

Quantum Computing

Naglis Šuliokas

Abstract: Being a relatively new field, quantum computing gained a lot of attention in the past 30 years. Shor's algorithm showed that prime factorization can be done exponentially faster than on classical (regular) computers, breaking the RSA encryption (used in internet communication). More use cases have been discovered lately, however, most of them are not yet implementable on current quantum computers. During the lecture we will look into the basics on how quantum computation works on theoretical level, with a simple example of quantum advantage and basic exercises.

Prerequisites: (optionally, not required, but would be helpful): linear algebra, logic computation, basics of quantum mechanics (postulates)

Quantum Computing Lecture Notes

Mathcamp
Forum 2026
CPH

Contents (1h20min)

also intro
about
Shor's algo

1. state & evolution (classical computing \rightarrow quantum computing)
2. Superdense coding (Superposition & Entanglement as qubits)
3. Deutsch-Jozsa algorithm (Q oracle, phase kickback, Deutsch)
4. Exercises
5. Physical implementation (photonic, trapped ion, superconducting)
6. Use cases (Crypto & Q sim)

Sources

1. Chuang & Nielsen
2. UvA QC & QIT notes
3. Quantum Soar YT
4. Building Q computers book

+ PART 1 & 2 is on my YT

PART 0 INTRO - PRIME FACTOR

General number field sieve

$$O(e^{1.9(\log N)^{1/3}(\log \log N)^{2/3}})$$

PART 1 STATE & EVOLUTION

1.1. Classical computing

1981 Feynman \rightarrow Shor (1994) $O((\log N)^2 (\log \log N))$

On the low level, computation can be formalized as changing device's state using logic gates:

$$S \xrightarrow{\text{GATE}} S'$$

Here

$$S \in \{0,1\}^n, S' \in \{0,1\}^m, \text{GATE} : \{0,1\}^n \rightarrow \{0,1\}^m.$$

This is exactly how things work in CPU logical unit, implemented using "transistor-like" hardware. One of universal gate sets is this:

(\rightarrow) NOT: NOT 1 = 0 ; NOT 0 = 1

OPPOSITE

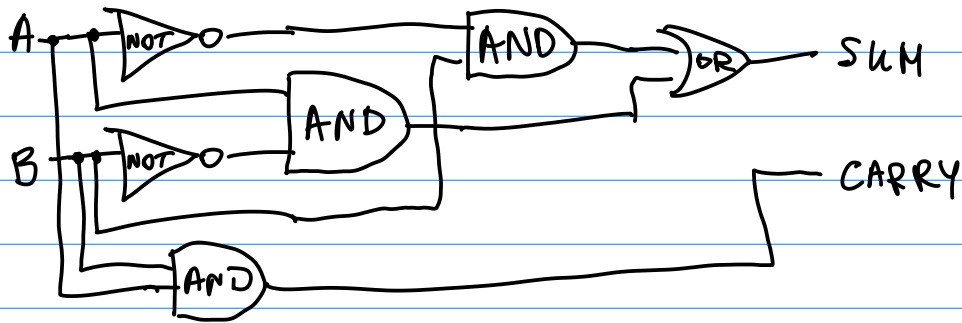
(\Rightarrow) AND: 1 AND 1 = 1 ; any other x AND $y = 0$

ARE BOTH 1?

(\Rightarrow) OR: 0 OR 0 = 0 ; any other x OR $y = 1$

IS AT LEAST ONE 1?

Basic computation example — half-adder. Here its logic circuit, logic expression and truth table:



$$\text{SUM} = A \text{ XOR } B = (\text{NOT } A \text{ AND } B) \text{ OR } (\text{NOT } B \text{ AND } A)$$

$$\text{CARRY} = A \text{ AND } B$$

A	B	CARRY	SUM
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

$0 + 0 = 00$
 $0 + 1 = 01$
 $1 + 0 = 01$
 $1 + 1 = 10_2 = 2_{10}$

1.2. Classical computing as vectors and matrices

Now we can choose another way to formalize computation:

State: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $|a\rangle \otimes |b\rangle = \begin{pmatrix} a_1 \cdot b_1 \\ a_1 \cdot b_2 \\ a_2 \cdot b_1 \\ a_2 \cdot b_2 \end{pmatrix}$

