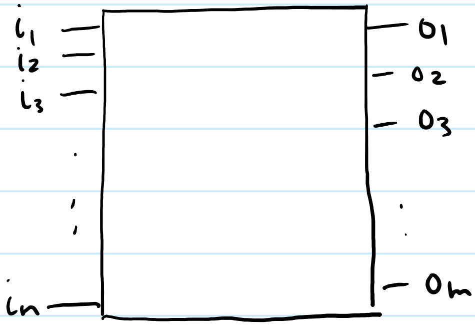
Quantum Complexity Classes - page 1

Monday, October 15, 2018 12:37 PM

First consider a classical circuit that computes a function from n bits to m bits.
(m could be larger than n, but it is typically smaller).

$$f: \{0,1\}^n \rightarrow \{0,1\}^m$$



the circuit is composed of gates from a finite set (e.g. OR, AND, NOT, ...)

A Universal Gate Set can be used to compute any Boolean function.
For example, the following sets are all universal:

{AND, NOT}, {OR, NOT}, {NAND}

We are typically interested in decision problems, in which the number of output bits is 1.

$$f: \{0,1\}^* \rightarrow \{0,1\}$$

$\{0,1\}^*$ contains strings of all lengths

Will need a different circuit for each input length.

Quantum Complexity Classes - page 2

Monday, October 15, 2018 12:37 PM

Decision problem: $f: \{0,1\}^* \rightarrow \{0,1\}$

can also be expressed as a language which is a subset of binary strings:

$L \subseteq \{0,1\}^*$ $x \in \{0,1\}^*$ $f(x) = 1 \longleftrightarrow x \in L$

Now lets define the class P:

P - deterministic polynomial time.

P is a set of languages.

$L \in P$ if and only if $\exists$ polynomial $p(n)$ and a family of circuits: $C_1, C_2, C_3, \ldots$ so that:

- if $|x| = n$ then $C_n(x) = (x \in L?)$
  Circuit C_n outputs the correct answer for all length-n binary strings.
- $|C_n|$ (# gates) $\leq p(n)$.
- there is a poly-time Turing Machine that on input 1^n, outputs C_n. *

Note that P does not depend on which gate set is chosen

* Uniformity condition: prevents us from encoding answers to hard problems in the circuit itself.
(hard-code output of C_n to be 0 or 1 depending on if $n \in$ undecidable L)

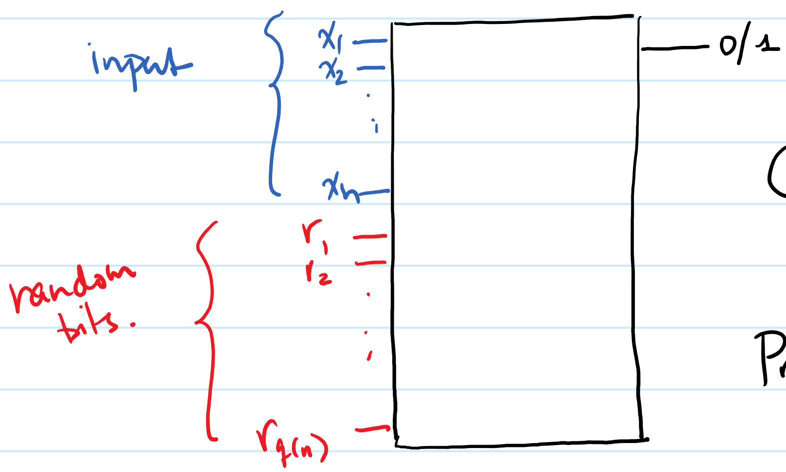
Quantum Complexity Classes - page 3

Monday, October 15, 2018 12:37 PM

Quantum Computation is by its nature probabilistic so we need to first define a probabilistic version of P.

BPP: Bounded Error Probabilistic Poly Time.

Allow the circuit to use random bits as part of the input - can define probability of error



$C(x,r) = 0/1$ deterministic.

$\text{Prob}_r[C(x,r)=1]$ ← averaged uniformly over all possible random strings r.

$L \in BPP$ iff $\exists$ polynomials $p(n)$, $q(n)$ and a family of circuits $C_1, C_2, C_3, \ldots$ such that.

