Quantum Algorithms
part II

Ian Glendinning

December 4, 2001

Outline

- Introduction
- Quantum Bits and Registers
- Quantum Circuits
- Quantum Algorithms
- Summary and Outlook

Quantum Bits and Registers

- Qubits
- The Bloch Sphere
- Multiple Qubits

Multiple Qubits

Two classical bits have four possible states, 00, 01, 10 and 11, and correspondingly a two qubit system has four *computational basis states*, denoted $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$, or more concisely $|0\rangle$, $|1\rangle$, $|2\rangle$ and $|3\rangle$.

A pair of qubits can also exist in superpositions of these states, and a general two-qubit state can be written:

$$\begin{aligned} |\psi\rangle &= \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \\ &= \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \alpha_3|3\rangle \qquad (1) \end{aligned}$$

where the α_n are complex numbers.

Multiple Qubits

In a similar way to the single qubit case, a measurement always gives one of the values 00, 01, 10 or 11, and the probability of measuring the result i is $|\alpha_i|^2$, so the normalization condition is

$$\sum_{i=0}^{3} |\alpha_i|^2 = 1$$

since the probabilities must sum to one.

Entanglement

An important two-qubit state is the *Bell state* or *EPR pair*

$$\frac{(|00\rangle - |11\rangle)}{\sqrt{2}}$$

This innocuous-looking state is responsible for many surprises!

Measuring one qubit gives 0 or 1, each with probability $\frac{1}{2}$, and a subsequent measurement of the other qubit always gives the same result as the first one - *even if the two qubits are physically separated by further than the distance light could have travelled!*

It is called an *entangled* state, because the measurement outcomes are correlated - more strongly than for *any classical system.*

Quantum Registers

More generally, we can consider a system of n qubits, an n-bit quantum register, with computational basis states of the form $|x_1 x_2 \ldots x_n\rangle$ where each x_i is either 0 or 1.

More concisely, we can write the basis states as $|i\rangle$ where $i = 0 \ldots 2^n - 1$.

A register can be in a superposition of basis states:

$$|\psi\rangle = \sum_{i=0}^{2^n-1} a_i |i\rangle$$

where the interpretation of the (complex) coefficients a_i is that $|a_i|^2$ is the probability that a measurement will yield the value $|i\rangle$

Quantum Registers

And since the probabilities must sum to 1 we have:

$$\sum_{i=0}^{2^n-1} |a_i|^2 = 1$$

In general 2^n complex numbers are needed to specify the state of an n-qubit quantum register - can't just list the state of each qubit.

For $n = 500$ this number is larger than the estimated number of atoms in the universe!

Nature manipulates huge quantities of data, even for systems of a few hundred atoms. We'd very much like to take advantage of this!

Vector Representation

The state of an n-qubit register can be represented as a vector in a space which is the tensor product of n 2D complex vector spaces, which is an example of a *Hilbert space* (David Hilbert):

$$C^2 \otimes C^2 \otimes \cdots \otimes C^2$$

The tensor product of two 2D vectors **a** and **b** is:

$$\mathbf{a} \otimes \mathbf{b} = \begin{pmatrix} a_1 \mathbf{b} \\ a_2 \mathbf{b} \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$$

Vector Representation

So for example, for 2-qubit states we have the four basis vectors:

$|00\rangle = |0\rangle \otimes |0\rangle$, $|01\rangle = |0\rangle \otimes |1\rangle$, $|10\rangle = |1\rangle \otimes |0\rangle$, $|11\rangle = |1\rangle \otimes |1\rangle$:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Vector Representation

Like the single-qubit basis vectors, n-qubit basis vectors are orthonormal, i.e. for $0 \leq i, j \leq 2^{n-1}$

$$\langle i|j\rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

Entangled states are states that cannot be written as tensor products of single qubit states, only as sums of tensor products of them. E.g.:

$(|00\rangle + |11\rangle)/\sqrt{2}$ is entangled, but

$(|00\rangle + |10\rangle)/\sqrt{2} = [(|0\rangle + |1\rangle) \otimes |0\rangle]/\sqrt{2}$ is not.