$|3\rangle = |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

$|5\rangle = |101\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

↑ tensor product

Gate: NOT = $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, AND = $\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, OR = $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$

With this formalization we can now do computation, where state change will be performed as matrix and vector multiplication. Here are the examples:

$$\text{NOT } 1 = \text{NOT } |1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$0 \text{ AND } 1 = \text{AND } |01\rangle = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$1 \text{ OR } 1 = \text{OR } |11\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$\begin{aligned} \text{NOT } 1 \text{ OR } 1 &= \text{OR } (\text{NOT } |1\rangle \otimes |1\rangle) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \end{aligned}$$

1.3. Quantum state and computation

By talking about quantum computation, we consider only a basic subset of discrete states and evolutions. We only talk about 2-dim Hilbert spaces and their composition via tensor products. For this lecture simplicity we will only consider one basis — $\{|0\rangle, |1\rangle\}$ (computational or Z basis).

State: $|2\rangle, |1\rangle, |0\rangle = \alpha|0\rangle + \beta|1\rangle, |2\rangle \otimes |\varphi\rangle$
 $\alpha, \beta \in \mathbb{C}$

Gates: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$X|0\rangle = |1\rangle$$

$$X|1\rangle = |0\rangle$$

$$Z|0\rangle = |0\rangle$$

$$Z|1\rangle = -|1\rangle$$

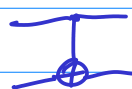
$$Y|0\rangle = i|1\rangle$$

$$Y|1\rangle = -i|0\rangle$$

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

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



$$\text{CNOT}|00\rangle = |00\rangle$$

$$\text{CNOT}|01\rangle = |01\rangle$$

$$\text{CNOT}|10\rangle = |11\rangle$$

$$\text{CNOT}|11\rangle = |10\rangle$$

Example of a universal gate set: $\{H, S, \text{CNOT}, T\}$

$$S = \sqrt{Z} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad Z = R_z(\pi)$$

$$T = \sqrt{S} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\frac{\pi}{4}i} \end{pmatrix} \quad S = R_z\left(\frac{\pi}{2}\right) \\ T = R_z\left(\frac{\pi}{4}\right)$$

1.4, Terminology & main properties

Another way to express arbitrary state:

$$|\psi\rangle = e^{i\gamma} \left(\cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right)$$

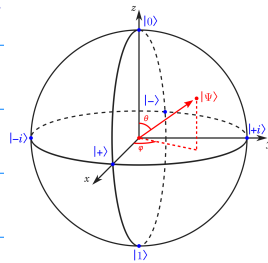
→ angle

↙ global phase ↘ (relative) phase

Z - phase gate (changes phase by π)

X, Y, Z, I - Pauli gates

$R_x(\theta), R_y(\theta), R_z(\theta)$ - Rotations in Bloch sphere



MEASUREMENT

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \rightarrow \quad P_z(0) = |\alpha|^2$$

$$P_z(1) = |\beta|^2$$

FIRST TYPE OF MAGIC
SUPERPOSITION

$$H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$HH|x\rangle = |x\rangle \quad ! \quad \text{MAGIC}$$

$$P(0) = \frac{1}{2}$$

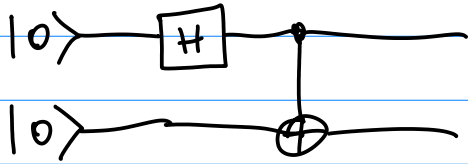
$$P(1) = \frac{1}{2}$$

$$P(0) = \frac{1}{2}$$

$$P(1) = \frac{1}{2}$$

Why do we care about phase?

SECOND TYPE OF MAGIC ENTANGLEMENT



$$\begin{aligned}
 |\Phi^+\rangle &= \text{CNOT} (H \otimes I) |00\rangle \\
 &= \text{CNOT} |+\rangle |0\rangle \\
 &= \frac{1}{\sqrt{2}} (\text{CNOT} |00\rangle + \text{CNOT} |10\rangle) \\
 &= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)
 \end{aligned}$$

$|0\rangle \otimes |0\rangle$
product state

Meaning:

$$\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$$

if 1st 0 $P(0) = \frac{1}{2} \rightarrow |\psi\rangle = N \frac{1}{\sqrt{2}} |0\rangle = |0\rangle$ → Fo sho 0

if 1st 1 $P(1) = \frac{1}{2} \rightarrow |\psi\rangle = N \frac{1}{\sqrt{2}} |1\rangle = |1\rangle$ → Fo sho 1

PART 2 Superdense coding

What do we do about phase? Intuition behind?

