Introduction to quantum computing

R. Vilela Mendes

Quantum computation basic features

Classical computers: a *bit* is a unit of information, takes values 0 or 1.
Quantum computers: a **qubit** corresponds to a two-state system, that is, a unit vector in the space C^2
$|0\rangle \leftrightarrow (1,0)$
$|1\rangle \leftrightarrow (0,1)$
(Notice the existence of states $\alpha|0\rangle + \beta|1\rangle \quad \forall \alpha, \beta \in C$
(**Superposition**)
For n qubits the space would be $C^2 \otimes C^2 \otimes \cdots \otimes C^2$.
Factorizable states

$$(\alpha_1|0\rangle + \beta_1|1\rangle) \times (\alpha_2|0\rangle + \beta_2|1\rangle)$$

Non-factorizable states.
(**Entanglement**)

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

Quantum computation basic features

The state

$$\frac{1}{\sqrt{2^n}} \sum_{i_1, i_2, \ldots, i_n = 0}^{1} |i_1, i_2, \ldots, i_n\rangle$$

is a superposition of all basis states of n qubits. Applying a unitary operation U_f : (**Reversible**)

$$\frac{1}{\sqrt{2^n}} \sum_{i_1, i_2, \ldots, i_n = 0}^{1} |i_1, i_2, \ldots, i_n\rangle \longmapsto \frac{1}{\sqrt{2^n}} \sum_{i_1, i_2, \ldots, i_n = 0}^{1} |f(i_1, i_2, \ldots, i_n)\rangle.$$

Applying U_f once computes f simultaneously on all the 2^n possible inputs (**Exponential Parallelism**)
To extract the exponential information one has to *observe* the system (*collapse of the wave function*)
Interference : exponentially many computations done in parallel may cancel in such a way that only the computations we are interested in remain. *It is the combination of exponential parallelism and interference what makes quantum computation powerful.*

A Model of Quantum Computation

System of two-state quantum particles (*qubits*)
n qubits$\in \mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \cdots \otimes \mathcal{C}^2$
Natural basis (2^n vectors) :

$$
\begin{aligned}
&|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle \\
&|0\rangle \otimes |0\rangle \otimes \cdots \otimes |1\rangle \\
&\vdots \ldots\ldots\ldots\ldots \\
&|1\rangle \otimes |1\rangle \otimes \cdots \otimes |1\rangle
\end{aligned}
$$

Denote

$$|i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle = |i_1, i_2, \ldots, i_n\rangle \equiv |i\rangle$$

$i_1, i_2, \ldots, i_n =$ binary representation of the integer i, between 0 and $2^n - 1$ (encoding of integers)
General state :

$$\sum_{i=0}^{2^n-1} c_i |i\rangle \qquad\qquad \sum_i |c_i|^2 = 1$$

Initial state :

$$|i\rangle$$

Elementary operations $\rightarrow$ **logical gates**

Quantum evolution of an isolated system is described by a unitary matrix $UU^\dagger = I$

Quantum gate on k qubits = unitary matrix U of dimension $2^k \times 2^k$

(1) *NOT* **gate** (operating on one qubit)

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

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Then $NOT|0\rangle = |1\rangle$ and $NOT|1\rangle = |0\rangle$

$$NOT(c_0|0\rangle + c_1|1\rangle) = c_0|1\rangle + c_1|0\rangle.$$

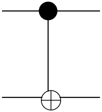
NOT gate operating on the first qubit of $\sum_i c_i|i_1 i_2 \ldots i_n\rangle$

$$\sum_i c_i(NOT|i_1\rangle)|i_2 \ldots i_n\rangle = \sum_i c_i|\neg i_1 i_2 \ldots i_n\rangle$$

(2) The controlled ***NOT*** **gate** (CNOT, acting on two qubits)
Computes the function: $(a, b) \longmapsto (a, a \oplus b)$
$(a \oplus b = (a + b) \bmod 2)$ with $a, b \in 0, 1$

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \rightarrow \begin{matrix} 00 \\ 01 \\ 10 \\ 11 \\ \text{control;target} \end{matrix}$$