Quantum Circuits

- Single Qubit Gates
- Multiple Qubit Gates
- Functions
- Quantum Parallelism

Single Qubit Gates

Classical computer circuits consist of wires and logic gates.

The only non-trivial classical single-bit gate is the NOT gate, defined by its 'truth table', in which $0 \rightarrow 1$ and $1 \rightarrow 0$, i.e. the states are interchanged.

We can define an analagous quantum NOT gate, which takes the state $|0\rangle$ to the state $|1\rangle$ and vice versa.

This does not tell us what happens to superpositions of the states $|0\rangle$ and $|1\rangle$ though.

The Quantum NOT Gate

In fact, the quantum NOT gate acts *linearly*, i.e. it takes the state:

$$\alpha|0\rangle + \beta|1\rangle$$

to the state in which the roles of $|0\rangle$ and $|1\rangle$ have been interchanged:

$$\alpha|1\rangle + \beta|0\rangle$$

It turns out that linearity is a general property of quantum mechanics. Why this should be so is not obvious, but that it is true is experimentally well verified.

Matrix Representation

The quantum NOT gate can be conveniently represented in matrix form, because of its linearity. It is conventionally called X, because in the Bloch sphere picture it performs a rotation of 180° about the x axis:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and using the vector notation for the state $\alpha|0\rangle + \beta|1\rangle$, we have

$$X \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

Unitarity

So single-qubit gates can be represented by 2×2 matrices

Recall that normalization requires that $\langle\psi|\psi\rangle = 1$, so if a quantum gate takes $|\psi\rangle \rightarrow |\psi'\rangle$ then we must also have $\langle\psi'|\psi'\rangle = 1$.

The appropriate condition on a matrix U representing a gate is that it be *unitary*, that is:

$$U^\dagger U = I$$

where $U^\dagger$ is the *adjoint* of U, defined by $U^\dagger = (U^T)^*$, and I is the identity matrix.

For example, for the NOT gate it is easy to verify that

$$X^\dagger X = I$$

Unitarity

In general, if $|\psi'\rangle = U|\psi\rangle$ then

$$\begin{aligned}\langle\psi'| &= |\psi'\rangle^\dagger \\ &= (U|\psi\rangle)^\dagger \\ &= \langle\psi|U^\dagger\end{aligned}$$

because $(A\mathbf{x})^\dagger = \mathbf{x}^\dagger A^\dagger$, so

$$\langle\psi'|\psi'\rangle = \langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle = 1$$

Unitarity turns out to be the *only* constraint on quantum gates, so any unitary matrix defines a valid quantum gate!

Combinations of unitary operators are also unitary.

The Hadamard Gate

In contrast to the classical case, there are many non-trivial single-qubit gates. One of the most useful is the *Hadamard* gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The gate changes $|0\rangle \rightarrow (|0\rangle + |1\rangle)/\sqrt{2}$ and $|1\rangle \rightarrow (|0\rangle - |1\rangle)/\sqrt{2}$

It turns out that in the Bloch sphere picture, all single-qubit gates correspond to rotations, and H corresponds to a 180° rotation about the axis defined by the vector with cartesian coordinates $(1, 0, 1)$.

The Hadamard Gate

The Hadamard gate can be implemented with a half-silvered mirror, and it has the property that $H^2 = I$, which is how the Mach-Zehnder interferometer works!

The two inputs to a half-silvered mirror correspond to the states $|0\rangle$ and $|1\rangle$. Consider the input $|0\rangle$, then after the first mirror the state is

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

and after the second mirror the state is

$$\begin{aligned} H(|0\rangle + |1\rangle)/\sqrt{2} &= [(|0\rangle + |1\rangle) + (|0\rangle - |1\rangle)]/2 \\ &= |0\rangle \end{aligned}$$

The Square Root of NOT Gate

Another operation with no classical analogue is the 'square root of NOT' gate, U_{SRN}, defined by $(U_{SRN})^2 = X$. It turns out that:

$$U_{SRN} = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\pi/4} & e^{-i\pi/4} \\ e^{-i\pi/4} & e^{i\pi/4} \end{pmatrix}$$

This gate corresponds to a rotation by 90° about the x axis in the Bloch sphere picture. (Recall that X corresponds to a 180° rotation about x.)

