INTRODUCTION TO

QUANTUM COMPUTING AND

QUANTUM INFORMATION

T. C. Dorlas (DIAS)

Workshop on Mathematical Analysis of Transport
in Mesoscopic Systems, Dublin 5-6 December 2008.

QUANTUM COMPUTING

A **qubit** is the quantum state of a two-level system, e.g. a spin-$\frac{1}{2}$ particle. If we choose an orthonormal basis $|0\rangle$, $|1\rangle$ in the (2-dim.) state space, we can write a general qubit as

$$\phi = a_0|0\rangle + a_1|1\rangle,$$

where we can normalise ϕ so that $|a_0|^2 + |a_1|^2 = 1$.

More generally, an n-qubit state is the state of an ensemble of n two-level systems, i.e. a vector in a given 2^n-dimensional Hilbert space. It can be written analogously in the form

$$\phi = \sum_{i_1,\ldots,i_n=0,1} a_{i_1,\ldots,i_n}|i_1,\ldots,i_n\rangle = \sum_{x\in\{0,1\}^n} a_x\,|x\rangle.$$

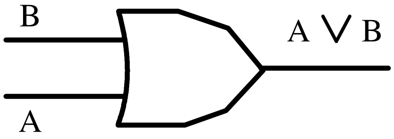
Basic Postulate: *A* **quantum computation** *is the controlled (unitary) evolution of an initially prepared n-qubit state and its subsequent measurement.*

ENTANGLEMENT

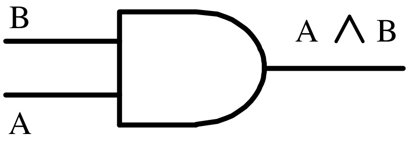
An n-qubit state with $n > 1$ is said to be **entangled** if it is *not* a tensor product of a k-qubit and an $n-k$-qubit ($k < n$). For example, the 2-qubit state $\phi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is entangled. Entanglement is essential for quantum computing.

Boolean Logic

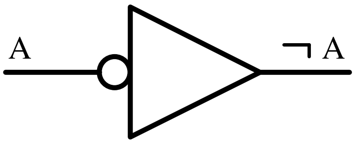
Basic circuit elements:



OR

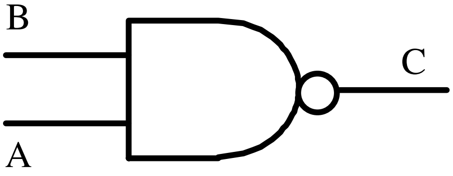


AND

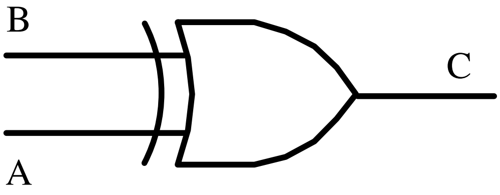


NOT

Two other important gates are:



