Introduction to Quantum Information Processing

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

Lecture 4 (2005)

Richard Cleve
DC 653
cleve@cs.uwaterloo.ca

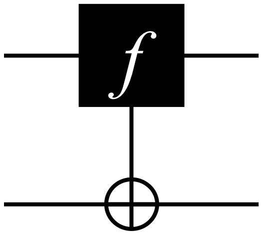
Course web site at:
http://www.cs.uwaterloo.ca/~cleve

Contents

- Recap: query algorithms
- One-out-of-four search
- Constant vs. balanced
- $H \otimes H \otimes \ldots \otimes H$
- Simon's problem

Query algorithms

Last time: quantum algorithm for computing $f(0)\oplus f(1)$ making just **1** query to f, whereas any classical algorithm requires **2** queries



This time: other, stronger quantum vs. classical separations

- Recap: query algorithms
- One-out-of-four search
- Constant vs. balanced
- $H \otimes H \otimes \ldots \otimes H$
- Simon's problem

One-out-of-four search

Let $f : \{0,1\}^2 \rightarrow \{0,1\}$ have the property that there is exactly one $x \in \{0,1\}^2$ for which $f(x) = 1$

Four possibilities:

x	$f_{00}(x)$
00	1
01	0
10	0
11	0

x	$f_{01}(x)$
00	0
01	1
10	0
11	0

x	$f_{10}(x)$
00	0
01	0
10	1
11	0

x	$f_{11}(x)$
00	0
01	0
10	0
11	1

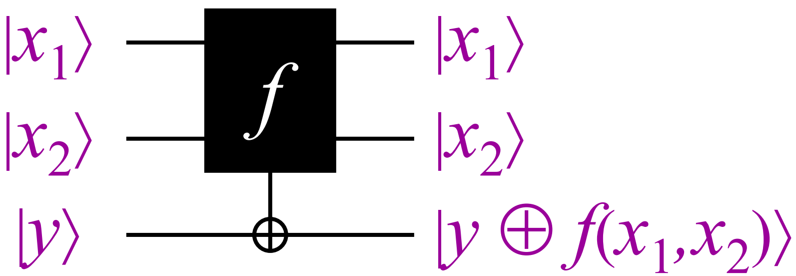
Goal: find $x \in \{0,1\}^2$ for which $f(x) = 1$

What is the minimum number of queries ***classically?*** ____

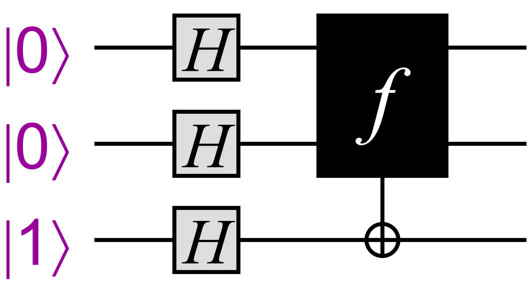
Quantumly? ____

Quantum algorithm (I)

Black box for 1-4 search:



Start by creating phases in superposition of all inputs to f:



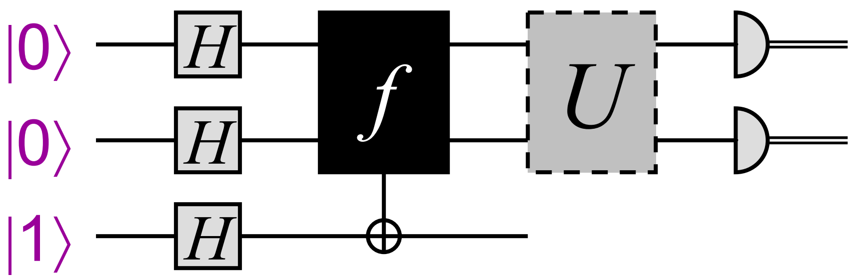
Input state to query?

$(|00\rangle + |01\rangle + |10\rangle + |11\rangle)(|0\rangle - |1\rangle)$

Output state of query?

$((-1)^{f(00)}|00\rangle + (-1)^{f(01)}|01\rangle + (-1)^{f(10)}|10\rangle + (-1)^{f(11)}|11\rangle)(|0\rangle - |1\rangle)$

Quantum algorithm (II)



← Apply the U that maps
← $|\psi_{00}\rangle, |\psi_{01}\rangle, |\psi_{10}\rangle, |\psi_{11}\rangle$ to
← $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ (resp.)

Output state of the first two qubits in the four cases:

Case of f_{00}? $|\psi_{00}\rangle = -|00\rangle + |01\rangle + |10\rangle + |11\rangle$

Case of f_{01}? $|\psi_{01}\rangle = +|00\rangle - |01\rangle + |10\rangle + |11\rangle$

Case of f_{10}? $|\psi_{10}\rangle = +|00\rangle + |01\rangle - |10\rangle + |11\rangle$

Case of f_{11}? $|\psi_{11}\rangle = +|00\rangle + |01\rangle + |10\rangle - |11\rangle$

What noteworthy property do these states have? **Orthogonal!**

Challenge Exercise: simulate the above U in terms of H, Toffoli, and NOT gates

one-out-of-N search?

Natural question: what about search problems in spaces larger than ***four*** (and without uniqueness conditions)?

For spaces of size ***eight*** (say), the previous method breaks down—the state vectors will not be orthogonal

Later on, we'll see how to search a space of size N with $O(\sqrt{N})$ queries ...

- Recap: query algorithms
- One-out-of-four search
- Constant vs. balanced
- $H \otimes H \otimes \ldots \otimes H$
- Simon's problem

Constant vs. balanced

Let $f : \{0,1\}^n \rightarrow \{0,1\}$ be either constant or balanced, where

- ***constant*** means $f(x) = 0$ for all x, or $f(x) = 1$ for all x
- ***balanced*** means $\sum_x f(x) = 2^{n-1}$

Goal: determine whether f is constant or balanced

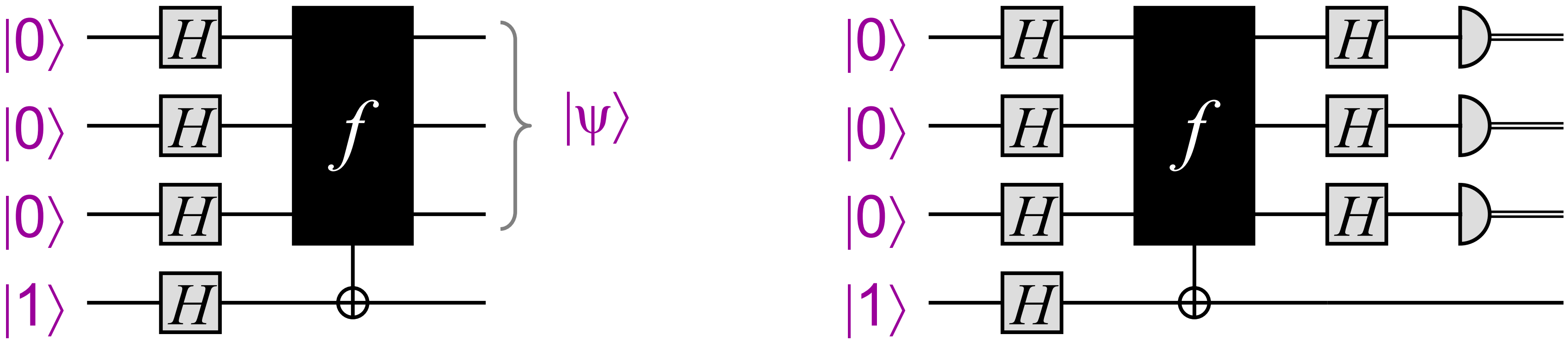
How many queries are there needed ***classically?*** ____

Example: if $f(0000) = f(0001) = f(0010) = \ldots = f(0111) = 0$ then it still could be either

Quantumly? ____

[Deutsch & Jozsa, 1992]

Quantum algorithm



Constant case: $|\psi\rangle = \pm \sum_x |x\rangle$ ***Why?***

Balanced case: $|\psi\rangle$ is ***orthogonal*** to $\pm \sum_x |x\rangle$ ***Why?***

How to distinguish between the cases? What is $H^{\otimes n}|\psi\rangle$?

