

Simple algorithms (Part I): Deutsch-Jozsa algorithm

March 17, 2008

by
Thomas Strub

advised by
Andrey Lebedev

Outline

Contents of this presentation

0. Hadamard gate
1. Classical computation on quantum computers
2. Basic concepts of quantum computation
3. The Deutsch algorithm
4. The Deutsch-Jozsa algorithm
5. Classes of quantum algorithms

0. Hadamard gate

Hadamard* gate

- The Hadamard gate is a unitary one-qubit gate:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad H = H^{-1}$$

- H maps computational basis states to superposition states:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$H \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |0\rangle \quad H \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |1\rangle$$

*) Jacques S. Hadamard (1865 – 1963), French mathematician

0. Hadamard gate

- *Hadamard transform vs. QFT**
- The Hadamard gate performs a quantum Fourier transform.
- The quantum Fourier transform is defined by

$$|j\rangle \xrightarrow{F} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle ,$$

and gives for $n = 1$:

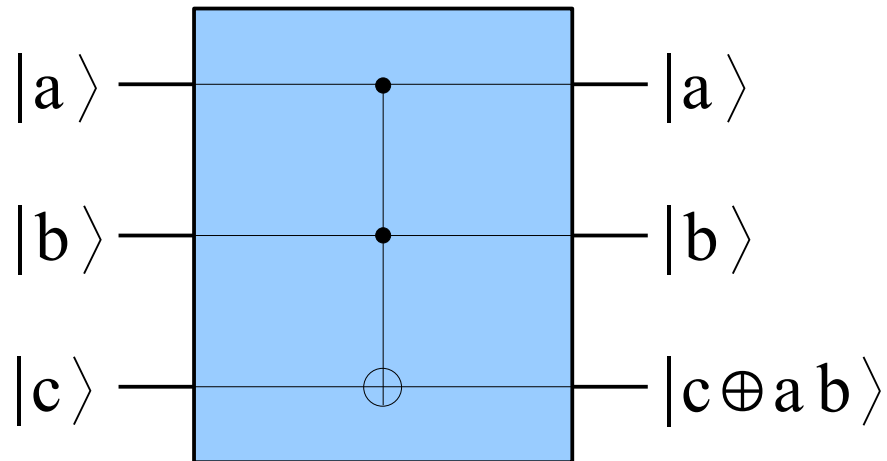
$$|j\rangle \xrightarrow{F} \frac{1}{\sqrt{2}} (|0\rangle + e^{\pi i j} |1\rangle) = H |j\rangle$$

*) Talk on April 14th by Markus Schmassmann

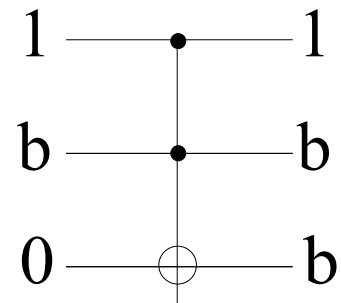
1. Classical computation on quantum computers

Toffoli gate

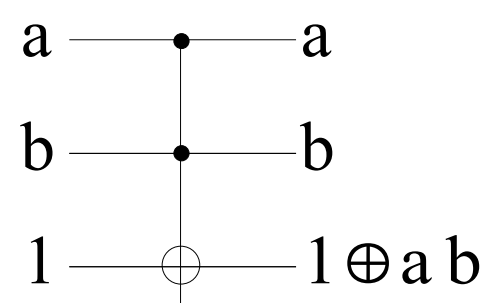
- Every classical circuit can be simulated by a quantum circuit using the reversible Toffoli gate.



FANOUT



NAND



- With the NAND gate and FANOUT gate every other classical gate can be simulated.

2. Basic concepts of quantum computation

Contents of this chapter

How can the *superposition*, *entanglement* and *interference* of quantum states help improve computation?

2.1 Quantum parallelism

2.2 Interference

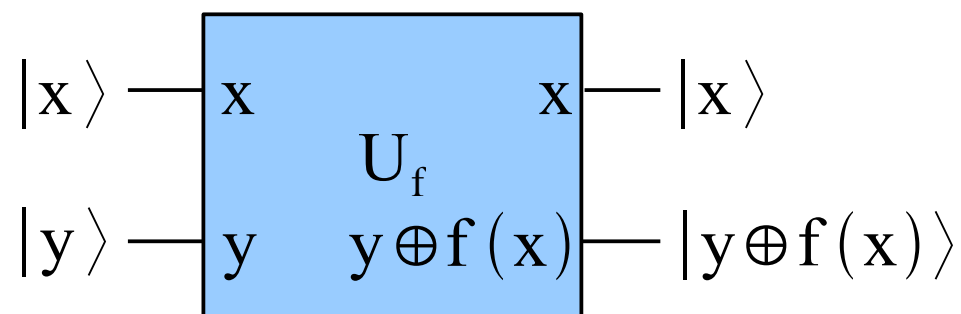
2.3 Phase kick-back by f-cNOT

2. Basic concepts of quantum computation

2.1 Quantum parallelism

A simple example

- Let $f(x): \{0,1\} \rightarrow \{0,1\}$ be an arbitrary one-bit function.
- The quantum gate U_f representing f is a so called f -controlled-NOT gate:



- U_f flips the target qubit if and only if $f(x) = 1$.

2. Basic concepts of quantum computation

- If the target qubit is set to 0, one gets the mapping

$$|x\rangle |0\rangle \xrightarrow{U_f} |x\rangle |0 \oplus f(x)\rangle = |x\rangle |f(x)\rangle.$$

- If x is not a basis state but a superposition like

$$|x\rangle = H |0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

the following entangled final state is produced:

$$\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right] |0\rangle \xrightarrow{U_f} \frac{|0\rangle |f(0)\rangle + |1\rangle |f(1)\rangle}{\sqrt{2}}$$

- The final state contains information about both $f(0)$ and $f(1)$ but in just one evaluation of f .