(also called the *exclusive or* XOR gate). Applies a *NOT* on the second (*target*) bit conditioned that the first (*control)* bit is 1
Black circle → control bit



A Model of Quantum Computation

All classical Boolean functions can be transformed to quantum gates. Classical reversible gates make a permutation on classical strings. Are unitary. Non-reversible functions may be converted to reversible functions. A function f from n bits to m bits goes to a reversible function from $n+m$ bits to $n+m$ bits:

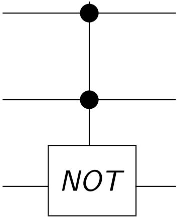
$$f : i \longmapsto f(i) \qquad \Longrightarrow \qquad f_r : (i,j) \longmapsto (i, f(i) \oplus j).$$

(3) **The AND gate**, $(a,b) \longmapsto ab$ becomes **the Toffoli gate** $(a,b,c) \longmapsto (a,b,ab \oplus c)$, described by a unitary matrix on three qubits:

$$T = \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 0 & 1 \\ & & & & & & 1 & 0 \end{pmatrix} \rightarrow \begin{matrix} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{matrix}$$

The Toffoli gate applies NOT to the last bit, conditioned that the other bits are 1

The Toffoli gate



A Model of Quantum Computation

(4) A non-classical gate: a general **rotation** on one qubit:

$$G_{\theta,\phi} = \begin{pmatrix} \cos(\theta) & \sin(\theta)e^{i\phi} \\ -\sin(\theta)e^{-i\phi} & \cos(\theta) \end{pmatrix}$$

- **Quantum computation = sequence of elementary quantum gates on the qubits**

$$|i\rangle \to |\alpha\rangle \in C^{2^n}$$

To extract the output from this state $\to$ *measurement*

If $|\alpha\rangle = \sum_i c_i |i_1, \ldots i_n\rangle$, a measurement of the first qubit gives 0 with probability $\mathrm{Prob}(0) = \sum_{\mathrm{i_2,\ldots i_n}} |\mathrm{c_{0,i_2,\ldots i_n}}|^2$, and $|\alpha\rangle$ collapses to

$$\frac{1}{\sqrt{\mathrm{Prob}(0)}} \sum_{i_2,\ldots i_n} c_{0,i_2,\ldots i_n} |0, i_2, \ldots i_n\rangle,$$

and gives 1 with probability $\mathrm{Prob}(1) = \sum_{\mathrm{i_2,\ldots i_n}} |\mathrm{c_{1,i_2,\ldots i_n}}|^2$, $|\alpha\rangle$ collapsing then to

$$\frac{1}{\sqrt{\mathrm{Prob}(1)}} \sum_{i_2,\ldots i_n} c_{1,i_2,\ldots i_n} |1, i_2, \ldots i_n\rangle,$$

A Model of Quantum Computation

Example :

$$\frac{1}{\sqrt{3}}\left(|00\rangle + |01\rangle - |11\rangle\right)$$

The probability to measure 0 in the left qubit is 2/3, and the probability to measure 1 is 1/3. Afterwards the state collapses to $\frac{1}{\sqrt{2}}\left(|00\rangle + |01\rangle\right)$ with probability $\Pr(0) = 2/3$ and to $-|11\rangle$ with probability $\Pr(1) = 1/3$.
The output is in general probabilistic
(5) **Hadamard gate**: a quantum subroutine that generates a random bit.

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

Applying the gate on a qubit in the state $|0\rangle$ or $|1\rangle$, yields $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.
A measurement of this qubit yields a random bit.

Universal quantum gates

Classical reversible computation

There is a single universal gate (the Toffoli gate). It computes the function

$$a, b, c \longmapsto a, b, ab \oplus c.$$

Any reversible function can be represented as a concatenation of Toffoli gates on different inputs

For the AND gate on a, b, input $c = 0$, and the last bit contains $ab \oplus 0 = AND(a, b)$

For the NOT gate (on the third bit), set the first two bits to 1

Now the NOT and AND gates are universal.