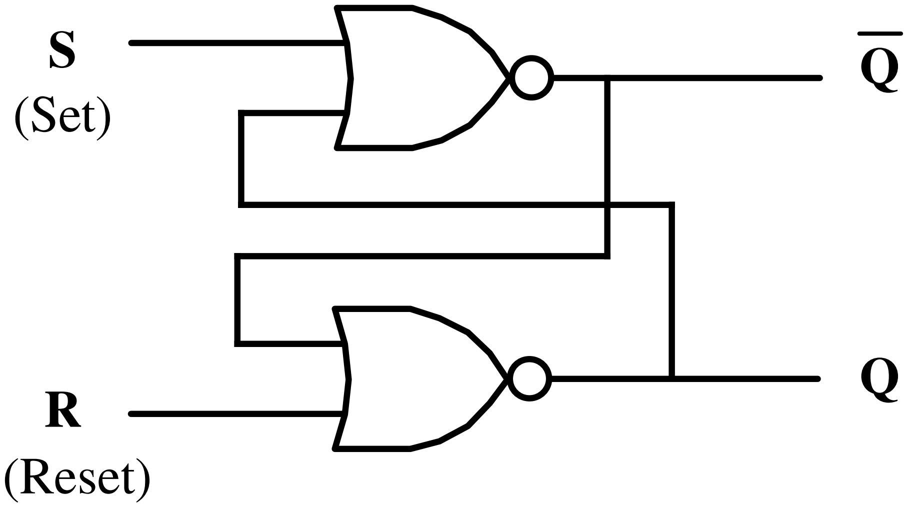
NAND



XOR

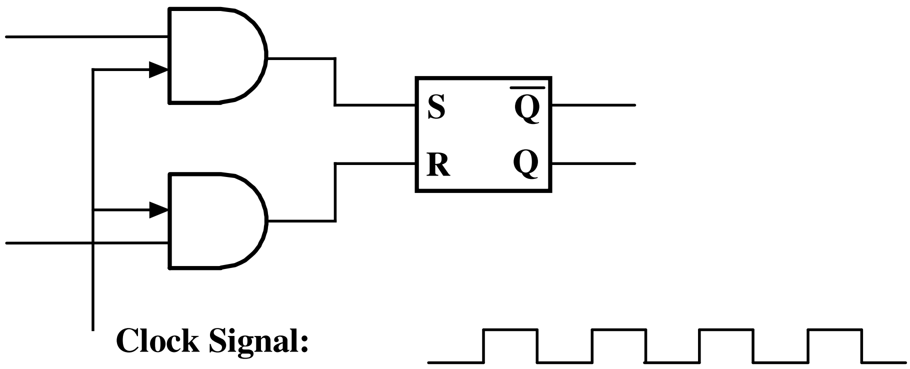
Example: Memory cells

Flip-Flop



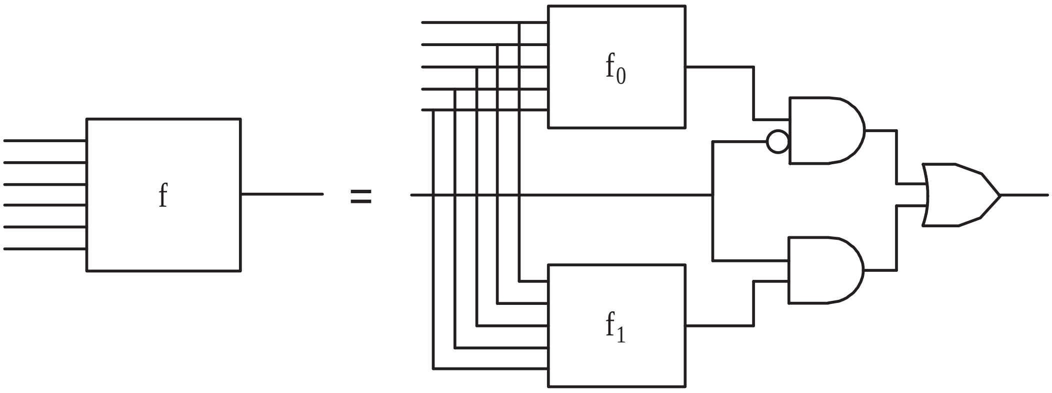
As shown below, flip-flop circuits need a clock signal to operate properly. A combination of such D-type flip-flops can act as a *shift register*.

Clock operation:



Theorem. *Every logical operation $f : \{0,1\}^n \to \{0,1\}^m$ can be expressed in terms of AND, OR and NOT.*

The proof is by induction, and uses the following diagram:



QUANTUM GATES

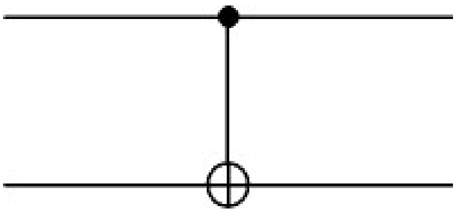
Definition. *A* **quantum gate** *with n inputs and outputs is specified by a unitary operator on an 2^n-dimensional Hilbert space.*

There is no quantum analogue of the classical AND gate, i.e. there is no unitary 4×4-matrix U such that $U|00\rangle = |00\rangle$, $U|01\rangle = |00\rangle$, $U|10\rangle = |10\rangle$ and $U|11\rangle = |11\rangle$.

