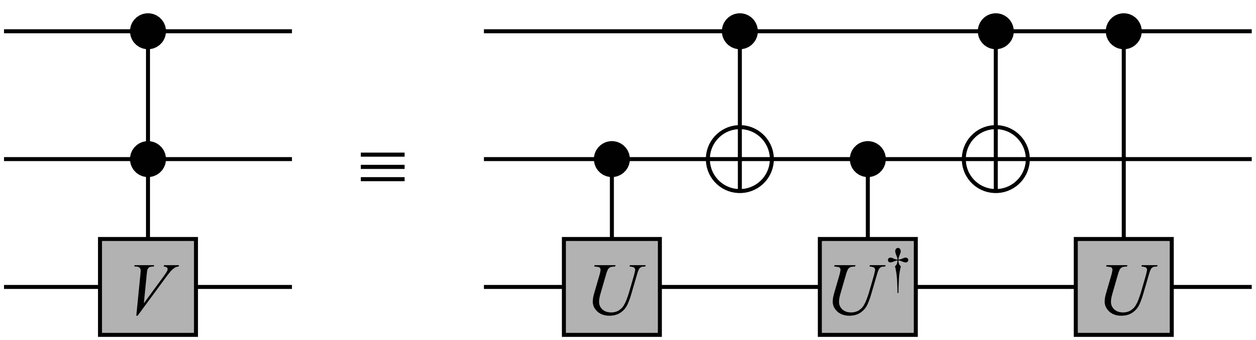
The fact implies that



where $P = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\lambda} \end{pmatrix}$

A universal set of gates (3)

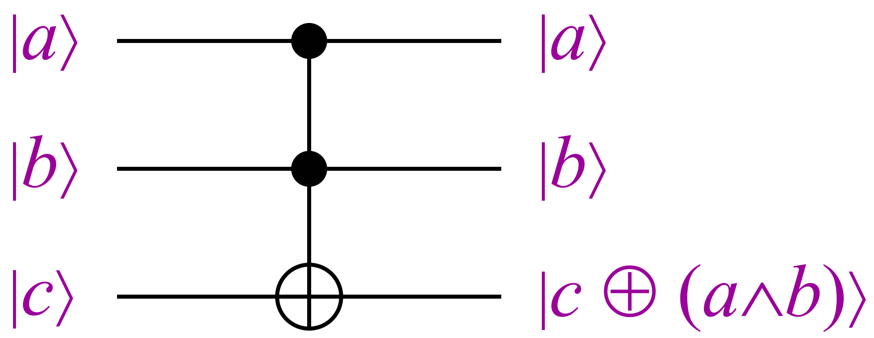
Controlled-U gates can also simulate controlled-controlled-V gates, for an arbitrary unitary one-qubit unitary V:



where $V = U^2$

A universal set of gates (4)

Example: Toffoli gate
"controlled-controlled-NOT"

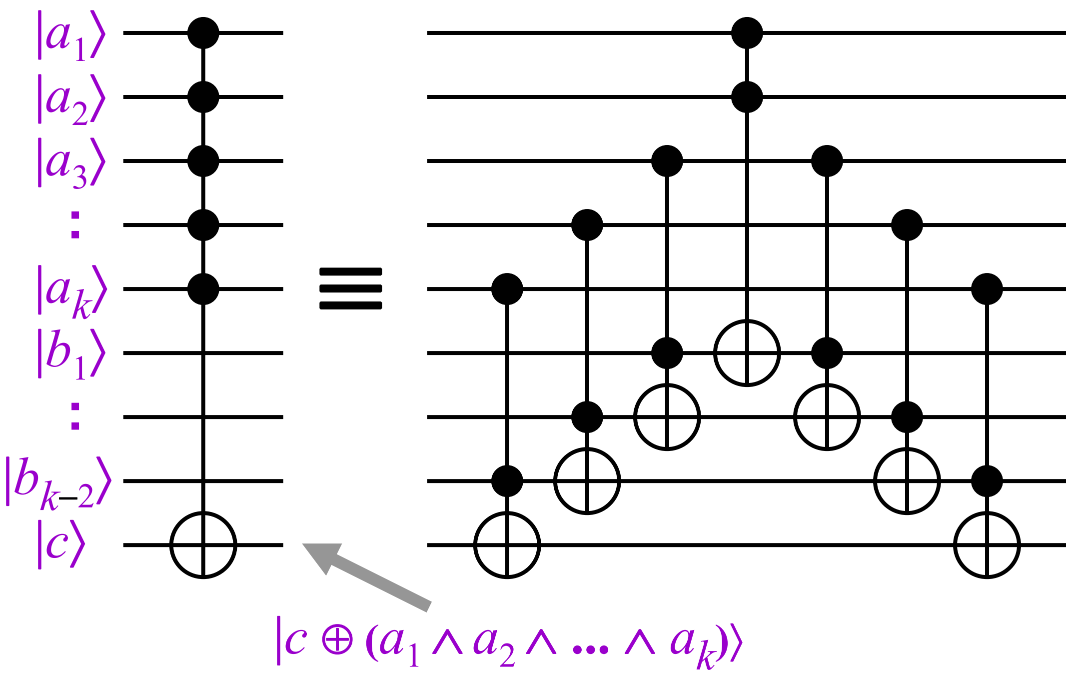


In this case, the one-qubit gates can be:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