2. Basic concepts of quantum computation

- For a multi-qubit function $f(\mathbf{x}): \{0,1\}^n \rightarrow \{0,1\}$ one can even get a higher performance:

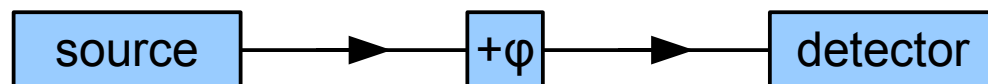
$$\frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \{0,1\}^n} |\mathbf{x}\rangle |0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \{0,1\}^n} |\mathbf{x}\rangle |f(\mathbf{x})\rangle$$

- 2^n parallel evaluations of f (in just one action of U_f)!
- But: We can only get one $f(x)$ for an undetermined x ! (measuring theory)
- Difference to a classical probabilistic computation?
 - The state carries (before the measurement) information of $f(x)$ for all x .
 - One can use this state to get *global* property of f .

2. Basic concepts of quantum computation

2.2 Interference

- Extracting global information of superposition states by interference.
- We look at an example:
 - Problem: We have two identically looking devices: One of them shifts the phase of a single passing photon by π , the other does nothing.

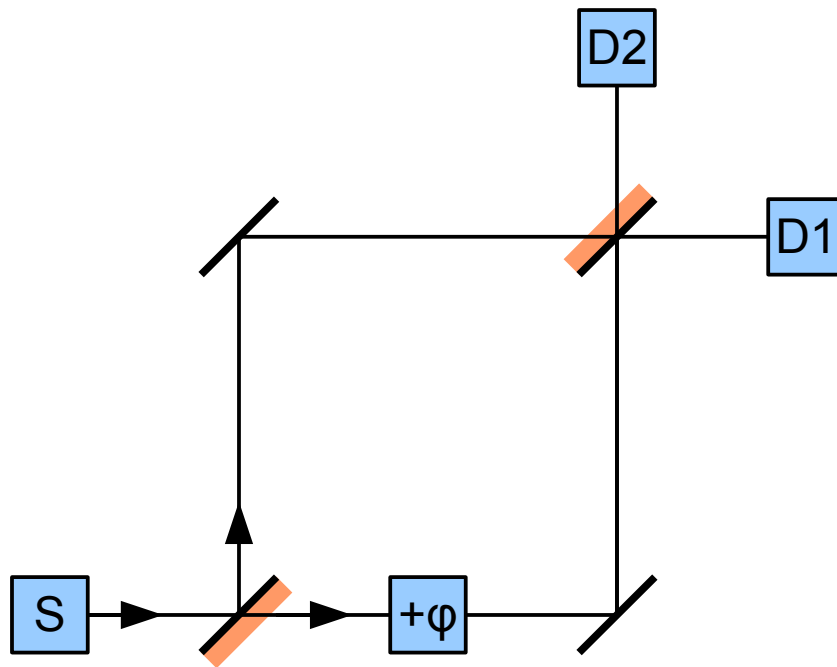


Find out which device is which!

2. Basic concepts of quantum computation

- Solution: Mach-Zehnder interferometer

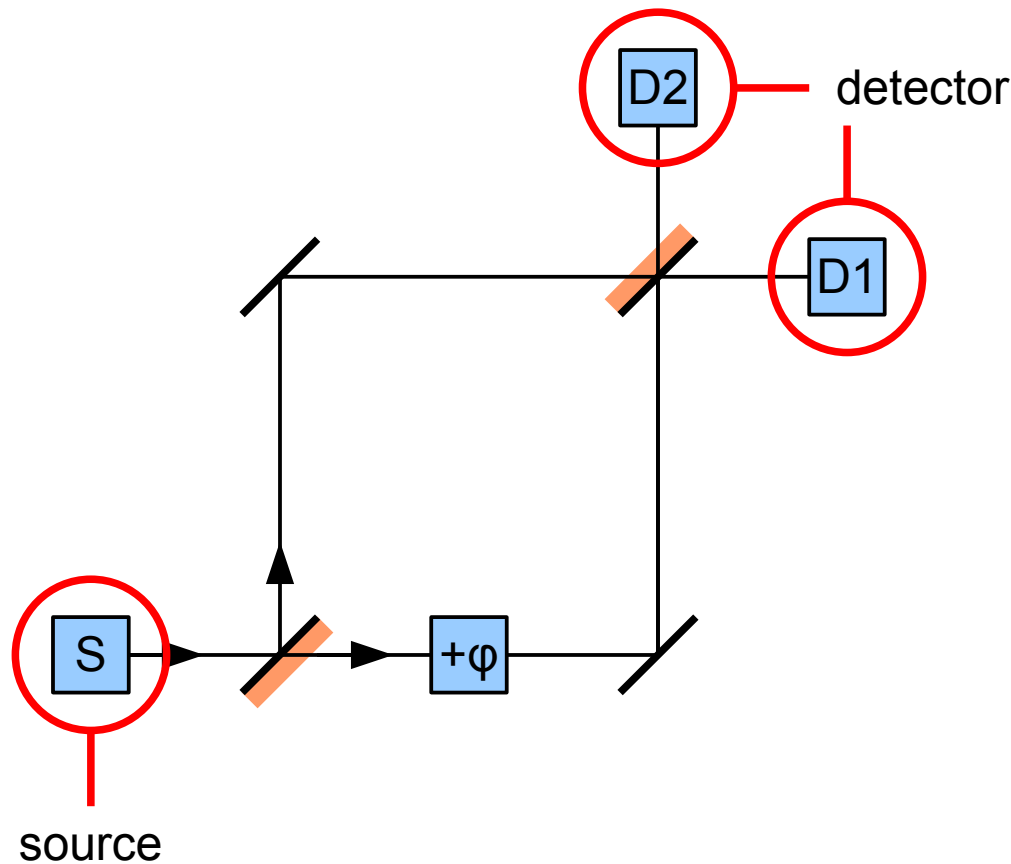
By interference one can solve the problem with only one photon.



