Introduction to Quantum Information Processing

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

Lecture 3 (2017)

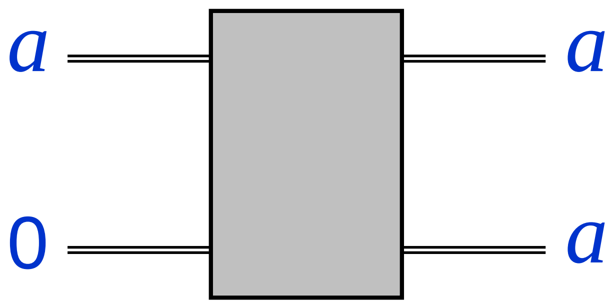
Jon Yard
QNC 3126
jyard@uwaterloo.ca

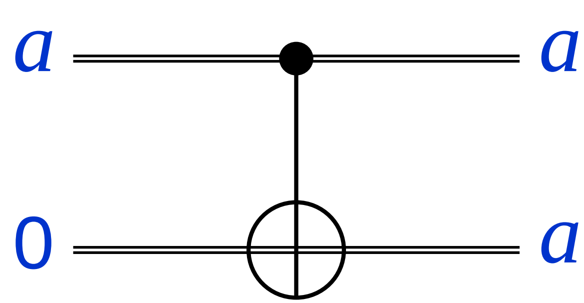
Shuffling rooms

- Thursday, Sept. 21st class is in **MC4058**
- Tuesday, Sept. 26th class is in…?

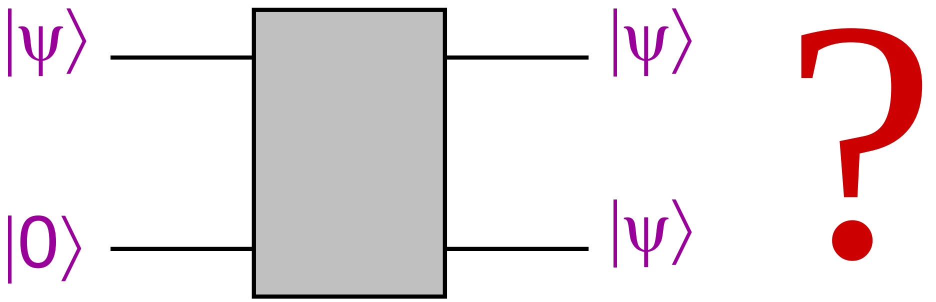
No-cloning theorem

Classical information can be copied

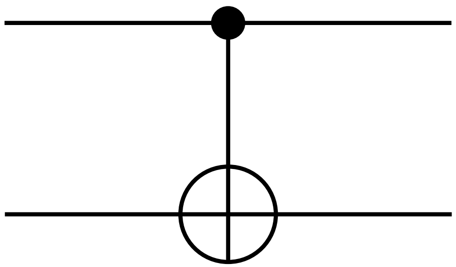




What about quantum information?



Candidate:



works fine for $|\psi\rangle = |0\rangle$ and $|\psi\rangle = |1\rangle$

... but it fails for $|\psi\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

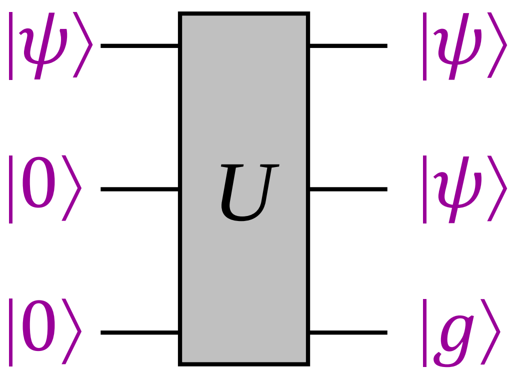
... where it yields output $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

instead of $|+\rangle|+\rangle = \frac{1}{4}|00\rangle + \frac{1}{4}|01\rangle + \frac{1}{4}|10\rangle + \frac{1}{4}|11\rangle$

No-cloning theorem

Theorem: there is ***no*** valid quantum operation that maps an arbitrary state $|\psi\rangle$ to $|\psi\rangle|\psi\rangle$

Proof:



Suppose there is an operation that is capable of cloning two different states $|\psi\rangle$ and $|\psi'\rangle$, yielding outputs $|\psi\rangle|\psi\rangle|g\rangle$ and $|\psi'\rangle|\psi'\rangle|g'\rangle$ respectively.