- C_n has $n + q(n)$ inputs. (input x → n; random string r → $q(n)$)
- $|C_n| \le p(n)$ $\forall n \in \mathbb{N}$.
- uniformity.
- if $x \in L$ and $|x| = n$ $\text{Prob}_r[C_n(x,r)=1] \ge 2/3$
- if $x \notin L$ and $|x| = n$ $\text{Prob}_r[C_n(x,r)=0] \ge 2/3$

For every input x, probability of error $\le 1/3$ → (last two conditions)

Quantum Complexity Classes - page 4

Monday, October 15, 2018 12:37 PM

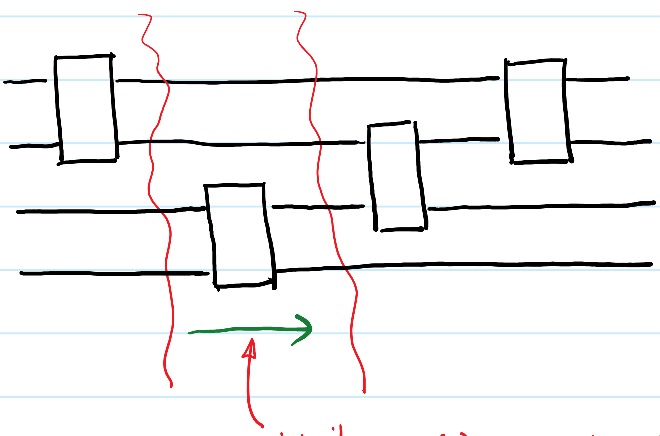
Note that the probability of error can be made arbitrarily small by repeating the computation (using fresh random bits) and taking the majority answer.

Quantum Circuits

The function computed by a quantum circuit must be unitary so:

input qubits = # output qubits.

A circuit is a sequence of primitive gates each of which acts on a small (usually 1-3) qubits:



unitary op on n qubits.
gate applied to two particular qubits tensor I on the rest

Quantum Complexity Classes - page 5

Monday, October 15, 2018 12:37 PM

Is there a universal gate set for quantum circuits?

Is there a finite set of gates that can be put together to compute <u>any</u> unitary operator acting on n qubits?

No... the set of unitary operators form a continuous space, so it is impossible for a finite gate set to generate all of them.

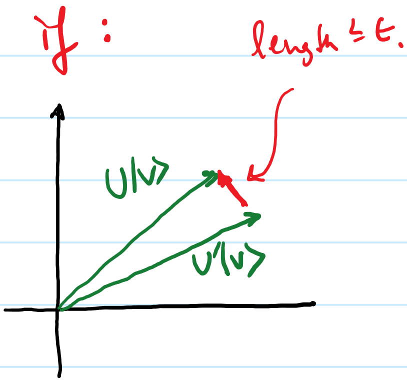
But it's possible that a finite gate set could <u>approximate</u> all of them.

Need a definition for what it means to approximate a linear operator.

Operator norm: $\|A\| = \max_{|\,|v\rangle| = 1} |A|v\rangle|$

U approximates U′ to within ϵ if:

$\|U - U'\| \le \epsilon$ → $\max_{|\,|v\rangle|} |(U-U')|v\rangle| \le \epsilon$



Quantum Complexity Classes - page 6

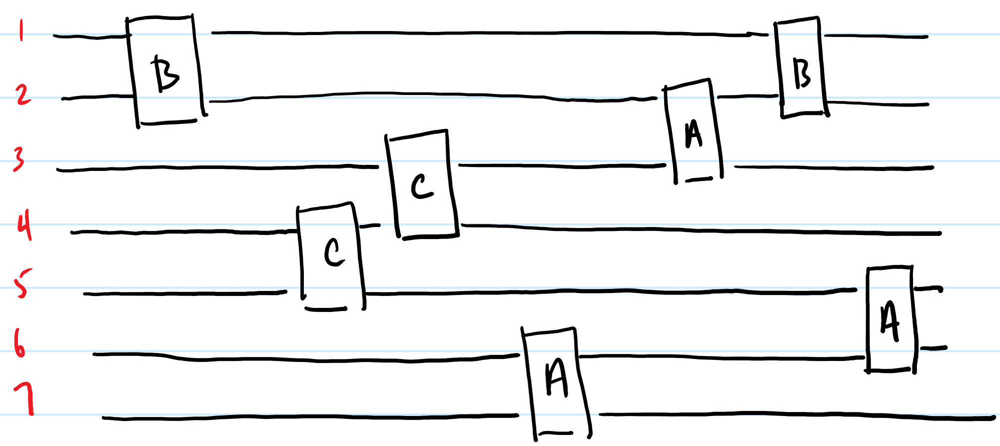
Wednesday, October 17, 2018 8:51 AM

A set of quantum gates G is **universal** if for every
- n
- U (unitary op on n qubits)
- ϵ

$\exists\ g_1, \ldots, g_\ell$ each $g_i \in G$

$$\| U - U_{g_1} U_{g_2} U_{g_3} \cdots U_{g_\ell} \| \leq \epsilon$$

U_{g_i} is the gate g_i applied to two particular qubits tensored w/ I on the rest.