Constant case: $H^{\otimes n}|\psi\rangle = \pm\, |00...0\rangle$

Balanced case: $H^{\otimes n}\, |\psi\rangle$ is orthogonal to $|0...00\rangle$

Last step of the algorithm: if the measured result is 000 then output "constant", otherwise output "balanced"

Probabilistic *classical* algorithm solving constant vs balanced

But here's a classical procedure that makes only **2** queries and performs fairly well probabilistically:

1. pick $x_1, x_2 \in \{0,1\}^n$ randomly
2. **<u>if</u>** $f(x_1) \neq f(x_2)$ **<u>then</u>** output balanced **<u>else</u>** output constant

What happens if f is constant? The algorithm always succeeds

What happens if f is balanced? Succeeds with probability ½

By repeating the above procedure k times:
$2k$ queries and one-sided error probability $(½)^k$

Therefore, for large n, $<< 2^n$ queries are likely sufficient

- Recap: query algorithms
- One-out-of-four search
- Constant vs. balanced
- $H \otimes H \otimes \ldots \otimes H$
- Simon's problem

About $H\otimes H\otimes \ldots \otimes H = H^{\otimes n}$

Theorem: for $x \in \{0,1\}^n$, $H^{\otimes n}|x\rangle = \frac{1}{2^{n/2}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}|y\rangle$

where $x \cdot y = x_1 y_1 \oplus \ldots \oplus x_n y_n$

Example: $H \otimes H = \frac{1}{2}\begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix}$

Pf: For all $x \in \{0,1\}^n$, $H|x\rangle = |0\rangle + (-1)^x|1\rangle = \sum_y (-1)^{xy}|y\rangle$

Thus, $H^{\otimes n}|x_1 \ldots x_n\rangle = \left(\sum_{y_1} (-1)^{x_1 y_1}|y_1\rangle\right) \ldots \left(\sum_{y_n} (-1)^{x_n y_n}|y_n\rangle\right)$

$= \sum_y (-1)^{x_1 y_1 \oplus \ldots \oplus x_n y_n}|y_1 \ldots y_n\rangle$ ∎

- Recap: query algorithms
- One-out-of-four search
- Constant vs. balanced
- $H \otimes H \otimes \ldots \otimes H$
- Simon’s problem

Quantum vs. classical separations

black-box problem	quantum	classical	
constant vs. balanced	**1** (query)	**2** (queries)	
1-out-of-4 search	**1**	**3**	
constant vs. balanced	**1**	**½ 2^n + 1**	**(only for exact)**
Simon's problem			**(probabilistic)**

Simon's problem

Let $f: \{\mathbf{0,1}\}^n \rightarrow \{\mathbf{0,1}\}^n$ have the property that there exists an $r \in \{\mathbf{0,1}\}^n$ such that $f(x) = f(y)$ iff $x \oplus y = r$ or $x = y$

Example:

x	$f(x)$
000	**011**
001	**101**
010	**000**
011	**010**
100	**101**
101	**011**
110	**010**
111	**000**

What is r is this case? ________

Answer: $r =$ **101**

A classical algorithm for Simon

Search for a ***collision***, an $x \neq y$ such that $f(x) = f(y)$

1. Choose $x_1, x_2, \ldots, x_k \in \{0,1\}^n$ randomly (independently)
2. For all $i \neq j$, if $f(x_i) = f(x_j)$ then output $x_i \oplus x_j$ and halt

A hard case is where r is chosen randomly from $\{\mathbf{0},\mathbf{1}\}^n - \{\mathbf{0}^n\}$ and then the "table" for f is filled out randomly subject to the structure implied by r

How big does k have to be for the probability of a collision to be a constant, such as ¾?

Answer: order $2^{n/2}$ (each (x_i, x_j) collides with prob. $O(2^{-n})$)

Classical lower bound

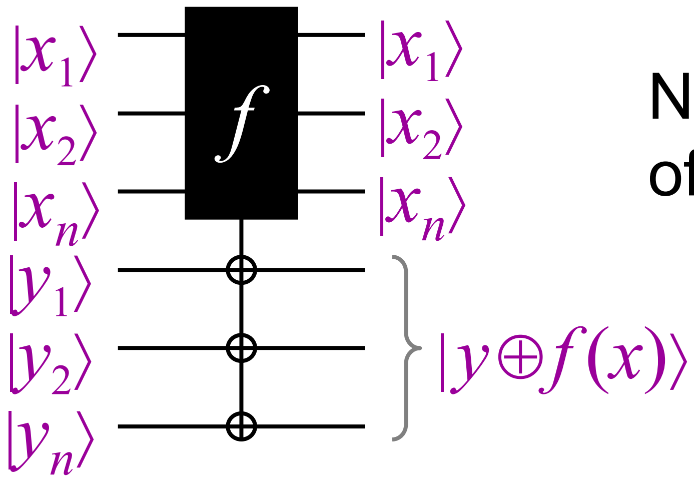
Theorem: ***any*** classical algorithm solving Simon's problem must make $\Omega(2^{n/2})$ queries

Proof is omitted here—note that the performance analysis of the previous algorithm does ***not*** imply the theorem

… how can we know that there isn't a ***different*** algorithm that performs better?

A *quantum* algorithm for Simon I

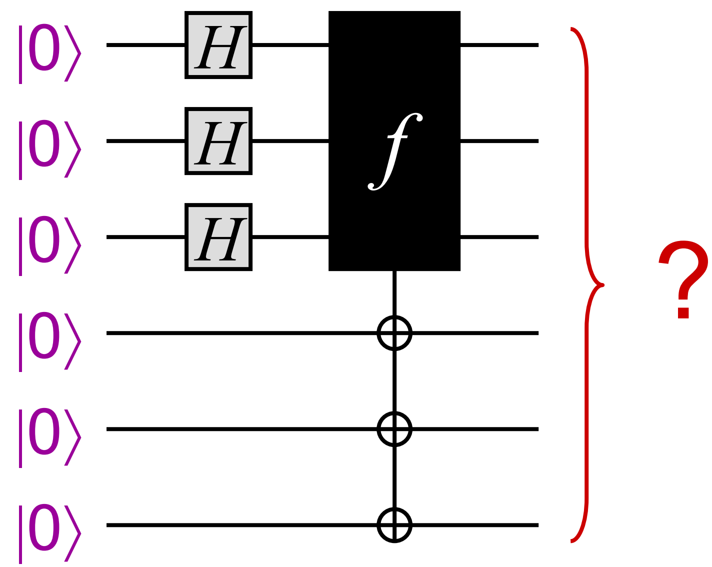
Queries:



Not clear what ***eigenvector*** of target registers is ...

Proposed start of quantum algorithm: query all values of f in superposition

What is the output state of this circuit?



THE END

A quantum algorithm for Simon II

Answer: the output state is $\sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle$

Let $T \subseteq \{\mathbf{0,1}\}^n$ be such that ***one*** element from each matched pair is in T (assume $r \neq$ **00...0**)

Example: could take $T = \{$**000**, **001**, **111**, **110**$\}$

Then the output state can be written as:

$$\sum_{x\in T} |x\rangle|f(x)\rangle + |x\oplus r\rangle|f(x\oplus r)\rangle$$

$$= \sum_{x\in T} \big(|x\rangle + |x\oplus r\rangle\big)|f(x)\rangle$$

x	$f(x)$
000	**011**
001	**101**
010	**000**
011	**010**
100	**101**
101	**011**
110	**010**
111	**000**

A quantum algorithm for Simon III

Measuring the second register yields $|x\rangle + |x \oplus r\rangle$ in the first register, for a random $x \in T$

How can we use this to obtain ***some*** information about r?

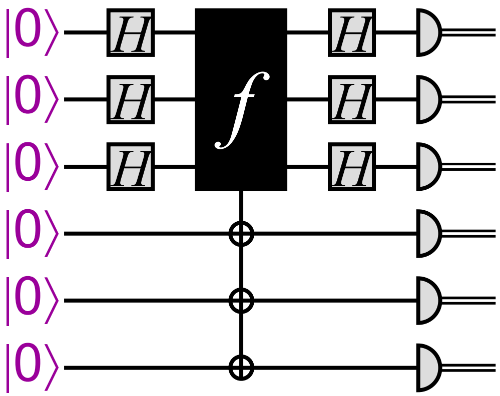
Try applying $H^{\otimes n}$ to the state, yielding:

$$\sum_{y \in \{0,1\}^n} (-1)^{x \bullet y} |y\rangle + \sum_{y \in \{0,1\}^n} (-1)^{(x \oplus r) \bullet y} |y\rangle$$

$$= \sum_{y \in \{0,1\}^n} (-1)^{x \bullet y} \left(1 + (-1)^{r \bullet y}\right) |y\rangle$$

Measuring this state yields y with prob. $\begin{cases} (1/2)^{n-1} & \text{if } r \cdot y = 0 \\ 0 & \text{if } r \cdot y \neq 0 \end{cases}$

A quantum algorithm for Simon IV



Executing this algorithm $k = O(n)$ times yields random $y_1, y_2, \ldots, y_k \in \{0,1\}^n$ such that $r \cdot y_1 = r \cdot y_2 = \ldots = r \cdot y_n = 0$

How does this help?

This is a system of k linear equations:

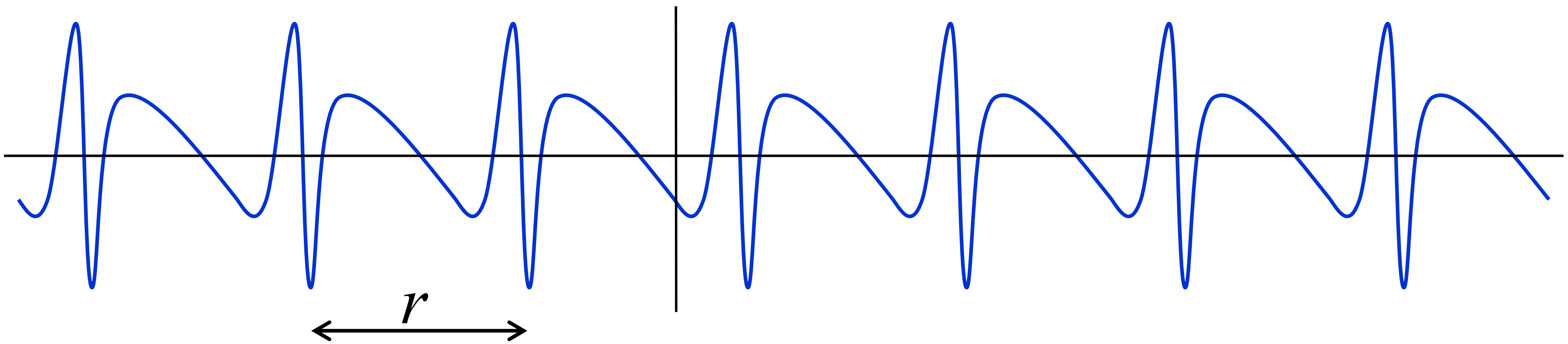
$$\begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1n} \\ y_{21} & y_{22} & \cdots & y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{k1} & y_{k2} & \cdots & y_{kn} \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