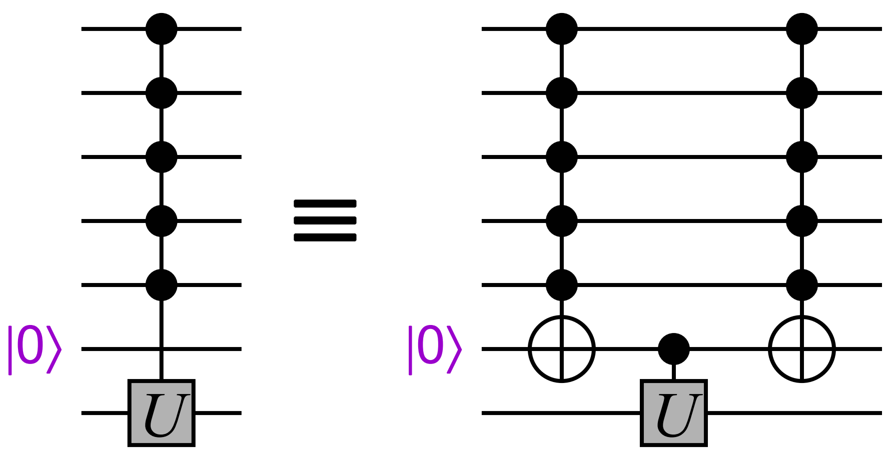
A universal set of gates (5)

From the Toffoli gate, ***generalized*** Toffoli gates (which are controlled-controlled- ... -NOT gates) can be constructed:



A universal set of gates (6)

From generalized Toffoli gates, ***generalized controlled-U*** gates (controlled-controlled- ... -U) can be constructed:



$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & 0 & 0 & 0 & 0 & U_{10} & U_{11} \end{pmatrix}$$

A universal set of gates (7)

The approach essentially enables any k-qubit operation of the simple form

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & U_{00} & 0 & 0 & U_{01} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & U_{10} & 0 & 0 & U_{11} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

to be computed with $O(k^2)$ CNOT and one-qubit gates

In a spirit similar to Gaussian elimination, any $2^k \times 2^k$ unitary matrix can be decomposed into a product of $O(4^k)$ of these

A universal set of gates (8)

This completes the proof sketch*

Thus, the set of ***all*** one-qubit gates and the CNOT gate are ***universal*** in that they can simulate any other gate set

Question: is there a ***finite*** set of gates that is universal?

Answer 1: strictly speaking, ***no***, because this results in only countably many quantum circuits, whereas there are uncountably many unitary operations on k qubits (for any k)

$*$ Actually we proved a slightly worse bound of $O(k^2 4^k)$

Approximately universal gate sets

Answer 2: yes, for universality in an ***approximate*** sense ...

To be continued ...

Introduction to Quantum Information Processing

CS 467 / CS 667
Phys 667 / Phys 767
C&O 481 / C&O 681

Lecture 12 (2008)

Richard Cleve
DC 2117
cleve@cs.uwaterloo.ca

Approximately universal sets of gates

Universal gate sets

The set of all one-qubit gates and the CNOT gate are ***universal*** in that they can simulate any other gate set

Quantitatively, any unitary operation U acting on k qubits can be decomposed into $O(4^k)$ CNOT and one-qubit gates

Question: is there a ***finite*** set of gates that is universal?

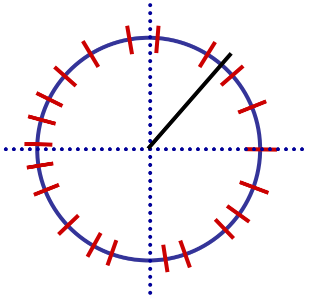
Answer 1: strictly speaking, ***no***, because this results in only countably many quantum circuits, whereas there are uncountably many unitary operations on k qubits (for any k)

***Approximately* universal gate sets**

Answer 2: yes, for universality in an ***approximate*** sense

As an illustrative example, any rotation can be approximated within any precision by repeatedly applying

$$R = \begin{bmatrix} \cos(\sqrt{2}\pi) & -\sin(\sqrt{2}\pi) \\ \sin(\sqrt{2}\pi) & \cos(\sqrt{2}\pi) \end{bmatrix}$$



some number of times

In this sense, R is ***approximately universal*** for the set of all one-qubit rotations: any rotation S can be approximated within precision ε by applying R a suitable number of times

It turns out that $O\left((1/\varepsilon)^c\right)$ times suffices (for a constant c)

Approximately universal gate sets

In three or more dimensions, the rate of convergence with respect to ε can be exponentially faster

Theorem 2: the gates CNOT, H, and $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$ are ***approximately universal***, in that any unitary operation on k qubits can be simulated within precision ε by applying $O\left(4^k \log^c(1/\varepsilon)\right)$ of them (c is a constant)

[Solovay, 1996][Kitaev, 1997]

Complexity classes

Complexity classes

Recall:

- **P (polynomial time):** problems solved by $O(n^c)$-size classical circuits (decision problems and uniform circuit families)
- **BPP (bounded error probabilistic polynomial time):** problems solved by $O(n^c)$-size ***probabilistic*** circuits that err with probability $\leq$ ¼
- **BQP (bounded error quantum polynomial time):** problems solved by $O(n^c)$-size ***quantum*** circuits that err with probability $\leq$ ¼
- **PSPACE (polynomial space):** problems solved by algorithms that use $O(n^c)$ memory.

Summary of previous containments

P $\subseteq$ **BPP** $\subseteq$ **BQP** $\subseteq$ **PSPACE** $\subseteq$ **EXP**