Since U preserves inner products,

$\langle\psi|\psi'\rangle = \langle\psi|\psi'\rangle\langle\psi|\psi'\rangle\langle g|g'\rangle$ so

$\langle\psi|\psi'\rangle(1 - \langle\psi|\psi'\rangle\langle g|g'\rangle) = 0$ so

$|\langle\psi|\psi'\rangle| = 0$ or 1

No-cloning theorem

802 *Nature Vol. 299 28 October 1982*

LETTERS TO NATURE

A single quantum cannot be cloned

W. K. Wootters*

Center for Theoretical Physics, The University of Texas at Austin, Austin, Texas 78712, USA

W. H. Zurek

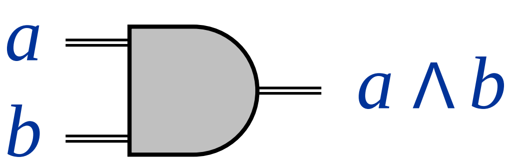
Theoretical Astrophysics 130–33, California Institute of Technology, Pasadena, California 91125, USA

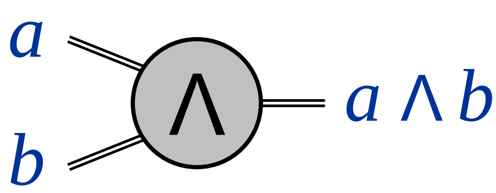
Classical computations as circuits

Classical (boolean logic) gates

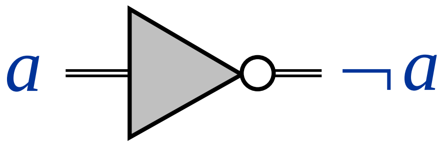
"old" notation | "new" notation

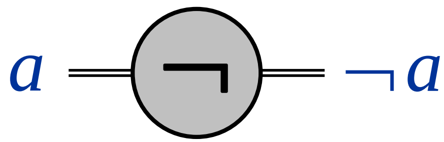
AND gate





NOT gate

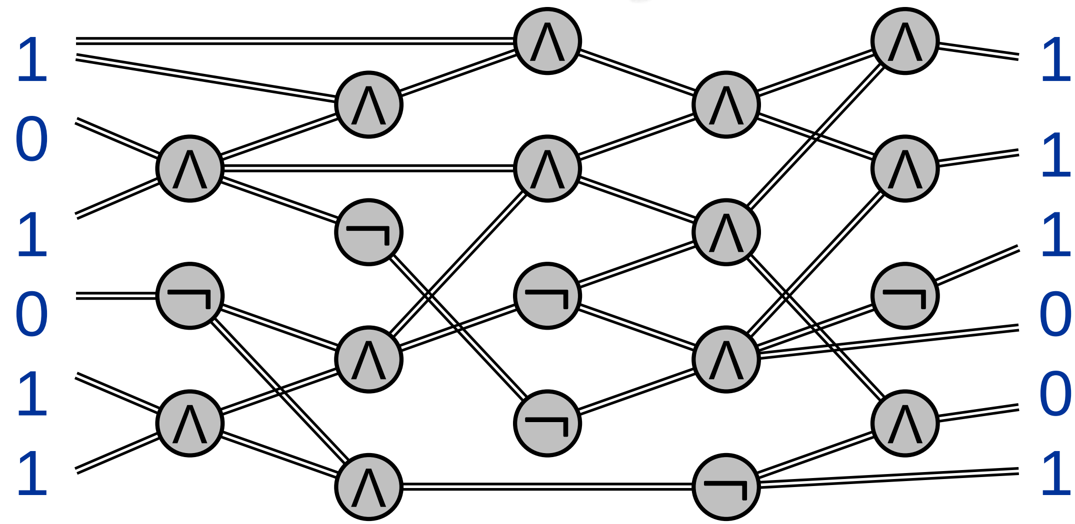




Note: an **OR** gate can be simulated by one **AND** gate and three **NOT** gates (since $a \vee b = \neg(\neg a \wedge \neg b)$)