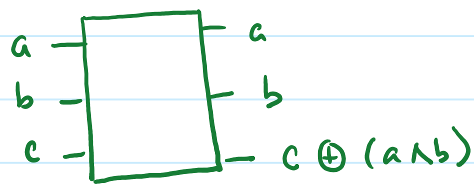
$$\underbrace{U_{A\,5\text{-}6}\, U_{B\,1\text{-}2}\, U_{A\,2\text{-}3}\, U_{A\,6\text{-}7}\, U_{C\,3\text{-}4}\, U_{C\,4\text{-}5}\, U_{B,1,2}}_{\text{unitary operator on } n \text{ qubits.}}$$

Quantum Complexity Classes - page 7

Wednesday, October 17, 2018 9:07 AM

Known universal gate sets:

- CNOT, 1-qubit gates. → Not finite but universal with no error.
- CNOT, H, one additional phase such as: $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/8} \end{bmatrix}$
- Tofolli, H
  - ↳ 3-qubit gate



What is the overhead in approximating U with a finite gate set?

* Any U on n qubits can be computed exactly with 2-qubit gates:

$$U = U_1 U_2 \cdots U_\ell \qquad U_i = G_{q_1(i)\, q_2(i)} \otimes I$$

$G_{q_1(i)\, q_2(i)}$: Unitary acting on qubits $q_1(i)$ and $q_2(i)$

I: Identity on all qubits except $q_1(i)$ $q_2(i)$

ℓ could be exponential in n - the # qubits.

Quantum Complexity Classes - page 8

Wednesday, October 17, 2018 9:07 AM

arbitrary U on n qubits $\xrightarrow{\text{no error}}$ product of ℓ 2-qubit gates $\xrightarrow{*}$ product of gates from a universal gate set. G

* Need to approximate an arbitrary 2-qubit gate with gates from G.

Solovay - Kitaev Theorem:

G is a set of 2-qubit gates.
If:

- G is closed under inverse
  ($g \in G \Leftrightarrow g^{-1} \in G$)
- G generates a dense subset for all 2-qubit gates.
  You can approximate any 2-qubit gate to within any ϵ using gates from G.

Then:
Only $O(\log^2(1/\epsilon))$ gates are required to simulate any 2-qubit gate to within ϵ using only gates from G.

Quantum Complexity Classes - page 9

Wednesday, October 17, 2018 9:20 AM

arbitrary U on n qubits $\xrightarrow{\text{no error}}$ product of ℓ 2-qubit gates $\xrightarrow{*}$ product of gates from a universal gate set G

$$U = U_1 U_2 U_3 \cdots U_\ell.$$

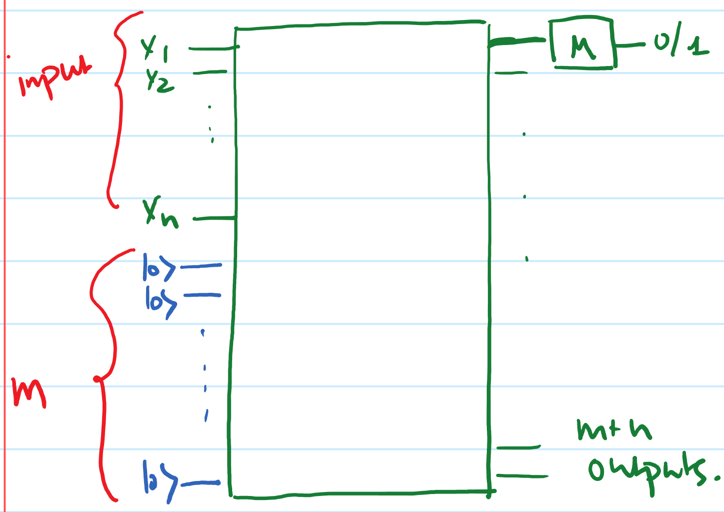
Errors add: If you want overall error ϵ, then you need to simulate each U_i to within error ϵ/ℓ.

Simulating each U_i with gates from G requires $O\left(\log^2\left(1/(\epsilon/\ell)\right)\right) = O\left(\log^2(\ell/\epsilon)\right)$ gates.