With high probability, there is a unique non-zero solution that is r (which can be efficiently found by linear algebra)

Preview of applications of black-box results

Period-finding

Given: $f : \mathbf{Z} \rightarrow \mathbf{Z}$ such that f is (strictly) r-periodic, in the sense that $f(x) = f(y)$ iff $x - y$ is a multiple of r (unknown)



Goal: find r

Classically, the number of queries required can be ***"huge"*** (essentially as hard as finding a collision)

There is a quantum algorithm that makes only a ***constant*** number of queries (which will be explained later on)

Simon's problem vs. period-finding

Period-finding problem: domain is **Z** and property is $f(x) = f(y)$ iff $x - y$ is a multiple of r

This problem meaningfully generalizes to domain $\mathbf{Z}^n$

Deutsch's problem: domain is $\mathbf{Z}_2$ and property is $f(x) = f(y)$ iff $x \oplus y$ is a multiple of r
($r = 0$ means $f(0) = f(1)$ and $r = 1$ means $f(0) \neq f(1)$)

Simon's problem: domain is $(\mathbf{Z}_2)^n$ and property is $f(x) = f(y)$ iff $x \oplus y$ is a multiple of r

Application of period-finding algorithm

Order-finding problem: given a and m (positive integers such that $\gcd(a,m) = 1$), find the minimum positive r such that $a^r \bmod m = 1$

Note that this is ***not*** a black-box problem!

No classical polynomial-time algorithm is known for this problem (in fact, the factoring problem reduces to it)

The problem reduces to finding the period of $f(x) = a^x \bmod m$, and the aforementioned period-finding algorithm in the black-box model can be used to solve it in polynomial-time

The function f is substituted into the black-box ...

On simulating black boxes

How *not* to simulate a black box

Given an explicit function, such as $f(x) = a^x \bmod m$, and a finite domain $\{0, 1, 2, ..., 2^n - 1\}$, simulate f-queries over that domain

Easy to compute mapping $|x\rangle|y\rangle|00...0\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle|g(x)\rangle$, where the third register is "work space" with accumulated "garbage" (e.g., two such bits arise when a Toffoli gate is used to simulate an AND gate)

This works fine as long as f is not queried in superposition

If f is queried in superposition then the resulting state can be $\sum_x \alpha_x |x\rangle|y \oplus f(x)\rangle|g(x)\rangle$ Can we just discard the third register?

No ... there could be entanglement ...

Overview of Lecture 4

- The one-out-of-four search problem
- The constant vs. balanced problem
- $H \otimes H \otimes \ldots \otimes H$
- Fourier sampling
- Preview of where black-box results are headed: period-finding
- Simulating black boxes

Overview of Lecture 8

- BV problem: **1** vs. ***n*** separation robust against probabilistic algorithms
- Preview of where black-box results are headed: period-finding
- Simulating black boxes
- Simon's problem: **1** vs. $\mathbf{2^{\mathit{n}/2}}$ separation robust against probabilistic algorithms

How *to* simulate a black box

Simulate the mapping $|x\rangle|y\rangle|00...0\rangle \rightarrow |x\rangle|y\oplus f(x)\rangle|00...0\rangle$, (i.e., clean up the "garbage")

To do this, use an additional register and:

1. compute $|x\rangle|y\rangle|00...0\rangle|00...0\rangle \rightarrow |x\rangle|y\rangle|f(x)\rangle|g(x)\rangle$ (ignoring the 2nd register in this step)
2. compute $|x\rangle|y\rangle|f(x)\rangle|g(x)\rangle \rightarrow |x\rangle|y\oplus f(x)\rangle|f(x)\rangle|g(x)\rangle$ (using CNOT gates between the 2nd and 3rd registers)
3. compute $|x\rangle|y\oplus f(x)\rangle|f(x)\rangle|g(x)\rangle \rightarrow |x\rangle|y\oplus f(x)\rangle|00...0\rangle|00...0\rangle$ (by reversing the procedure in step 1)

Total cost: around twice the cost of computing f, plus n auxiliary gates

Quantum vs. classical separations

black-box problem	quantum	classical	
constant vs. balanced	**1** (query)	**2** (queries)	
1-out-of-4 search	**1**	**3**	
constant vs. balanced	**1**	**½ 2^n + 1**	**(only for exact)**
BV problem	**1**	***n***	**(probabilistic)**

BV problem

BV problem

[Bernstein & Vazirani, 1993]

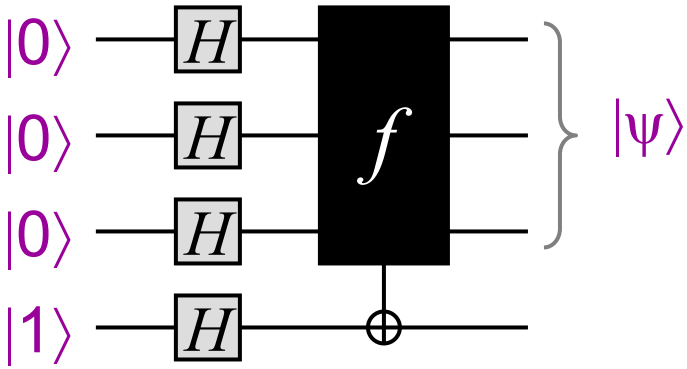
Let $f : \{0,1\}^n \rightarrow \{0,1\}$ be of the form $f(x) = a_1 x_1 \oplus ... \oplus a_n x_n$, where $(a_1, ... , a_n) \in \{0,1\}^n$ is unknown

Goal: determine $(a_1, ... , a_n)$

Classically: n queries needed, even to succeed with probability > ½ (why?)

Quantumly: 1 query suffices

Quantum algorithm for BV



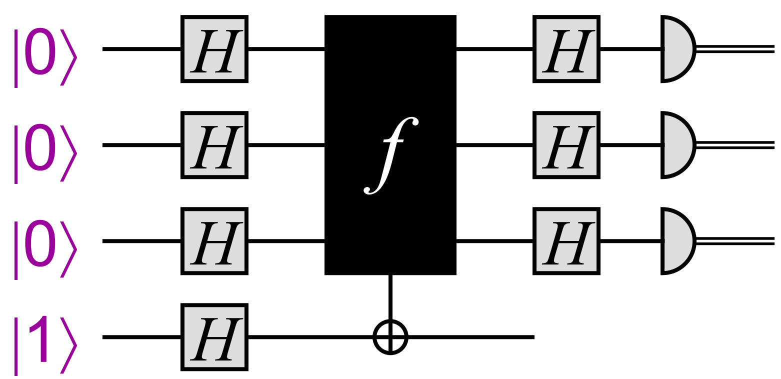
where $|\psi\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{a \bullet x} |x\rangle$

Question: what is $|\psi\rangle$?

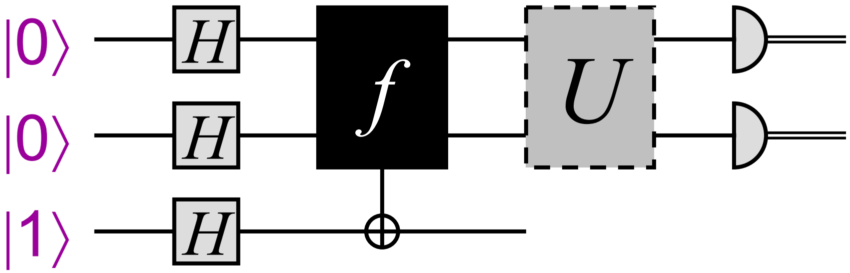
Answer: $|\psi\rangle = H^{\otimes n}|a_1, \ldots, a_n\rangle$

Therefore, $H^{\otimes n}|\psi\rangle = |a_1, \ldots, a_n\rangle$

Final algorithm:



Quantum algorithm



where $U = \sum_{ab \in \{0,1\}^2} |ab\rangle\langle\psi_{ab}|$

Output state of the first two qubits in the four cases:

$|\psi_{00}\rangle = -|00\rangle + |01\rangle + |10\rangle + |11\rangle$

$|\psi_{01}\rangle = +|00\rangle - |01\rangle + |10\rangle + |11\rangle$

$|\psi_{10}\rangle = +|00\rangle + |01\rangle - |10\rangle + |11\rangle$

$|\psi_{11}\rangle = +|00\rangle + |01\rangle + |10\rangle - |11\rangle$

Note that these states are ***orthogonal!***

Challenge Exercise: simulate the above U in terms of H, Toffoli, and NOT gates

Simple quantum algorithms in the query scenario

Query scenario

Input: a function f, given as a black box (a.k.a. oracle)

$$x \;—\; \boxed{f} \;—\; f(x)$$

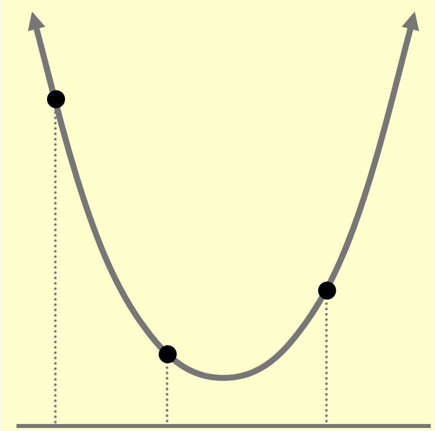
Goal: determine some information about f making as few queries to f (and other operations) as possible

Example: polynomial interpolation

Let: $f(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_d\, x^d$

Goal: determine c_0 , c_1 , c_2 , … , c_d

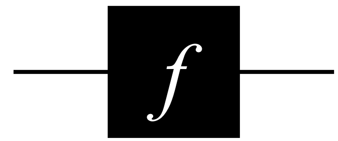
Question: How many f-queries does one require for this?