General Single Qubit Gate

There are infinitely many two by two unitary matrices, and thus infinitely many single qubit gates, but an arbitrary single qubit rotation can be expressed as:

$$V(\theta,\phi) = \begin{pmatrix} \cos(\theta/2) & -ie^{-i\phi}\sin(\theta/2) \\ -ie^{i\phi}\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

Furthermore, good approximations to gates for arbitrary θ and ϕ can be built from gates with only special fixed values of the angles, so only a *finite* set of gates are required.

Multiple Qubit Gates

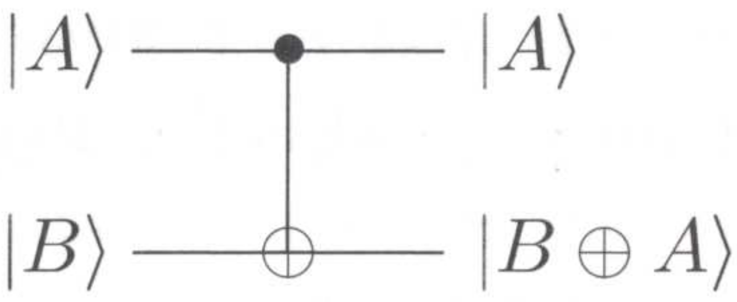
- The prototypical multi-qubit gate is the *controlled*-NOT or CNOT gate
- The gate has two inputs, known as the *control* qubit and the *target* qubit and two outputs
- If the control qubit is set to 0, the target qubit is unchanged, and if the control qubit is set to 1, the target qubit is flipped:

$$U_{CN}|00\rangle = |00\rangle, U_{CN}|01\rangle = |01\rangle$$

$$U_{CN}|10\rangle = |11\rangle, U_{CN}|11\rangle = |10\rangle$$

The Controlled-NOT Gate

CNOT is a generalization of the classical XOR gate, since its action may be summarized as $|A, B\rangle \rightarrow |A, B \oplus A\rangle$, where $\oplus$ is addition modulo two, which is what the XOR gate does.



Note that we are using the abbreviated notation $|A, B\rangle$ to mean $|A\rangle \otimes |B\rangle$, which is also sometimes written $|A\rangle|B\rangle$

The Controlled-NOT Gate

Another way to represent CNOT is as a matrix:

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

And as for single qubit gates, U_{CN} is unitary, i.e. $U_{CN}^{\dagger} U_{CN} = I$

Universality

- n-qubit quantum gates can be represented by $2^n \times 2^n$ unitary matrices

- It can be shown that any $n \times n$ unitary matrix can be formed by composing the 2-qubit 'controlled-not' gate (U_{CN}), and general rotation of a single qubit $V(\theta, \phi)$

- The U_{CN} and $V(\theta, \phi)$ gates can be combined to make a controlled rotation, which is a single universal gate

Reversibility

- $U^\dagger U = I \Rightarrow U^\dagger = U^{-1}$, so unitary operations always have an inverse
- Quantum computations are therefore reversible, unlike some classical ones
- It might seem that not all classical compuations can be implemented by a quantum computer
- But at the expense of extra qubits to maintain the initial state, any classical operation can be implemented by a unitary one

Functions

Suppose $f(x) : \{0,1\} \rightarrow \{0,1\}$ is a function with a one-bit domain and range.