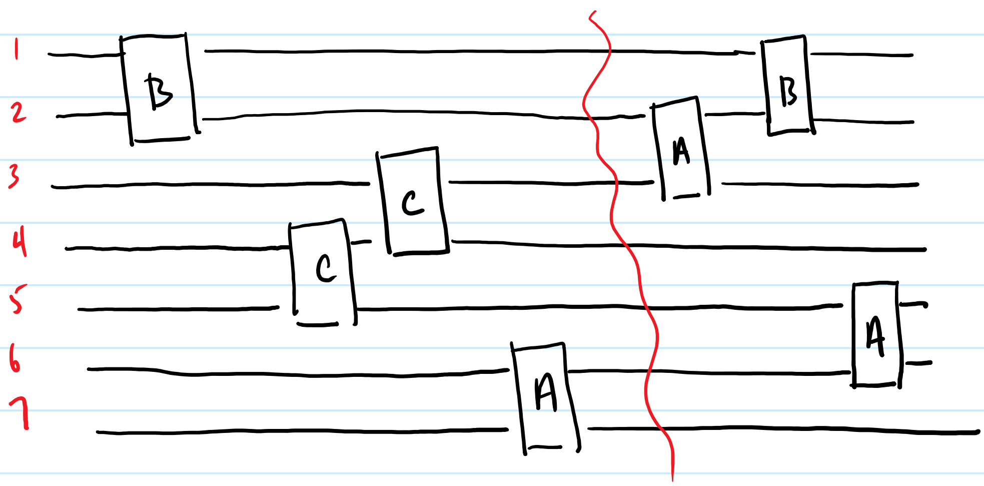
Overall # gates: $O\left(\ell \log^2(\ell/\epsilon)\right)$

Quantum Complexity Classes - page 10

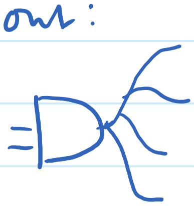
Friday, October 19, 2018 9:00 AM



Quantum circuits need "scratch space" for intermediate computation built into the input of the circuits.



Classical circuits can create extra space by fan out:



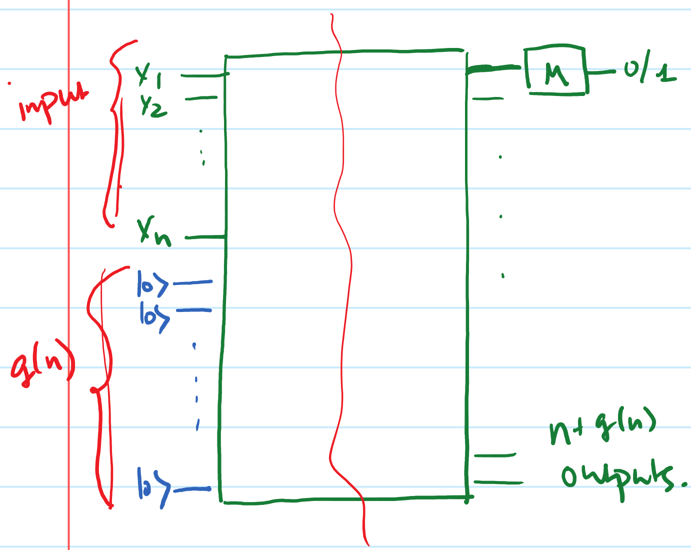
this essentially copying data.

Friday, October 19, 2018 8:43 AM

BQP (Quantum analog of BPP)

$L \in BQP$ if $\exists$ polynomials $p(n)$ + $q(n)$ and a family of circuits $C_1, C_2, \ldots$

→ made from a finite universal gate set.



The $q(n)$ $|0\rangle$'s provide extra space for the computation + storage of intermediate results.

- On input x where $|x| = n$. C_n takes as input $x\ 0^{q(n)}$. ($n + q(n)$ inputs)
- output is the measurement of the first qubit in the 0/1 basis.
- $|C_n| \leq p(n)$ $\forall n$.
- Uniformity.
- $x \in L$ $|x| = n$
  $\Pr[C_n(x, 0^{q(n)}) = 1] \geq 2/3$.

  $x \notin L$ $|x| = n$.
  $\Pr[C_n(x\, 0^{q(n)}) = 0] \geq \frac{2}{3}$

Note: the input is a classical bit string.
the output is a classical bit.

What goes on in the middle is quantum.

