Seminar 1

Introduction to Quantum Computing

Before going in…

- I am also a beginner in this field…

- If you are interested, you can search more using:
- Quantum Computing since Democritus (Scott Aaronson)
- Quantum Computation and Quantum Information (Nielsen & Chuang)
- Quantum Computer Science: An Introduction (David Mermin)

Before going in…

- Nielsen & Chuang is considered as the standard text. This presentation is based on Nielsen & Chuang.
- Though primarily based on the first part of the book, I shall add some details.
- I reckon that I distributed the files before this seminar.
- Today, let's discuss the basics.

- Hmm.. will I be able to cover this whole presentation in 50 min?

Schedule

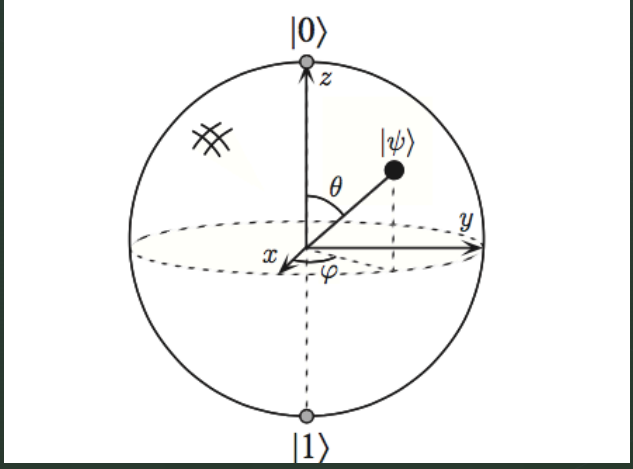
- 1. Introduction to Quantum Computing - Today
- 2. Some Formalisms in Quantum Mechanics
- 3. Quantum Computations
- 4. Realisations of Quantum Computers
- 5. Quantum Noise, Operations, and Distances
- 6. Error Corrections
- 7. Quantum Entropy & Information Theory
- * Unfortunately, I should study from topic 4.

Qubits

- Don’t be confused: Quantum bits are “Mathematical” objects – we need to incorporate those into the real physical world.
- Think it as the quantum ket: $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$.
- The special states $|0\rangle$ and $|1\rangle$ are known as **computational basis states**, and form an orthonormal basis for this vector space.
- I will assume that you know how to interpret this state.

Bloch Sphere

- Rewrite $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ to $|\psi\rangle = \cos\theta|0\rangle + \exp(i\varphi)\sin\theta|1\rangle$
- The two angular variables define a sphere (The Bloch Sphere)
- How much information is stored in one qubit?



Multiple Qubits

- $|\psi\rangle = \alpha 00|00\rangle + \alpha 01|01\rangle + \alpha 10|10\rangle + \alpha 11|11\rangle$. For two qubits.
- Quite straightforward!

- Ex. What if we measured the first qubit and retrieved 0? What is the state then?
- Ans: $\frac{a_{00}|00\rangle + a_{01}|01\rangle}{\sqrt{|a_{00}|^2 + |a_{01}|^2}}$
- We can generalise this to n qubits!

Single Qubit Gates

- The NOT Gate: $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ This is little different from the classical analogue…
- The Z Gate : $Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- The Hadamard Gate: $H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- Note. Single Qubit Gates must still maintain the normalisation conditions: Must be a Unitary operator!