We can compute this value using a two-bit quantum computer which starts in the state $|x, y\rangle$, using a function U_f, defined as:

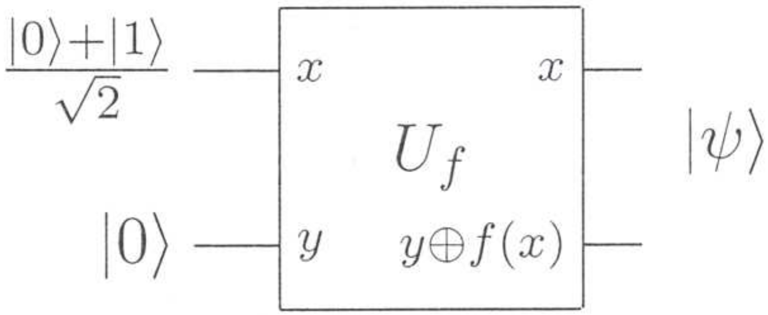
$$U_f|x, y\rangle = |x, y \oplus f(x)\rangle$$

which can be shown to be unitary, and efficiently implementable.

U_f can be generalised to domains and ranges of more than one qubit, and is an important building block for quantum algorithms.

Quantum Parallelism

Consider the following circuit, which applies U_f to the superposition state $(|0\rangle + |1\rangle)/\sqrt{2}$, which can be created with a Hadamard gate acting on $|0\rangle$:



The output state is:

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

Quantum Parallelism

This is a remarkable state! The different terms contain information about $f(0)$ and $f(1)$, and it is almost as if we have evaluated $f(x)$ for two values of x simultaneously. This is *quantum parallelism.*

This procedure can easily be generalized to functions of an arbitrary number of qubits. We first create a superposition state, using a *Hadamard transform*, which is just n Hadamard gates acting in parallel on n qubits. For example, for $n = 2$, acting on $|00\rangle$ it gives:

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

Quantum Parallelism

We write this $H^{\otimes 2}$, and more generally, the result of the Hadmard transform on n qubits initially all in the $|0\rangle$ state, written $|0\rangle^{\otimes n}$, is

$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

By applying a linear number of gates (n), we have generated a state with an equal superposition of all 2^n basis states, an exponential number of terms!

Quantum Parallelism

Quantum parallel evaluation of a function f with an n bit input and 1 bit output can thus be peformed by starting with the $n+1$ bit state $|0\rangle^{\otimes n}|0\rangle$, and applying $H^{\otimes n}$ to the first n bits, followed by U_f, giving:

$$U_f\left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|0\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}U_f|x\rangle|0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle$$

So in some sense we have computed all possible values of f simultaneously!

However, measurement of the above state would give only $f(x)$ for a single random value of x, which a classical computer can do easily.

Quantum Parallelism

- Quantum computation requires more than just quantum parallelism to be useful
- It requires the ability to extract information about more than one value of $f(x)$ from such superposition states
- The solution is to use destructive interference between states
- The combination of *exponential parallelism* and *interference* is what makes quantum computation powerful