However, the XOR gate does generalise. It is usually called the **controlled-NOT** gate, and is defined by

$$U_{\mathrm{CN}}|00\rangle = |00\rangle, \quad U_{\mathrm{CN}}|01\rangle = |01\rangle,$$
$$U_{\mathrm{CN}}|10\rangle = |11\rangle, \quad U_{\mathrm{CN}}|11\rangle = |10\rangle.$$

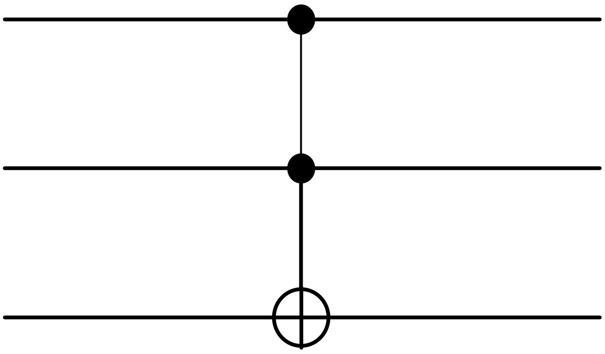
Alternative symbol:



The NOT gate has an obvious quantum analogue, which is a 1-qubit gate. To complete the Boolean algebra, we complement this with the so-called **Toffoli gate** on 3 qubits:

$$\begin{aligned}
U_{\mathrm{Tof}}|000\rangle &= |000\rangle, & U_{\mathrm{Tof}}|001\rangle &= |001\rangle,\\
U_{\mathrm{Tof}}|010\rangle &= |010\rangle, & U_{\mathrm{Tof}}|011\rangle &= |011\rangle,\\
U_{\mathrm{Tof}}|100\rangle &= |100\rangle, & U_{\mathrm{Tof}}|101\rangle &= |101\rangle,\\
U_{\mathrm{Tof}}|110\rangle &= |111\rangle, & U_{\mathrm{Tof}}|111\rangle &= |110\rangle.
\end{aligned}$$

The symbol for a Toffoli gate is as follows:



These gates suffice for generating all Boolean gates, i.e. permutations of basis elements. However, we would like to decompose every quantum gate into elementary gates.

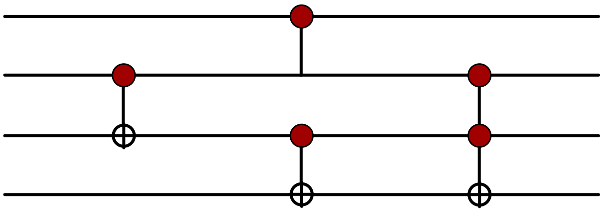
Definition. *A* **quantum circuit** *on n qubits is a collection of quantum gates acting sequentially, each on a subset of the qubits.*

Definition. A set $\{U_1, \ldots, U_n\}$ of quantum gates is called **universal** if any unitary gate U operating on an n-qubit register with arbitrarily large n can be approximated with arbitrary precision $\epsilon > 0$ by a circuit $C_{U,\epsilon}$ consisting of gates from that set.

Example. An example of a quantum circuit on 4 qubits is

$$(\mathbf{1}_2 \otimes U_{\text{Tof}})(U_{\text{CN}} \otimes U_{\text{CN}})(\mathbf{1}_2 \otimes U_{\text{CN}} \otimes \mathbf{1}_2).$$

($\mathbf{1}_2$ is the 2×2 identity matrix.)
This circuit has the following circuit diagram:



Example. The **Hadamard gate** defined by the matrix

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

It cannot be represented as a quantum circuit of NOT gates, CNOT gates, and Toffoli gates.