Visualisation on the Bloch Sphere

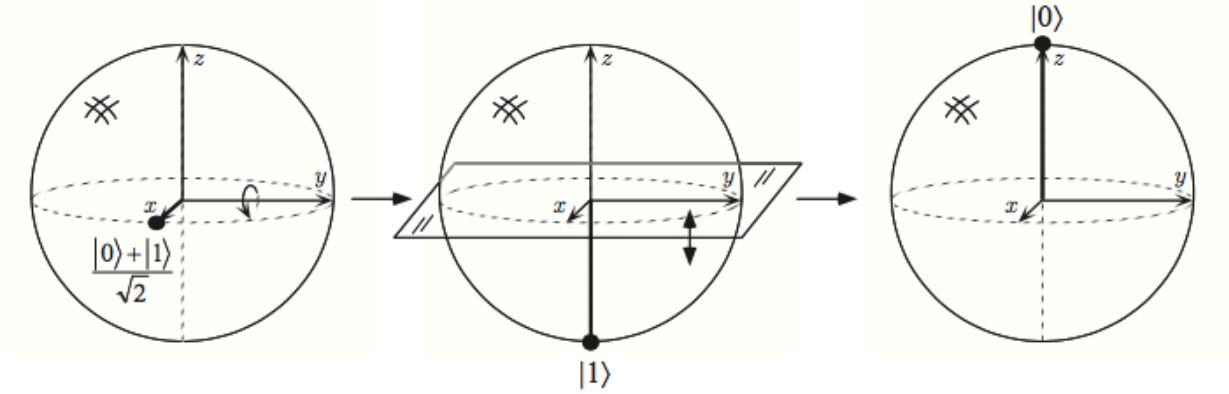


Figure 1.4. Visualization of the Hadamard gate on the Bloch sphere, acting on the input state $(|0\rangle + |1\rangle)/\sqrt{2}$.

Arbitrary Single Qubit Gates

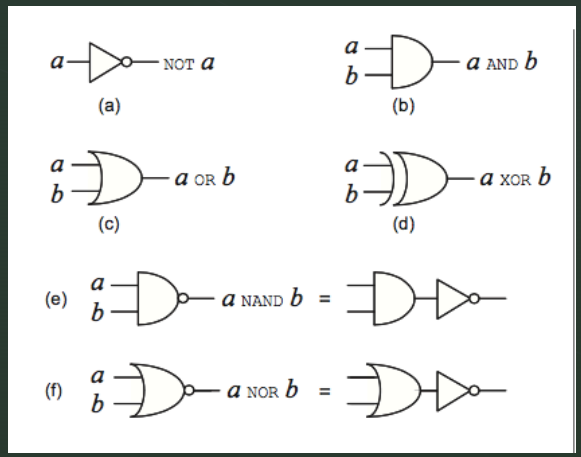
- Note that the operation is a rotation on the Bloch Sphere.
- Property of the SU(2) Group: An arbitrary gate can be represented by a product of finite number of other gates as

$$U = e^{ia}\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}\begin{bmatrix} cos\frac{\gamma}{2} & -sin\frac{\gamma}{2} \\ sin\frac{\gamma}{2} & cos\frac{\gamma}{2} \end{bmatrix}\begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix}$$

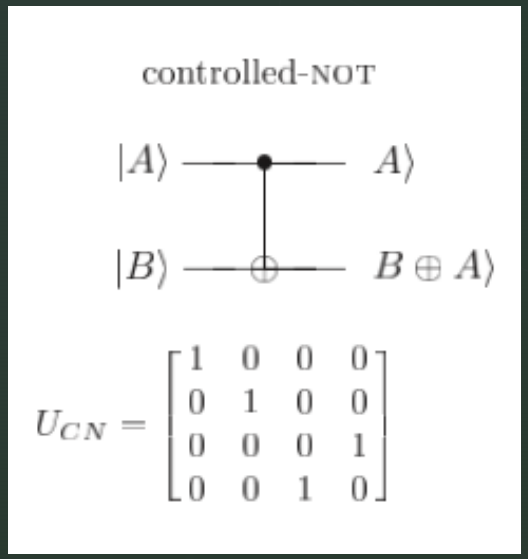
- Look Sakurai Ch. 3 or Nielsen Ch 4 for further details.

Multiple Qubit Gates

- Some Examples of Classical Gates: AND, OR, XOR, NAND, NOR (Look at the Figure below)
- We shall see whether these gates can be represented in Quantum Computing.

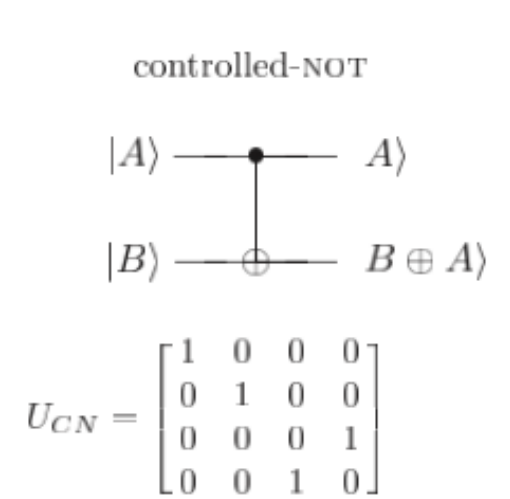


The CNOT Gate



- The Controlled-NOT gate functions as follows:
- There are two inputs: One is the control and other is the target.
- If Control=0 : Nothing happens.
- If Control=1 : Target is flipped.