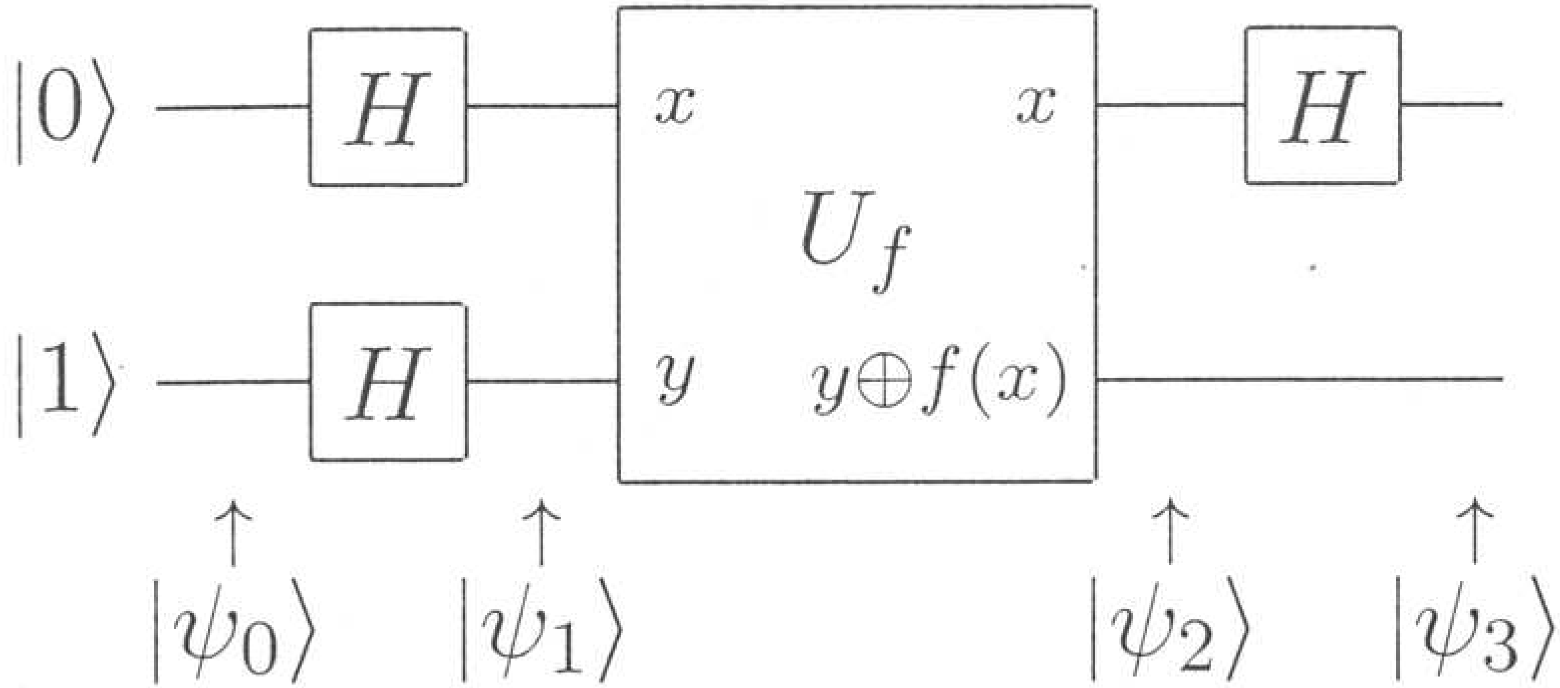
Quantum Algorithms

- Deutsch (1985): two function evaluations for the price of one
- Deutsch-Jozsa (1992): $O(2^n)$ evaluations for the price of one
- Shor (1994): factorizing large numbers
- Grover (1996): unstructured search
- Categories of Quantum Algorithms

Deutsch's Algorithm

- Consider a coin that is either fair (head on one side, tail on the other) or not fair (same on both sides)
- How many times do we need to look at the coin to decide whether it's fair?
- Classically twice - once for each side - but in the quantum world we need only look once - at a superposition of both sides!
- I will describe a simplified and improved version of the original agorithm, due to Cleve, Ekert, Macchiavello and Mosca (1998)
- Represent the coin by a boolean function $f : \{0, 1\} \rightarrow \{0, 1\}$

Deutsch's Algorithm



Deutsch's Algorithm

The input state is

$$|\psi_0\rangle = |0\rangle|1\rangle$$

and after the Hadamard gates we have

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

Now

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

which is easily checked by considering the cases $f(x) = 0$, $f(x) = 1$

Deutsch's Algorithm

Therefore

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

and the final Hadamard gate on the first qubit gives

$$\begin{aligned} |\psi_3\rangle &= \pm|0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \quad \text{if } f(0)=f(1) \\ &= \pm|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \quad \text{if } f(0)\neq f(1) \end{aligned}$$

which we can write as:

Deutsch's Algorithm

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

So by measuring the first qubit we can determine $|f(0) \oplus f(1)\rangle$, and determine a *global property* of $f(x)$ using only *one* evaluation of it.

