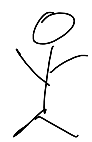
Lecture 3.1

Plan

- classical circuits
- quantum circuits
- universal gate sets
- first quantum algorithms

Last week:

Alice

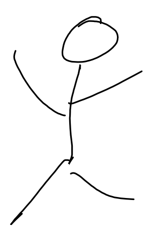


Bob

Entanglement

classical communication

This week



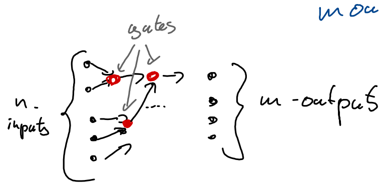
Alice

alone in her Lab

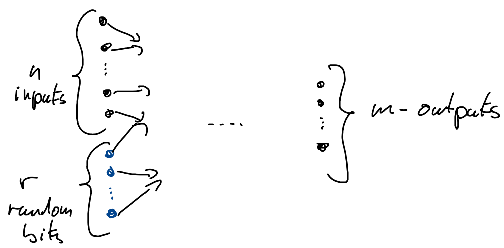
Superposition

Classical circuits

Def (boolean circuit): finite, directed, acyclic graph with and, or, and not gates as internal nodes together with n input and m output nodes.



Randomized circuits: boolean circuit + r random bits



Discuss with your neighbour:

What are the relevant concepts to define P?

A boolean circuit C computes $f: \{0,1\}^n \longmapsto \{0,1\}^m$
if $C(x) = f(x)$ for all inputs

A randomized circuit C computes $f: \{0,1\}^n \longmapsto \{0,1\}^m$
if $f(x) = C(x)$ with probability at least $\frac{2}{3}$

Observation: Running randomized circuit several times and taking majority vote, we can decrease error probability

A circuit family $\mathcal{C} = \{C_n\}$ is a set of circuits $C_n : \{0,1\}^n \longmapsto \{0,1\}$ for all input sizes with a single output bit.

A language $\mathcal{L}$ is a subset of bitstrings: $\mathcal{L} \subseteq \{0,1\}^* = \bigcup_{n\geq 1} \{0,1\}^n$

Def: A circuit $\mathcal{C}$ decides/recognizes a language $\mathcal{L}$ if
$\forall n \; \forall x \in \{0,1\}^n \quad C_n(x) = 1$ if $x \in \mathcal{L}$ and $C_n(x) = 0$ otherwise

Interpretation: Decision problem. Recognize bit strings with a certain property.

uniformly polynomial family

There is a Turingmachine that outputs C_n on input n using only logarithmic space

Fact: C_n can only have $\mathcal{O}(n^k)$ gates

Def (P): A language is in the complexity class P if it can be decided by a uniform poly. family

Remark: Equivalent to decidable by poly-time Turing-machine.

Interpretation: problems whose solution can be efficiently found

Same ideas for randomized circuits leads to BPP (Bounded-error Probabilistic Polynomial time)

$\Leftrightarrow$ Languages that can be efficiently recognized by a non-deterministic Turing machine with prob $\geq \frac{2}{3}$

Interlude: Big $\mathcal{O}$ notation / Landauer notation

Notation to express / compare scalings of functions

Def ($\mathcal{O}$): given $g, f : \mathbb{R} \mapsto \mathbb{R}$, we say that $f = \mathcal{O}(g)$
if there are constants $x_0, C \in \mathbb{R}$, $C > 0$
s.t. $\forall x \geq x_0 : \quad |f(x)| \leq C \cdot |g(x)|$

Interpretation: f grows at most as fast as g

Ex: $f = \mathcal{O}(1) \Rightarrow |f(x)| \leq C$

Give two examples $f_1(x) =$

$f_2(x) =$

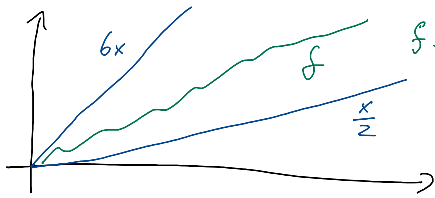
Def (Ω): given $f, g : \mathbb{R} \mapsto \mathbb{R}$, we say that $f = \Omega(g)$
if there are constants $C > 0$, $x_0 \in \mathbb{R}$
s.t. $\forall x \geq x_0 : \quad |f(x)| \geq C \, |g(x)|$

Interpretation: f grows at least as fast as g

Def (Θ): given $f, g : \mathbb{R} \longmapsto \mathbb{R}$, we say that $f = \Theta(g)$
if there are constants $c_1, c_2 > 0$, $x_0 \in \mathbb{R}$
s.t. $\forall x \geq x_0 : \quad c_1 |g(x)| \leq f(x) \leq c_2 |g(x)|$

Interpretation: f grows as fast as g

Example:



$f = \Theta(x)$

Questions

- if $f = \Theta(g)$, then $\forall c \in \mathbb{R}$ $f + c = \Theta$
- $\sin(x) = \Theta(\quad)$
- Is $\cos(x) = \Omega(x)$?

Big-O-notation often used to count resources to perform a computation depending on input size.

