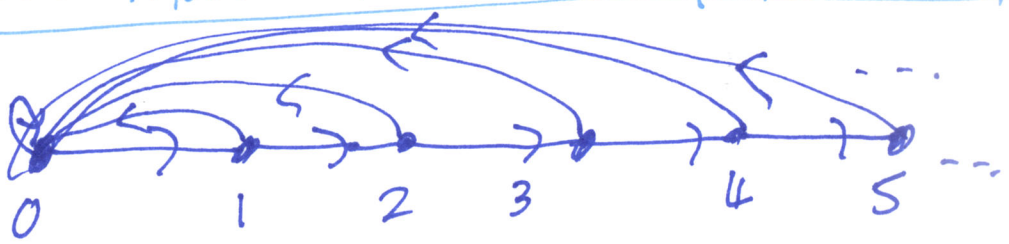
CSE596 Lecture Mon 12/3 Fall 2018

Why no good randomized algm is known for GAP on directed graphs



Simplest example (IMHO) of a best-known randomized algm involves not NL vs L, or poly time vs exp. time, but $\tilde{O}(n^2)$ vs $\tilde{O}(n^3)$

MATCHECK: INST: Three $n \times n$ matrices A, B, C (over some field F)
QUES: Does $A \cdot B = C$?

Deterministically solve by multiplying $A \cdot B$, but this is $\tilde{O}(n^3)$ time simple way
$\tilde{O}(n^{2.37\ldots})$ with a horrific constant factor

Randomized:
- Generate 1 or more vectors $v_1, \ldots v_r \in F^n$.
- For $j = 1$ to r, check whether $C v_j = A(B v_j)$.
- If any check fails, say no
  If all checks succeed, then $\leq 1/2^r$ chance of getting a "bad v_j" each time

$\tilde{O}(n^2)$ time Repeat $\tilde{O}(n^2)$ time ∴ whole is $\tilde{O}(n^2)$ time

Abstractly, let $D = A \cdot B - C$. If $D \neq 0$ then D has at least one 1.

π_V

Then whether $v_j = 0$ or 1 flips the Parity of $Dv = A(Bv) - Cv$.

π_{Parity}

∴ We have a randomized algm R st. for all instances $x = \langle A, B, C \rangle$:
$x \in$ MATCHECK $\Rightarrow$ Pr[all checks succeed] $= 1 \Rightarrow$ Pr[R is right] $= 1$.
$x \notin$ MATCHECK $\Rightarrow$ Pr[all succeed] $\leq 1/2^r \Rightarrow$ Pr[R is wrong] $< 1/2^r$.

Defn: A language $L \subseteq \{0,1\}^*$ belongs to **BQP** [Bounded error Quantum Poly time] if there is a polynomial $p(n)$ and a quantum algorithm Q s.t. ② for all n and inputs $x \in \{0,1\}^n$:

$x \in L \Rightarrow Pr[Q(x) \text{ measures } 1 \text{ on qubit } 1] \geq \frac{3}{4}$ ie $Pr[Q(x) \text{ is right}] \geq 3/4$

$x \notin L \Rightarrow Pr[Q(x) \text{ measures } 1 \text{ on line } 1] \leq 1/4$ ie. $Pr(Q \text{ is wrong}) \leq \frac{1}{4}$

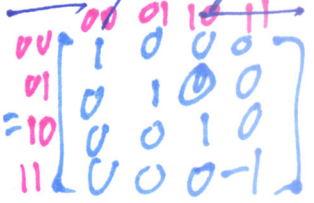
Ie $Pr[Q(x) = L(x)]$ always $\geq 3/4$.
Ie $Pr[Q(x) \text{ is right}) \geq 3/4$.

} Can amplify "error $\leq 1/4$" to "error $\leq 1/2^r$" by $O(r)$ repeated trials.

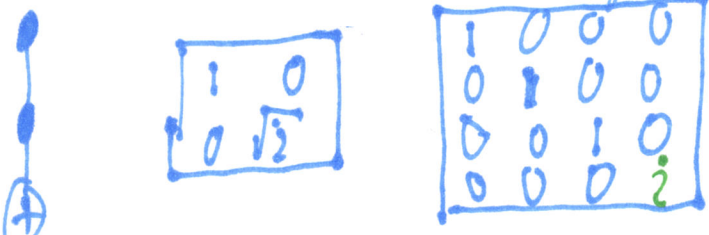
The MATCHLOCK example, when time is poly vs exp not n^2 vs n^3, typifies the definition of classical BPP. Thus $P \subseteq BPP \subseteq BQP$

Problems for which BQP may be larger include FACTORING, DISCRETE LOG, and $A \cdot B \stackrel{?}{=} C$ problems where A, B, C are exponentially big.