The CNOT Gate



$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- The CNOT gate is the modulo 2 computation for Qubits, just as XOR gates do in classical counterparts.
- The CNOT gate is the generalisation of XOR gates.

Other Classical Gates

- Question: As we have seen a generalisation of XOR, do we have the counterparts for other classical gates?
- Answer: No. Can we determine the initial states by looking at the final output? (Reversible vs Irreversible)
- Note. Quantum gates must be unitary!

Universality

- Thm. Any multiple qubit logic gate may be composed from CNOT and single qubit gates.
- Similarily, any classical logic gate may be composed form NAND gates. XOR or NOT does not. Think of parity.

Measurements in bases other than the computational bases

- TL;DR : Yes we can.
- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$, where the + and – kets are the bases for the x direction in spins.
- It is possible in principle to measure a quantum system of many qubits with respect to an arbitrary orthonormal basis. Just as we do in QM!
- Stern-Gerlach Experiment

Quantum Circuits

- With the gates we have learnt, now let’s construct a ‘circuit’ to do some specific tasks.
- Look at the circuit below. The ’wire’ need not represent the physical connection, but rather the flow of time.

Some Rules on Constructing Circuits

- It's quite the same with how we do on classical computing, but we have some more restrictions.

- 1. No Loops – the wires are connected by TIME!
- 2. No joining of wires (FANIN): This is irreversible.
- 3. No Split of wires (FANOUT): We CANNOT copy qubits!

Example

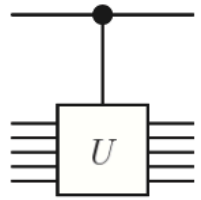


Figure 1.8. Controlled-U gate.

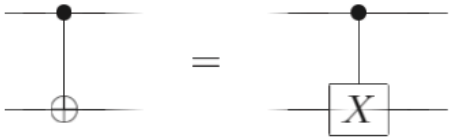


Figure 1.9. Two different representations for the controlled-NOT.

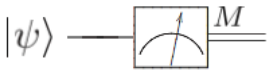
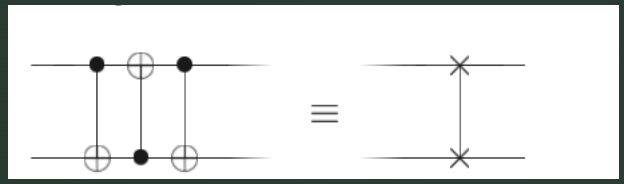


Figure 1.10. Quantum circuit symbol for measurement.



- What does this circuit do? Try it out!
- Cf) All circuits start at 00000…

The No-Cloning Theorem

- This is a rather easy proof, so I shall state here
- Suppose a Quantum Machine that has two Slots A and B; A is the data slot and B is the target slot.
- Both start as a pure Quantum state $|\psi\rangle$ and $|s\rangle$.

The No Cloning Theorem

- Some Unitary evolution that clones the data slot is now applied:

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} U\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle.$$

- Suppose this procedure works for two states (I didn't say the two are different!)

$$U\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle$$
$$U\left(|\varphi\rangle \otimes |s\rangle\right) = |\varphi\rangle \otimes |\varphi\rangle.$$

- Take the Inner Product of the two equations above:

$$\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2.$$

The No Cloning Theorem

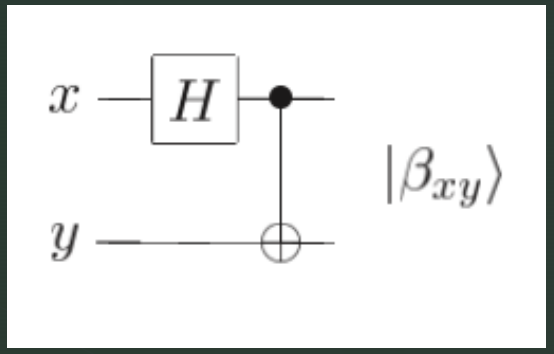
- The machine can only copy states that are either:
  1. Identical or differs by a phase factor
  2. Are orthonormal to each other.
- -> General Cloning Machines are impossible!