What is $\sqrt{3}$? Something intermediate without meaning.

$$3 \xrightarrow{\sqrt{\quad}} \sqrt{3} \xrightarrow{\cdot\sqrt{5}} \sqrt{15} \xrightarrow{+2} 15$$

Here

$$|\Phi^+\rangle$$

$$|\Phi^+\rangle \quad |\Phi^-\rangle$$

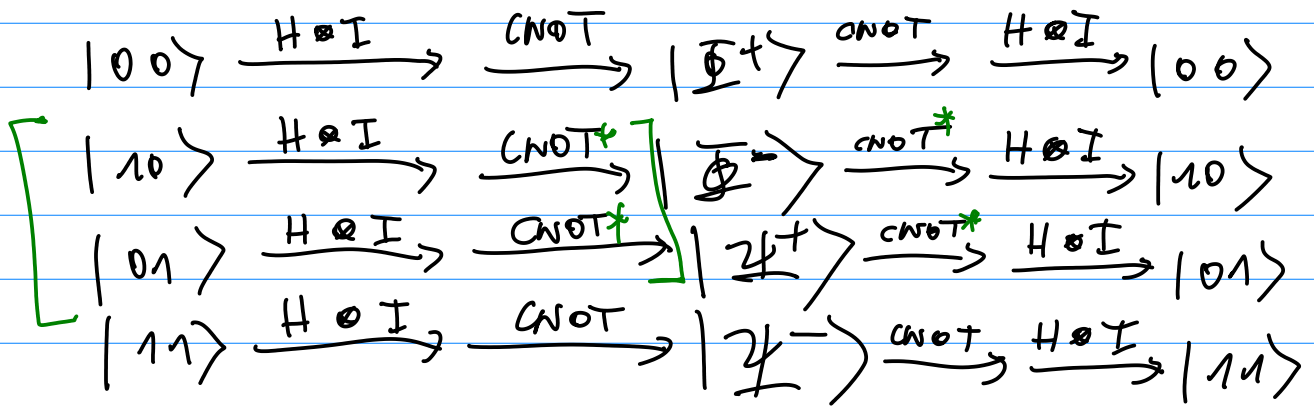
$$|\Psi^+\rangle \quad |\Psi^-\rangle$$

$$\begin{aligned}
 &|00\rangle \\
 &|01\rangle \\
 &|10\rangle \\
 &|11\rangle
 \end{aligned}$$

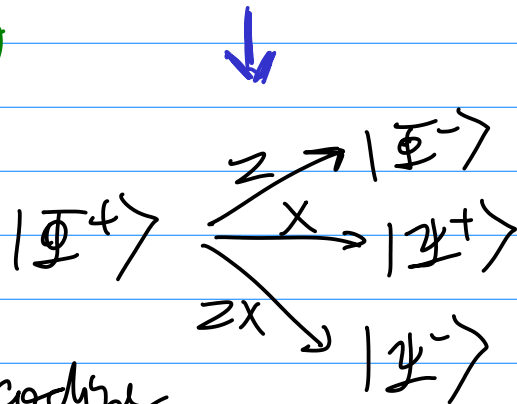
2.1. Bell states

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$$



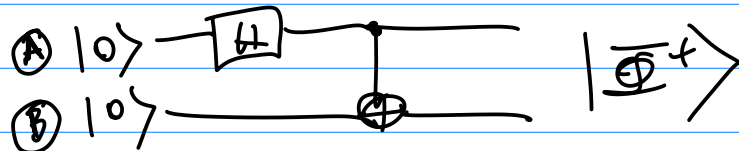
✶ - This idea of encoding/decoding the same qubit pair can be only one with CNOTs (C-2, T-1). Otherwise $|10\rangle$ is switched with $|01\rangle$



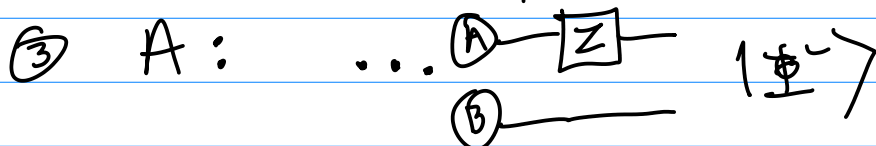
2.2. Superdense coding

Example: Alice sends 10 to Bob.