It is easy to see that any single-qubit gate U can be written in the form

$$U = \Phi(\delta) PS(\alpha) R(\theta) PS(\beta)$$

for real numbers α, β, θ and δ, where $\Phi(\delta) = e^{i\delta}\mathbf{1}$, and

$$PS(\alpha) = \begin{pmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{pmatrix},$$

and

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Theorem. *If δ_0, α_0 and θ_0 are irrational multiples of π, then $\Phi(\delta_0)$, $PS(\alpha_0)$ and $R(\theta_0)$ together with the CNOT gate are universal.*

Outline of the proof. To construct a general $n \times n$ unitary gate U, we diagonalise it in the form

$$U = \sum_{x \in \{0,1\}^n} e^{i\sigma(x)} P_{\psi_x}.$$

Here $e^{i\sigma(x)}$ are the eigenvalues of U, and P_{ψ_x} are one-dimensional projections onto an orthonormal system of eigenvectors ψ_x. Given any normalised vector ψ, let S_{ψ_x} be a unitary matrix such that $S_{\psi_x}\psi_x = |11\ldots 1\rangle$.

Then we can write U as follows:

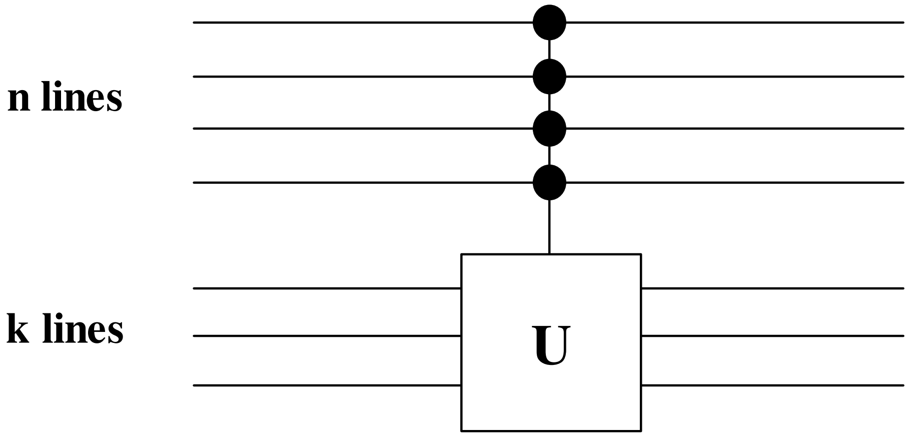
$$U = \prod_{x\in\{0,1\}} S_{\psi_x}^{-1} X_{\sigma(x)} S_{\psi_x},$$

where S_ψ is a unitary such that $S_\psi\psi = |1\ldots 1\rangle$ and where

$$X_{\sigma(x)} = \Lambda_{n-1}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\sigma(x)} \end{pmatrix}.$$

For general k-qubit gate U, $\Lambda_n(U)$ is defined as a block-diagonal $2^{n+k} \times 2^{n+k}$ matrix with one block equal to the 2^n-dimensional identity matrix, and the other equal to U.

The corresponding diagram is



Both $\Lambda_n(U)$ and S_ψ are constructed by induction.

Example. Consider the *inversion about the average operator* D_n. It can be written as $D_n = 2P - I$, where P is the one-dimensional projection onto the vector $(1, \ldots, 1)^T$. Eigenvalues are therefore 1 and -1 ($2^n - 1$ times). In particular,

