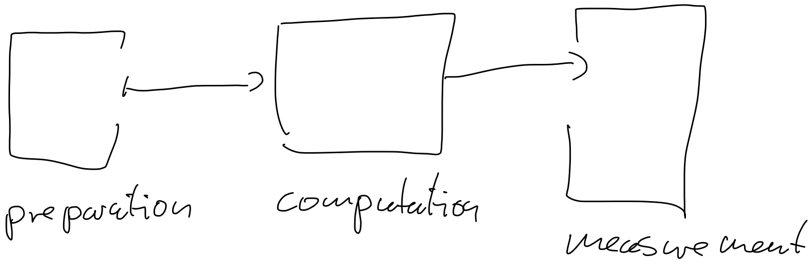
quantum circuits



How are these three parts described?

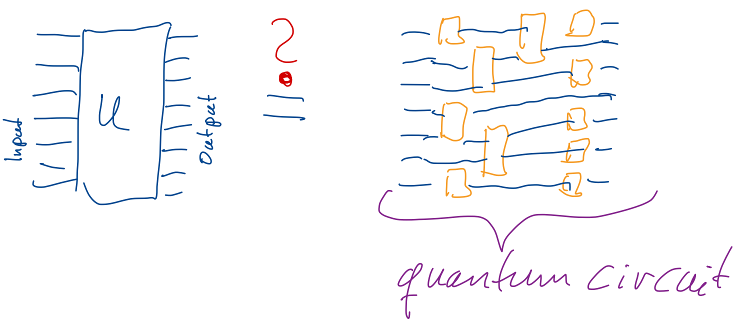
- States:
- transformations:
- measurements:

So far: two extremes

single/two-qubit operations
name some

unitary operations on n-qubits

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 gates	• 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 X

$$d(\mathcal{U}, X) \overset{?}{=}$$

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

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

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

Proof: exercises

Interpretation: bound on difference observable in experiment.

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

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

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

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

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

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

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

Sketch of argument : (Details in exercises)

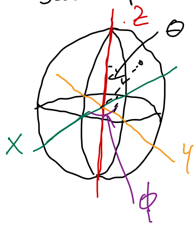
a) Identify $U \in U(2)$ as rotation in $\mathbb{R}^3$ (Bloch sphere)

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

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



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

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

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

$HTHT \hat{=} \theta$ rotation around
$$\vec{n} = \left(\cos\left(\tfrac{\pi}{8}\right), \sin\left(\tfrac{\pi}{8}\right), \cos\left(\tfrac{\pi}{8}\right)\right)$$
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.
$$d\left((THTH)^N, R_{\vec{n}}(\theta')\right) \le \varepsilon$$

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 $\mathcal{G}^\dagger = \mathcal{G}$ and $\mathcal{G}$ universal for all single qubit operations. Then $\forall\, S\in\mathcal{U}(2)$ and $\varepsilon > 0$ there is $m = \mathcal{O}(\log^c(\varepsilon^{-1}))$ with $c > 3$ s.t.
$$d(U_{i_1}\cdots U_{i_m}, S) \le \varepsilon$$

The complexity class BQP

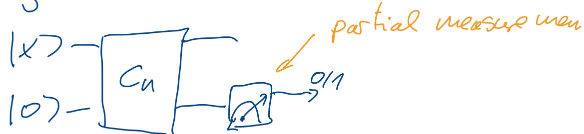
P: languages decidable in poly-time

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

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

always possible via Toffoli gates

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.

Oracles & query complexity

slightly different framework for complexity

- Want to solve given problem
- As a resource we have acces to a black-box (oracle) that reveals some information / implements a sub-routine
- How often do we have to use the black-box to solve our original problem?

Example: given oracle for fixed $x \in \{0,1\}^n$
$x = (x_0, \dots, x_{n-1})$
Oracle does the following
on input $i \in \{0, \dots, n-1\}$
Oracle returns x_i

Possible problem: Is there an $x_j = 0$?

Quantum oracles

Unitary operation $O_x : \mathbb{C}^{2^n} \otimes \mathbb{C}^2 \longrightarrow \mathbb{C}^{2^n} \otimes \mathbb{C}^2$

answer

s.t. $|i, 0\rangle \xmapsto{O_x} |i, x_i\rangle$ for $i \in \{0,1\}^n$

↳ target register

address qubit

O_x has to be unitary!

specify action on $|i, 1\rangle$

$$O_x : |i, b\rangle \longmapsto |i, x_i \oplus b\rangle$$

count one application of O_x as single query

Phase oracle $O_{x,\pm}$

compute

$O_x |i\rangle |-\rangle$

Deutsch's problem

posed by

David Deutsch 1985 (probabilistic solution)

Problem: given $f: \{0,1\} \mapsto \{0,1\}$

is f a constant function $f(0) = f(1)$

or is f a balanced function $f(0) \neq f(1)$

We are only given access to f as a black-box and want to minimize its use

Classical solution:

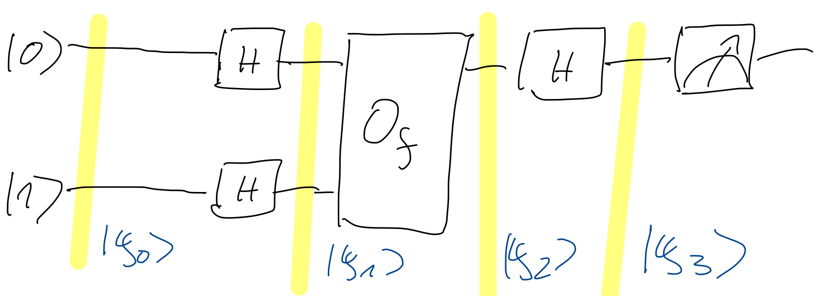
Need to determine both $f(0)$ & $f(1)$ in order to compare them $\Rightarrow$ two uses of the oracle.

quantum algorithm

Assume access to quantum oracle

$$O_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

quantum circuit



a) Determine $|\psi_0\rangle$, $|\psi_1\rangle$, $|\psi_2\rangle$

b) How does $|\psi_2\rangle$ look like depending on whether f is constant or balanced.

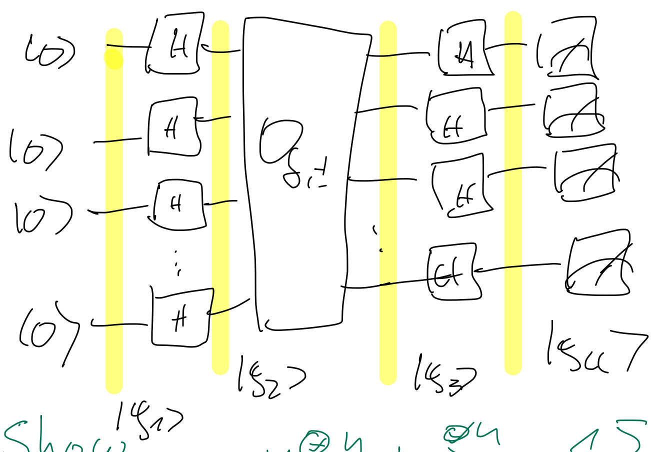
c) determine $|\psi_3\rangle$ & the measurement statistik $\rightarrow$ what do we learn about f?

Deutsch - Jozsa (1992)

solution with single oracle call Cleve et al. 1998

Problem: given $x \in \{0,1\}^N$ with $N = 2^n$
with either
(a) x is constant $\hat{=}$ $x_i = x_j \ \forall i,j$
(b) $N/2$ of the $x_i = 0$ and $\frac{N}{2}$ of the $x_i = 1$

quantum algorithm



Show

$$H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle$$

for $i \in \{0,1\}^n$ $$H^{\otimes n} |i\rangle = \frac{1}{\sqrt{2^n}} \sum_{j \in \{0,1\}^n} (-1)^{i \cdot j} |j\rangle$$

$$\Rightarrow |\psi_2\rangle = \frac{1}{\sqrt{2^4}} \sum_{i \in \{0,1\}^4} |i\rangle$$

$$|\psi_3\rangle = O_{f,\pm}\left(\frac{1}{\sqrt{2^4}} \sum_{i \in \{0,1\}^4} |i\rangle\right)$$

$$= \frac{1}{\sqrt{2^4}} \sum_{i \in \{0,1\}^4} (-1)^{x_i} |i\rangle$$

$$|\psi_4\rangle = \frac{1}{2^4} \sum_{i \in \{0,1\}^4} (-1)^{x_i} \sum_{j \in \{0,1\}^4} (-1)^{i \cdot j} |j\rangle$$

$$= \frac{1}{2^4} \sum_{i \in \{0,1\}^4} \sum_{j \in \{0,1\}^4} (-1)^{x_i + i \cdot j} |j\rangle$$

What is the coefficient of $|0\rangle^{\otimes 4}$?

<u>answer</u>: $i \cdot 0 = 0 \Rightarrow$ have to consider

$$\frac{1}{2^4} \sum_{i \in \{0,1\}^4} (-1)^{x_i} = \begin{cases} 1 & \text{if all } x_i = 0 \\ -1 & \text{if all } x_i = 1 \\ 0 & \text{if } x \text{ is balanced} \end{cases}$$

$\Rightarrow$ Final measurement gives $|0\rangle^{\otimes n}$ with prob. 1 if and only if x is constant.

classical algorithm

deterministic without error:

need in worst-case scenario $2^{n-1}+1$ queries

$\Rightarrow$ exponential separation

randomized algorithm

check k randomly chosen x_i
if they are all equal assume x constant otherwise assume x balanced.

error prob. decreases exponentially with k in case of balanced case.

$\Rightarrow O(1) \Rightarrow$ No quantum speed-up

:(

Bernstein - Vazirani

problem: $x \in \{0,1\}^N$ for $N = 2^n$

such that there is $a \in \{0,1\}^n$

with

$x_i = i.a \mod 2$

Find a

Same algorithm as for Deutsch-Jozsa

Looking at output $|\psi_3\rangle$ we find

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{x_i} |i\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{(i.a \mod 2)} |i\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{i.a} |i\rangle$$

Apply $H^{\otimes n}$ to this state

Classical algorithm

answer contains n bits. Each call to the oracle reveals 1 bit

$\Rightarrow$ minimum number of calls n

also for randomized algorithms

$\Rightarrow$ quantum speed-up also for randomized alg.

<u>but</u> only polynomial :-(