① A & B meet & entangle

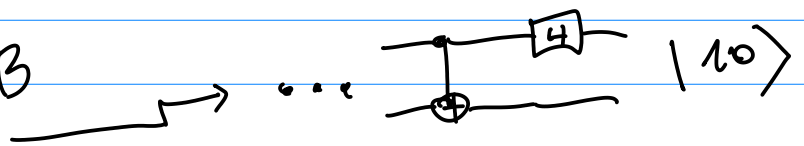


② A is far away from B



④ A sends qubit to B

⑤ B decodes:



Calculation algebraic:

$$|00\rangle \xrightarrow{H \otimes I} |10\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

$$\xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$\xrightarrow{Z \otimes I} \frac{1}{\sqrt{2}}(Z|0\rangle \otimes |0\rangle + Z|1\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Phi^-\rangle$$

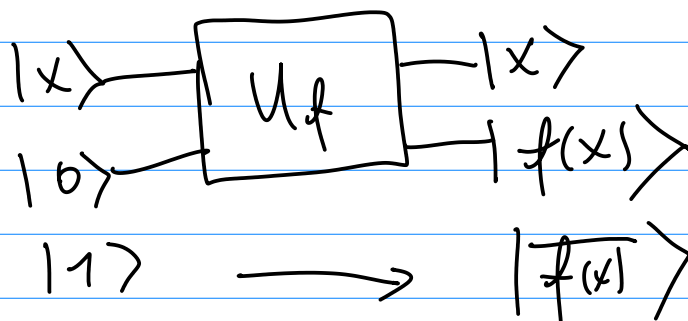
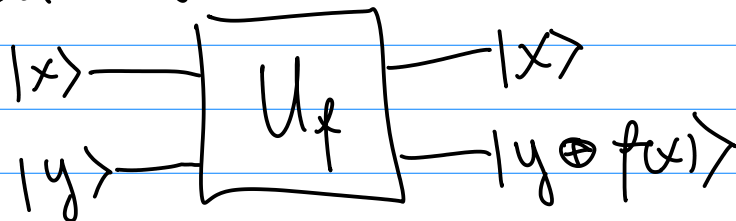
$$\xrightarrow{CNOT} \frac{1}{\sqrt{2}}(CNOT|00\rangle - CNOT|11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) = |-0\rangle$$

$$\xrightarrow{H \otimes I} |10\rangle$$

PART 3 DEUTSCH-JOSZA ALGO

3.1. Quantum oracle

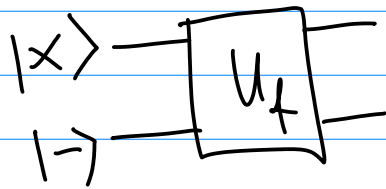
Standard oracle:



3.2. Phase oracle

What happens if $|y\rangle = |-\rangle$?

$$\begin{aligned} |0\rangle &\longrightarrow |f(x)\rangle \\ |1\rangle &\longrightarrow |\overline{f(x)}\rangle \end{aligned}$$



$$\begin{aligned} |x\rangle |-\rangle &\xrightarrow{U_f} |y\rangle = \frac{1}{\sqrt{2}} (|x\rangle |f(x)\rangle - |x\rangle |\overline{f(x)}\rangle) \\ &= \begin{cases} \text{if } f(x)=0, \frac{1}{\sqrt{2}} (|x\rangle |0\rangle - |x\rangle |1\rangle) = |x\rangle |-\rangle \\ \text{if } f(x)=1, \frac{1}{\sqrt{2}} (|x\rangle |1\rangle - |x\rangle |0\rangle) = -|x\rangle |-\rangle \end{cases} \\ &= (-1)^{f(x)} |x\rangle |-\rangle \end{aligned}$$