$$D_2 = \prod_{i=1}^{3} S_{\psi_i}^{-1} \Lambda_1(\sigma^z) S_{\psi_i},$$

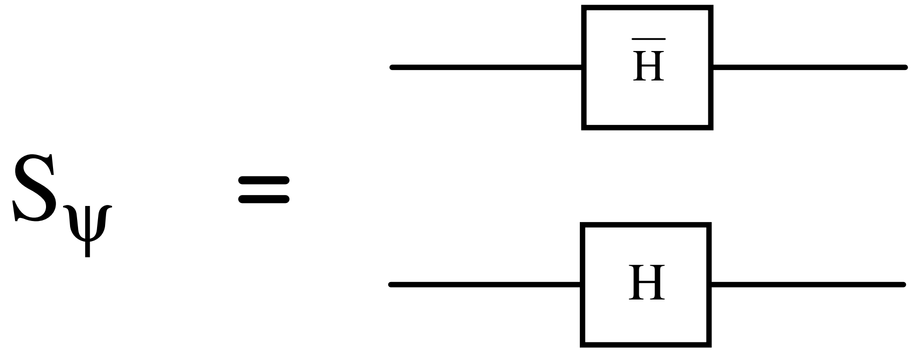
where

$$\psi_1 = \frac{1}{2} \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \psi_2 = \frac{1}{2} \begin{pmatrix} 1 \\ i \\ -1 \\ -i \end{pmatrix}, \psi_3 = \frac{1}{2} \begin{pmatrix} 1 \\ -i \\ -1 \\ i \end{pmatrix}.$$

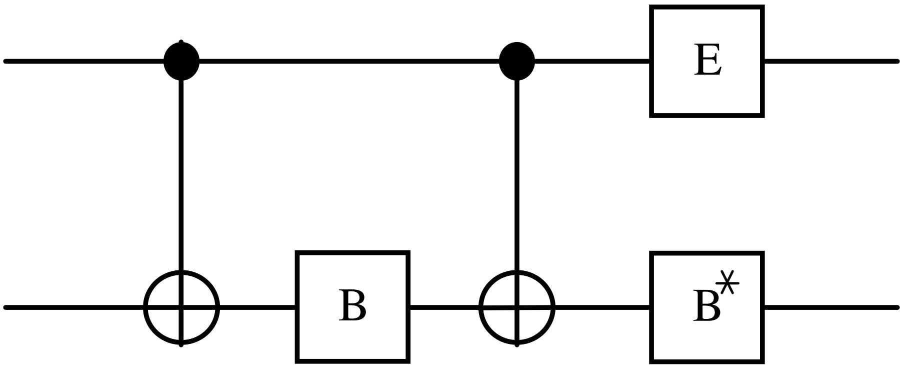
For S_{ψ_1} we can take

$$S_{\psi_1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = U_{\bar{H}} \otimes U_H.$$

Circuit diagram:



The circuit for $\Lambda_1(\sigma^z)$ is more complicated. The circuit diagram is as follows:



In formula this reads as follows:

$$\Lambda_1(\sigma^z) = (E \otimes B^*)\Lambda_1(\sigma^x)(\mathbf{1} \otimes B)\Lambda_1(\sigma^x)$$

with $E = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ and $B = \begin{pmatrix} e^{i\pi/4} & 0 \\ 0 & e^{-i\pi/4} \end{pmatrix}$.

This is seen as follows:

$$
\begin{aligned}
&(E \otimes B^*)\Lambda_1(\sigma^x)(\mathbf{1} \otimes B)\Lambda_1(\sigma^x) = \\
&= \begin{pmatrix} B^* & 0 \\ 0 & iB^* \end{pmatrix} \begin{pmatrix} \mathbf{1} & 0 \\ 0 & \sigma^x \end{pmatrix} \begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix} \begin{pmatrix} \mathbf{1} & 0 \\ 0 & \sigma^x \end{pmatrix} \\
&= \begin{pmatrix} \mathbf{1} & 0 \\ 0 & iB^*\sigma^x B\sigma^x \end{pmatrix} = \begin{pmatrix} \mathbf{1} & 0 \\ 0 & i(B^*)^2 \end{pmatrix} = \begin{pmatrix} \mathbf{1} & 0 \\ 0 & \sigma^z \end{pmatrix}.
\end{aligned}
$$

ALGORITHMS

Grover's Search Algorithm

Problem: *Given a binary function* $f : \{0,1\}^n \to \{0,1\}$ *such that there is a unique* $x_0 \in \{0,1\}^n$ *for which* $f(x_0) = 1$*, determine* x_0*.*

Grover's quantum algorithm for this problem is as follows:
1. Apply H_n to $|0^{(n)}\rangle$ to get $2^{-n/2} \sum_{x \in \{0,1\}^n} |x\rangle$.
2. Apply V_f.
3. Apply the *inversion about the average* operator D_n.
4. Repeat steps 2 and 3 $\lfloor \pi 2^{n/2-2} \rfloor$ times.
5. Measure x. If $f(x) \neq 1$, goto step 1, else $x_0 = x$.