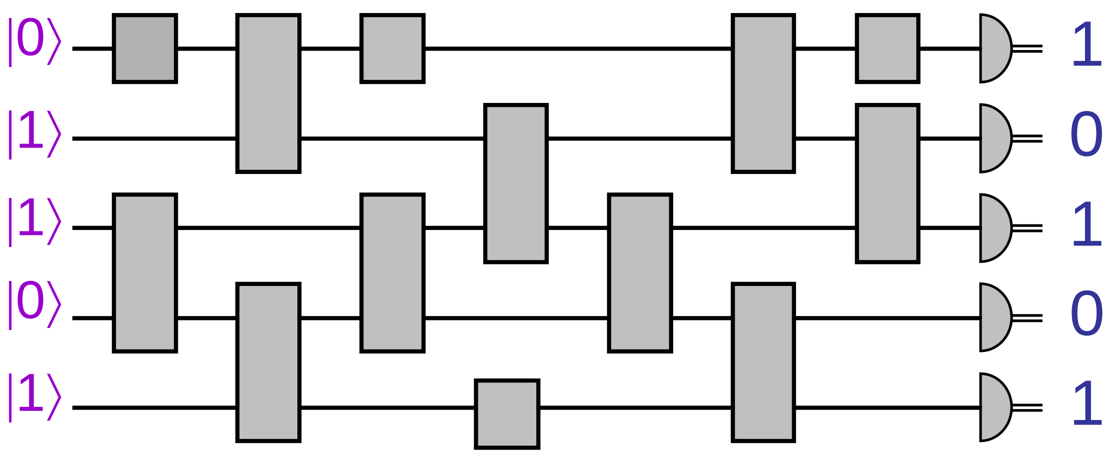
Models of computation

Classical circuits:



data flow →

Quantum circuits:



Multiplication problem

Input: two n-bit numbers (e.g. $101 = 5$ and $111 = 7$)

Output: their product (e.g. $100011 = 35$)

- "Grade school" algorithm costs $O(n^2)$ [scales up *polynomially*]
- Best currently-known ***classical*** algorithm costs slightly less than $O(n \log n \operatorname{loglog} n)$

  [to be precise, $O(n \log n \, 2^{O(\log^* n)})$ – see Fürer's algorithm)]
- Best currently-known ***quantum*** method: same

Factoring problem

Input: an n-bit number (e.g. $100011 = 35$)

Output: their prime factors (e.g. $101 = 3$, $111 = 7$)

- Trial division costs $\approx 2^{n/2}$
- Best currently-known ***classical*** algorithm costs $\approx 2^{n^{1/3}}$

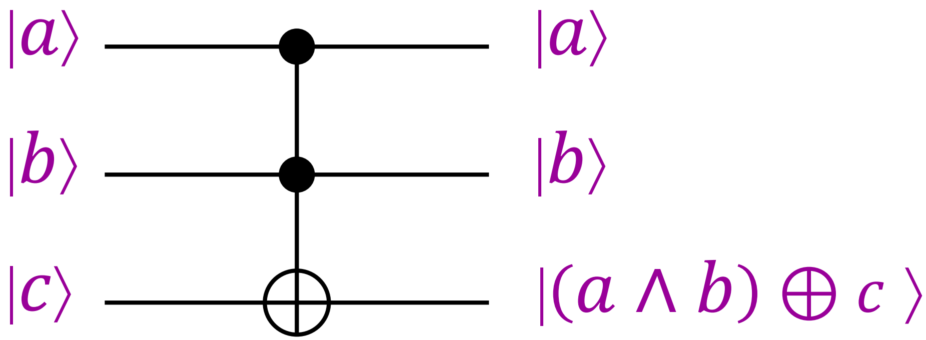
[more precisely, $2^{O(n^{1/3} \log^{2/3} n)} \neq O(\text{poly}(n))$ (general number field sieve)]