- What if non-unitary? What if impure?...
- I shall present on the Mixed Ensembles next time.

More Advanced Example 1: Bell States

- Calculate the outputs for the following circuit.

In	Out
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} \equiv \|\beta_{11}\rangle$



- Look Ch 12 in Griffiths or Ch 3.10 in Sakurai for further details.

More Advanced Example 2: Quantum Teleportation

- Both Alice and Bob generated a EPR pair, and took one qubits each.
- Alice then wants to send her qubit $|\psi\rangle$ (not the EPR pair but the information) but she does NOT know the state of her qubit and can only send classical information.
- Note: Since the qubit is on continuous Bloch sphere, sending all the information even if she knew the state will take forever. Also, by the No Cloning Theorem, she cannot copy the qubit.

More Advanced Example 2: Quantum Teleportation

- An Overview: Interact Alice's qubit with the EPR state she has.
- Then, she shall send the classical results (00, 01, 10, 11) to Bob.
- Depending on the results, Bob shall perform different operations on his EPR state.

- Let's look more deeply in the next slide.

More Advanced Example 2: Quantum Teleportation

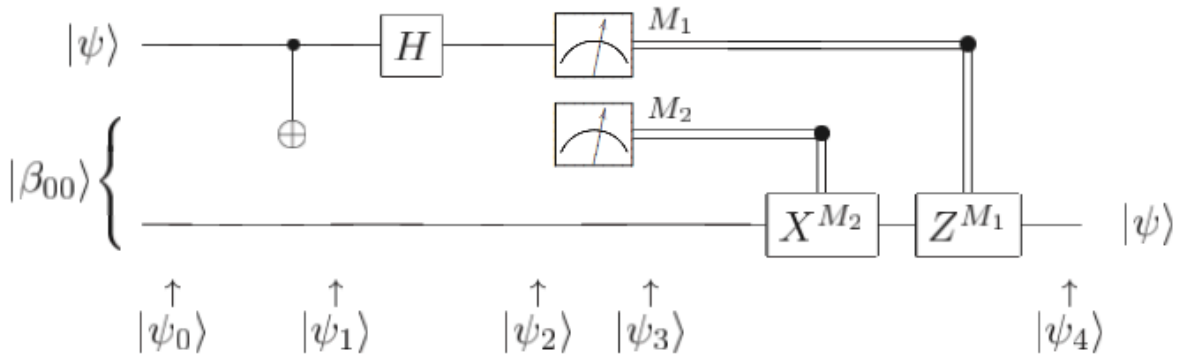


Figure 1.13. Quantum circuit for teleporting a qubit. The two top lines represent Alice's system, while the bottom line is Bob's system. The meters represent measurement, and the double lines coming out of them carry classical bits (recall that single lines denote qubits).

Explanations

- $|\psi\rangle = \alpha|0\rangle+\beta|1\rangle$: State to be Teleported (both coefficients unknown)
- The state input into the circuit $|\psi 0\rangle$ is $|\psi 0\rangle = |\psi\rangle|\beta 00\rangle$
  $=\frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle))$
- (First two qubits: Alice's, third qubit: Bob's)
- Follow the Instructions! -> Apply the CNOT gate to Alice's Qubits
- $\frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle+|01\rangle))$

Explanations

- First Qubit through the Hadamard Gate: ½(α(|0⟩ + |1⟩)(|00⟩ + |11⟩) + β(|0⟩ − |1⟩)(|10⟩ + |01⟩))
- Regroup the terms so that Alice's two qubits are represented together: ½(|00⟩ (α|0⟩ + β|1⟩) + |01⟩ (α|1⟩ + β|0⟩) + |10⟩ (α|0⟩ - β|1⟩) + |11⟩ (α|1⟩ - β|0⟩))
- By Alice measuring the state, Bob's state is determined. However, since we have 4 possibilities, Alice must send her measurement results to Bob.
- Question: Is this a violation of the No Cloning Theorem?