3.3. Deutsch algorithm

$f(x)$ — constant or balanced?
 $x \in \{0,1\}$

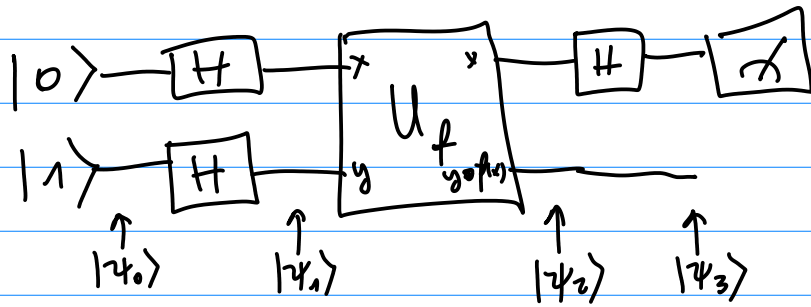
$f(x)=0$ or $f(x)=1$	$f(x)=x$ or $f(x)=\overline{x}$
----------------------------	---------------------------------------

Classical — need to call $f(x)$ 2 times.

Quantum — enough to call $f(x)$ 1 time.

Any quantum algorithm:

- 1) Superposition
- 2) Interference effects



$$|\psi_0\rangle = |01\rangle, \quad |\psi_1\rangle = (H \otimes H)|01\rangle = |+-\rangle,$$

$$|\psi_2\rangle = \begin{cases} \text{if } f(0) = f(1), & \begin{matrix} 00 \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)|-\rangle \\ 11 \rightarrow \frac{1}{\sqrt{2}}(-|00\rangle - |10\rangle)|-\rangle \end{matrix} \\ \text{if } f(0) \neq f(1), & \begin{matrix} 10 \rightarrow \frac{1}{\sqrt{2}}(-|00\rangle + |10\rangle)|-\rangle \\ 01 \rightarrow \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle)|-\rangle \end{matrix} \end{cases} \pm |+-\rangle$$

$$|\psi_3\rangle = \begin{cases} \pm |0-\rangle, & \text{if constant} \\ \pm |1-\rangle, & \text{if balanced} \end{cases} \Rightarrow \text{measure 1st qubit.}$$

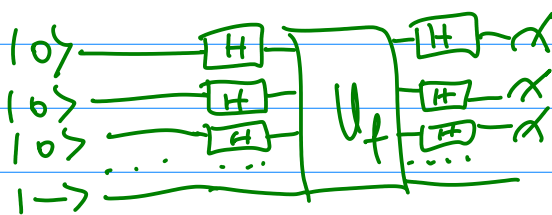
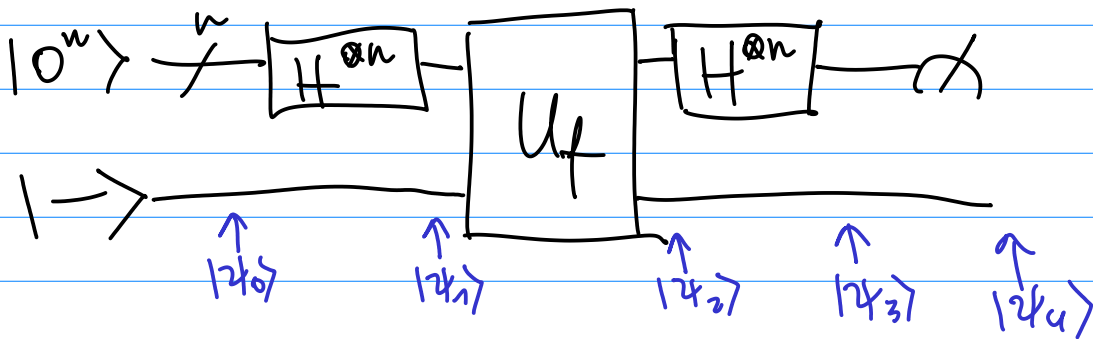
3.4. Deutsch-Jozsa algorithm

$f(x)$ — constant or balanced? (assuming can not be either)

$x \in \{0,1\}^n$ $f(x) = 1$ or $f(x) = 0$ $f(\text{half } x_s) = 1$ AND $f(\text{half } x_s) = 0$

Classical — need $2^{n-1} + 1$ queries

Quantum — ONE QUERY



← for visualization

$$H^{\otimes n} |0\rangle^{\otimes n} = \overbrace{H|0\rangle H|0\rangle \dots H|0\rangle}^n = |+\rangle \dots |+\rangle =$$

$$= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \dots = \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} |z\rangle$$

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

Example:

$$H|000\rangle = \frac{1}{\sqrt{8}} (|000\rangle + |001\rangle + |010\rangle + |011\rangle + \dots)$$