Here the operator D_n is defined by

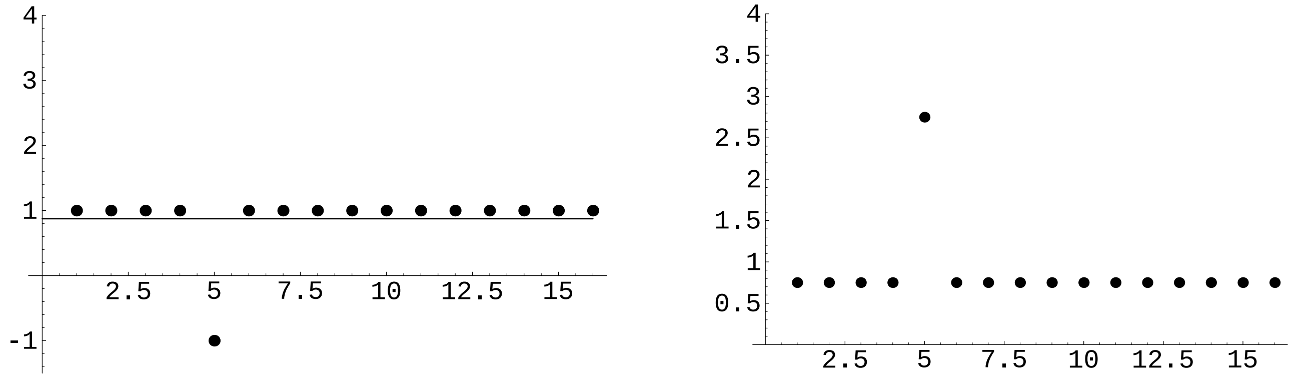
$$D_n \left(\sum_{x \in \{0,1\}^n} a_x |x\rangle \right) = \sum_{x \in \{0,1\}^n} (2M - a_x)|x\rangle,$$

where $M = 2^{-n} \sum_{x \in \{0,1\}^n} a_x$. Moreover, V_f is defined by

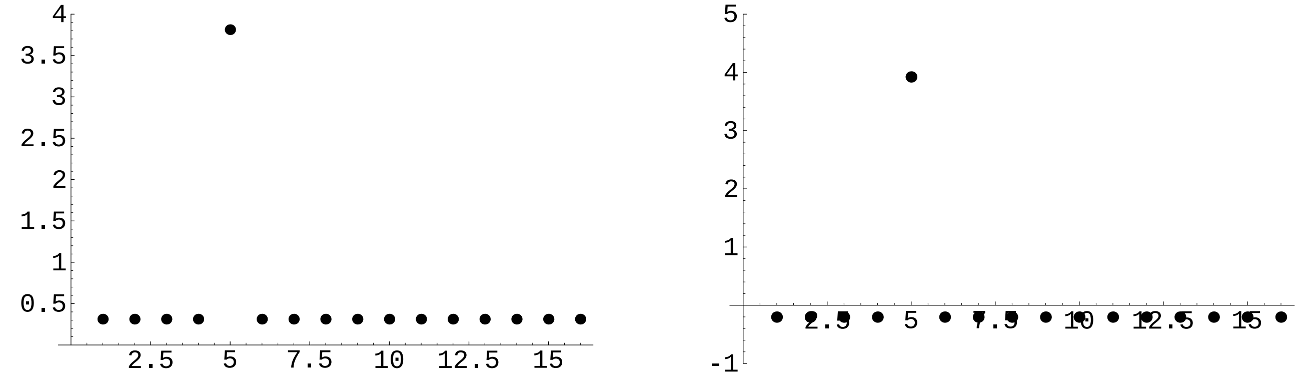
$$V_f \, |x\rangle = (-1)^{f(x)} |x\rangle.$$

Basic idea of the algorithm: V_f changes the sign of the amplitude of $|x_0\rangle$, and D_n reflects all amplitudes about the average.