2. Basic concepts of quantum computation

- Solution: Mach-Zehnder interferometer

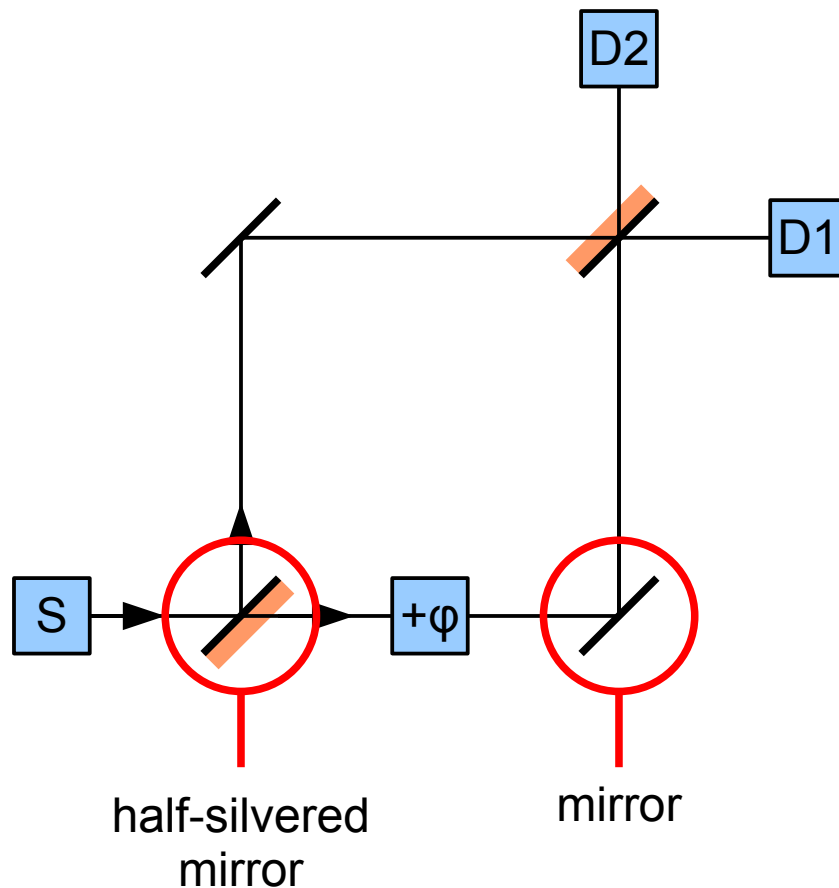
By interference one can solve the problem with only one photon.



2. Basic concepts of quantum computation

- Solution: Mach-Zehnder interferometer

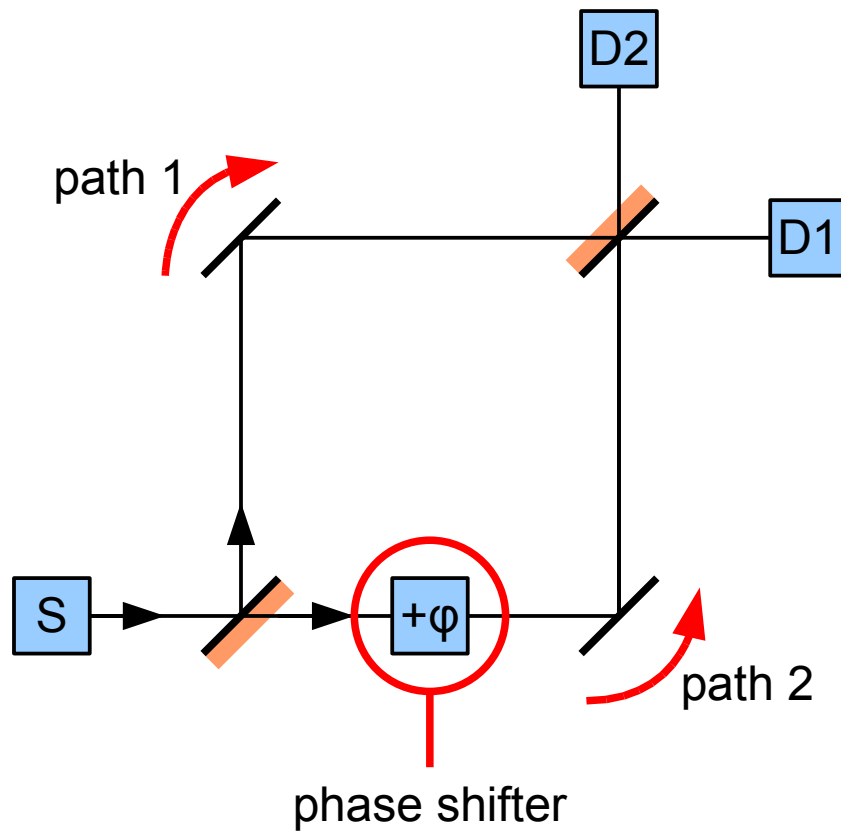
By interference one can solve the problem with only one photon.



2. Basic concepts of quantum computation

- Solution: Mach-Zehnder interferometer

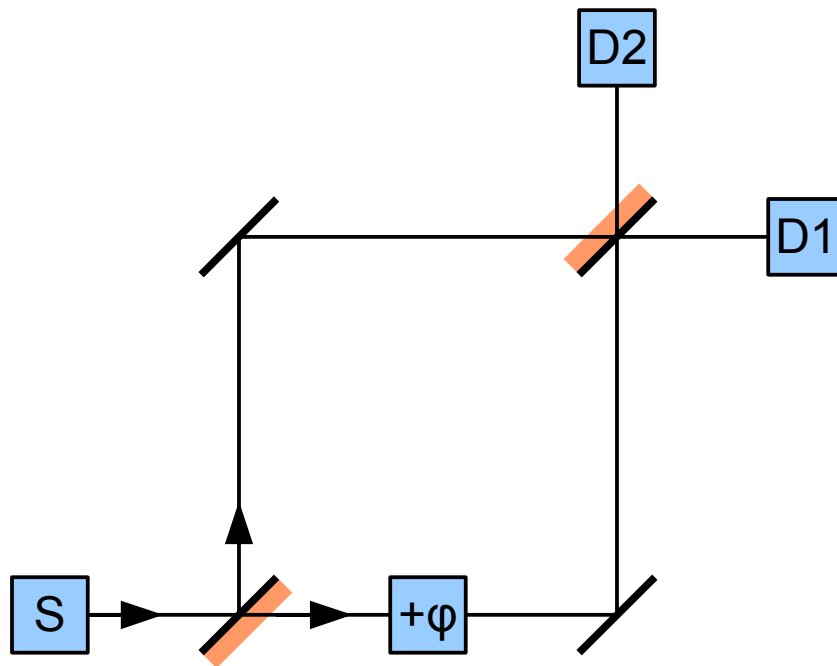
By interference one can solve the problem with only one photon.