- The presumed hardness of factoring is the basis of the security of many cryptosystems (e.g. RSA)
- Shor's ***quantum*** algorithm costs $\approx n^2$ [less than $O(n^2 \log n \log\log n)$]
- Implementation would break RSA — and many other public-key cryptosystems

Simulating ***classical*** circuits with ***quantum*** circuits

Toffoli gate

(Sometimes called a "controlled-controlled-NOT" gate)



In the computational basis, it negates the third qubit iff the first two qubits are both $|1\rangle$

Matrix representation:

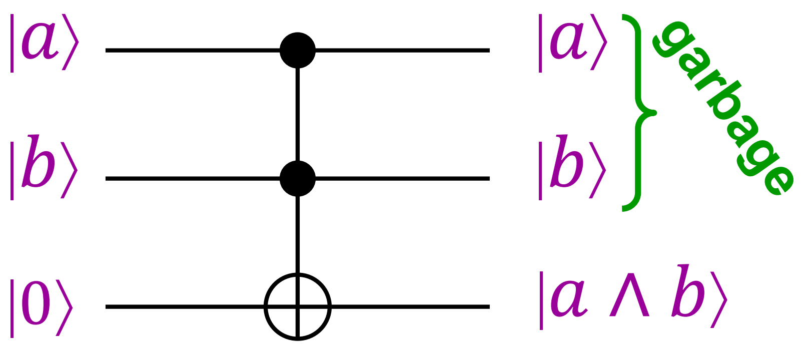
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Quantum simulation of classical

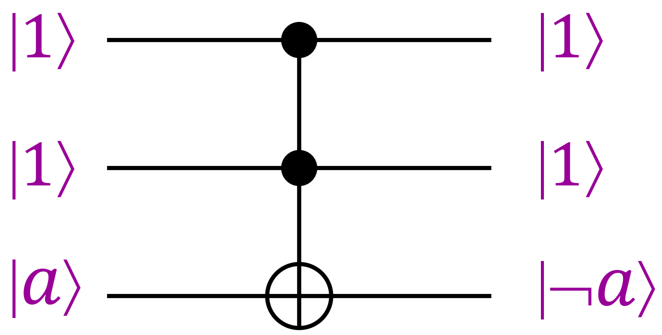
Theorem: a classical circuit of size s can be simulated by a quantum circuit of size $O(s)$

Idea: using Toffoli gates, one can simulate:

AND gates



NOT gates

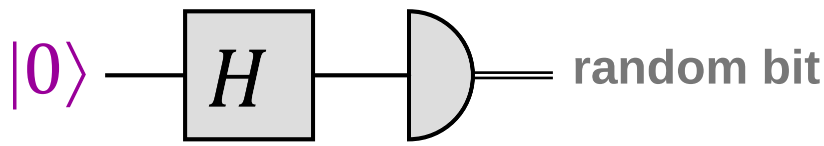


We will have to deal with the garbage later on

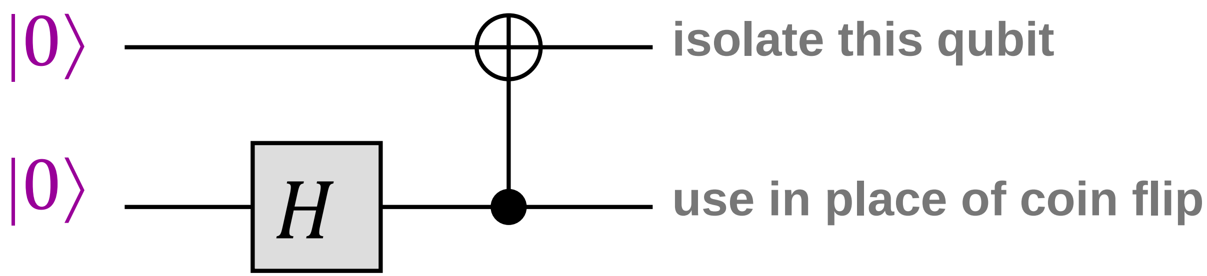
Simulating probabilistic algorithms

Since quantum gates can simulate **AND** and **NOT**, the outstanding issue is how to simulate randomness