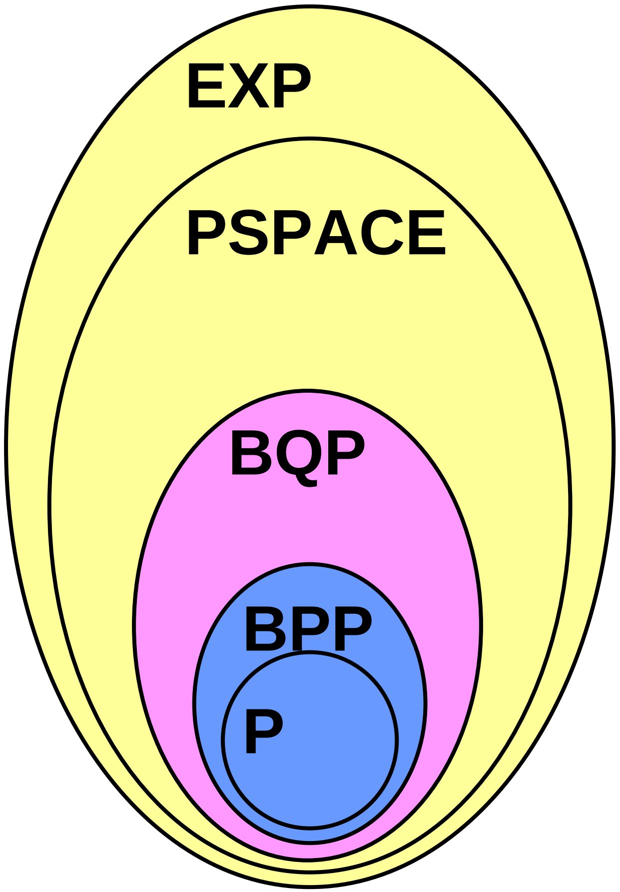
We now consider further structure between **P** and **PSPACE**

Technically, we will restrict our attention to ***languages*** (i.e. $\{0,1\}$-valued problems)

Many problems of interest can be cast in terms of languages

For example, we could define

FACTORING = $\{(x,y) : \exists\, 2 \le z \le y$, such that z divides $x\}$



NP

Define **NP (non-deterministic polynomial time)** as the class of languages whose ***positive*** instances have "witnesses" that can be verified in polynomial time

Example: Let **3-CNF-SAT** be the language consisting of all **3-CNF** formulas that are satisfiable

3-CNF formula:

$$f(x_1,\ldots,x_n) = (x_1 \vee \bar{x}_3 \vee x_4) \wedge (\bar{x}_2 \vee x_3 \vee \bar{x}_5) \wedge \cdots \wedge (\bar{x}_1 \vee x_5 \vee \bar{x}_n)$$

$f(x_1,\ldots,x_n)$ is ***satisfiable*** iff there exists $b_1,\ldots,b_n \in \{0,1\}$ such that $f(b_1,\ldots,b_n) = 1$

No sub-exponential-time algorithm is known for **3-CNF-SAT**

But poly-time verifiable witnesses exist (namely, $b_1, \ldots, b_n$)

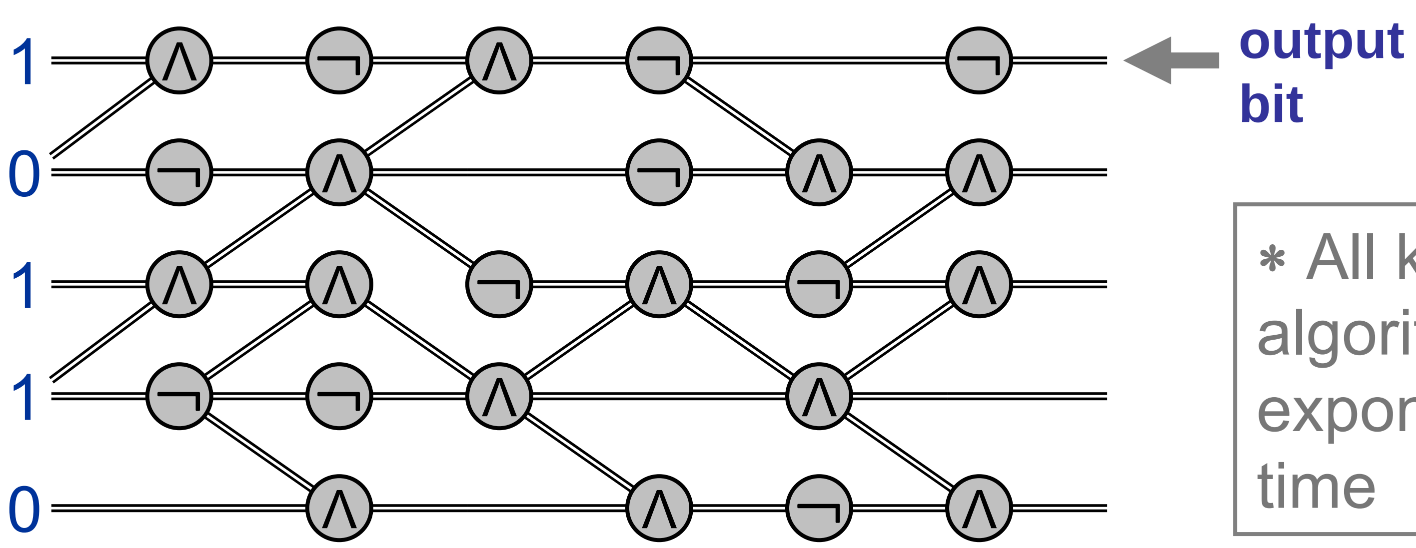
Other "logic" problems in NP

- ***k*-DNF-SAT**:

$$f(x_1,\ldots,x_n) = (x_1 \wedge \bar{x}_3 \wedge x_4) \vee (\bar{x}_2 \wedge x_3 \wedge \bar{x}_5) \vee \cdots \vee (\bar{x}_1 \wedge x_5 \wedge \bar{x}_n)$$

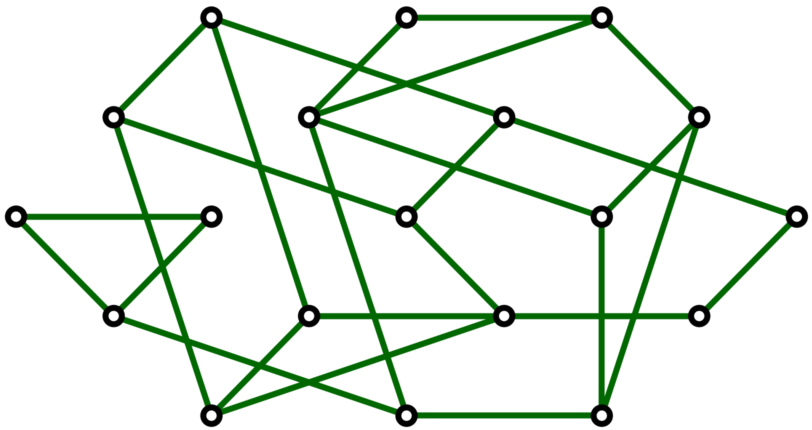
> ∗ But, unlike with *k*-**CNF-SAT**, this one is known to be in **P**