The standard model for universal quantum computing models Q as a family $[C_n]_{n=1}^{\infty}$ of quantum circuits using at least one gate beside Clifford Gates $H, I, X, Y, Z, S, CNOT, CZ$

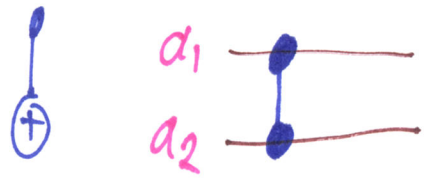


The three most common other gates are:



Toffoli T CS

All non-Clifford.



Recall H-T-H-? gives irrational probabilities for 1 and so BQP involves not simply coinflips.

The argument over BQP has two levels:

① Whether the Quantum Fourier Transform is really feasible to implement with $O(n^2)$ circuit of basic gates.

see QFT_n Recursion below.

② Those gates involve "Higher T Twists": $\begin{bmatrix} 1 & 0 \\ 0 & \sqrt[4]{i} \end{bmatrix}$ $TW_0 = I$, $TW_1 = Z$, $TW_2 = S$, $TW_3 = T$

$\begin{bmatrix} 1 & 0 \\ 0 & \sqrt[8]{i} \end{bmatrix}$ ... down to $\boxed{TW_n} = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt[2^n]{i} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i^{1/2^n} \end{bmatrix}$

Do we only need to approximate such high precision?

exponentially small.

Added: Examples of the QFT. QFT_n takes $\omega = e^{2\pi i/N}$ where $N = 2^n$. called "a primitive Nth root of unity"

$$\boxed{QFT_n[i,j] = \omega^{ij} \quad i,j \in 0,\dots,N-1.}$$

$n=1$: $N=2$, $\omega = e^{2\pi i/2} = e^{\pi i} = -1$. Row 0 and Column 0 are always all 1s. So $QFT_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = H_1$ Normalize $\frac{1}{\sqrt{2}}$.

$n=2$, $N=4$, $\omega = e^{2\pi i/4} = e^{i\pi/2} = i$,

Then $\omega^2 = -1$, $\omega^3 = -i$, $\omega^4 = 1$. $QFT_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \cdot \frac{1}{2}$

As with the Hadamard transforms, the normalizing constant is $\frac{1}{\sqrt{N}} = 2^{-n/2}$.

$n=3$, $N=8$, $\omega = e^{\pi i/4} = \sqrt{i}$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & i & \omega^3 & -1 & \omega^5 & -i & \overline{\omega} \\ 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & \omega^3 & -i & \omega & -1 & \overline{\omega} & i & \omega^5 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & \omega^5 & i & \overline{\omega} & -1 & \omega & -i & \omega^3 \\ 1 & -i & -1 & i & 1 & -i & -1 & i \\ 1 & \overline{\omega} & -i & \omega^5 & -1 & \omega^3 & i & \omega \end{bmatrix}$$

$\omega^2 = i$

$\omega^3 = i\omega = -\omega^7 = -\overline{\omega}$

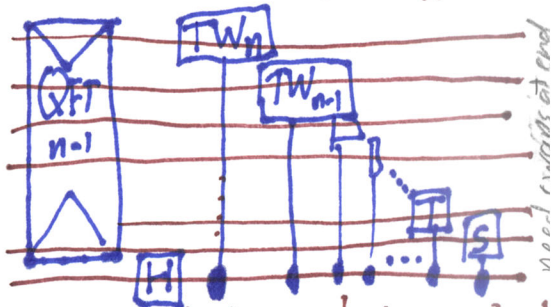
$\omega^4 = -1$

$\omega^5 = -\omega$

$\omega^6 = -i$

$\omega^7 = \omega^{-1} = \overline{\omega}$.

$QFT_n =$ Recursion



Important Fact: The state $X = \left(0.5, \frac{i}{2}, -0.5, \frac{-i}{2}\right)$ equals $a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle$ where $a_0 = \frac{1}{2}$, $a_1 = \frac{i}{2}$, $a_2 = \frac{-1}{2}$, $a_3 = \frac{-i}{2}$ as a vector over $\mathbb{C}$ i.e. $a_0 e_0 + a_1 e_1 + a_2 e_2 + a_3 e_3$ the standard basis. All quantum circuits C, being linear transformations, obey the linear rule $Cx = [C](a_0 e_0 + a_1 e_1 + a_2 e_2 + a_3 e_3) = a_0 Ce_0 + a_1 Ce_1 + a_2 Ce_2 + a_3 Ce_3 = \sum_{j=0}^{3} a_j C|j\rangle$. Thus the behavior of C on any input state is a linear function of its behaviors on basis states, so can bitwise string