Quantum case

Here the operations are continuous

A unitary matrix U is approximated to within ε by U' if $|U - U'| \leq \varepsilon$

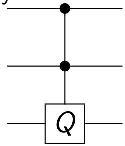
Because unitary evolution preserves the norm, if S gates are used it suffices to approximate each one to within $O(\frac{\varepsilon}{S})$

A set of quantum gates is called universal if for any ε and any U, U can be approximated to within ε by a sequence of gates of the set

Several different sets

Examples:

1) D. Deutsch; Proc. Roy. Soc. London A 425 (1989) 73



The *NOT* matrix in the Toffoli gate is replaced by another unitary matrix on one qubit, Q, such that Q^n approximates any $2 \otimes 2$ matrix. Consider the two following matrices :

$$R = \begin{pmatrix} \cos(2\pi\alpha) & \sin(2\pi\alpha) \\ -\sin(2\pi\alpha) & \cos(2\pi\alpha) \end{pmatrix}, W = \begin{pmatrix} 1 & 0 \\ 0 & e^{i2\pi\alpha} \end{pmatrix}.$$

α irrational, chosen such that the sequence

$$\alpha \bmod 1, 2\alpha \bmod 1, 3\alpha \bmod 1, \cdots$$

hits the ϵ-neighborhood of any number in $[0, 1]$, within poly$(\frac{1}{\epsilon})$ steps.

The generalized Toffoli gates $\{R_n, W_n\}$ *with* $Q = R$ *and* W *are a universal set*

Sketch of the proof :

With R any rotation in the real plane is approximated, and with W any rotation in the complex plane.

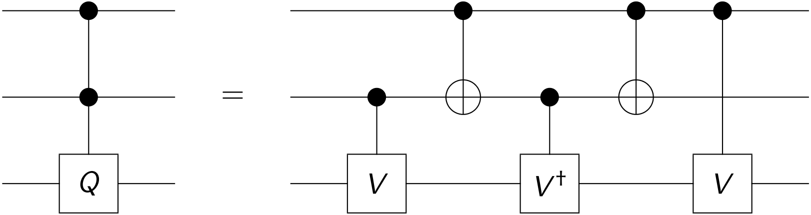
Consider $\{R_3, W_3\}$. Given an arbitrary 8×8 unitary matrix U, denote its eigenvectors as $|\psi_j\rangle$ with eigenvalues $e^{i\theta_j}$. U is determined by $U|\psi_j\rangle = e^{i\theta_j}|\psi_j\rangle$. Define $U_k|\psi_j\rangle = \begin{cases} |\psi_j\rangle & \text{if } k \neq j \\ e^{i\theta_k}|\psi_k\rangle & \text{if } k = j \end{cases}$. Then $U = U_7 U_6 \dots . U_0$.

U_k can be achieved by first taking $|\psi_k\rangle$ to $|111\rangle$ by a transformation T. Then apply W the correct number of times to approximate $|111\rangle \longmapsto e^{i\theta_k}|111\rangle$ and then we take $|111\rangle$ to $|\psi_k\rangle$ by T^{-1}

T is constructed with W and R. Therefore all three qubit operations are approximated.

By the same reasoning $\{R_n, W_n\}$ is dense in $U(2^n)$ and $\{R_n, W_n\}$ is obtained from $\{R_3, W_3\}$ by recursion. ■

2) There is a sequence of two bit gates that constructs a matrix on three qubits of the form of a generalized Toffoli gate:



where $V = \sqrt{Q}$. Thus, *two-qubit gates are universal*.

Universal quantum gates

3) One-qubit matrix conditioned on other qubit can be expressed as a sequence of one-qubit matrices and $CNOT'$s. So the generalized Toffoli gate of Deutsch can be written as a finite sequence of one-qubit gates and $CNOT'$s. This shows that

$$\{\text{One-qubit gates, } CNOT\} \text{ is universal}$$

(Barenco et al.; Phys. Rev. A 52, 3457 (1995))

Preparation of initial states and discrete Fourier Transform
Given $|i\rangle$, applying the Hadamard gate to each one of the qubits one obtains

$$|i\rangle \xrightarrow{FT} \frac{1}{\sqrt{N}} \sum_{j} (-1)^{i \cdot j} |j\rangle$$

i, j strings of length n and $i \cdot j = \sum_{k=1}^{n} i_k j_k \ mod \ 2$
(Discrete Fourier transform over the group Z_2^n)
$FT^{-1} = FT$
If $|i\rangle = |0^n\rangle$ one obtains $\frac{1}{\sqrt{N}} \sum_{i=1}^{2^n} |i\rangle$