- **CIRCUIT-SAT**:



> ∗ All known algorithms exponential-time

“Graph theory” problems in NP



- ***k*-COLOR**: does G have a k-***coloring***?
- ***k*-CLIQUE**: does G have a ***clique*** of size k?
- **HAM-PATH**: does G have a ***Hamiltonian path***?
- **EUL-PATH**: does G have an ***Eulerian path***?

"Arithmetic" problems in NP

- **FACTORING** = $\{(x, y) : \exists 2 \leq z \leq y$, such that z divides $x\}$

- **SUBSET-SUM**: given integers $x_1, x_2, \ldots, x_n, y$, do there exist $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$ such that $x_{i_1} + x_{i_2} + \ldots + x_{i_k} = y$?

- **INTEGER-LINEAR-PROGRAMMING**: linear programming where one seeks an ***integer-valued*** solution (its existence)

P vs. NP

All of the aforementioned problems have the property that they ***reduce*** to **3-CNF-SAT**, in the sense that a polynomial-time algorithm for **3-CNF-SAT** can be converted into a poly-time algorithm for the problem

Example:

algorithm for **3-COLOR**

algorithm for **3-CNF-SAT**

If a polynomial-time algorithm is discovered for **3-CNF-SAT** then a polynomial-time algorithm for **3-COLOR** easily follows

In fact, this holds for ***any*** problem **X** $\in$ **NP**, hence **3-CNF-SAT** is ***NP-hard*** ...

P vs. NP

All of the aforementioned problems have the property that they ***reduce*** to **3-CNF-SAT**, in the sense that a polynomial-time algorithm for **3-CNF-SAT** can be converted into a poly-time algorithm for the problem

Example:

If a polynomial-time algorithm is discovered for **3-CNF-SAT** then a polynomial-time algorithm for **3-COLOR** easily follows

In fact, this holds for ***any*** problem **X** $\in$ **NP**, hence **3-CNF-SAT** is ***NP-hard*** ... Also **NP-hard: CIRCUIT-SAT**, k-**COLOR**, ...

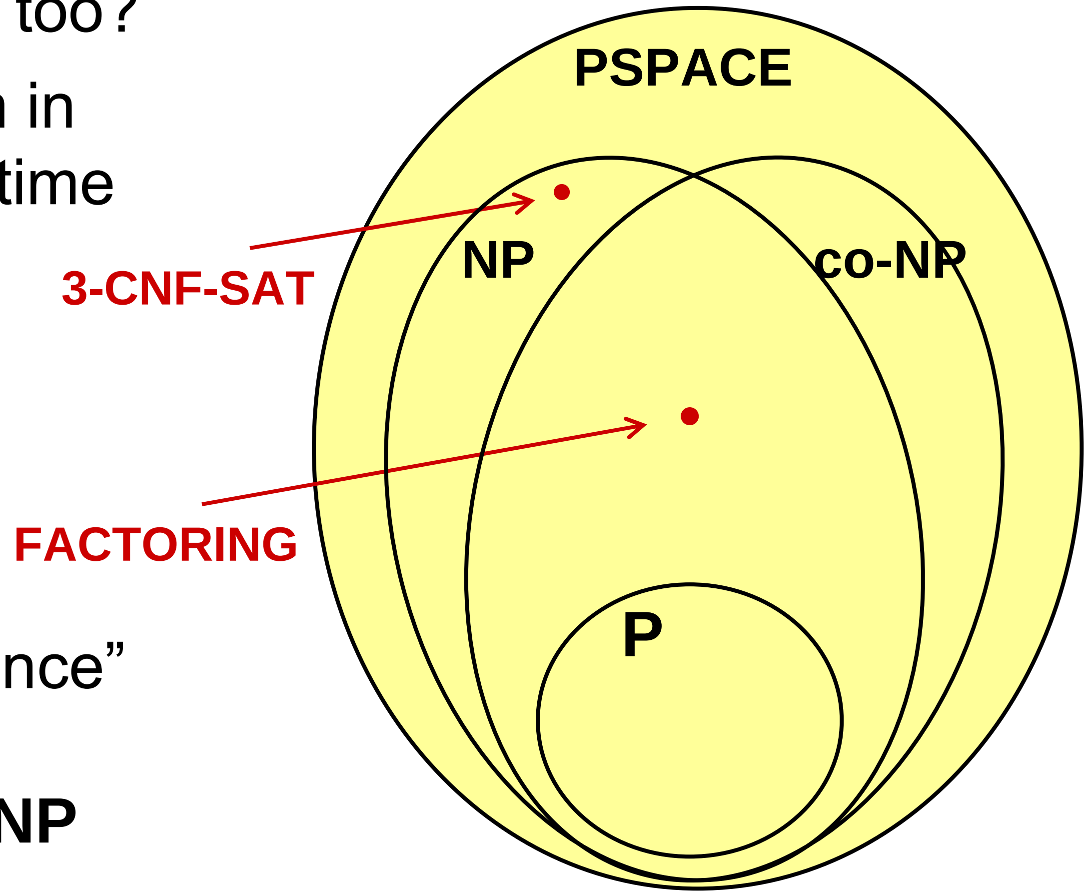
FACTORING vs. NP

Is **FACTORING NP**-hard too?

If so, then ***every*** problem in **NP** is solvable by a poly-time quantum algorithm!