To simulate "coin flips", one can use the circuit:



It can also be done without intermediate measurements:



Exercise: prove that this works

Simulating ***quantum*** circuits with ***classical*** circuits

Classical simulation of quantum

Theorem: a quantum circuit of size s acting on n qubits can be simulated by a classical circuit of size $O(sn^2 2^n) = O(2^{cn})$

Idea: to simulate an n-qubit state, use an array of size 2^n containing values of all 2^n amplitudes within precision 2^{-n}

α_{000}
α_{001}
α_{010}
α_{011}
:
α_{111}

Can adjust this state vector whenever a unitary operation is performed at cost $O(n^2 2^n)$

From the final amplitudes, can determine how to set each output bit

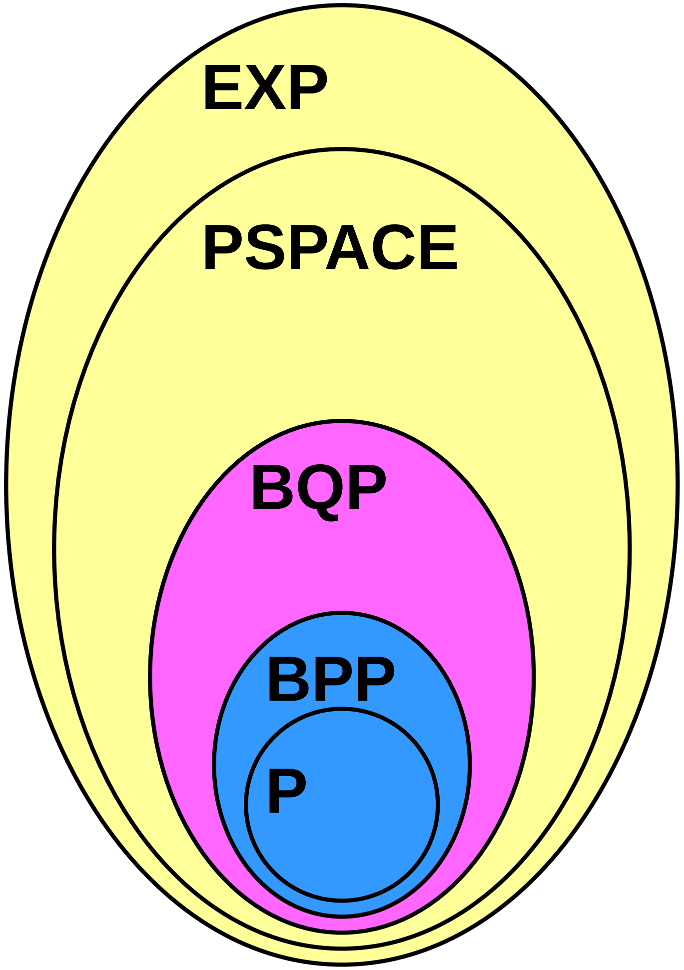
Exercise: show how to do the simulation using only a polynomial amount of ***space*** (memory) (see Preskill's lecture notes)

Some *complexity* classes

- **P (polynomial time):** the problems solved by $O(n^c)$-size classical circuits [technically, we restrict to decision problems and to “uniform circuit families”]
- **BPP (bounded error probabilistic polynomial time):** the problems solved by $O(n^c)$-size ***probabilistic*** circuits that are correct with probability $\geq 2/3$
- **BQP (bounded error quantum polynomial time):** the problems solved by $O(n^c)$-size ***quantum*** circuits that are correct with probability $\geq 2/3$
- **EXP (exponential time):** the problems solved by $O\left(2^{n^c}\right)$-size circuits

Summary of basic containments

P ⊆ BPP ⊆ BQP ⊆ PSPACE ⊆ EXP



We will return to this picture
in more detail later in the course.
See Aaronson's book or the
Complexity Zoo for (much) more.

https://complexityzoo.uwaterloo.ca/Complexity_Zoo