Answer: $d + 1$

Deutsch's problem

Let f: $\{0,1\} \rightarrow \{0,1\}$



There are ***four*** possibilities:

x	$f_1(x)$
0	0
1	0

x	$f_2(x)$
0	1
1	1

x	$f_3(x)$
0	0
1	1

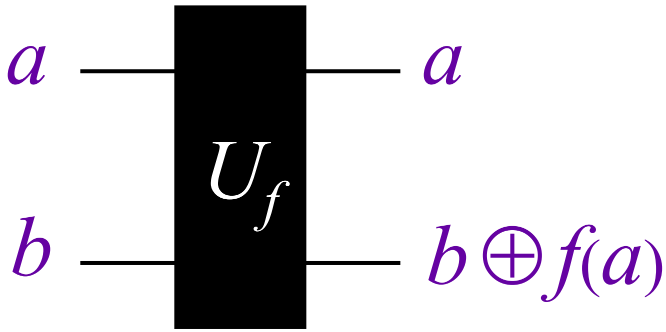
x	$f_4(x)$
0	1
1	0

Goal: determine whether or not $f(0) = f(1)$ (i.e. $f(0) \oplus f(1)$)

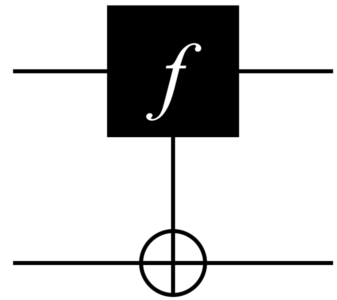
Any classical method requires ***two*** queries

What about a quantum method?

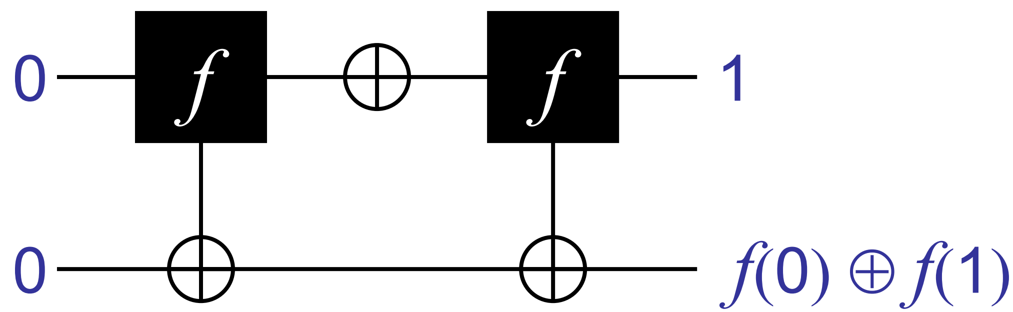
Reversible black box for f



alternate notation:

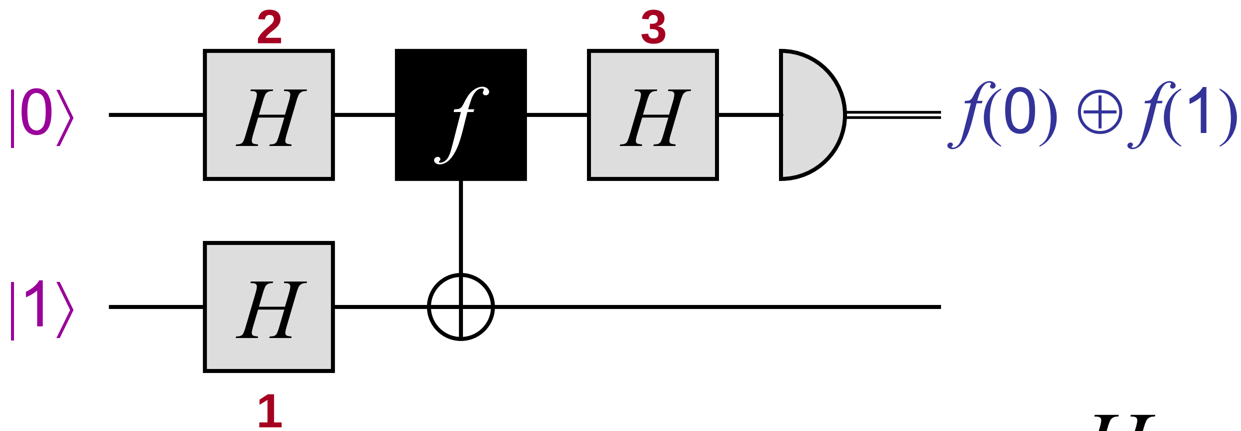


A classical algorithm:
(still requires 2 queries)



2 queries + **1** auxiliary operation

Quantum algorithm for Deutsch



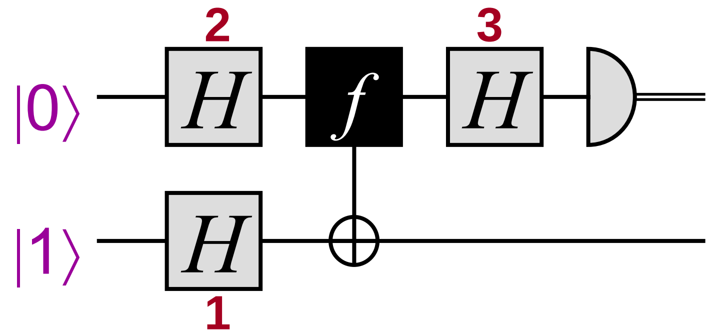
$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

1 query + **4** auxiliary operations

How does this algorithm work?

Each of the three H operations can be seen as playing a different role ...

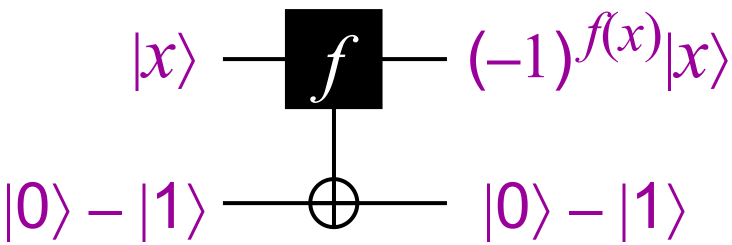
Quantum algorithm (1)



1. Creates the state $|0\rangle - |1\rangle$, which is an eigenvector of

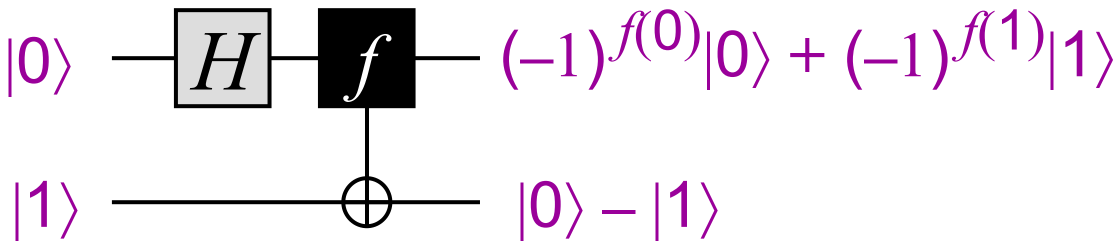
$$\begin{cases} \textbf{NOT} \text{ with eigenvalue } -1 \\ I \quad \text{with eigenvalue } +1 \end{cases}$$

This causes f to induce a ***phase shift*** of $(-1)^{f(x)}$ to $|x\rangle$



Quantum algorithm (2)

2. Causes f to be queried ***in superposition*** (at $|0\rangle + |1\rangle$)



x	$f_1(x)$
0	0
1	0

x	$f_2(x)$
0	1
1	1

x	$f_3(x)$
0	0
1	1

x	$f_4(x)$
0	1
1	0

f_1, f_2: $\pm(|0\rangle + |1\rangle)$

f_3, f_4: $\pm(|0\rangle - |1\rangle)$

Quantum algorithm (3)

3. Distinguishes between $\pm(|0\rangle + |1\rangle)$ and $\pm(|0\rangle - |1\rangle)$

$$\pm(|0\rangle + |1\rangle) \xleftrightarrow{H} \pm|0\rangle$$

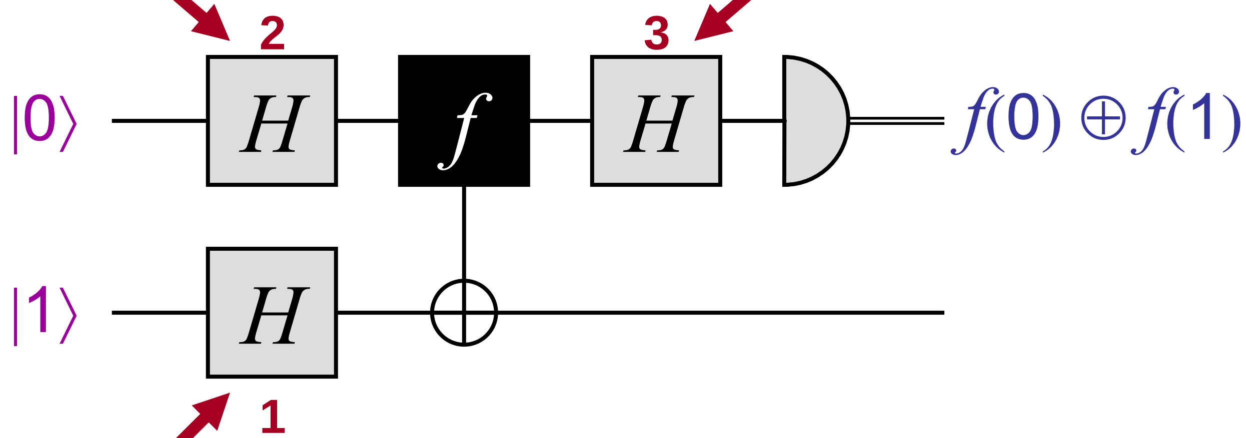
$$\pm(|0\rangle - |1\rangle) \xleftrightarrow{H} \pm|1\rangle$$