Example. First iteration of the Grover algorithm:



Second and third iterations of the Grover algorithm.



Shor's Algorithm.

Problem: *Factorise a large integer into prime factors.*

One can show that this problem can be reduced to finding a non-trivial solution of $x^2 \equiv 1 \pmod{n}$.

This in turn can be reduced to finding the period of the function $f_{n,x}(k) = x^k \bmod n$. This is also called the **order** of x, i.e. the smallest r such that $x^r \equiv 1 \pmod{n}$.

Algorithm.

1. Choose $x \in \{2, \ldots, n-1\}$ randomly.
2. Check that $\gcd(x, n) = 1$. If not, then we have a factor of n.
3. Find the period r of $x^k \bmod n$.
4. If r is odd, or $x^{r/2} \equiv \pm 1 \pmod{n}$ then goto 1., otherwise STOP.

If this algorithm stops then $x^{r/2}$ is a non-trivial solution of $x^2 \equiv 1 \pmod{n}$.

To compute the period of $f_{n,x}(k)$, Shor proposed to use the **quantum Fourier transform** defined by

$$QFT_q : |a\rangle \mapsto \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi iac/q} |c\rangle.$$

His algorithm has three stages:

(I) Create a state with the period we need to determine.

(II) Apply the QFT.

(III) Extract the period by measurement and a classical computation.

Example of the Shor algorithm. To explain how this algorithm works, we consider the simple example $n = 143$ and $x = 5$. The steps are as follows:

(I) Start with two registers, each of length $l = \lceil \log n \rceil = 8$, initialised to 0, and apply a Hadamard transform to the first. This yields with $q = 2^l = 256$, $\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, 0\rangle$.

Then applying $U_{f_{n,x}}$ given by

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

we obtain the state

$$\begin{aligned}
&\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \pmod{n}\rangle \\
&= \frac{1}{16} \sum_{j=0}^{14} (|20j, 1\rangle + |20j+1, 5\rangle + \ldots + |20j+15, 34\rangle) + \\
&+ \frac{1}{16} \sum_{j=0}^{13} (|20j+16, 27\rangle + \ldots + |20j+19, 86\rangle).
\end{aligned}$$

(II) Applying the QFT we get

$$\frac{1}{256}\sum_{c=0}^{255}\left[\sum_{j=0}^{12} e^{5\pi icj/32}[|c,1\rangle + \ldots + e^{15\pi ic/128}|c,34\rangle]\right.$$
$$\left. + \sum_{j=0}^{11} e^{5\pi icj/32}[e^{\pi ic/8}|c,27\rangle + \ldots + e^{19\pi ic/128}|c,86\rangle]\right].$$

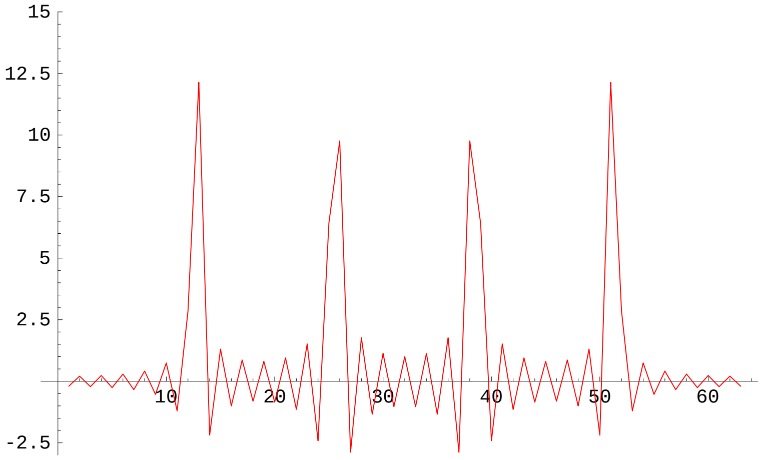
(III) Summing over j we get the functions