Example: matrix-multiplication.

$f: \mathbb{N} \longmapsto \mathbb{N}$, $f(n)$ is the minimal number of multiplications necessary to multiply to $n \times n$-matrices

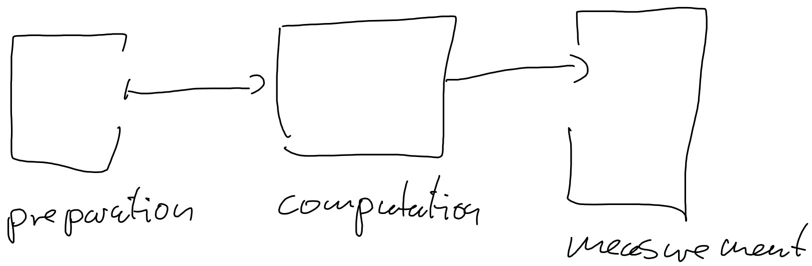
Find α, such that $f = \Theta(n^\alpha)$

$\Theta(n)$ multiplications for n^2 entries

Fun fact: Can do better: $\Theta(n^\omega)$ $\omega < 3$

$\to$ Can multiply two 2×2 matrices with 7 instead of 8 multiplications

quantum circuits



How are these three parts described?

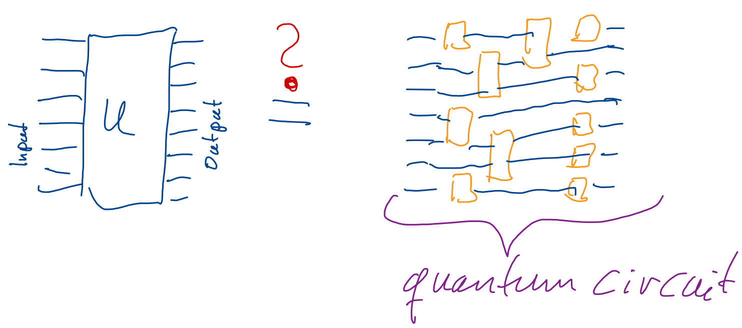
- States:
- transformations:
- measurements:

So far: two extremes

single/two-qubit operations ⟷ unitary operations on n-qubits

name some

Question:



Universal gate sets

Fact: Any boolean function can be implemented using only or, and & not gates (nand is sufficient).

Is there a quantum analogue?

classical	quantum
• classical gate	• unitary operations
• act locally (few bits)	• act locally (few qubits)
• non-reversible	• reversible
• discrete set of functions & inputs	• continuum

Reversibility: Not problematic. classical computation can be made reversable

How to (approximately) implement all unitary operations?

Interlude: Approximating unitaries

Def: given unitaries $U, V \in U(2^n)$, we define
$$d(U,V) = \max_{\substack{|\psi\rangle \in \mathbb{C}^{2^n} \\ \langle\psi|\psi\rangle = 1}} \| (U-V)|\psi\rangle \|$$

Derives from operator norm: A $n \times n$ matrix
$$\|A\|_\infty := \max_{\||\psi\rangle\| = 1} \|A|\psi\rangle\|$$

Interpretation: Find state on which U & V act most differently

What is the difference between $\mathcal{U}$ and V

$$d(\mathcal{U}, V) \stackrel{?}{=}$$

Hint $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ $|\alpha|^2 + |\beta|^2 = 1$

Motivation:

Prop: Let $\{E_i\}_{i=1}^{m}$ be a measurement $|\psi\rangle \in \mathbb{C}^{2^n}$ a pure state. Then for all unitaries U, V

$$\left| tr(E_i U |\psi\rangle\langle\psi| U^*) - tr(E_i V |\psi\rangle\langle\psi| V^*) \right| \leq 2\, d(U, V)$$

Proof: exercises

Interpretation: bound on difference observable in experiment.

Prop: Given $U_1, \dots, U_m$ and $V_1, \dots, V_m$ unitaries, then

$$d(U_1 U_2 \cdots U_m, V_1 V_2, \dots, V_m) \leq \sum_{i=1}^{m} d(U_i, V_i)$$

Interpretation: sufficient to achieve $d(U_i, V_i) \leq \varepsilon/m$ to achieve global error $\leq \varepsilon$

Back to original question

Fact: Any unitary can be approximated by using only single qubit operations and CNOT.

Def (universal gate set): A set of quantum gates $\mathcal{G} \subseteq \mathcal{U}(2^n)$ is said to universal if $\forall \varepsilon > 0$ and $S \in \mathcal{U}(2^n)$ there is a sequence $U_1, \dots, U_m \in \mathcal{G}$, s.t.

$$d(U_1 \cdots U_m, \mathcal{G}) \leq \varepsilon$$

Hence, CNOT + single qubit operation are universal.

Remarks: 1) m could be very large depending on n, ε

2) Not very satisfactory, single qubit op. are still continuous set.

Idea: approx single qubit gates with fixed discrete set.