Summary of Deutsch's algorithm

Makes only one query, whereas two are needed classically

produces superpositions of inputs to f: $|0\rangle + |1\rangle$

extracts phase differences from $(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$



constructs eigenvector so f-queries induce phases: $|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$

universality of two-qubit gates

A universal set of gates

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

(This was stated in Lecture 5 without a proof)

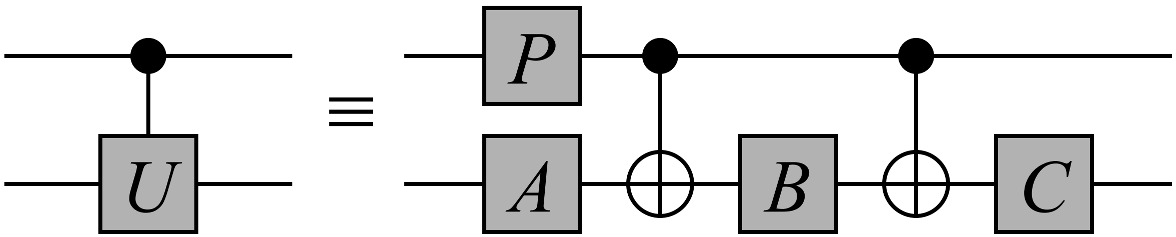
Proof sketch (for a slightly worse bound of $O(k^2 4^k)$) **:**
We first show how to simulate a controlled-U, for any one-qubit unitary U

Fact: for any 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 $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

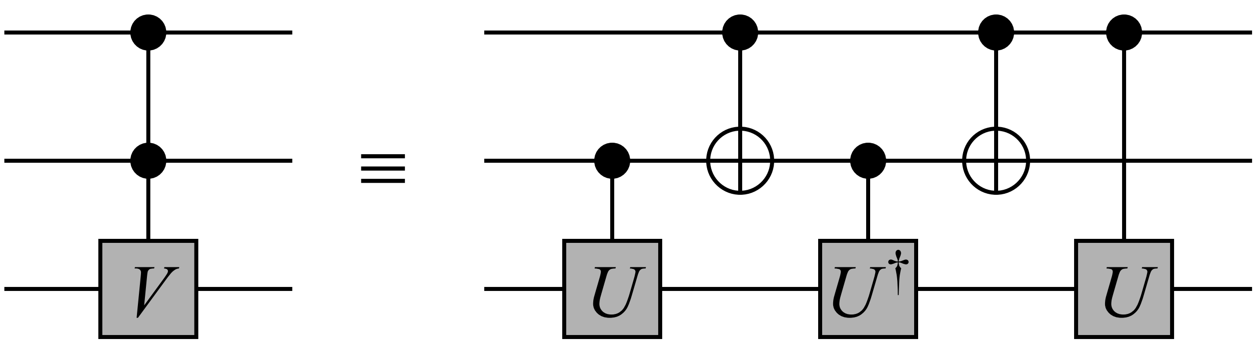
A universal set of gates

The aforementioned fact implies



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

Using such controlled-U gates, one can simulate controlled-controlled-V gates, for any unitary V, as follows:

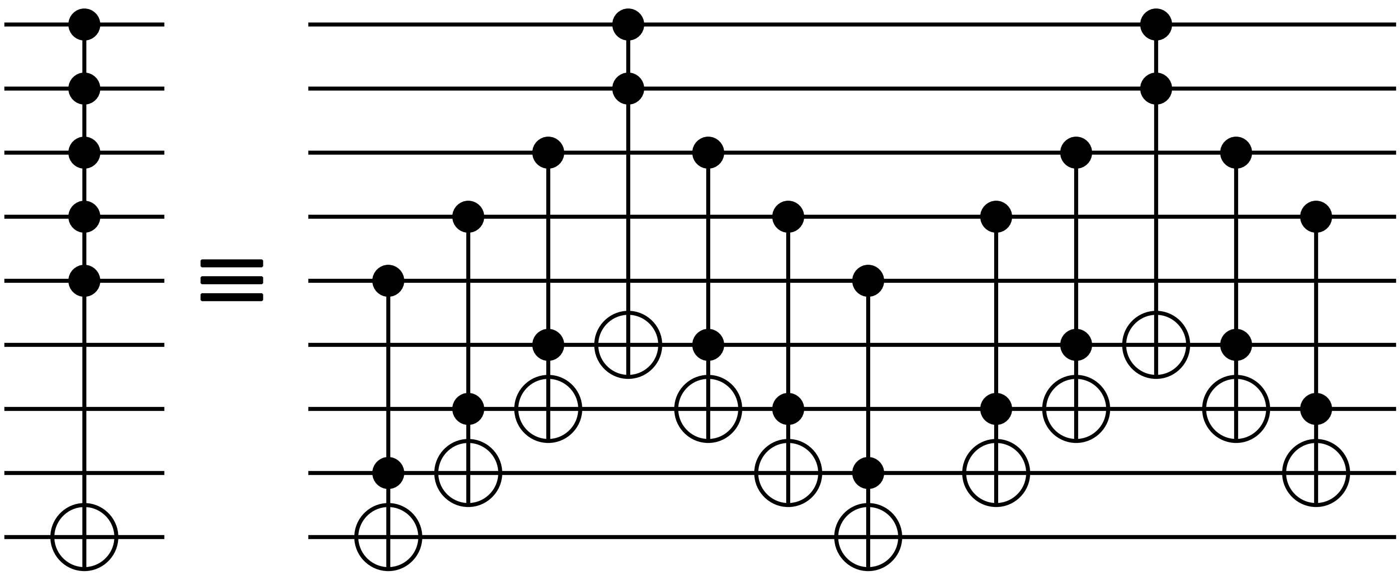


where $V = U^2$

A universal set of gates

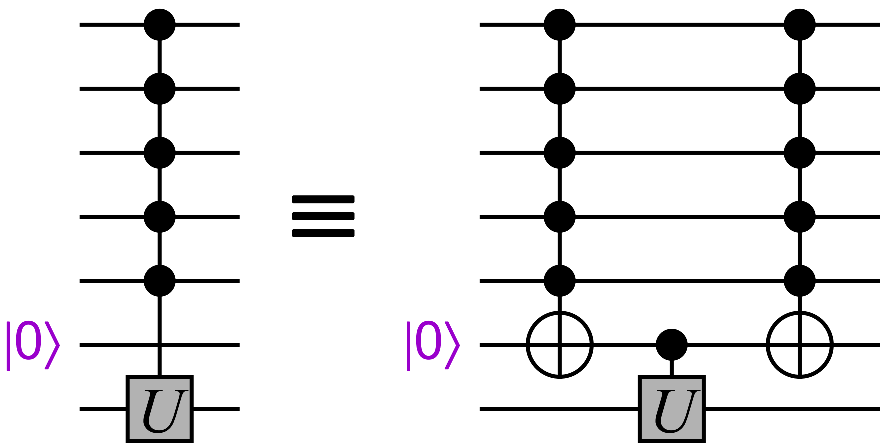
When $U = X$, this construction yields the 3-qubit ***Toffoli gate***

From this gate, ***generalized*** Toffoli gates can be constructed:



A universal set of gates

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

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

Any $2^k \times 2^k$ unitary matrix can be decomposed into a product of $O(4^k)$ such simple matrices

A universal set of gates

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)

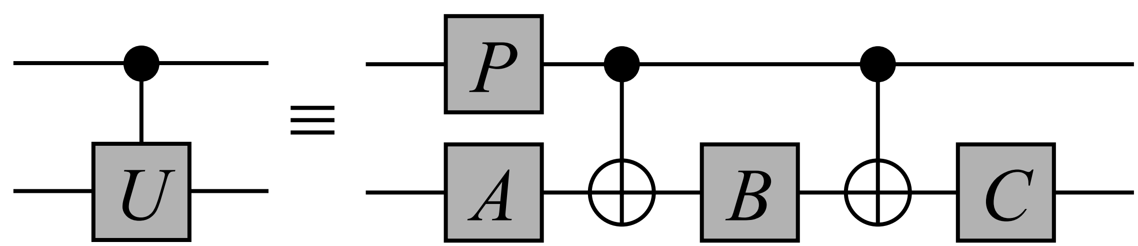
Universal sets of gates

Universal gate set

Theorem 1: The CNOT gate, along with all one-qubit unitaries is a universal set in that any k-qubit unitary operation can be decomposed into $O(4^k)$ such gates