2. Basic concepts of quantum computation

Quantum mechanical solution

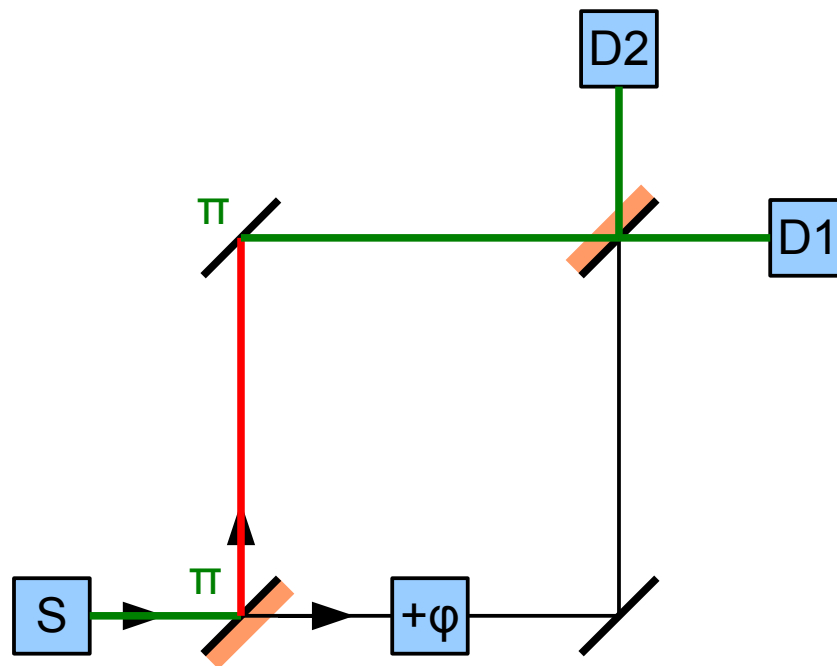
- The photon takes *both* paths at the same time.
- The photon interferes behind the last mirror with itself.



2. Basic concepts of quantum computation

Quantum mechanical solution

- The photon takes *both* paths at the same time.
- The photon interferes behind the last mirror with itself.

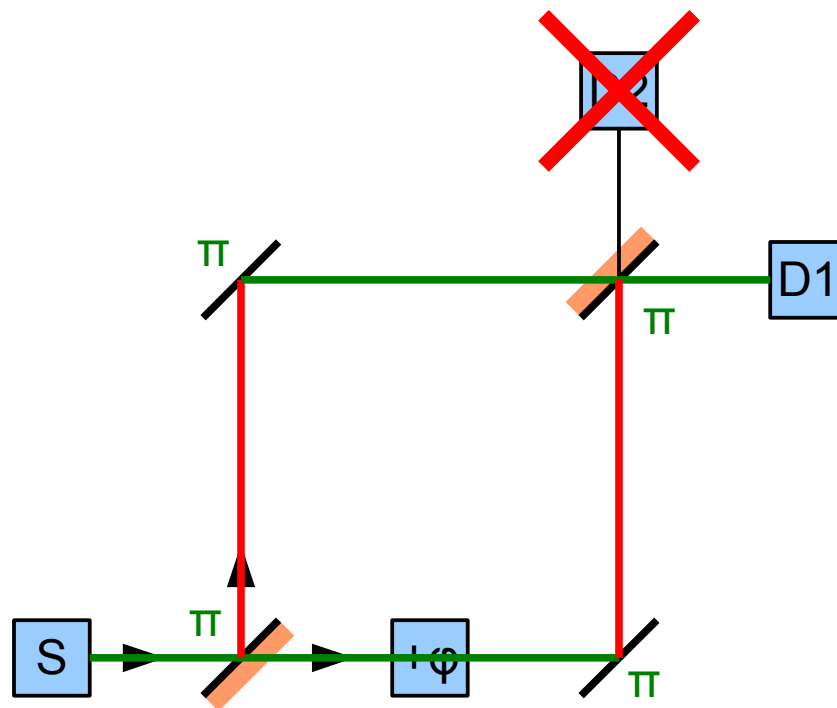


$$\varphi = 0:$$

2. Basic concepts of quantum computation

Quantum mechanical solution

- The photon takes *both* paths at the same time.
- The photon interferes behind the last mirror with itself.

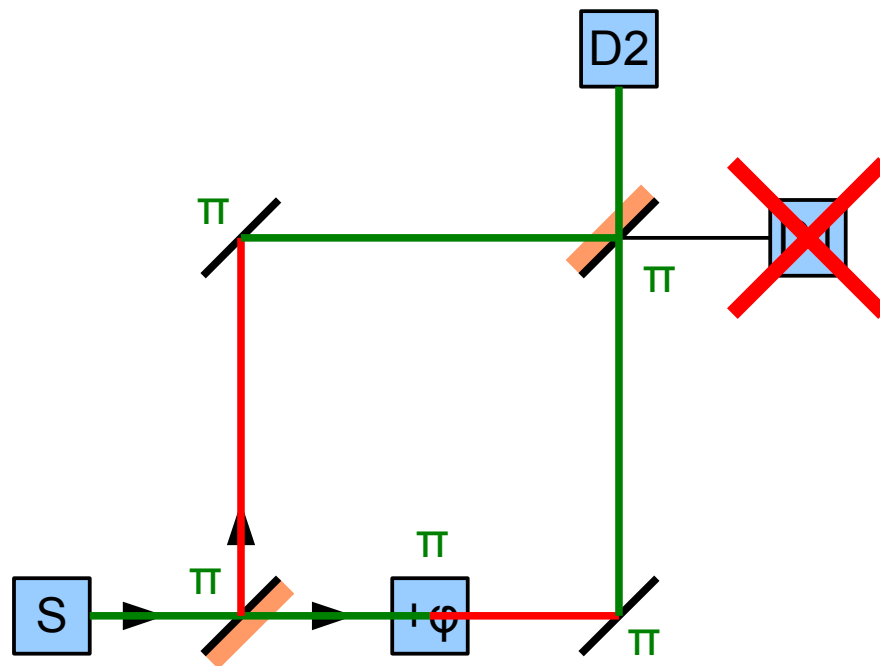


$\phi = 0$:
D1 detects photon

2. Basic concepts of quantum computation

Quantum mechanical solution

- The photon takes *both* paths at the same time.
- The photon interferes behind the last mirror with itself.