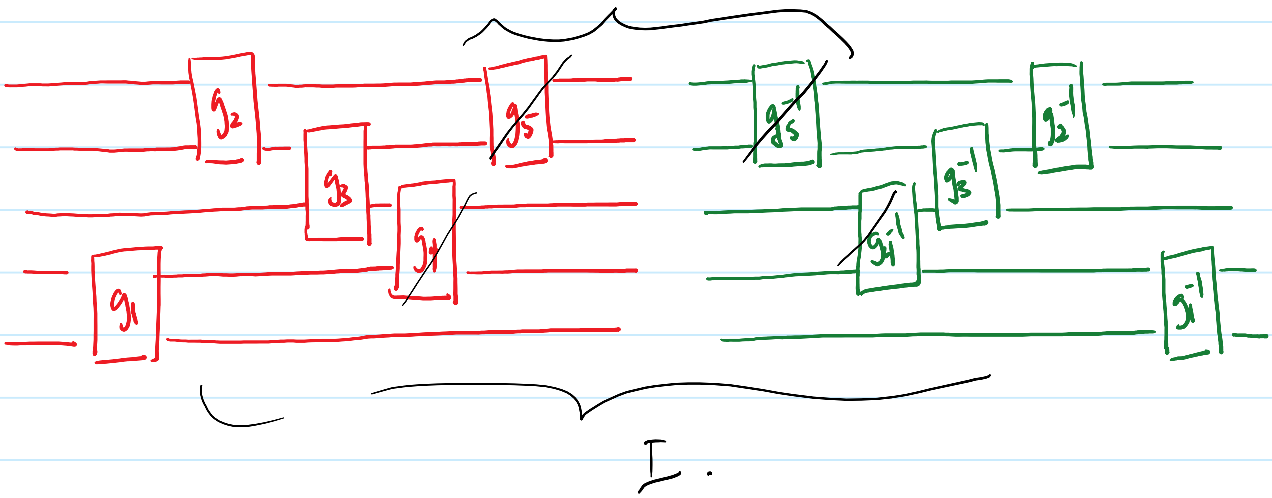
Quantum Complexity Classes - page 12

Friday, October 19, 2018 8:54 AM

Quantum circuits are reversible.

For every quantum circuit there is a reverse circuit that computes the inverse function:

reverse the order of the gates & replace each gate by its inverse: $g^{+} = g^{-1}$



$CNOT(CNOT) = I$

Quantum Complexity Classes - page 13

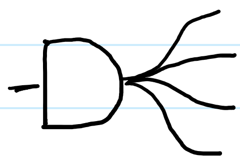
Friday, October 19, 2018 9:05 AM

We would expect that P, BPP $\subseteq$ BQP

Translation: any function that can be computed efficiently with a classical circuit can also be computed efficiently using a quantum circuit

However, there are some issues to be worked out:

- Quantum circuits must be reversible but classical circuits don't have to be.



- Fan out from a gate is easy for classical circuits but problematic for quantum circuits because of No Cloning Theorem

In order to show P $\subseteq$ BQP, we need to show that every classical circuit can be made into a reversible circuit.

→ Just need to show that every gate in a Universal gate set can be made reversible.

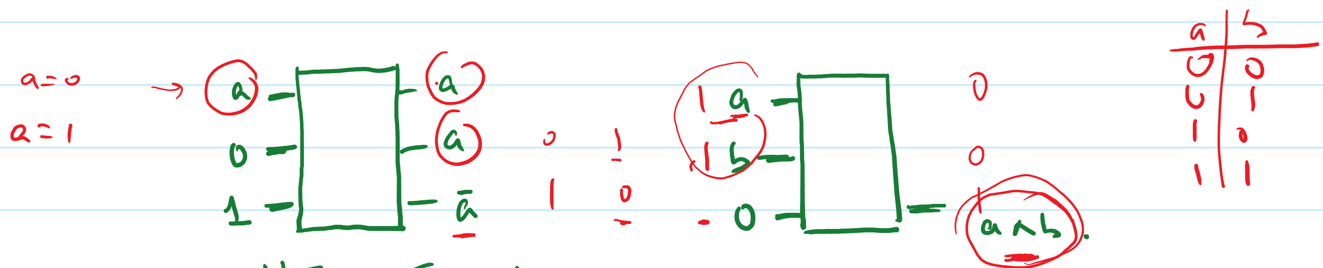
Friday, October 19, 2018 9:14 AM

Will use a Fredkin gate (controlled SWAP):

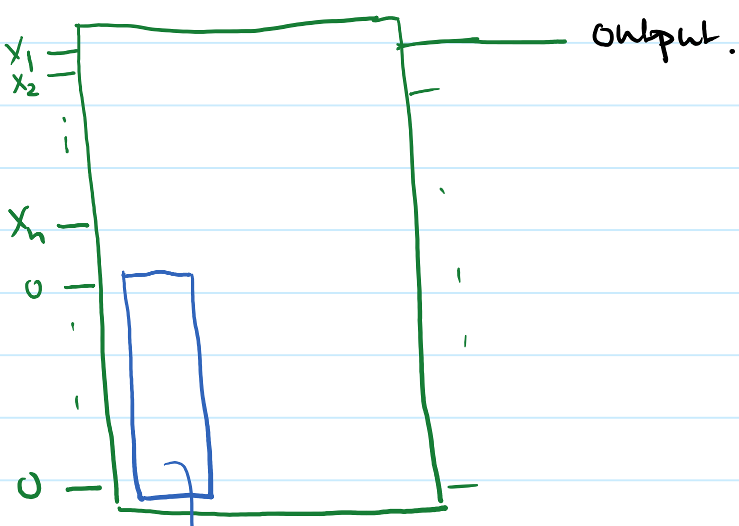
$$(0, b, c) \longrightarrow (0, b, c)$$
$$(1, b, c) \longrightarrow (1, c, b)$$

$F^2 = I$ so F is reversible.

Some of the inputs will be hard-coded to produce certain effects.