Deutsch and Jozsa's algorithm

> *f a Boolean function from $\{1, N\}$ to $\{0, 1\}$ ($N = 2^n$). It is asserted that $f(i)$ is either constant or balanced (half are 0 and half are 1). Distinguish between the two cases.*

Query to an oracle : $|i\rangle|j\rangle \longmapsto |i\rangle|j \oplus f(i)\rangle$
(A classical algorithm needs $O(N)$ queries)

Quantum algorithm :
$|0^n\rangle \otimes |1\rangle$
Apply Fourier transform on the first register
Apply Hadamard to the last qubit
$\Longrightarrow \qquad \frac{1}{\sqrt{N}} \sum_{i=1}^{2^n} |i\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right)$
Call the oracle $\rightarrow |i\rangle|j\rangle \longmapsto |i\rangle|j \oplus f(i)\rangle$
$\Longrightarrow \qquad \frac{1}{\sqrt{N}} \sum_{i=1}^{2^n} (-1)^{f(i)} |i\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right)$
Apply the inverse Fourier transform to the first register
$\Longrightarrow \qquad |\psi\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right)$
Measure the first register
If the result is $0^n \Longrightarrow f$ is CONSTANT
Else $\Longrightarrow f$ is BALANCED
Measurement is done by projecting on $|0^n\rangle$. If f is constant the probability is one. If f is balanced the probability is zero.

The RSA cryptosystem (Rivest, Shamir, Adleman, 1977)

Public key system (trapdoor one-way function). Security based on the difficulty of factoring large integers, $t(n) \sim \exp\left(n^{1/3}\right)$

\# AT THE RECEIVER END

Pick $N = pq$, p and q two distinct large odd primes

Choose at random E coprime with $\phi(N) = (p-1)(q-1)$

Compute $B = E^{-1} \bmod \phi(N)$

PUBLIC KEY $= (E, N)$

PRIVATE KEY $= (B, N)$

Broadcast public key, keep private key for yourself

\# SENDER

Code each symbol in the message as a number from 0 to $n-1$ according to some known code $\{M_i\}$

Compute $\{C_i = M_i^E \bmod N\}$

Send $\{C_i\}$

\# RECEIVER

Compute $\{C_i^B \bmod N = M_i\}$

Cracking RSA with quantum computers

- Let the message be M^E
- Find order r of $M^E \bmod N$ (r is also the order of M because E is coprime to $(P-1)(Q-1)$)
- Find $D' = E^{-1} \bmod r$ (Euclid's algorithm)
- $\left(M^E\right)^{D'} = M \bmod N$ (because $M^r = 1 \bmod N$)

Finding order $\bmod N$. Shor's algorithm

Basic idea: create a state with periodicity r and then apply Fourier transform over Z_Q to reveal the periodicity

Fourier transform over Z_Q

$$|a\rangle \rightarrow \frac{1}{\sqrt{Q}} \sum_{b=0}^{Q-1} e^{2\pi i a b / Q} |b\rangle$$

Shor's algorithm

- $|\overrightarrow{0}\rangle \otimes |\overrightarrow{0}\rangle$
- Apply Fourier transform over Z_Q on the first register $\frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} |l\rangle \otimes |\overrightarrow{0}\rangle$
- Call subroutine that computes $|l\rangle|d\rangle \to |l\rangle|d \oplus Y^l \bmod N\rangle$ $\frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} |l\rangle \otimes |Y^l \bmod N\rangle$
- Measure the second register $\frac{1}{\sqrt{A}} \sum_{l=0|Y^l=Y^{l_0}}^{Q-1} |l\rangle \otimes |Y^{l_0}\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |jr + l_0\rangle \otimes |Y^{l_0}\rangle$
- Apply Fourier tarnsform over Z_Q on the first register $\frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} \left(\frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} e^{2\pi i (jr+l_0)k/Q} \right) |k\rangle \otimes |Y^{l_0}\rangle$
- Measure the first register. Let k_1 be the result.
- Approximate the fraction $\frac{k_1}{Q}$ by a fraction with denominator smaller than N using continued fractions.
- If the denominator d does not satisfy $Y^d = 1 \bmod N$, throw it away. Else call the denominator r_1.
- Repeat all previous steps poly(log(N)) times to get $r_1, r_2, r_3, \ldots$
- Output the minimal r.