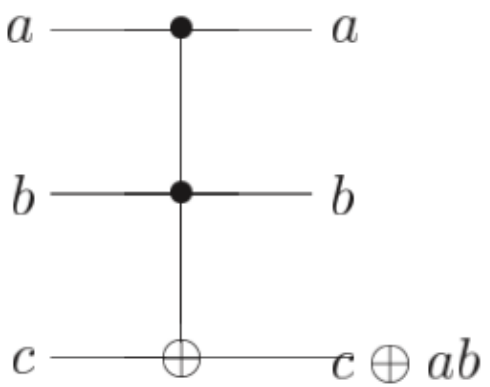
Classical Computations in Quantum Computers

- Quantum vs Classical = Unitary vs Non-Unitary (Reversibility)
- However, any classical circuit can be replaced by an equivalent circuit containing only reversible elements.
- Any ideas on how to do this?

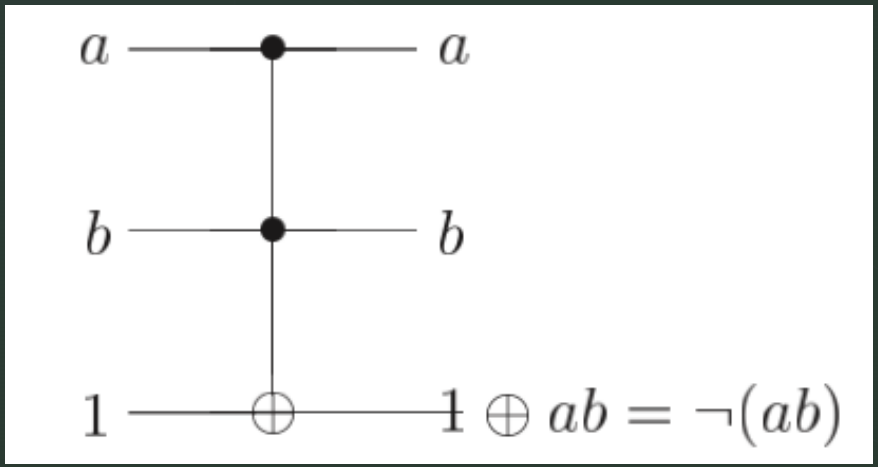
The Toffoli Gate

- This is essentially close to a CNOT gate, but it has two inputs!

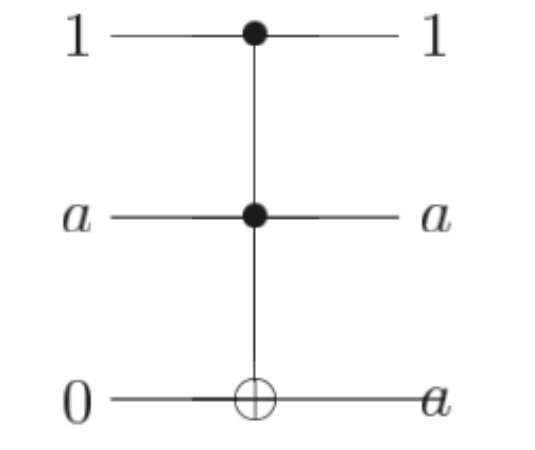
Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



Simulation of NAND and FANOUT in Quantum Computing



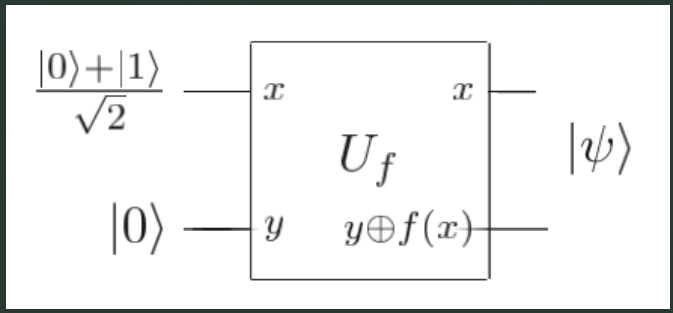
NAND



FANOUT

Representing a Function in Quantum Algorithms

- With an appropriate sequence of logic gates it is possible to transform $|x, y\rangle$ into $|x, y \oplus f(x)\rangle$.
- If y = 0, then the final state of the second qubit is just the value f (x).



Result: $\frac{1}{\sqrt{2}}(|0,f(0)\rangle+|1,f(1)\rangle)$

The different terms contain information about both f(0) and f (1), as if we evaluated different values of f simultaneously.