$\varphi = 0$:
D1 detects photon

$\varphi = \pi$:
D2 detects photon

2. Basic concepts of quantum computation

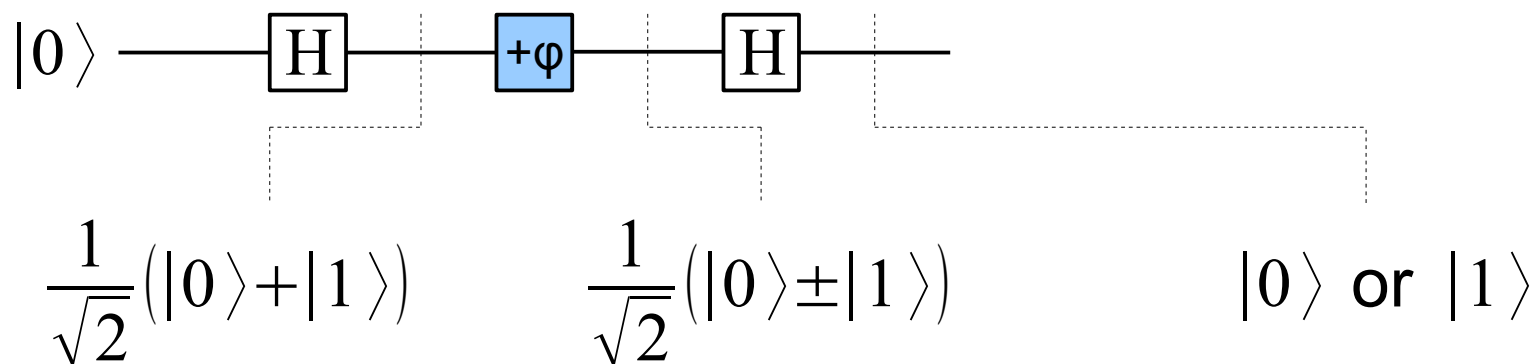
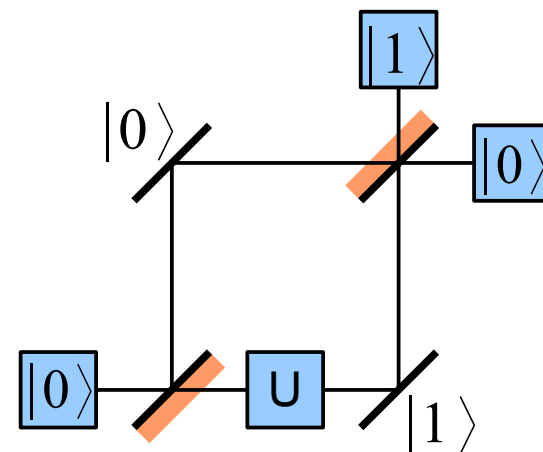
Connection to quantum computation

- Label path 1 as $|0\rangle$ and path 2 as $|1\rangle$.

→ Phase shifter can be seen as a

single qubit gate $U_{0,\pi} = \begin{bmatrix} 1 & 0 \\ 0 & \pm 1 \end{bmatrix}$.

→ Half-silvered mirrors become Hadamard gates:



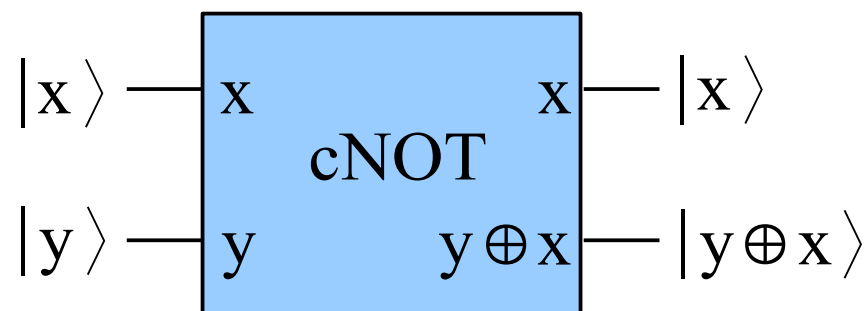
2. Basic concepts of quantum computation

2.3 Phase Kick-Back by f-cNOT

- Consider first a cNOT gate with the following initial state (control qubit x ; target qubit y):

$$|x\rangle = |0\rangle \text{ or } |1\rangle$$

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



- The target qubit is an eigenstate of cNOT gate:

$$|0\rangle|y\rangle \xrightarrow{\text{cNOT}} |0\rangle|y \oplus 0\rangle = +|0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

$$|1\rangle|y\rangle \xrightarrow{\text{cNOT}} |1\rangle|y \oplus 1\rangle = -|1\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

2. Basic concepts of quantum computation

→ The eigenvalue is a global phase shift and can be moved in front of the control qubit.

- Summarised, for $b \in \{0, 1\}$

$$|b\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \xrightarrow{\text{cNOT}} (-1)^b |b\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

- If now the control qubit is in a superposition too:

$$\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \xrightarrow{\text{cNOT}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

→ This is often called 'phase kick-back'.

2. Basic concepts of quantum computation

- If now a f-cNOT gate is chosen, the phase kick-back is controlled by f(b):

$$|b\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \xrightarrow{f\text{-cNOT}} (-1)^{f(b)} |b\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

- The relative phase shift in control qubit depends on the function f.

2. Basic concepts of quantum computation

Summary

Using f -controlled gates one gets the following tools:

- *Quantum parallelism* (control qubit in superposition) gives in just one query of the function f a final state containing all information about f .
- *Phase Kick-Back* (target qubit in superposition) puts the eigenvalue of the target qubit in front of the control qubit. By that, different paths get different phase shifts.
- *Interference* brings different paths together and causes certain states to cancel out by destructive interference.

3. The Deutsch algorithm

Contents of this chapter

Formulation and solution of a problem which can be solved faster by a quantum algorithm than by any classical algorithm.

3.1 Deutsch's problem

3.2 Classical solution

3.3 Quantum algorithm

3.4 Deutsch vs. Mach-Zehnder interferometer

3.5 Historical notes: The original algorithm

3. The Deutsch algorithm

3.1 Deutsch's problem

- A unknown one-bit function f

$$f : \{0, 1\} \rightarrow \{0, 1\}$$

is either constant or balanced.

→ Find out whether f is constant or balanced.