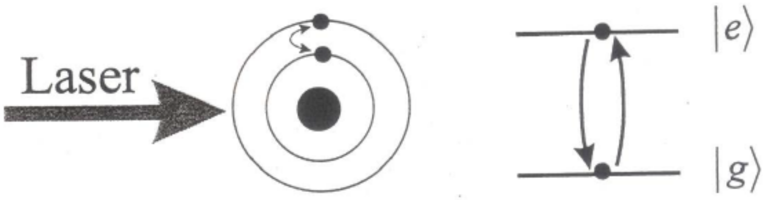
Cold trapped ions, quantum dots, nuclear magnetic resonance, superconducting qubits, optical qubits, $\cdots$

Requirements

- To store qubits reliably
- A set of universal gates
- Reliable measurement of the qubit states
- Error correction to compensate for decoherence effects

One-qubit quantum gates on single atoms

Rabi oscillations



Physical implementations of quantum computation

$$\begin{pmatrix} |g\rangle \\ |e\rangle \end{pmatrix} \rightarrow \begin{pmatrix} \cos(\Omega_R t)|g\rangle + \sin(\Omega_R t)|e\rangle \\ -\sin(\Omega_R t)|g\rangle + \cos(\Omega_R t)|e\rangle \end{pmatrix}$$

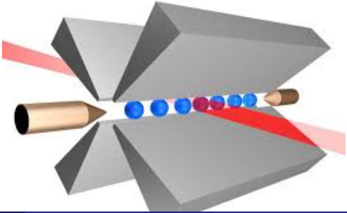
For $\Omega_R t = \frac{\pi}{2}$ it is the transformation $\overline{H}=\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$

Together with phase shifts

$$\begin{pmatrix} |g\rangle \\ |e\rangle \end{pmatrix} \rightarrow \begin{pmatrix} |g\rangle \\ \exp(i\theta)\,|e\rangle \end{pmatrix}$$

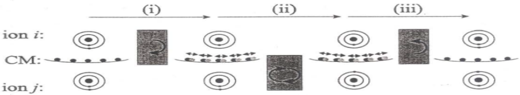
by non-resonant laser field $\Longrightarrow$ all unitary transformations on one-qubit

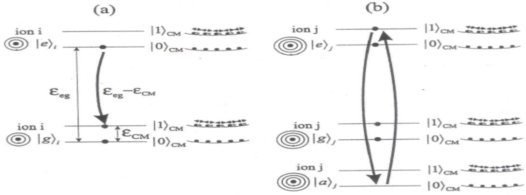
The ion trap



The conditional sign gate (CS)

$$\begin{pmatrix} |0_i 0_j\rangle \\ |0_i 1_j\rangle \\ |1_i 0_j\rangle \\ |1_i 1_j\rangle \end{pmatrix} \rightarrow \begin{pmatrix} |0_i 0_j\rangle \\ |0_i 1_j\rangle \\ |1_i 0_j\rangle \\ -|1_i 1_j\rangle \end{pmatrix}$$