$$f(c) = \sum_{j=0}^{12} e^{5\pi icj/32} = \frac{\sin\left(\frac{65}{64}\pi c\right)}{\sin\left(\frac{5}{64}\pi c\right)}$$

and

$$g(c) = \sum_{j=0}^{11} e^{5\pi icj/32} = \frac{\sin\left(\frac{60}{64}\pi c\right)}{\sin\left(\frac{5}{64}\pi c\right)}.$$

These attain maxima at $c = 13, 26, 38, 52$:



A measurement of c therefore leads with high probability to $c = 13, 26, 38$ or $c = 52$, irrespective of what value the second register has. One now determines the period by expanding c/q as a partial fraction:

$$\frac{13}{256} = \frac{1}{19 + \frac{1}{1 + \frac{1}{2 + \frac{1}{4}}}} \approx \frac{1}{20}.$$

One can prove that in general for large n the probability is strongly concentrated near values of c which are very close to multiples of $1/r$. Hence $x = 5^{10} \bmod 143 = 12$ is a solution. Therefore 143 has a common factor with 11 or 13. In fact, both are factors.

IMPLEMENTATION

Many possible implementations have been proposed, e.g.

- Using Nuclear Magnetic Resonance;
- Using trapped ions;
- Using Josephson junctions;
- Using the Quantum Hall effect;
- Using quantum dots.

The proposal by Cirac and Zoller using trapped ions:

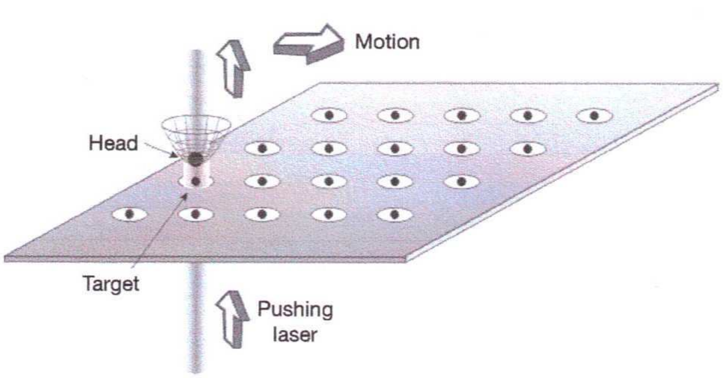
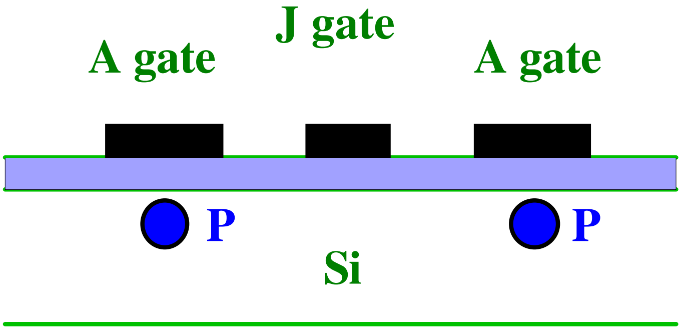


Figure 2 Scalable quantum computer. We envisage a two-dimensional array of independent ion traps[23], and a different ion (Head) that moves above this plane, approaching any particular ion. By switching on a laser propagating in the perpendicular direction to the plane, we can perform the two-qubit gate between the target ion and the head as explained above. In particular, we can swap the state of that ion to the head, which immediately allows us to perform entanglement operations between distant ions.

Kane's NMR computer:



(1) A-gates control the hyperfine interaction;

(2) J-gates turn on and off electron-mediated coupling between nuclear spins;

(3) A global a.c. magnetic field flips nuclear spins at resonance.