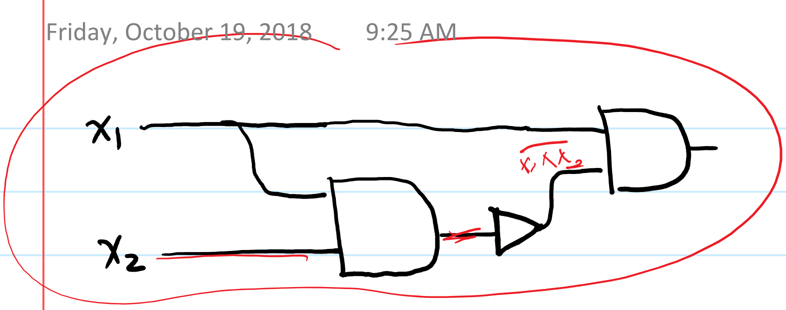
NOT and Fanout.

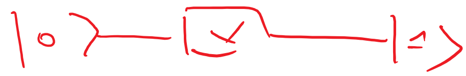


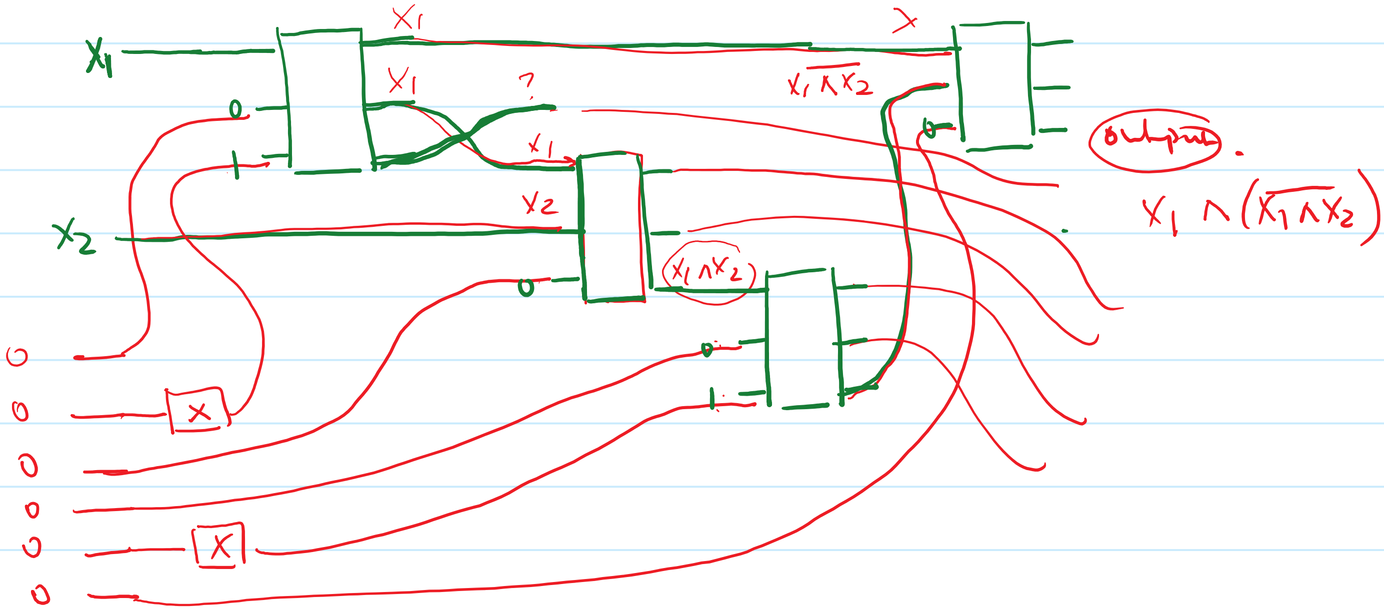
fix the auxiliary bits for the Fredkin gates (by applying X to create 1)
These will depend on $|x| = n$ but not on x.

Quantum Complexity Classes - page 14

Friday, October 19, 2018 9:25 AM







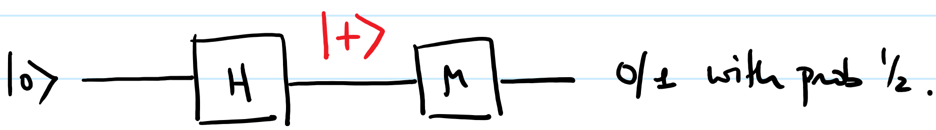
Monday, October 22, 2018 8:40 AM

We have shown that $P \subseteq BQP$

What about $BPP \subseteq BQP$?

Need a source of random bits.