- There are four possibilities for f :

$$f_1 : 0 \rightarrow 0, 1 \rightarrow 1$$

$$f_2 : 0 \rightarrow 1, 1 \rightarrow 0$$

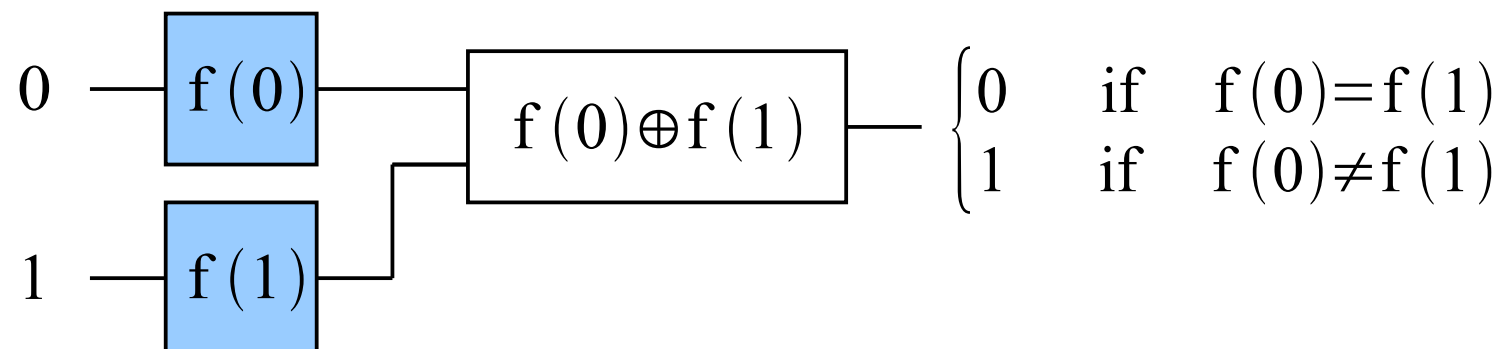
$$f_3 : 0 \rightarrow 1, 1 \rightarrow 1$$

$$f_4 : 0 \rightarrow 0, 1 \rightarrow 0$$

3. The Deutsch algorithm

3.2 Classical solution

- One has to evaluate f twice to solve the problem:

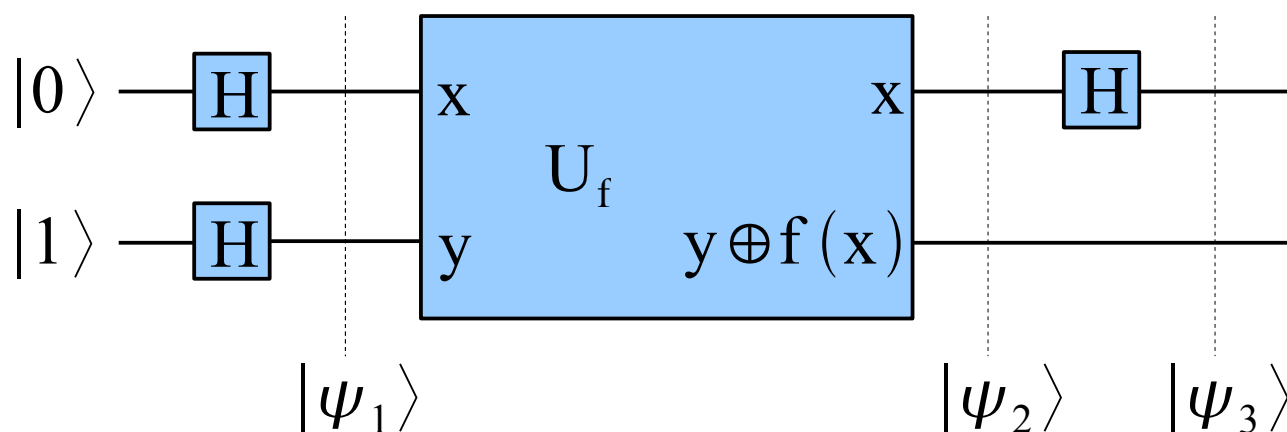


- In return one gets the full information about f .

3. The Deutsch algorithm

3.3 Quantum algorithm

- The function f can be represented by a f -cNOT gate
 - Only one evaluation of f is needed!
 - The quantum circuit looks like this:



3. The Deutsch algorithm

- The action of the first Hadamard gates gives

$$|\psi_1\rangle = H|0\rangle H|1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

- Now use (chapter 2):

$$|x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \xrightarrow{U_f} (-1)^{f(x)} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

to derive

$$\begin{aligned} |\psi_2\rangle &= U_f \frac{1}{2} (|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\ &= \frac{1}{2} \left((-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right) (|0\rangle - |1\rangle) \end{aligned}$$

3. The Deutsch algorithm

- Look at the two cases:

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2} \left((-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right) (|0\rangle - |1\rangle) \\ &= \begin{cases} (-1)^{f(0)} \frac{1}{2} (|0\rangle + |1\rangle) (|0\rangle - |1\rangle) & \text{if } f(0) = f(1) \\ (-1)^{f(0)} \frac{1}{2} (|0\rangle - |1\rangle) (|0\rangle - |1\rangle) & \text{if } f(0) \neq f(1) \end{cases} \end{aligned}$$

- The difference in the results appears in the relative phase difference in the first qubit:

$$|\psi_2\rangle = \begin{cases} \pm \frac{1}{2} (|0\rangle + |1\rangle) (|0\rangle - |1\rangle) & \text{if } f(0) = f(1) \\ \pm \frac{1}{2} (|0\rangle - |1\rangle) (|0\rangle - |1\rangle) & \text{if } f(0) \neq f(1) \end{cases}$$