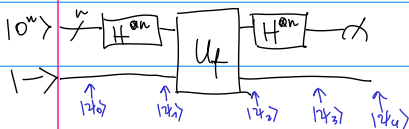
$$H^{\otimes n} |x\rangle^{\otimes n} = \left[\begin{array}{l} H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ H|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle) \end{array} \right]$$

$$= H|x_0\rangle H|x_1\rangle \dots H|x_n\rangle =$$

$$= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_0} |1\rangle) \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1} |1\rangle) \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_2} |1\rangle) \dots =$$

$$= \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle$$

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



$$|\psi_0\rangle = |0^n\rangle \rightarrow$$

$$|\psi_1\rangle = H^{\otimes n} |0\rangle^{\otimes n} \rightarrow = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \rightarrow$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle \rightarrow$$

$$|\psi_3\rangle = (H^{\otimes n} \otimes I) \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle \rightarrow = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} H^{\otimes n} |x\rangle \rightarrow =$$

$$= \left(\frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} \frac{1}{\sqrt{2^n}} \sum_z (-1)^{x \cdot z} |z\rangle \right) \rightarrow =$$

all possible x_s here calculated

$$= \left(\frac{1}{2^n} \sum_{x \in \mathcal{Z}} (-1)^{f(x) + x \cdot z} \right) |z\rangle \quad \text{doesn't matter} \rightarrow |z\rangle$$

$$\rightarrow a_1 |000\dots\rangle + a_2 |000\dots 1\rangle + \dots$$

$z_1 \qquad z_2$

$$(-1)^{f(x_1) + x_1 \cdot z_1 + x_1 \cdot z_2 + \dots + x_1 \cdot z_n} + (-1)^{f(x_2) + x_2 \cdot z_1 + \dots}$$

$|z\rangle \rightarrow a_1$ is the amplitude of $|000\dots 0\rangle$

$$a_1 = \frac{1}{2^n} \left((-1)^{f(x_1)} + (-1)^{f(x_2)} + \dots \right) = \frac{1}{2^n} \sum_x (-1)^{f(x)}$$

if $f(\forall x) = 0$:

$\hookrightarrow 2^n$ elements: $00\dots 0, 00\dots 1, \dots$

$$a_1 = \frac{1}{2^n} (1 + 1 + \dots) = \frac{1}{2^n} \cdot 2^n = 1$$

(100% the $|000\dots 0\rangle$ state)

if $f(\forall x) = 1$:

$$a_1 = \frac{1}{2^n} (-1 - 1 - \dots) = -1 \quad (\text{still 100\% } |000\dots 0\rangle \text{ state})$$

if $f(50\% x_s) = 1$:
 $f(50\% x_s) = 0$

$$a_1 = \frac{1}{2^n} (-1 - 1 - 1 \dots + 1 + 1 + 1) = 0$$

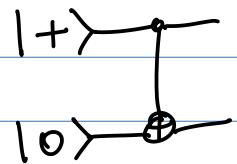
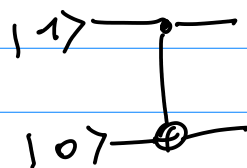
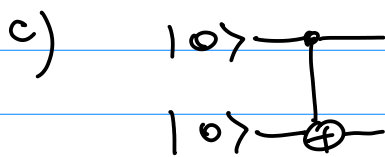
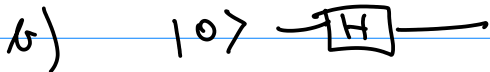
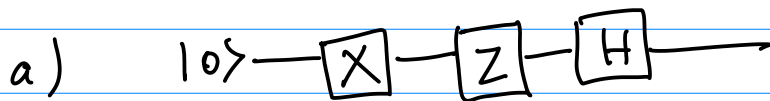
Constant
 \rightarrow output $|000\dots\rangle$

Balanced
 \rightarrow output NOT $|000\dots\rangle$

One query & problem solved :)