Walsh-Hadamard Transform

- Generalisation to n qubits
- Obviously, the result if prepared with the initial state of 0 shall be $(|00\rangle+|01\rangle+|10\rangle+|11\rangle)/2$
- Parallel Action to n gates: Tensor!
- Combine the result of the transform and one more 0 state to Uf: $\frac{1}{\sqrt{2^n}}\sum_x |x\rangle\langle f(x)|$

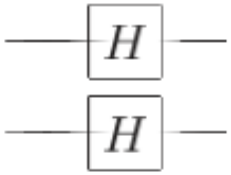


Figure 1.18. The Hadamard transform $H^{\otimes 2}$ on two qubits.

The Deutsch Algorithm

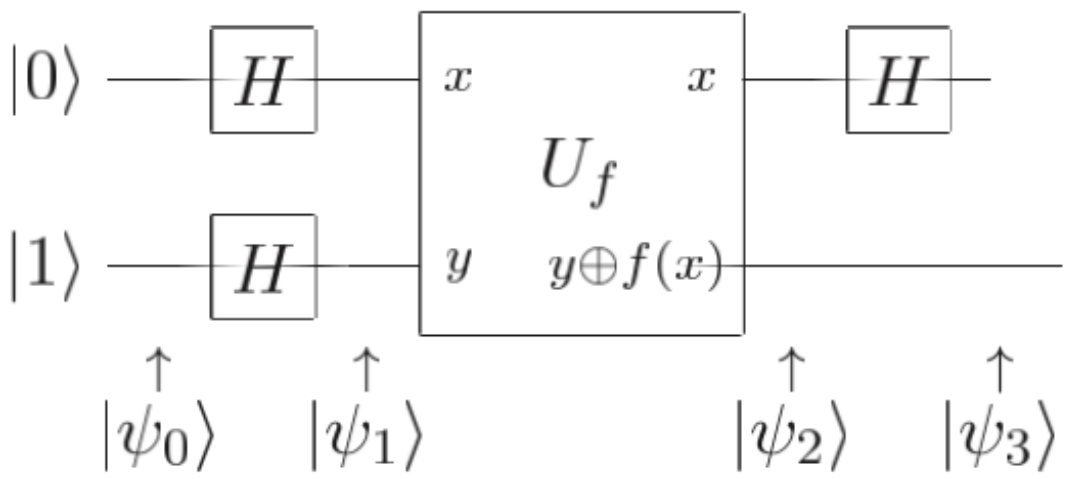


Figure 1.19. Quantum circuit implementing Deutsch's algorithm.

The Deutsch Algorithm

- Input: $|\psi 0\rangle = |01\rangle$
- Passes the Hadamard gate: $|\psi 1\rangle = ((|0\rangle+|1\rangle)/\sqrt{2}\,)(|0\rangle-|1\rangle\,)/\sqrt{2}$
- Note. If we apply Uf to $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$ then we obtain the state $(-1)^{f(x)}\frac{1}{\sqrt{2}}(|x\rangle(|0\rangle - |1\rangle))$.

$$|\psi_2\rangle = \begin{cases} \pm\left[\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm\left[\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1). \end{cases}$$

The Deutsch Algorithm

- Final Step: Apply the Hadamard Gate once again.

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle \left[\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm|1\rangle \left[\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1). \end{cases}$$

- Since f (0) $\oplus$ f (1) is 0 if f (0) = f (1) and 1 otherwise, rewrite this as $|\psi 3\rangle = \pm|f(0) \oplus f(1)\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- We can get the values for f with one calculation!

Generalisation: The Deutsch-Jozsa Algorithm

- Simple. This (on the right) was for two separate states.

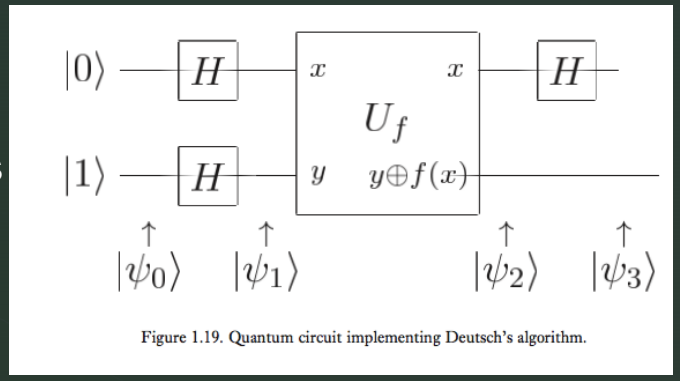


Figure 1.19. Quantum circuit implementing Deutsch's algorithm.