But **FACTORING** has not been shown to be **NP**-hard

Moreover, there is "evidence" that it is not **NP**-hard: **FACTORING** $\in$ **NP**$\cap$**co-NP**

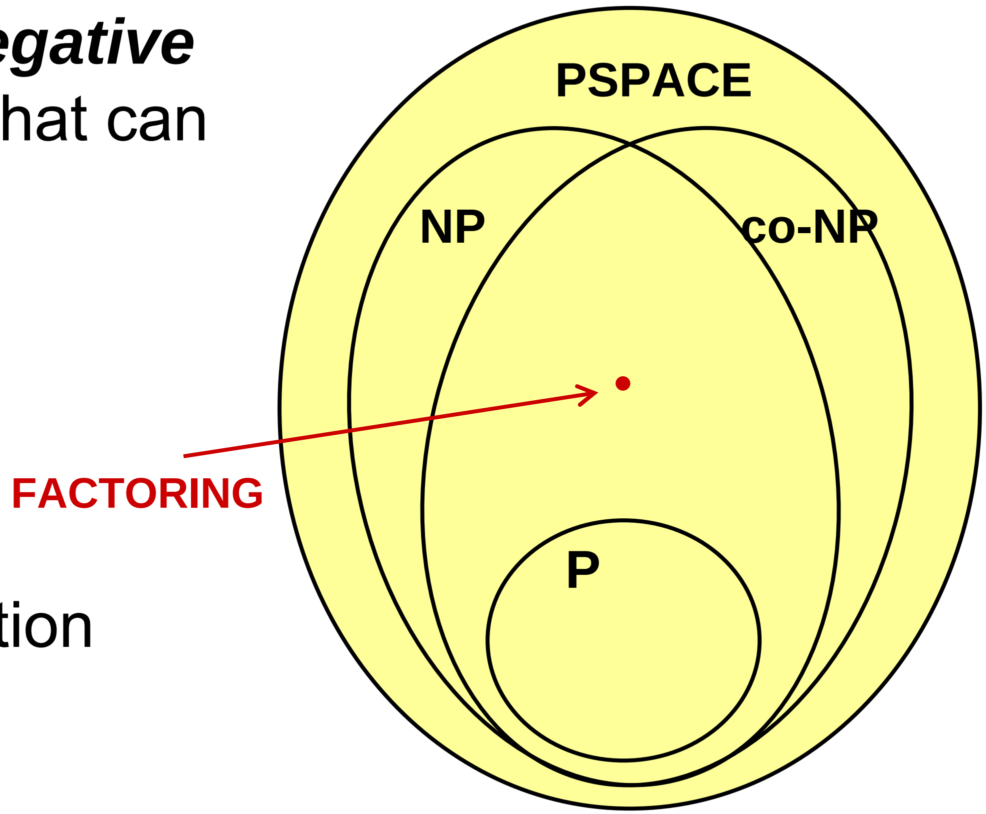


If **FACTORING** is **NP**-hard then **NP** = **co-NP**

FACTORING vs. co-NP

FACTORING $= \{(x, y) : \exists\, 2 \leq z \leq y,$ s.t. z divides $x\}$

co-NP: languages whose ***negative*** instances have "witnesses" that can be verified in poly-time



Question: what is a good witness for the negative instances?

Answer: the prime factorization $p_1, p_2, \ldots, p_m$ of x will work

Can verify primality and compare $p_1, p_2, \ldots, p_m$ with y, all in poly-time

Introduction to Quantum Information Processing

CS 467 / CS 667
Phys 667 / Phys 767
C&O 481 / C&O 681

Lecture 13 (2008)

Richard Cleve
DC 2117
cleve@cs.uwaterloo.ca

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

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

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

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

7. The first qubit of $|01\rangle - |10\rangle$

Answers later on ...

This is a probabilistic mixed state

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 k^{th} 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***:

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

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 $\big((|0\rangle, \tfrac{1}{2}), (|1\rangle, \tfrac{1}{2}) \big)$ 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

$\big((|0\rangle + |1\rangle, \tfrac{1}{2}), (|0\rangle - |1\rangle, \tfrac{1}{2}) \big)$?

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: kth 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 beginning of lecture):

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

$$
\left.
\begin{array}{l}
3. \begin{cases} |0\rangle \text{ with prob. } \tfrac{1}{2} \\ |1\rangle \text{ with prob. } \tfrac{1}{2} \end{cases} \\[2em]
4. \begin{cases} |0\rangle + |1\rangle \quad \text{with prob. } \tfrac{1}{2} \\ |0\rangle - |1\rangle \quad \text{with prob. } \tfrac{1}{2} \end{cases} \\[2em]
6. \begin{cases} |0\rangle \qquad\qquad \text{with prob. } \tfrac{1}{4} \\ |1\rangle \qquad\qquad \text{with prob. } \tfrac{1}{4} \\ |0\rangle + |1\rangle \quad \text{with prob. } \tfrac{1}{4} \\ |0\rangle - |1\rangle \quad \text{with prob. } \tfrac{1}{4} \end{cases}
\end{array}
\right\} \quad \rho = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
$$

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)**

Characterizing density matrices

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

Three properties of ρ :

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

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)

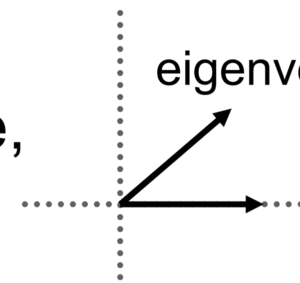
$$D = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_d \end{bmatrix}$$

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

eigenvectors:



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

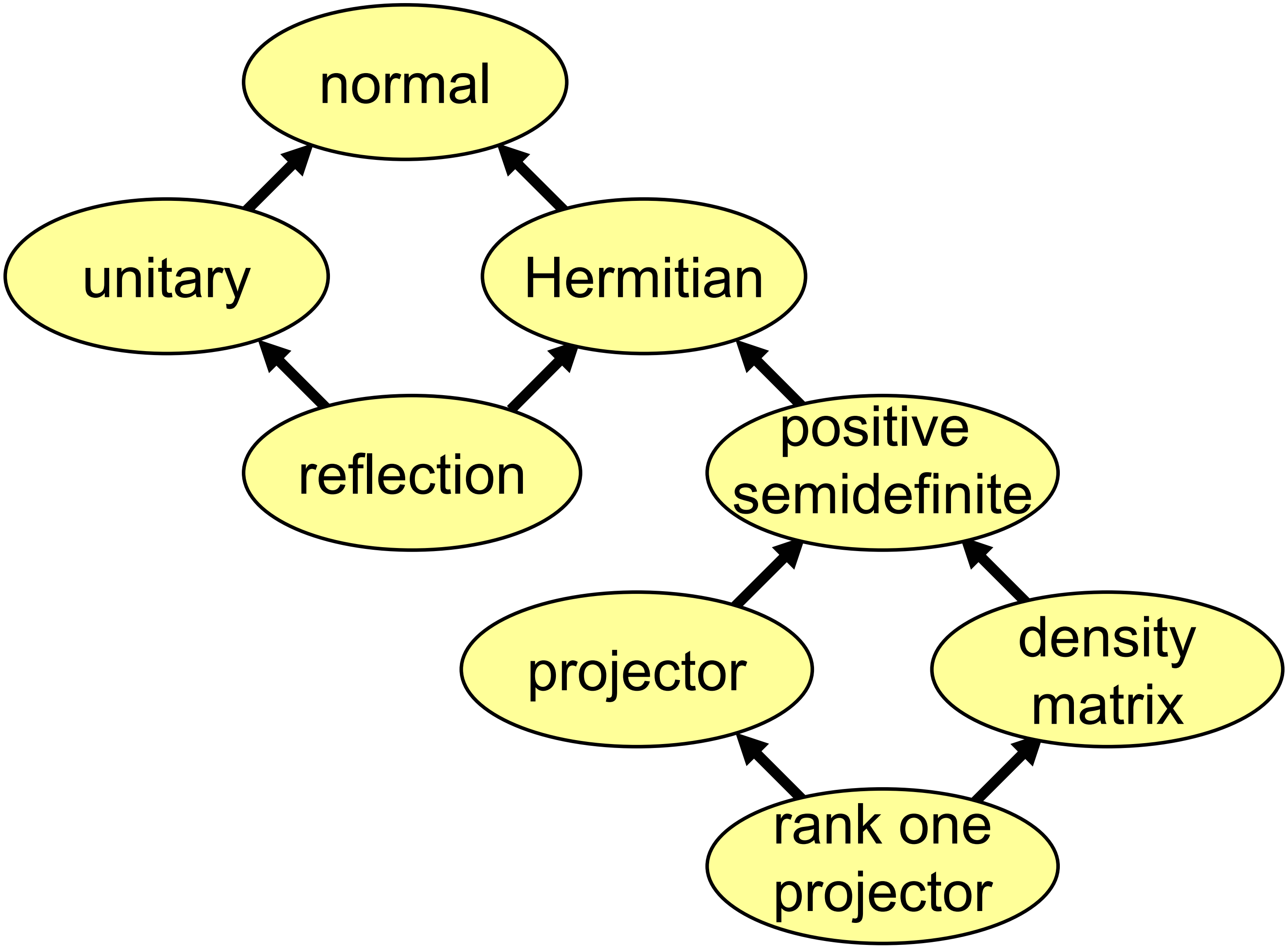
Projector: Hermitian and $M^2 = M$, which implies that M is positive semidefinite and $\lambda_k \in \{0,1\}$, for all k

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



Introduction to Quantum Information Processing

CS 467 / CS 667
Phys 667 / Phys 767
C&O 481 / C&O 681

Lecture 14 (2008)

Richard Cleve

DC 2117

cleve@cs.uwaterloo.ca

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

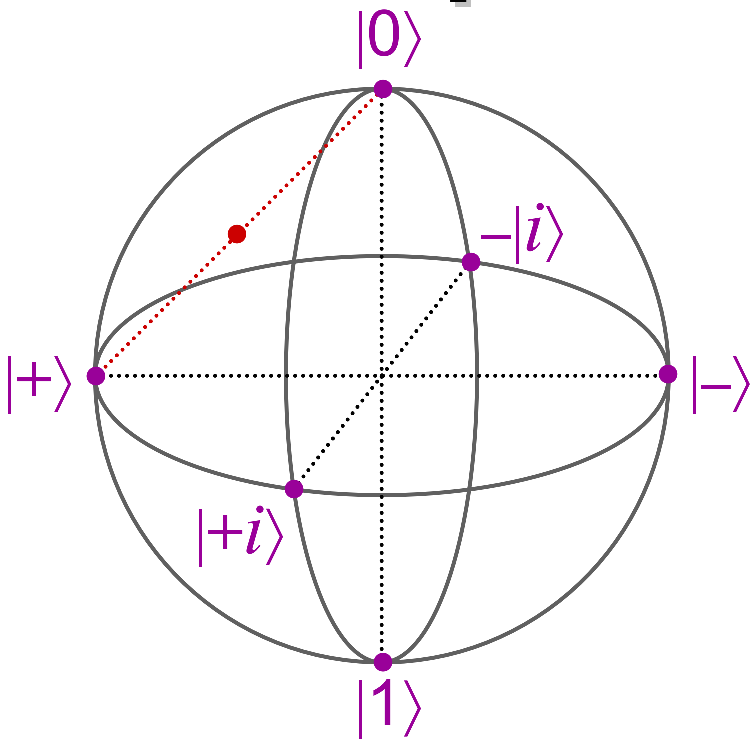
First consider the case of pure states $|\psi\rangle\langle\psi|$, where, without loss of generality, $|\psi\rangle = \cos(\theta)|0\rangle + e^{2i\phi}\sin(\theta)|1\rangle$ $(\theta, \phi \in \mathbf{R})$