PART 4 Exercises

1. Compute the final state + probability to measure 1s.



2. Construct a circuit that prepares given state from 0s:

a) $|\psi\rangle = \frac{1}{\sqrt{2}} (|1\rangle + |0\rangle) |0\rangle$

b) $|\psi\rangle = \frac{1}{\sqrt{2}} (|10\rangle + |11\rangle)$

c) $|\psi\rangle = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

d) $|\psi\rangle = \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle)$

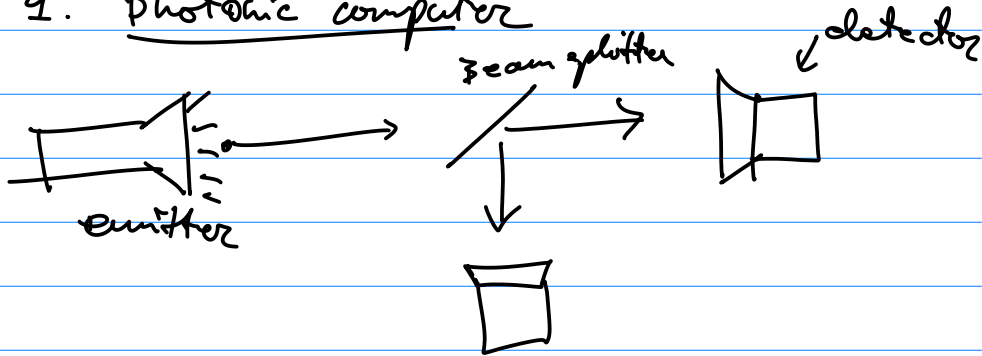
e) $|\psi\rangle = |\Phi^-\rangle = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)$

4. Calculate the state

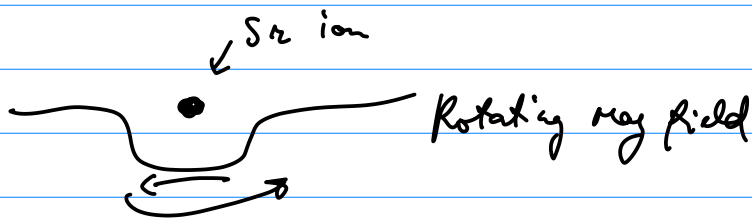
$$|\psi\rangle = H^{\otimes 3} |101\rangle$$

PART 5 Physical implementation

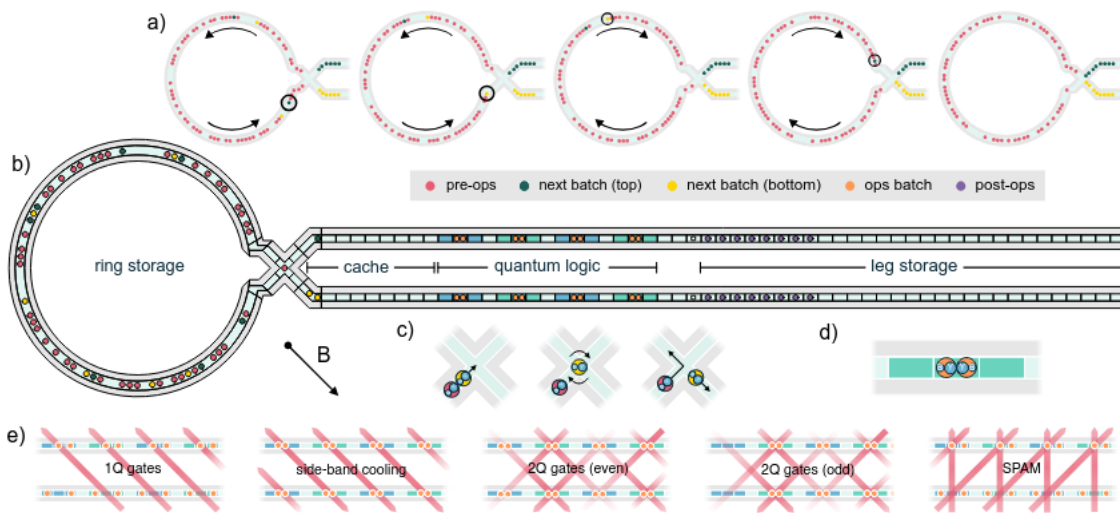
1. Photonic computer



2. Trapped ion computer



And other...



Quantum Helix

PART 6 Use cases

1. Cryptography

SHOR'S ALGORITHM
for primary number
factorization

2. Simulation

Variational Quantum Eigensolver

↳ Chemistry — ground state energy, other energies.
(drug discovery)

↳ Combinatorics — max-cut problem
(logistics)

IBM gives students 10min/month runtime

Just a hype?