- Do it on n states!

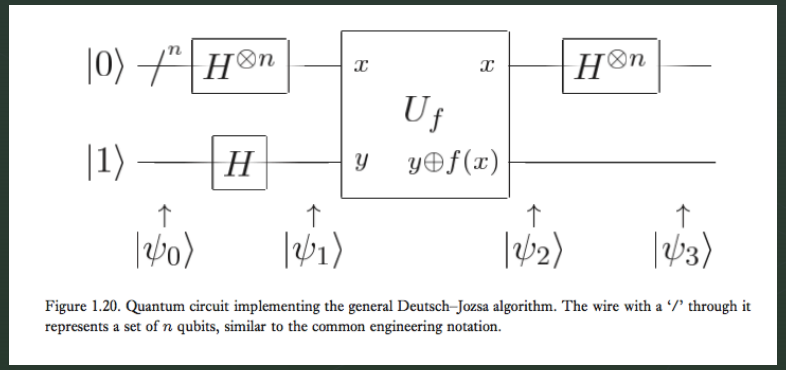


Figure 1.20. Quantum circuit implementing the general Deutsch–Jozsa algorithm. The wire with a '/' through it represents a set of n qubits, similar to the common engineering notation.

Generalisation: The Deutsch-Jozsa Algorithm

- The algorithm is the solution to the following problem (Deutsch's Problem)
- Alice, in London, selects a number x from 0 to 2^n − 1 , and mails it in a letter to Bob, in New York.
- Bob calculates some function f(x) and replies with the result, which is either 0 or 1.
- either f(x) is constant for all values of x, or else f(x) is balanced, which means that 0 and 1 appears in equal probability.
- Goal: determine with certainty whether Bob has chosen a constant or a balanced function. How fast can she do?

Generalisation: The Deutsch-Jozsa Algorithm

- Classical: Srsly, we need to calculate exponential amount of data…
- Quantum: We are good to go in one attempt!

Generalisation: The Deutsch-Jozsa Algorithm

- C
  d
- Q

Algorithm: Deutsch–Jozsa

Inputs: (1) A black box U_f which performs the transformation $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$, for $x \in \{0, \ldots, 2^n - 1\}$ and $f(x) \in \{0, 1\}$. It is promised that $f(x)$ is either *constant* for all values of x, or else $f(x)$ is *balanced*, that is, equal to 1 for exactly half of all the possible x, and 0 for the other half.

Outputs: 0 if and only if f is constant.

Runtime: One evaluation of U_f. Always succeeds.

Procedure:

1.	$\|0\rangle^{\otimes n}\|1\rangle$	initialize state
2.	$\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \|x\rangle \left[\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}\right]$	create superposition using Hadamard gates
3.	$\rightarrow \sum_x (-1)^{f(x)}\|x\rangle \left[\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}\right]$	calculate function f using U_f
4.	$\rightarrow \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)}\|z\rangle}{\sqrt{2^n}} \left[\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}\right]$	perform Hadamard transform
5.	$\rightarrow z$	measure to obtain final output z

Generalisation: The Deutsch-Jozsa Algorithm

- Few Caveats though exist:

- 1. What if we just use a probabilistic classical computer? Few trial and error will be sufficient.
- 2. The Deutsch Problem does not have any practical applications.

Other Quantum Algorithms

- Deutsch-Jozsa Algorithm/Shor Algorithm
- Fourier Transforms (Quantum Version of the FFT!)
- Quantum Search Algorithms
- Quantum Simulations