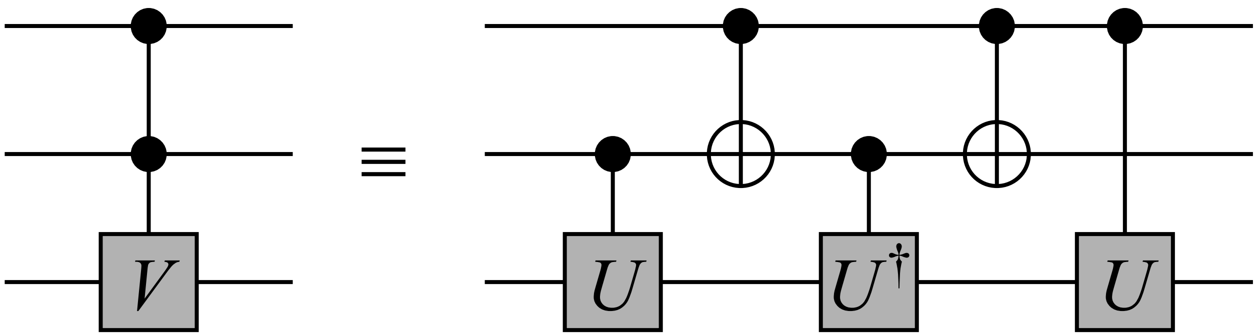
Some key steps of the proof:

For any unitary operation U, there exist one-qubit unitaries P, A, B, C such that:



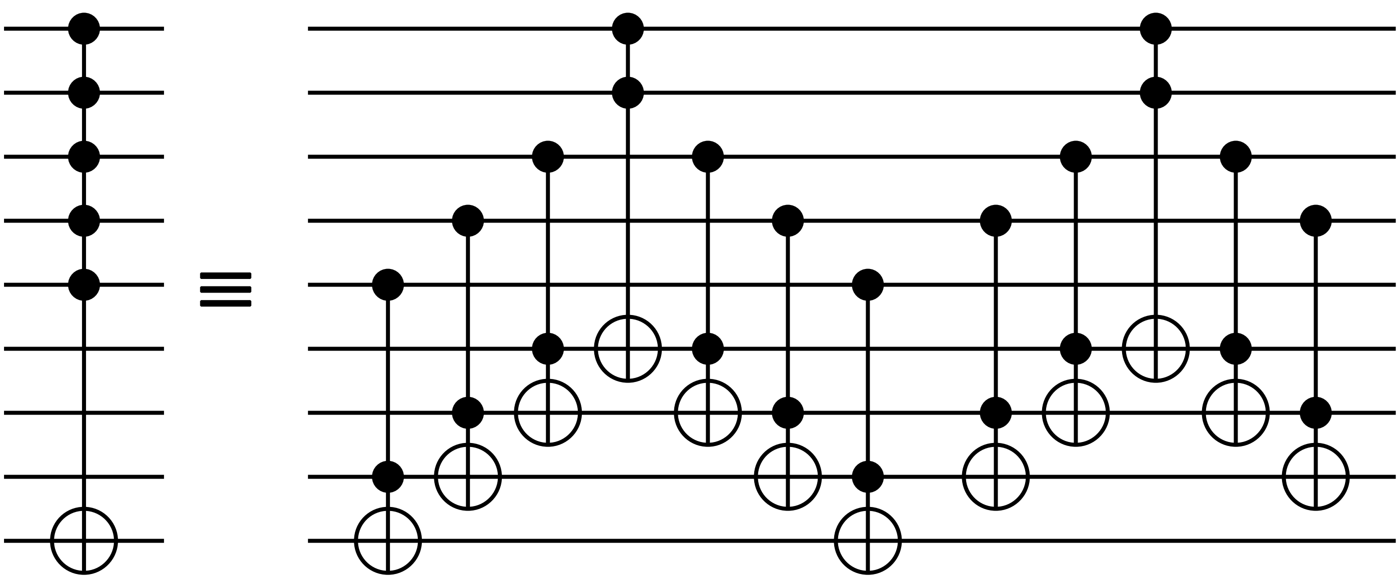
Universal gate set (II)

controlled-controlled-V



where $V = U^2$

From this gate, ***generalized*** Toffoli gates can be constructed:



Universal gate set (III)

The approach leads to the k-qubit operations of the form

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

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

Any $2^k \times 2^k$ unitary matrix can be decomposed into a product of $O(4^k)$ such simple matrices

Approximately universal gate set

Theorem 2: the gates CNOT, H, and $S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ 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)

Density operators

Density matrices

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

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

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

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

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

Density matrices (II)

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

$\big((p_1, |\psi_1\rangle), (p_2, |\psi_2\rangle), \ldots, (p_n, |\psi_n\rangle)\big)$

The ***density matrix*** associated with such a mixture is:

$$\rho = \sum_{k=1}^{n} p_k \left|\psi_k\right\rangle\!\left\langle\psi_k\right|$$

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

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

$\big((½, |0\rangle + |1\rangle), (½, |0\rangle - |1\rangle)\big)$ has the same density matrix!

General quantum operations

General quantum operations

Characterizing properties of ρ :

- ρ positive semi-definite
- Tr$\rho = 1$

$$\rho = \sum_{k=1}^{n} p_k \left|\psi_k\right\rangle\left\langle\psi_k\right|$$

General quantum operations (aka. ***completely positive trace preserving operations***, ***admissible operations***)**:**

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

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

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

General quantum operations (II)

Example 2: 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 (III)

Example 3 (discarding 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 $\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}\langle 00| + \frac{1}{\sqrt{2}}\langle 11|\right)$ becomes $\begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix}$

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

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

Separable states

Separable states

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

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

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

(ie. a mixture of product states)

Example: the state

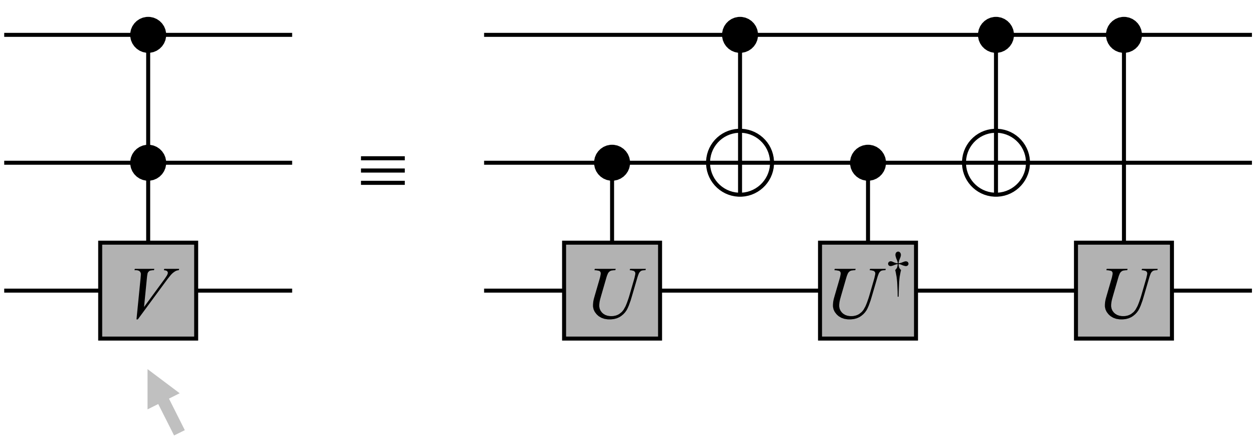
$$\rho = \tfrac{1}{2}\big(|00\rangle + |11\rangle\big)\big(\langle 00| + \langle 11|\big) + \tfrac{1}{2}\big(|00\rangle - |11\rangle\big)\big(\langle 00| - \langle 11|\big)$$

is separable, since $\rho = \tfrac{1}{2}|0\rangle\langle 0| \otimes |0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| \otimes |1\rangle\langle 1|$

Universal gate set

Theorem 1: The CNOT gate, along with all one-qubit unitaries is a universal set in that any k-qubit unitary operation can be decomposed into $O(4^k)$ such gates

Some components of the proof:



where $V = U^2$

controlled-controlled-V

How teleportation works

Initial state: $(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle)$ (omitting the $1/\sqrt{2}$ factor)

$$= \alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle$$

$$\begin{aligned} &= \tfrac{1}{2}(|00\rangle + |11\rangle)(\alpha|0\rangle + \beta|1\rangle) \\ &+ \tfrac{1}{2}(|00\rangle - |11\rangle)(\alpha|1\rangle + \beta|0\rangle) \\ &+ \tfrac{1}{2}(|01\rangle + |10\rangle)(\alpha|0\rangle - \beta|1\rangle) \\ &+ \tfrac{1}{2}(|01\rangle - |10\rangle)(\alpha|1\rangle - \beta|0\rangle) \end{aligned}$$

Protocol: Alice measures her two qubits ***in the Bell basis*** and sends the result to Bob (who then "corrects" his state)

Review of partial measurements

Suppose one measures just the ***first*** qubit of the state

$$\frac{1}{2}|00\rangle + \frac{i}{\sqrt{3}}|01\rangle + \sqrt{\frac{5}{12}}|11\rangle = \sqrt{\frac{7}{12}}|0\rangle\left(\sqrt{\frac{3}{7}}|0\rangle + i\sqrt{\frac{4}{7}}|1\rangle\right) + \sqrt{\frac{5}{12}}|1\rangle|1\rangle$$

What is the result?