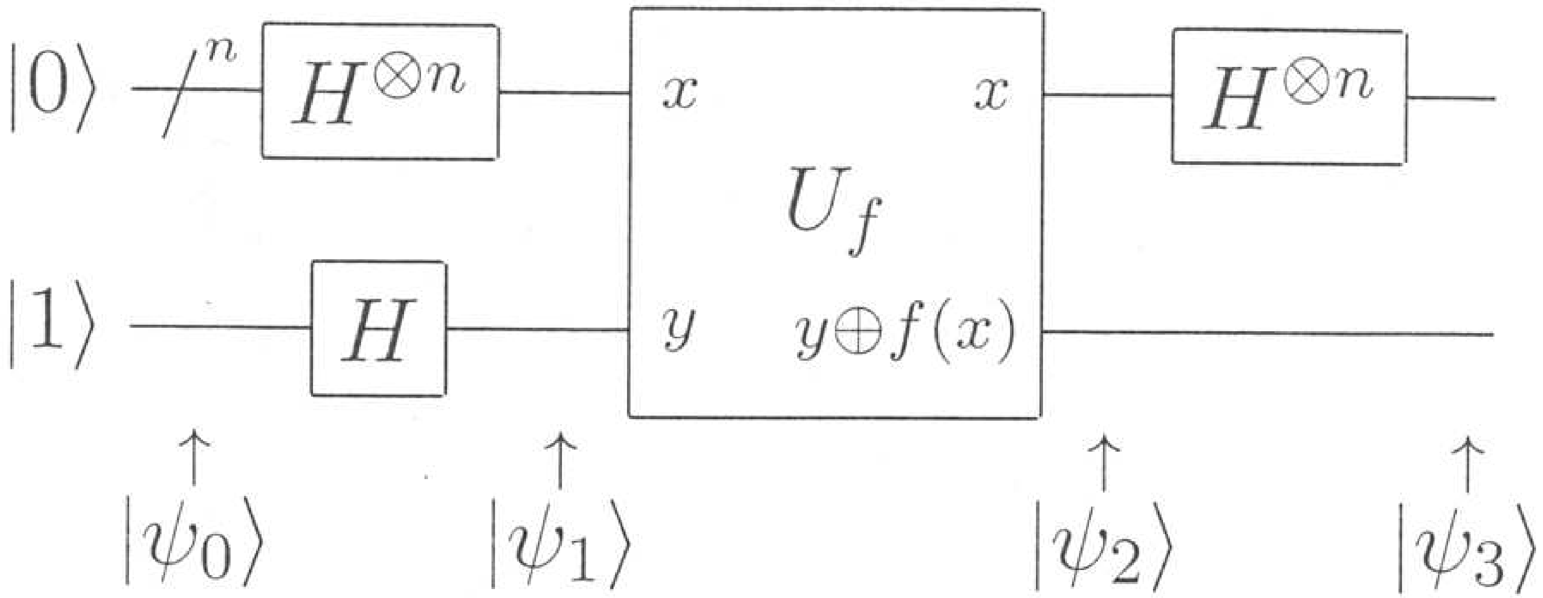
This is faster than any classical apparatus, which would require at least two evaluations.

Cf. classical randomized algorithms, where outcomes $f(0)$ and $f(1)$ exclude each other. In the quantum case they can *interfere* to give a global property. This is the essence of many quantum algorithms.

The Deutsch-Jozsa Algorithm

- A generalisation of Deutsch's algorithm
- Given a function $f : \{0,1\}^n \to \{0,1\}$ which is either *constant* for all values of x or *balanced*, i.e. equal to 1 for exactly half of all possible x, and 0 for the other half
- How many times do we have to evaluate the function (given as a black box) to determine whether it is constant or balanced?
- The circuit is almost identical to that for Deutsch's algorithm, except for an n-bit register for x

The Deutsch-Jozsa Algorithm



The Deutsch-Jozsa Algorithm

- The n-bit output register is zero if an only if f is constant
- Classically $2^{n-1}+1$ evaluations of f are required, but the Deutsch-Jozsa algorithm requires just one evaluation!
- This seems impressive, but this is not a very important problem, with no known applications
- Also, a probabilistic classical computer can quickly determine whether f is constant or balanced with high probability
- Nevertheless, this algorithm contains the seeds of more impressive quantum algorithms