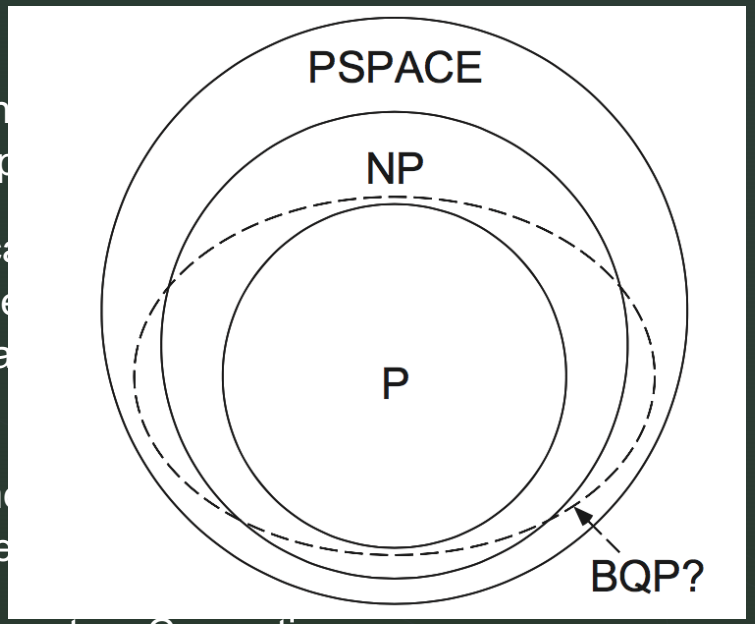
- Later!

Computational Complexity Theory

- P: class of computational problems that can be solved quickly on a classical computer
- NP: class of problems which have solutions which can be quickly checked on a classical computer
- PSAPCE: problems which can be solved using resources which are few in spatial size, but not necessarily in time
  -> Assumed to be larger than P and NP but never proved
- BPP: class of problems that can be solved using randomized algorithms in polynomial time, if a bounded probability of error is allowed in the solution to the problem.
- BQP: Analogue of BPP in Quantum Computing.

Computational Complexity Theory

- P: class of computational problems that can be solved quickly on a classical computer
- NP: class of problems which
  checked on a classical comp
- PSAPCE: problems which c
  few in spatial size, but not n
  -> Assumed to be larger tha
- BPP: class of problems that
  algorithms in polynomial tim
  allowed in the solution to the
- BQP: Analogue of BPP in Quantum Computing.



Stern-Gerlach Experiment

- We all know what this experiment is meant to show ☺
- Is this experiment compatible with the Qubit Model?

- What about electron spin being a proof that qubits can exist and be realised in the real world?

Possibility of Realisations in the Physical World

- Problem with Noise: Are there any fundamental obstacles (noises) which shall prevent the realisation?
- What if QM is wrong?

- How can we make this ‘excellent’ thing running in the real world? NMR? Ion Trap?

Quantum Information

- Quantum Information focuses on the following three objectives. (Primarily. Of course, this isn't it!)
- 1. Identify elementary classes of static resources in quantum mechanics.
- 2. Identify elementary classes of dynamical processes in quantum mechanics.
- 3. Quantify resource tradeoffs incurred performing elementary dynamical processes.

The Shannon Entropy

- The formula is given as $H(p_j) = -\sum_j p_j log p_j$, where p_j represents the probability for each state j.
- Think of a coin toss: In what probability distribution will the system have the maximum entropy?

- Cf) This concept is applied in statistical mechanics, especially considering the complex systems.

Some theorems in Quantum Information

- The Noiseless Coding Theorem
- The Noisy Channel Coding Theorem
- Schumacher's Noiseless Channel Coding Theorem
- So on and so on…

- The implications are quite hard; let's look these on a latter time.

Quantum Distinguishability

- The rules of QM makes us impossible to distinguish between arbitrary states (kets).
- For example, if we measured |1>, can we know what exact state was the measurement derived from?
- Quantum state contains information that CANNOT be accessed by measuring: important in Cryptography!

Quantum Distinguishability

- What if we can distinguish non-orthogonal states?
- 1. Using EPR pairs, faster-than-light communications are feasible.
- 2. We can make a cloning machine!

Entanglements

- We still don’t know very well abt entanglements…
- How many qubits must two parties exchange if they are to create a particular entangled state shared between them, given that they share no prior entanglement?
- Can we transform entanglement from one form into another?

Acknowledgements

- The overall text was amended using Nielsen & Chuang, Quantum Computations and Quantum Information, 10th anniversary edition, Cambridge University Press, 2010.

- The figures used in this presentation is also an excerpt from Nielsen and Chuang.

- This presentation is NOT intended for commercial uses, but for education.