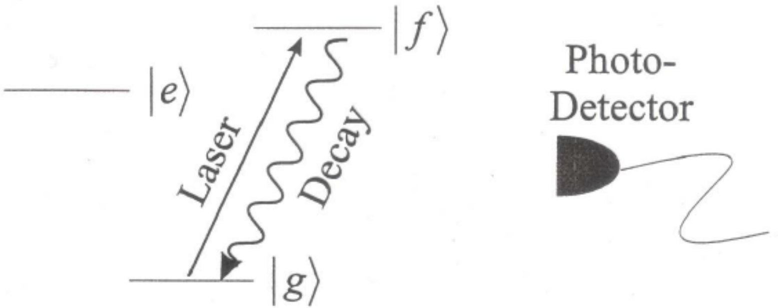




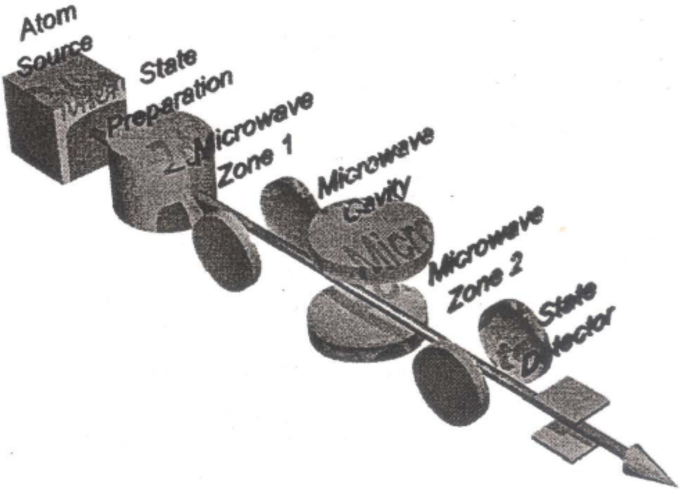
CNOT $= \overline{H} \circ$ CS $\circ \, \overline{H}$

$$\begin{array}{l} |g_i g_j\rangle|0\rangle \\ |g_i e_j\rangle|0\rangle \\ |e_i g_j\rangle|0\rangle \\ |e_i e_j\rangle|0\rangle \end{array} \rightarrow \begin{array}{l} |g_i g_j\rangle|0\rangle \\ |g_i e_j\rangle|0\rangle \\ |g_i g_j\rangle|1\rangle \\ |g_i e_j\rangle|1\rangle \end{array} \rightarrow \begin{array}{r} |g_i g_j\rangle|0\rangle \\ |g_i e_j\rangle|0\rangle \\ |g_i g_j\rangle|1\rangle \\ -|g_i e_j\rangle|1\rangle \end{array} \rightarrow \begin{array}{r} |g_i g_j\rangle|0\rangle \\ |g_i e_j\rangle|0\rangle \\ |e_i g_j\rangle|0\rangle \\ -|e_i e_j\rangle|0\rangle \end{array}$$

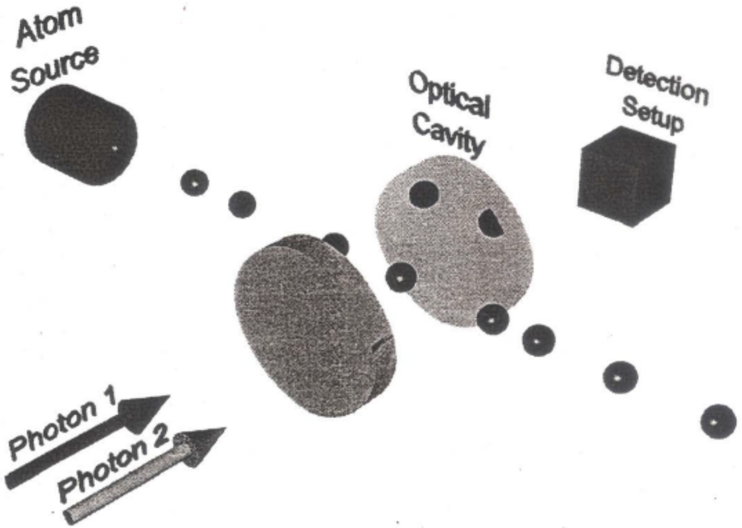
Measuring the qubits. The quantum-jump technique



Flying qubits
Atoms

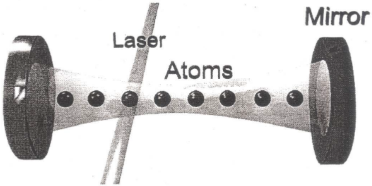


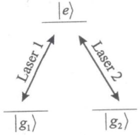
Photons


Atom
Source
Optical
Cavity
Detection
Setup
Photon 1
Photon 2

Physical implementations of quantum computation

Cavity quantum electrodynamics





Other implementations. See for example
http://quantum.phys.cmu.edu/QCQI/QC_CMU1