$$\begin{cases} 0,\ \ \sqrt{\frac{3}{7}}|0\rangle + i\sqrt{\frac{4}{7}}|1\rangle & \text{with prob. } 7/12 \\ 1,\ \ |1\rangle & \text{with prob. } 5/12 \end{cases}$$

A universal set of gates

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

(This was stated in Lecture 5 without a proof)

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

Fact: for any one-qubit unitary U, there exist A, B, C, and λ, such that:

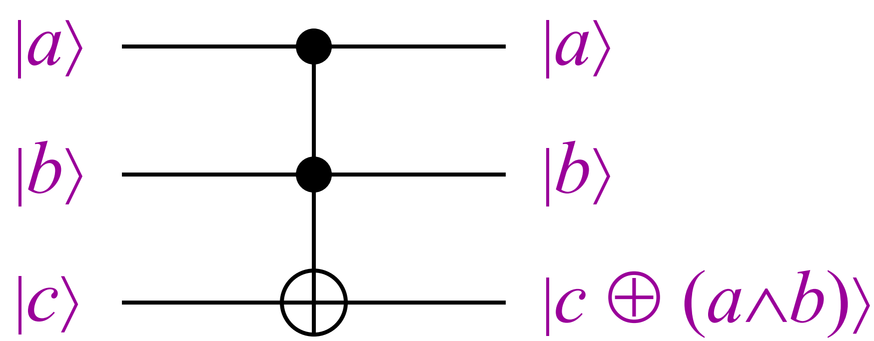
- $A\,B\,C = I$
- $e^{i\lambda} A\,X\,B\,X\,C = U$, where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Universal sets of gates

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

Therefore, CNOT and all one-qubit gates are ***universal*** (classical analogue: AND and NOT gates)

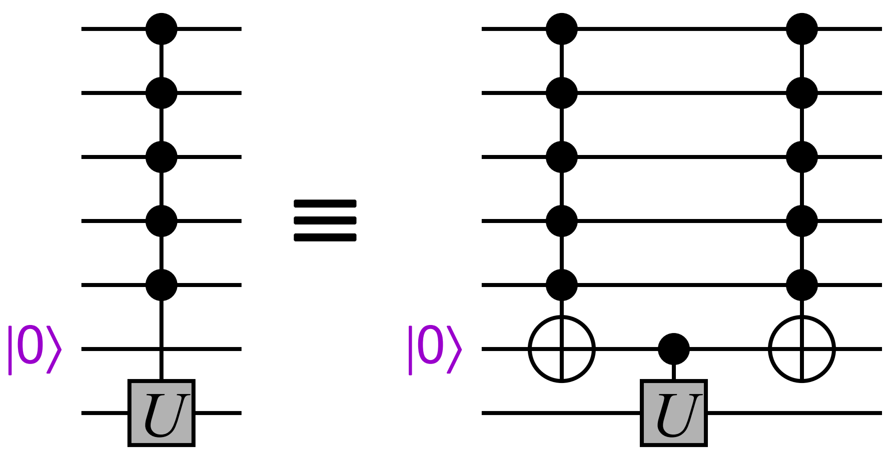
Example: Toffoli gate
"controlled-controlled-NOT"



Can be simulated by CNOT, H, and $W = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

A universal set of gates

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

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

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

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

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

Theorem: the gates CNOT, H, and $S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

are ***approximately universal***, in the sense 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)

Say something about basic idea …?

[Solovay, 1996][Kitaev, 1997]

Density matrices II

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

$\big((p_1, |\psi_1\rangle), (p_2, |\psi_2\rangle), \ldots, (p_n, |\psi_n\rangle)\big)$

The ***density matrix*** associated with such a mixture is:

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

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

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

Same for $\big((½, |0\rangle + |1\rangle), (½, |1\rangle\ |0\rangle - |1\rangle)\big)$

A universal set of gates

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

(This was stated in Lecture 5 without a proof)

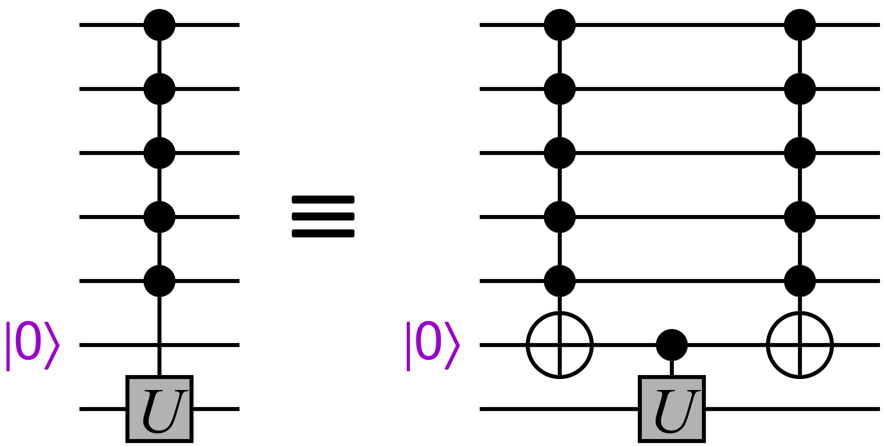
Proof sketch (for a slightly worse bound of $O(k^2 4^k)$) **:**
We first show how to simulate a controlled-U, for any one-qubit unitary U

Fact: for any 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 $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

A universal set of gates

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

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

Any $2^k \times 2^k$ unitary matrix can be decomposed into a product of $O(4^k)$ such simple matrices

A universal set of gates

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?

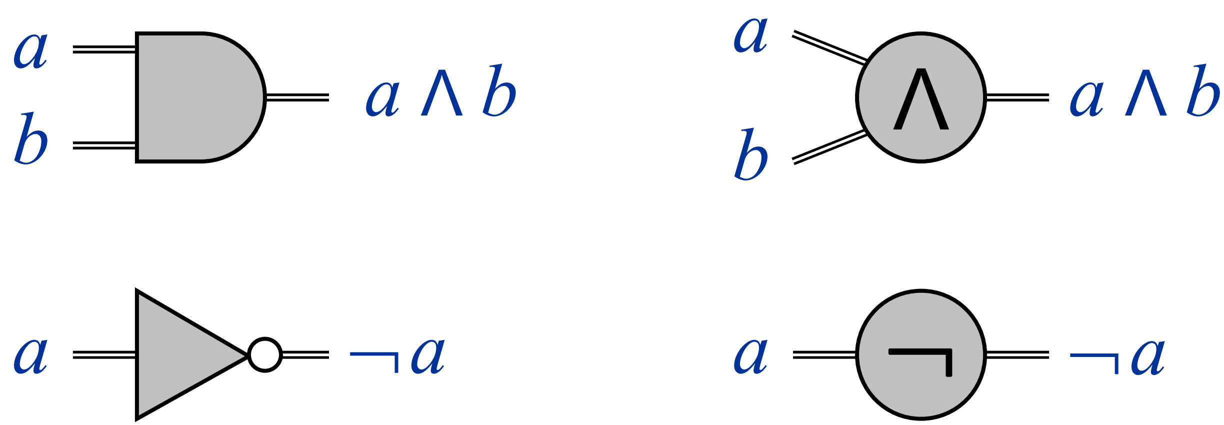
Answer 1: strictly speaking, ***no***, because this results in only countably many quantum circuits, whereas there are uncountably many unitary operations on k qubits (for any k)