Universality of $\{H, \text{phase}, CNOT, \frac{\pi}{8}\}$

Fill in yourself

$H =$ $\qquad =$

$\text{phase} = |0\rangle\langle 0| + i\,|1\rangle\langle 1| =$

$T = \qquad = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$

$CNOT = \qquad = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Claim I: $\{H, P, P^\dagger, T, T^\dagger, CNOT\}$

is universal

Claim II: Introduces an overhead of only

$$\mathcal{O}\left(\log^c\left(\tfrac{1}{\varepsilon}\right)\right), \quad c < 3$$

$\hat{=}$ given a quantum circuit with m single qubit + CNOT gates, we can approximate it with

$\mathcal{O}\left(m \log^c\left(\tfrac{m}{\varepsilon}\right)\right)$ gates from

$$\{H, P, P^\dagger, T, T^\dagger, CNOT\}$$

Sketch of argument: (Details in exercises)

a) Identify $U \in \mathcal{U}(2)$ as rotation in $\mathbb{R}^3$ (Bloch sphere)

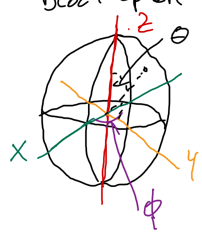
$\hat{=}$ $\begin{cases} \text{rotation axis } \vec{n} \in \mathbb{R}^3 \\ \text{rotation angle } \theta \in [0, 2\pi) \end{cases}$ $\quad R_{\vec{n}}(\theta)$

b) Fact: given $\vec{n}, \vec{m} \in \mathbb{R}^3$ non-parallel

then $R_{\vec{r}}(\theta) = R_{\vec{n}}(\theta_1) R_{\vec{m}}(\theta_2) R_{\vec{n}}(\theta_3)$

$\hat{=}$ TWO rotation axis are sufficient to rotate around an arbitrary axis

c) Bloch Sphere



$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2} e^{i\phi}|1\rangle$ $\quad \theta \in [0,\pi]$, $\phi \in [0, 2\pi]$

$T \hat{=} \frac{\pi}{4}$ rotation around z-axis

$HTH \hat{=} \frac{\pi}{4}$ rotation around x-axis

$HTHT \hat{=} \theta$ rotation around

$\vec{n} = \left(\cos\left(\frac{\pi}{8}\right), \sin\left(\frac{\pi}{8}\right), \cos\left(\frac{\pi}{8}\right)\right)$

with $\cos\left(\frac{\theta}{2}\right) = \cos^2\left(\frac{\pi}{8}\right)$

Fact: θ is irrational modulo π

$\Rightarrow R = \overline{\{k\theta \bmod 2\pi \mid k \in \mathbb{N}\}} = [0, 2\pi)$

$\Rightarrow \forall \theta' \in (0, 2\pi) \; \exists N$ s.t.

$$d\left(\left(THTH\right)^N, R_{\vec{n}}(\theta')\right) \leq \varepsilon$$

Same argument for $HTHT$ leads to $\vec{n}' \nparallel \vec{n}$

$\Rightarrow$ can rotate in two non-parallel directions up to arbitrary precision

$\Rightarrow$ Can perform arbitrary single qubit operations up to arbitrary precision

$\Rightarrow$ universality

More detailed analysis leads to bound on precision.

Thm (Solovay-Kitaev)

Given $\mathcal{G} = \{U_i\}_{i=1}^{K}$ with $U_i \in \mathcal{U}(2)$ and $\mathcal{G}^{+} = \mathcal{G}$ and $\mathcal{G}$ universal for all single qubit operations. Then $\forall S \in \mathcal{U}(2)$ and $\varepsilon > 0$ there is $m = O(\log^c(\varepsilon^{-1}))$ with $c > 3$ s.t.

$$d(U_{i_1} \cdots U_{i_m}, S) \leq \varepsilon$$

The complexity class BQP

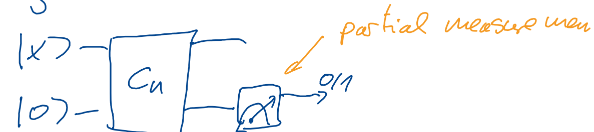
P: languages decidable in poly-time

BPP: languages decidable in poly-time with randomized classical circuit

BQP: problems efficiently solvable on a quantum computer

Def (BQP) a language L is in BQP if there exists a family $\{C_n\}$ of quantum circuits on $n+1$ qubits with the number of single qubit + two qubit gates in C_n polynomial in n

s.t. $\forall x \in \{0,1\}^n$:



$\mathrm{Prob}(0) \geq \frac{2}{3}$ if $x \notin L$

$\mathrm{Prob}(1) \geq \frac{2}{3}$ if $x \in L$

Quantum parallelism

always possible via Toffoli gates

consider $f: \{0,1\}^n \longmapsto \{0,1\}^m$. Assume we can construct a quantum circuit $U_f\, |z\rangle|0\rangle = |z\rangle|f(z)\rangle \;\forall z \in \{0,1\}^n$

then: $$\frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |z\rangle|0\rangle \xmapsto{U_f} \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |z\rangle\underline{|f(z)\rangle}$$

All possible outputs of the function computed in one go

$\boxed{\text{But:}}$ Measurement only reveals randomly a single result.