How about

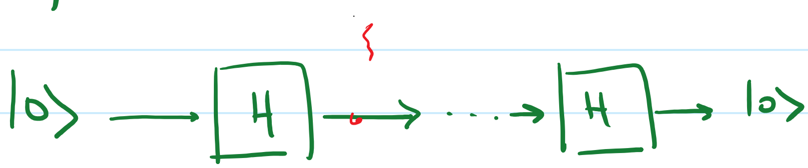


Measurement can be difficult to implement at intermediate stages.

Can it be deferred to the end?

Problem: interference can reduce randomness.

For example:

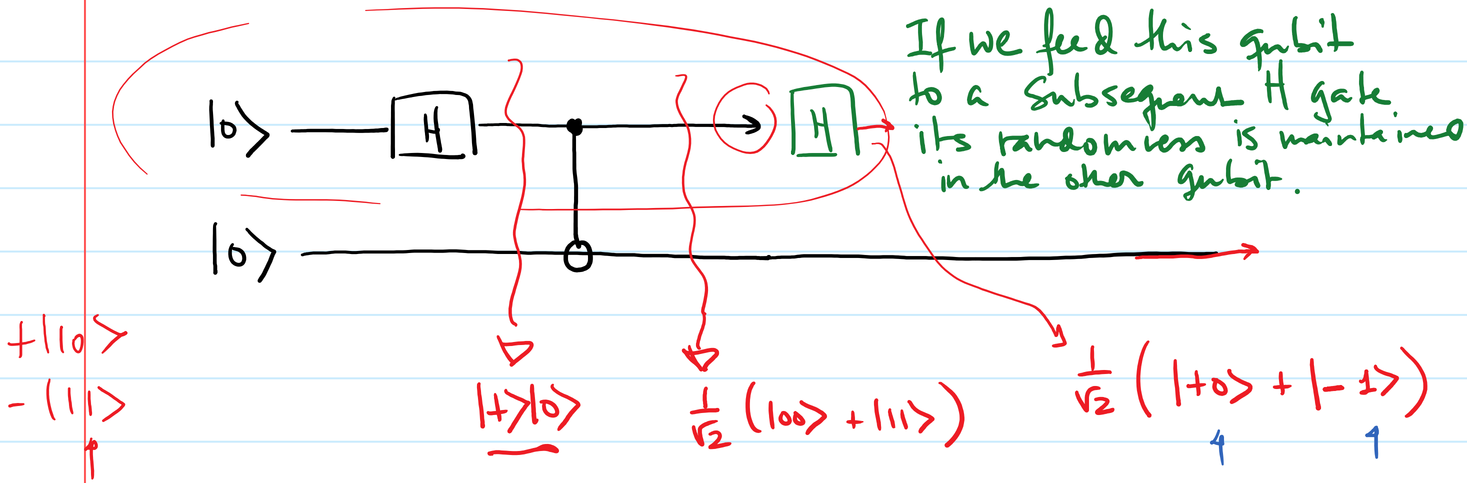


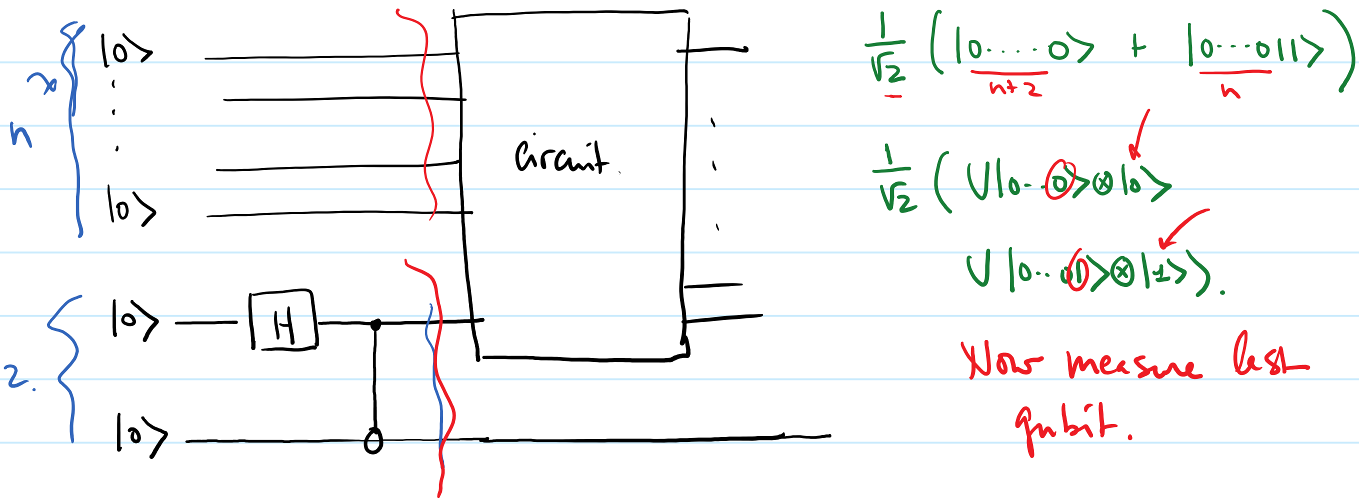
applying a second H gate would completely unrandomize the qubit.