Classical (boolean logic) gates

“old” notation   “new” notation

AND gate

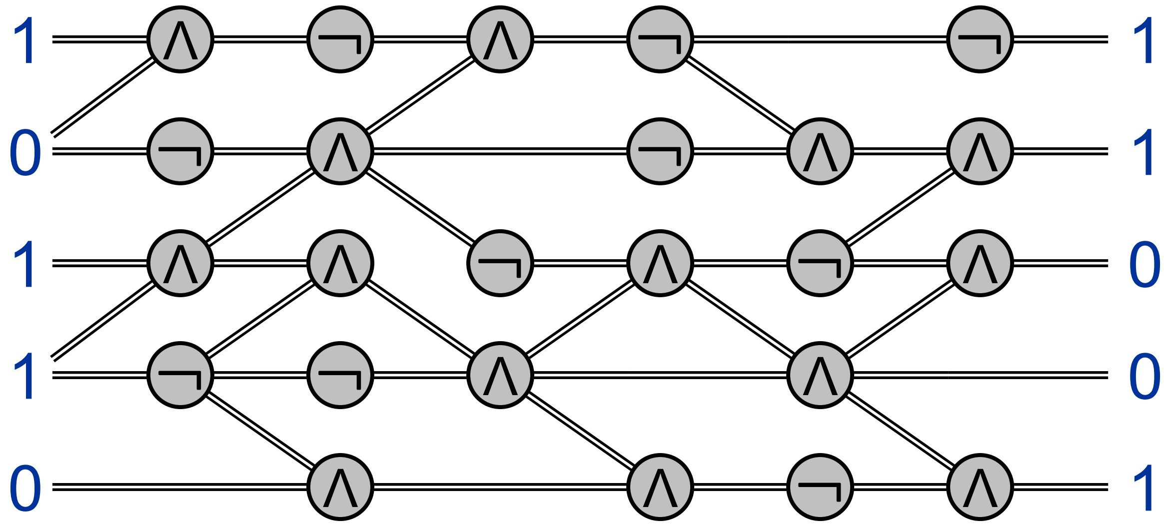
NOT gate



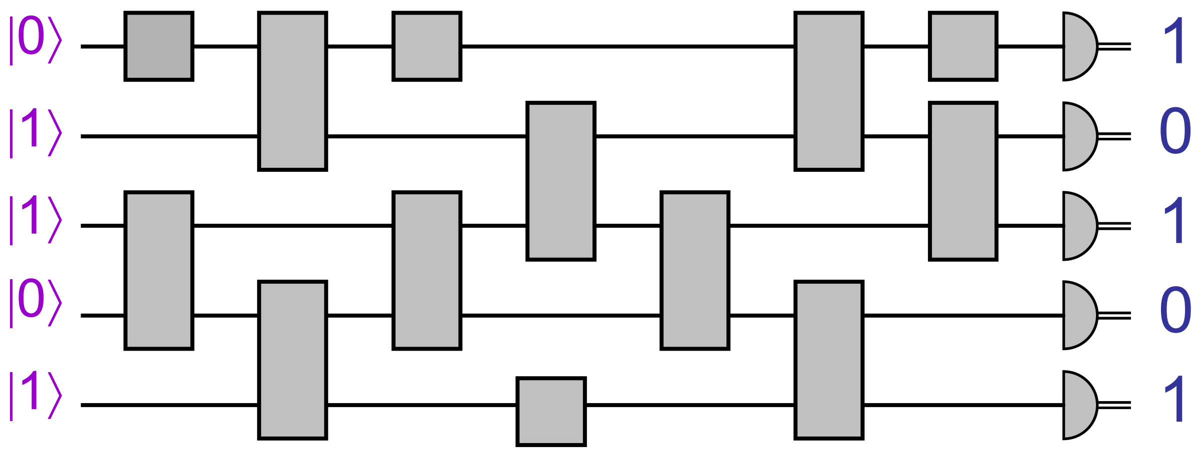
Note: an **OR** gate can be simulated by one **AND** gate and three **NOT** gates

Models of computation

Classical circuits:



Quantum circuits:



Multiplication problem

Input: two n-bit numbers (e.g. 101 and 111)

Output: their product (e.g. 100011)

- "Grade school" algorithm costs $O(n^2)$
- Best currently-known ***classical*** algorithm costs $O(n \log n \operatorname{loglog} n)$
- Best currently-known ***quantum*** method: same

Factoring problem

Input: an n-bit number (e.g. 100011)

Output: their product (e.g. 101, 111)

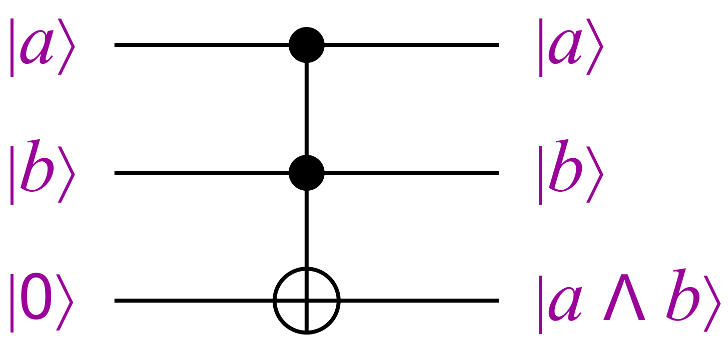
- Trial division costs $\approx 2^{n/2}$
- Best currently-known ***classical*** algorithm costs $\approx 2^{n^{1/3}}$
- Hardness of factoring is the basis of the security of many cryptosystems (e.g. RSA)
- Shor's ***quantum*** algorithm costs $\approx n^2$
- Implementation would break RSA and many other cryptosystems

Quantum vs. classical circuits

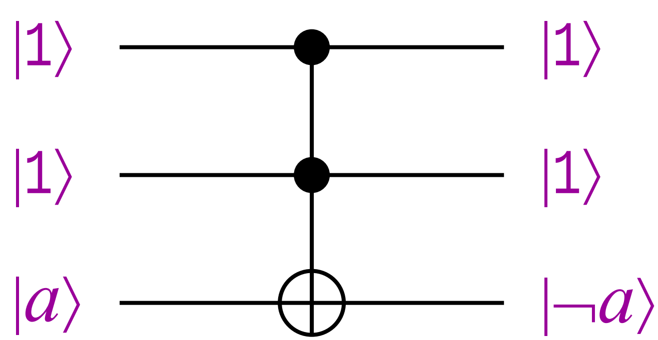
Theorem: a classical circuit of size s can be simulated by a quantum circuit of size $O(s)$

Idea: using Toffoli gates, one can simulate:

AND gates



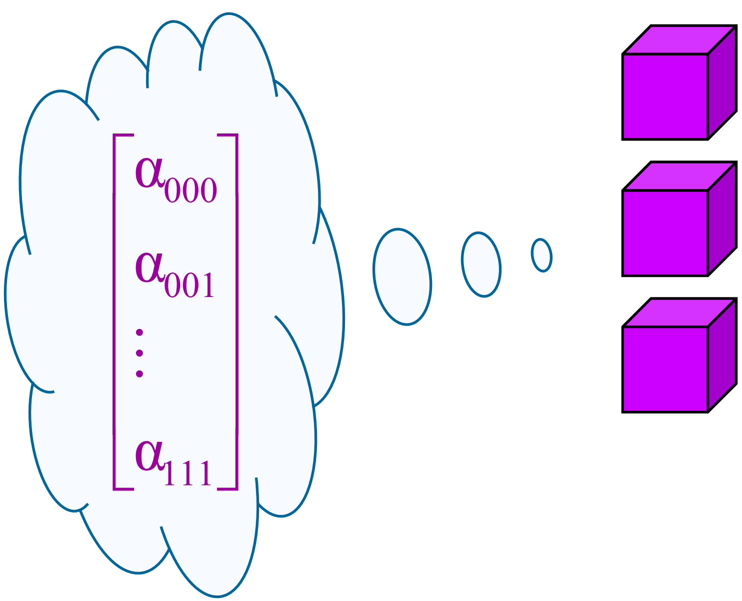
NOT gates



Operations on quantum states

Unitary operations: “rotations” to quantum states

Measurements: produce classical information



$$\mapsto \begin{cases} 000 & \text{with prob } |\alpha_{000}|^2 \\ 001 & \text{with prob } |\alpha_{001}|^2 \\ \vdots & \quad\vdots \qquad\qquad \vdots \\ 111 & \text{with prob } |\alpha_{111}|^2 \end{cases}$$

… and quantum state collapses

Quantum Fourier Transform

The polynomial-time algorithm for factoring is based on the ***quantum Fourier transform (QFT)***

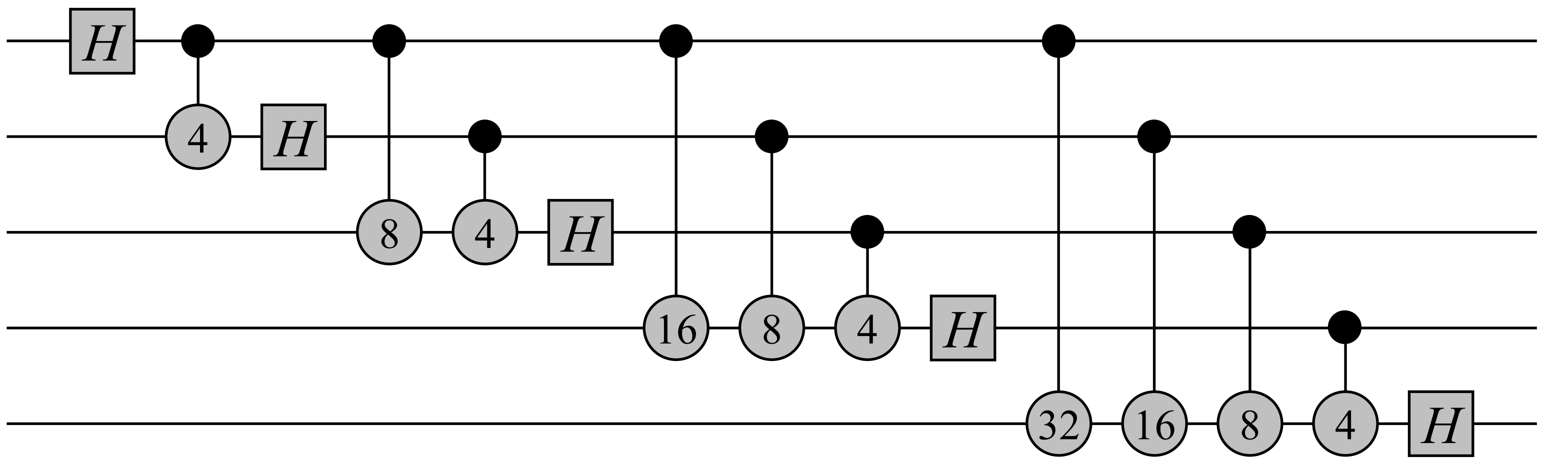
$$F_N = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \dots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots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

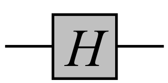
where $\omega = e^{2\pi i/N}$ (and N is exponentially large)

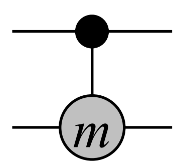
The QFT "extracts information about periodicity"

Computing the QFT

Quantum circuit for F_{32}:



Gates: 

$= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ 

$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi i/m} \end{bmatrix}$

For F_{2^n} costs $O(n^2)$ gates (exact) & $O(n \log n)$ gates (approx)

[Shor, 1994] [Coppersmith, 1994] [C, 1994]

Outline

- Qubits, unitary ops, and projective measurements
- Superdense coding
- Teleportation
- Universal sets of gates

- No-cloning theorem
- Density operators
- General quantum operations
- Separable states