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

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)

Basic properties of the trace

Basic properties of the trace

The ***trace*** of a square matrix is defined as $\mathrm{Tr}\,M = \sum_{k=1}^{d} M_{k,k}$

It is easy to check that

$\mathrm{Tr}(M+N) = \mathrm{Tr}\,M + \mathrm{Tr}\,N$ and $\mathrm{Tr}(M\,N) = \mathrm{Tr}(N\,M)$

The second property implies $\mathrm{Tr}(M) = \mathrm{Tr}(U^{-1}MU) = \sum_{k=1}^{d} \lambda_k$

Calculation maneuvers worth remembering are:

$\mathrm{Tr}(|a\rangle\langle b|M) = \langle b|M|a\rangle$ and $\mathrm{Tr}(|a\rangle\langle b|c\rangle\langle d|) = \langle b|c\rangle\langle d|a\rangle$

Also, keep in mind that, in general, $\mathrm{Tr}(M\,N) \neq \mathrm{Tr}\,M\,\mathrm{Tr}\,N$

Partial **trace (1)**

Two quantum registers (e.g. two qubits) in states σ and μ (respectively) are ***independent*** if then the combined system is in state $\rho = \sigma \otimes \mu$

In such circumstances, if the second register (say) is discarded then the state of the first 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***)

We can <u>define</u> the ***partial trace***, $\mathrm{Tr}_2\,\rho$, as the unique linear operator satisfying the identity $\mathrm{Tr}_2(\sigma \otimes \mu) = \sigma$

index means 2nd system traced out

For example, it turns out that

$$\mathrm{Tr}_2\Big(\big(\tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|11\rangle\big) \otimes \big(\tfrac{1}{\sqrt{2}}\langle 00| + \tfrac{1}{\sqrt{2}}\langle 11|\big)\Big) = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Partial trace (2)

Example: 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 $A_1 = I \otimes \langle 1| = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

For the resulting quantum operation, state $\sigma \otimes \mu$ becomes σ

For d-dimensional registers, the operators are $A_k = I \otimes \langle \phi_k|$, where $|\phi_0\rangle, |\phi_1\rangle, \ldots, |\phi_{d-1}\rangle$ are an orthonormal basis

Partial trace (3)

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

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

POVMs

(Positive Operator Valued Measurements)

POVMs (1)

Positive operator valued measurement (POVM):

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

Then the corresponding POVM is a stochastic operation on ρ that, with probability $\mathrm{Tr}\left(A_j \rho A_j^\dagger\right)$ produces the 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 …

POVMs (2)

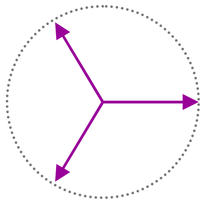
When $A_j = |\phi_j\rangle\langle\phi_j|$ are orthogonal projectors and $\rho = |\psi\rangle\langle\psi|$,

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

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

POVMs (3)

Example 3 (trine state "measurent"):



Let $|\varphi_0\rangle = |0\rangle$, $|\varphi_1\rangle = -1/2|0\rangle + \sqrt{3}/2|1\rangle$, $|\varphi_2\rangle = -1/2|0\rangle - \sqrt{3}/2|1\rangle$

Define $A_0 = \sqrt{2/3}|\varphi_0\rangle\langle\varphi_0| = \sqrt{\frac{2}{3}}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

$A_1 = \sqrt{2/3}|\varphi_1\rangle\langle\varphi_1| = \frac{1}{4}\begin{bmatrix} \sqrt{2/3} & +\sqrt{2} \\ +\sqrt{2} & \sqrt{6} \end{bmatrix}$ $\quad A_2 = \sqrt{2/3}|\varphi_2\rangle\langle\varphi_2| = \frac{1}{4}\begin{bmatrix} \sqrt{2/3} & -\sqrt{2} \\ -\sqrt{2} & \sqrt{6} \end{bmatrix}$

Then $A_0^\dagger A_0 + A_1^\dagger A_1 + A_2^\dagger A_2 = I$

If the input itself is an unknown trine state, $|\varphi_k\rangle\langle\varphi_k|$, then the probability that classical outcome is k is 2/3 = 0.6666…

General quantum operations

General quantum operations (1)

General quantum operations (a.k.a. ***“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

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 4 (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 $A_1 = I \otimes \langle 1| = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

State $\rho \otimes \sigma$ becomes ρ

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

Note 1: it's the same density matrix as for $\left((\tfrac{1}{2}, |0\rangle), (\tfrac{1}{2}, |1\rangle)\right)$

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

Distinguishing mixed states

Distinguishing mixed states (1)

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

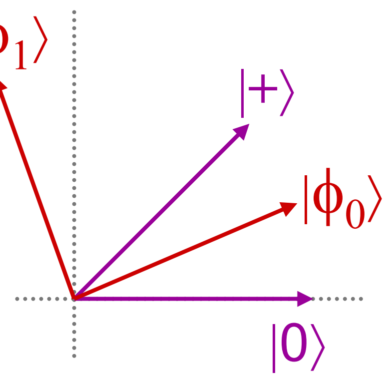
$$\begin{cases} |0\rangle & \text{with prob. } 1/2 \\ |0\rangle + |1\rangle & \text{with prob. } 1/2 \end{cases}$$

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

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

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

ρ_1 also arises from this orthogonal mixture:



… as does ρ_2 from:

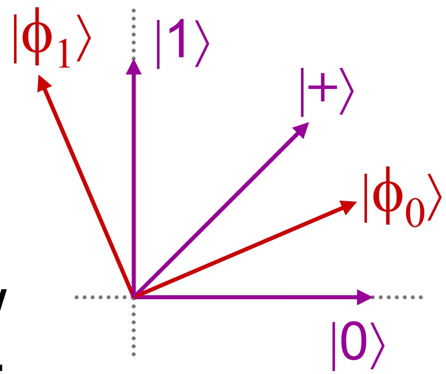
$$\begin{cases} |\phi_0\rangle & \text{with prob. } \cos^2(\pi/8) \\ |\phi_1\rangle & \text{with prob. } \sin^2(\pi/8) \end{cases}$$

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

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:

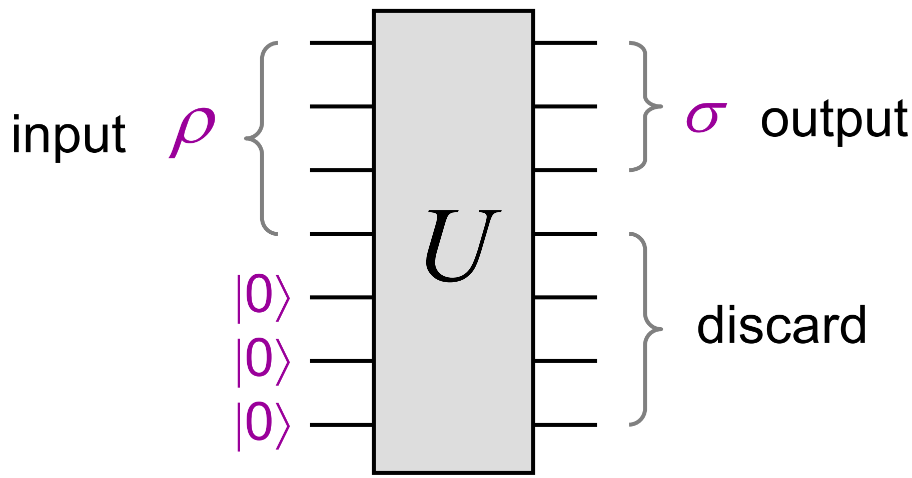
Distinguish between two ***classical*** coins, whose probabilities of "heads" are $\cos^2(\pi/8)$ and ½ respectively (details: exercise)

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

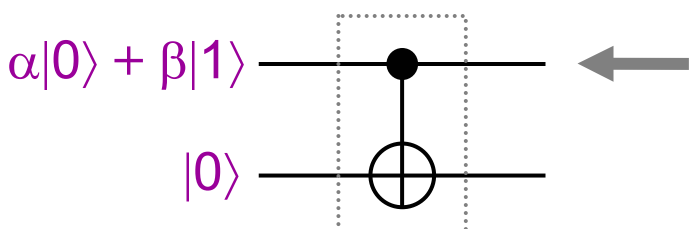
Simulations among operations

Simulations among operations (1)

Fact 1: any ***general quantum operation*** can be simulated by applying a unitary operation on a larger quantum system:



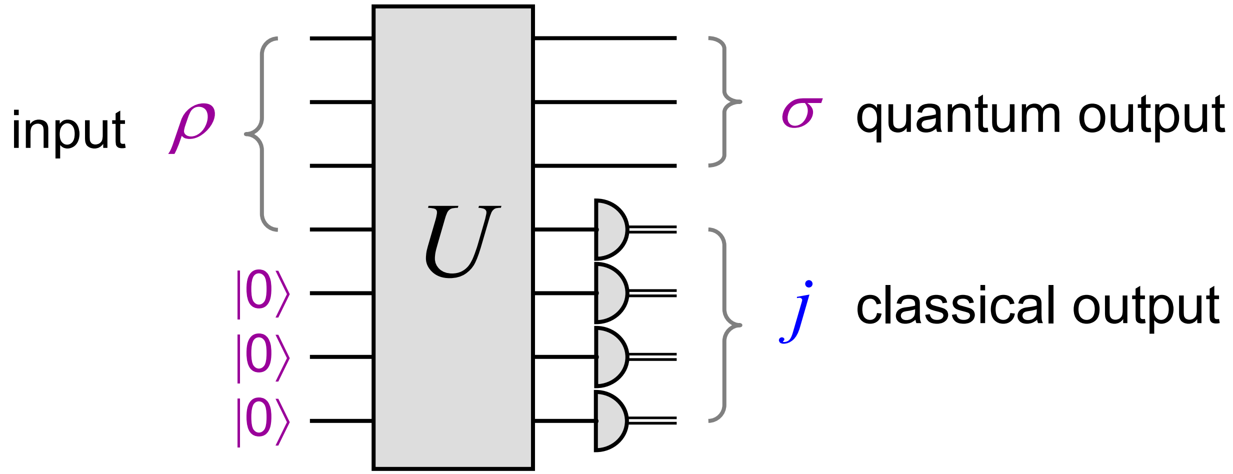
Example: decoherence



$$\rho = \begin{bmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{bmatrix}$$

Simulations among operations (2)

Fact 2: any ***POVM*** can also be simulated by applying a unitary operation on a larger quantum system and then measuring:



Separable states

Separable states

A bipartite (i.e. two register) state ρ is a:

- ***product state*** if $\rho = \sigma \otimes \xi$

- ***separable state*** if $\rho = \sum_{j=1}^{m} p_j \sigma_j \otimes \xi_j \quad (p_1, \ldots, p_m \geq 0)$

(i.e. a probabilistic mixture of product states)

Question: which of the following states are separable?

$$\rho_1 = \tfrac{1}{2}\big(|00\rangle + |11\rangle\big)\big(\langle 00| + \langle 11|\big)$$

$$\rho_2 = \tfrac{1}{2}\big(|00\rangle + |11\rangle\big)\big(\langle 00| + \langle 11|\big) + \tfrac{1}{2}\big(|00\rangle - |11\rangle\big)\big(\langle 00| - \langle 11|\big)$$