3. The Deutsch algorithm

- By applying the Hadamard gate H_x on the first qubit we get

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

or summarised

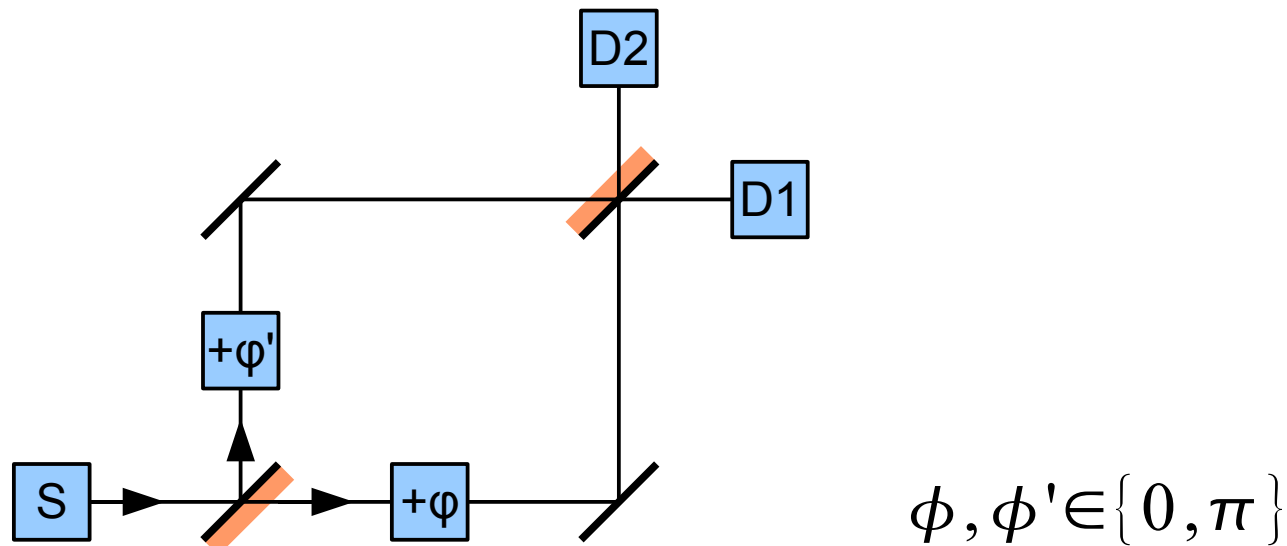
$$|\psi_3\rangle = \pm |f(0) \oplus f(1)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right].$$

→ A measurement of the first qubit gives us with certainty the outcome 0, if f is constant and 1, if f is balanced!

3. The Deutsch algorithm

3.4 Deutsch vs. Mach-Zehnder interferometer

- Deutsch's problem is equivalent to the Mach-Zehnder interferometer with *two* phase shifters:



- One can only tell about the phase difference $|\varphi - \varphi'|$
either: $\varphi = \varphi'$ ($\leftrightarrow f(x)$ constant)
or: $\varphi \neq \varphi'$ ($\leftrightarrow f(x)$ not constant)

3. The Deutsch algorithm

3.5 Historical notes: The original algorithm

- The original algorithm published by David Deutsch (1985) only succeeded with probability $\frac{1}{2}$.
- The average time solving the problem was the same as in the classical case (i.e. 2 evaluations of f).
- The algorithm presented here was published by R. Cleve, A. Ekert, C. Macchiavello and M. Mosca in the paper '*Quantum Algorithms Revisited*' in 1996.

4. The Deutsch-Jozsa algorithm

Contents of this chapter

Formulation and solution of the generalised problem of Deutsch: The Deutsch-Jozsa algorithm.

4.1 The problem

4.2 Classical solutions

4.3 Quantum algorithm

4.4 Efficiency comparison

4.5 Historical notes: The original algorithm

4. The Deutsch-Jozsa algorithm

4.1 The problem

A unknown n-qubit function

$$f(\mathbf{x}) : \{0, 1\}^n \rightarrow \{0, 1\}$$

is either constant or balanced.

- Find out whether f is constant or balanced by just one evaluation of f !
- n control qubits are needed (with 2^n basis states).

4. The Deutsch-Jozsa algorithm

4.2 Classical solutions

Deterministic Turing machine

- Number of evaluations needed
 - best case: 2 $f(\mathbf{x}_0) \neq f(\mathbf{x}_1)$
 - worst case: $2^{n-1} + 1$ $f(\mathbf{x}_i) = f(\mathbf{x}_0) \quad \forall i \leq 2^{n-1}$
 - in average: $3 - \frac{1}{2^{n-1}}$

4. The Deutsch-Jozsa algorithm

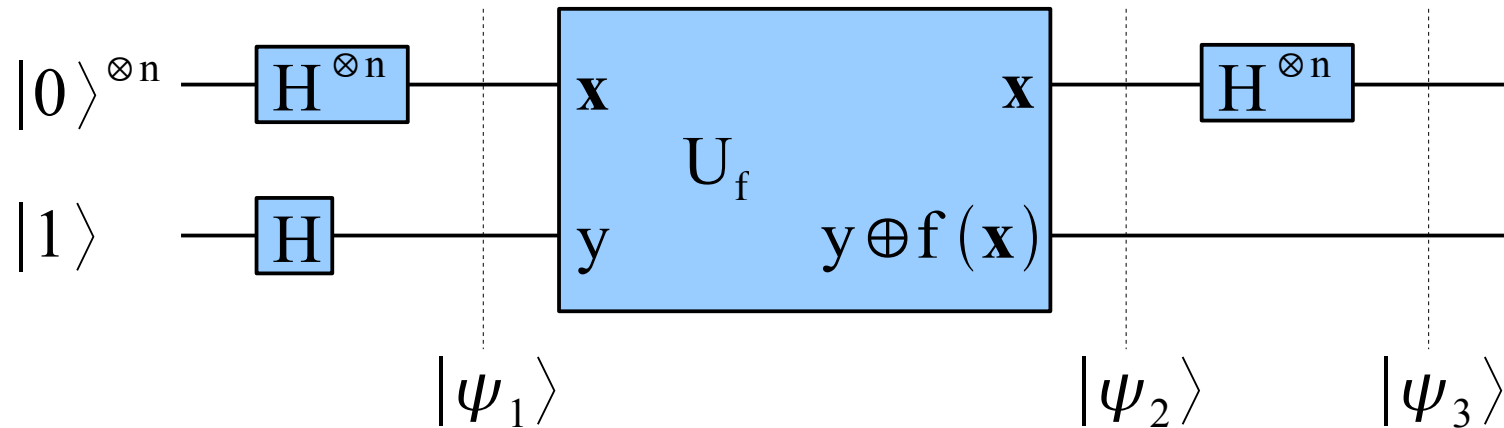
Probabilistic Turing machine

- Deterministic algorithm but with a random permutation σ of the input values \mathbf{x}_i : $\mathbf{x}'_i = \mathbf{x}_{\sigma(i)}$.
- Number of evaluations needed
 - best case: 2 $f(\mathbf{x}_{\sigma(0)}) \neq f(\mathbf{x}_{\sigma(1)})$
 - worst case: $2^{n-1} + 1$ $f(\mathbf{x}_{\sigma(i)}) = f(\mathbf{x}_{\sigma(0)}) \quad \forall i \leq 2^{n-1}$
- For $m < 2^{n-1} + 1$ queries on f , the probability p_{succ} getting the right answer is

$$p_{\text{succ}} \geq 1 - p_{\text{fail}} = 1 - \frac{1}{2^{m-1}}.$$

4. The Deutsch-Jozsa algorithm

4.3 Quantum algorithm



- initial state for the target qubit is $|y\rangle = |1\rangle$.
- n control qubits form the first register $|x\rangle$:

$$|x\rangle = |0\rangle^{\otimes n} = \underbrace{|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle}_n$$