Instead: entangle the |+⟩ state with a fresh qubit that will never be used again

Quantum Complexity Classes - page 16

Monday, October 22, 2018 8:40 AM

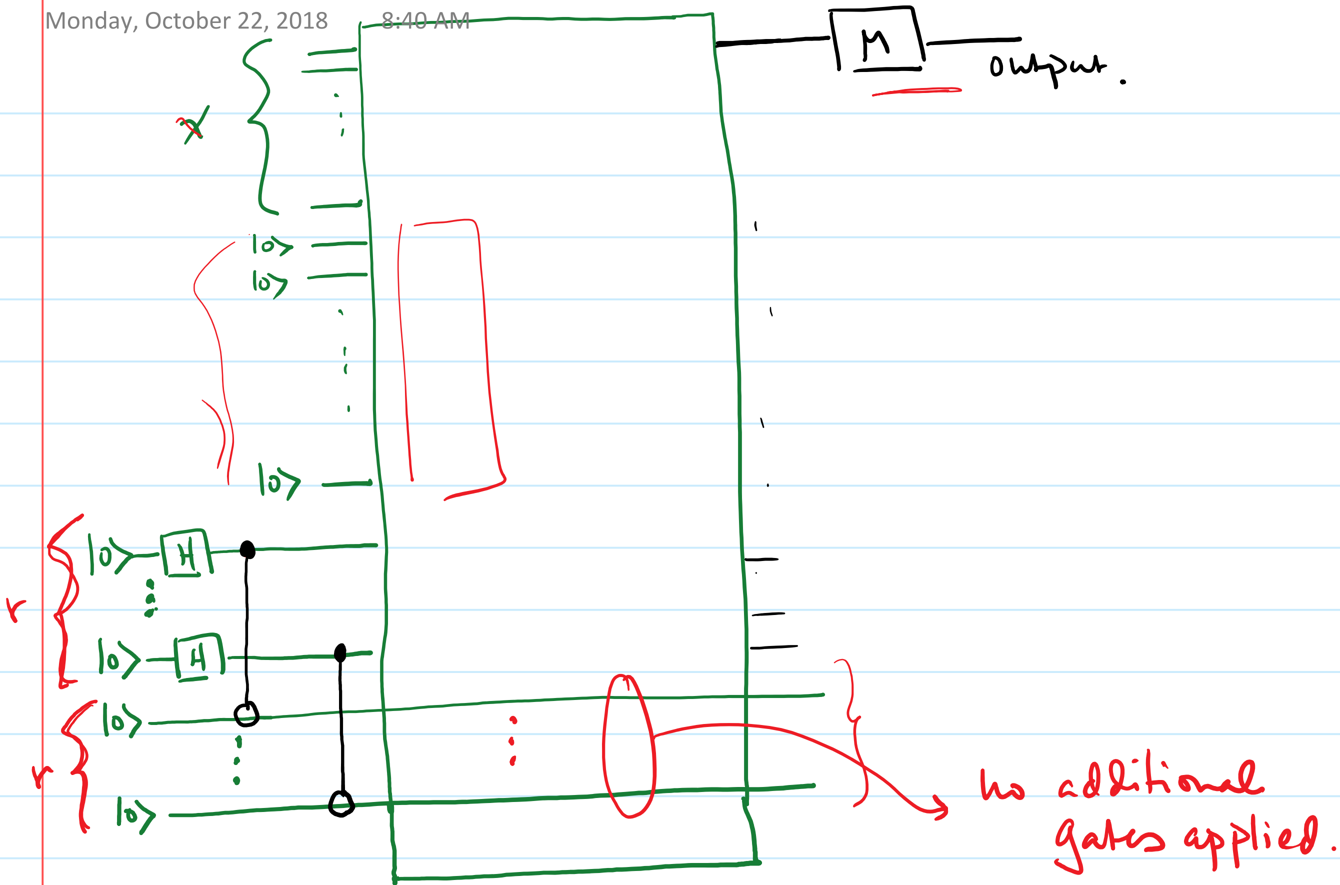




Actually, we don't even need to measure the last qubit at all.

Quantum Complexity Classes - page 17

Monday, October 22, 2018 8:40 AM



We have shown that:

$$P \subseteq BPP \subseteq BQP \subseteq PSPACE$$

- P: deterministic poly-time (classical)
- BPP: probabilistic poly-time (classical)
- BQP: Quantum poly-time.
- PSPACE: classical poly. space (no limits on time)

We don't expect a proof that $P \neq BQP$.
We don't even know how to prove $P \neq PSPACE$.