4. The Deutsch-Jozsa algorithm

- The state after the first Hadamard gate is

$$|\psi_1\rangle = H^{\otimes n} |0\rangle^{\otimes n} \otimes H |1\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \{0,1\}^n} |\mathbf{x}\rangle \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

where $\frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \{0,1\}^n} |\mathbf{x}\rangle$ is an equally weighted superposition over all 2^n basis states.

- Applying U_f gives

$$\begin{aligned} |\psi_2\rangle &= U_f \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \{0,1\}^n} |\mathbf{x}\rangle \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \\ &= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \{0,1\}^n} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \end{aligned}$$

- The phase shift is pulled back (i.e. -1) if $f(\mathbf{x}) = 1$).

4. The Deutsch-Jozsa algorithm

- For the final step, look at the action of H:

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

now derive

$$\begin{aligned} H^{\otimes n} |x\rangle &= H |x_1\rangle H |x_2\rangle \dots H |x_n\rangle \\ &= \frac{1}{\sqrt{2}} \sum_{z_1 \in \{0,1\}} (-1)^{x_1 z_1} |z_1\rangle \dots \frac{1}{\sqrt{2}} \sum_{z_n \in \{0,1\}} (-1)^{x_n z_n} |z_n\rangle \\ &= \frac{1}{\sqrt{2^n}} (|0\rangle^{\otimes n} + (-1)^{x_1} |1\rangle |0\rangle^{\otimes n-1} + \dots + (-1)^{x_1 + x_2 + \dots + x_n} |1\rangle^{\otimes n}) \\ &= \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle \end{aligned}$$

4. The Deutsch-Jozsa algorithm

- Using this for the second action of H:

$$\begin{aligned} |\psi_3\rangle &= H^{\otimes n} \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \{0,1\}^n} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \\ &= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \{0,1\}^n} (-1)^{f(\mathbf{x})} \frac{1}{\sqrt{2^n}} \sum_{\mathbf{z} \in \{0,1\}^n} (-1)^{\mathbf{x} \cdot \mathbf{z}} |\mathbf{z}\rangle \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \\ &= \frac{1}{2^n} \sum_{\mathbf{x}, \mathbf{z} \in \{0,1\}^n} (-1)^{f(\mathbf{x}) \oplus \mathbf{x} \cdot \mathbf{z}} |\mathbf{z}\rangle \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \end{aligned}$$

- The first register (first n qubits) can be written as a superposition over all 2^n basis states:

$$a_{00\dots 0} |0\rangle^{\otimes n} + a_{10\dots 0} |1\rangle |0\rangle^{\otimes n-1} + \dots + a_{11\dots 1} |1\rangle^{\otimes n}$$

4. The Deutsch-Jozsa algorithm

- Look at $a_{00\dots 00}$ (amplitude of the basis state $|0\rangle^{\otimes n}$):

$$a_{00\dots 00} = \left[\frac{1}{2^n} \sum_{\mathbf{x}, \mathbf{z} \in \{0, 1\}^n} (-1)^{f(\mathbf{x}) \oplus \mathbf{x} \cdot \mathbf{z}} \right]_{|\mathbf{z}\rangle = |0\rangle^{\otimes n}} = \frac{1}{2^n} \sum_{\mathbf{x} \in \{0, 1\}^n} (-1)^{f(\mathbf{x})}$$

→ If f is constant: $a_{00\dots 00} = \pm 1$

→ If f is balanced: $a_{00\dots 00} = 0$

→ A measurement of the first register gives us with certainty the answer 'constant', if all n qubits are in the state $|0\rangle$. If only one qubit is set to $|1\rangle$, the function is balanced!

4. The Deutsch-Jozsa algorithm

4.4 Efficiency comparison

- There is an *exponential gap* between the (worst case) classical algorithm and the quantum algorithm:

$$M_{\text{classical}} = 2^{n-1} + 1 \quad M_{\text{quantum}} = 1 \quad M = \text{no. queries of } f$$

- The probability p_{fail} getting the wrong answer with the classical probabilistic algorithm drops exponentially with m , independent of n :

$$p_{\text{fail}} \leq \frac{1}{2^{m-1}}$$

- For every small $\varepsilon > 0$ there is a constant m_ε (for all n) such that $p_{\text{fail}} < \varepsilon$. Therefore one could claim a *linear gap* for a *exponentially small error*.

4. The Deutsch-Jozsa algorithm

4.5 Historical notes: The original algorithm

- Published by David Deutsch and Richard Jozsa in 1992.
- The algorithm required originally two evaluations instead of only one.
- It was the base for Grover's and Shor's algorithm.

5. Classes of quantum algorithms

The three classes of algorithms

There are three classes of quantum algorithms known which provides an advantage over classical algorithms:

- I. Quantum algorithms which are based on the quantum Fourier transform (Deutsch-Jozsa, Shor).
- II. Quantum search algorithm (Grover).
- III. Quantum simulation (Simulation of multi-particle systems).

Summary

- Any classical circuit can be simulated with Toffoli gates.
- *Quantum parallelism, interference* and the *phase kick-back* can be used to improve quantum computation: Superposition is used to compute different paths at the same time which are brought together by interference.
- With this it is possible to get *global* properties of functions without the knowledge of the specific values of $f(x)$.
- The Deutsch-Jozsa algorithm is based on quantum Fourier transform and is more efficient than any classical algorithm.

Thanks...

- for listening,
- to Pascal Steger (for the Laser pointer thing),
- to my adviser Andrey Lebedev,
- to the rest of the Proseminar crew

Enjoy your meal...