# Quantum computing for physics research

Bertrand Georgeot

Quantware group, Lab. de Physique Théorique, UMR 5152 du CNRS
Université Paul Sabatier, Toulouse, France www.quantware.ups-tlse.fr

Permanent researchers: Bertrand Georgeot, Dima Shepelyansky (researchers CNRS), Daniel Braun, Klaus Frahm, Robert Fleckinger (professors UPS),

Non permanent researchers: Olivier Giraud, José Lages (postdocs), Oleg Zhirov (visitor) Marcello Terraneo, Stefano Bettelli, Jae-Won Lee (former postdocs) Benjamin Lévi, Andrei Pomeransky (former PhD students)

SUPPORT: ARO/NSA/ARDA (USA), IST-FET EDIQIP (EU), RTN (EU), ACI (France)

- Quantum algorithms for physical systems: complex systems show generically classical or quantum chaos. How to simulate them? What new information can be gained?
- Real quantum computers run with errors and imperfections: dynamical errors different from static imperfections. Effect of these errors on a computation? Appearance of a quantum chaos regime?

# Brief idea of quantum computing...

- A quantum computer is not only **faster** than classical devices, it is **something else**: new computer science, with new properties $\Rightarrow$ may change **complexity class** of problems
- The efficiency of quantum computation compare to classical computation **depends on the problem**: to benefit from the power of quantum computation, one should ask **certain types of questions.**
- Can be realized in **many different quantum physical systems**
- **But:** much more sensitive to noise than classical computers $\Rightarrow$ **enormous experimental challenge**, but **no physical reason** why it should not be realizable
- Important applications: **code-breaking**, **simulation of physical systems**

## Why a quantum computer?

- smaller and smaller size of processors in classical computers $\Rightarrow$ quantum scale will be reached eventually
- easier to simulate quantum mechanics on quantum computers (Feynman)
- massive gain of computing time on some non-quantum problems (Shor, Grover)
- gives insight on quantum mechanics

# Quantum computer

- **classical computer**: building blocks: **bits** $0$ **or** $1$
- **quantum computer**: building blocks: **qubits = two-level system** $|0>$ **et** $|1>$
  Any state of the form $(\alpha|0\rangle + \beta|1\rangle)$ is allowed, but **measurement** gives only one value (with probabilities $|\alpha|^2$ and $|\beta|^2$).
- The power of quantum computation **does not come** from the continuous range of values of $\alpha, \beta$. Quantum computer are effectively **digital**.
- A quantum computer can be thought as a set of $n$ qubits (Hilbert space of dimension $N = 2^n$). General quantum state of the computer: $\sum_{i=0}^{N-1} a_i|i\rangle$ with $\sum_{i=0}^{N-1} |a_i|^2 = 1$.
- **Logical operations**: **unitary transformations** in Hilbert space $\Rightarrow$ **reversible computation**, no dissipation ($\neq$ classical computation). Only source of irreversibility comes from quantum measurements.
- **Quantum information theory** $\Rightarrow$ The information contained in a quantum state can be measured in units of qubits

# Quantum gates

One acts on the wave function of the quantum computer through **unitary transformation**. In practice, one uses **elementary quantum gates** which are **local** and compose them to build the unitary evolution needed.

- **Hadamard gate** applied to one qubit $|0\rangle \longrightarrow (|0\rangle + |1\rangle)/\sqrt{2}$; $|1\rangle \longrightarrow (|0\rangle - |1\rangle)/\sqrt{2}$;
- **phase gate** applied to one qubit $|0\rangle \longrightarrow |0\rangle$; $|1\rangle \longrightarrow i|1\rangle$;
- **controlled not** or **CNOT** applied to two qubits: $|00\rangle \longrightarrow |00\rangle$; $|01\rangle \longrightarrow |01\rangle$;$|10\rangle \longrightarrow |11\rangle$; $|11\rangle \longrightarrow |10\rangle$; the second qubit is changed if the first is in the state $|1\rangle$;
- **controlled controlled not** or **Toffoli gate** applied to three qubits: the third qubit is changed if the first two are both in the state $|1\rangle$.

**Universal** sets of quantum gates are enough to build any unitary transformations (for example, one-qubit gates +CNOT). **Different** universal sets are possible, their choice depends on experimental implementations.

# Quantum superposition

**SUPERPOSITION PRINCIPLE** : $\Rightarrow$ Possibility of manipulation of **many registers** at the same time

$n$ qubits $\Rightarrow N = 2^n$ states such as $|00100...\rangle$

**Quantum states**: of the form $\Sigma_{i=0}^{N-1} a_i |i>$; information is contained in the amplitudes $a_i$ associated to the registers. **To act on $N$ such amplitudes:**

- **Classical**: $N$ operations needed
- **Quantum**: possible in $1$ operations

$\longrightarrow$ **Exponential** gain (in computing time) possible

# Quantum entanglement

Qubits can present correlations impossible to obtain classically (cf Bell's theorem)

- Entanglement of a quantum state describes its degree of non-factorizability in products of one-qubit states.
- Example: Einstein-Podolsky-Rosen paradox; measuring one qubit of the state $(|00\rangle + |11\rangle)/\sqrt{2}$ influences the other one, whatever their distance.
- Entanglement can be **quantified** (although there are competing ways of doing it). It is crucial for, say, quantum teleportation.
- Entanglement is believed to be a key resource in quantum computation, but it is not clearly understood exactly how.

# Classical algorithms

- Modify strings of bits $0$ and $1$ through possibly irreversible transformations ($\Rightarrow$ dissipation, heat production)
- Input: chain of $N$ bits $\Rightarrow n = \log_2 N$ size of the input
- Modifies the input in $M$ operations $\Rightarrow$ **complexity**

  $M$ polynomial in $n = \log_2 N \Rightarrow$ **polynomial** algorithm (complexity class P) (example: arithmetic operations,...)

  $M$ exponential in $n \Rightarrow$ **exponential** algorithm (example: factoring, traveling salesman,...)
- Millenium problem: $P = NP$
- Classical complexity result: complexity class does not depend on the device

# Quantum algorithms

$n$ qubits $\Rightarrow N = 2^n$ quantum basis states such as 011001...

Procedure to perform an algorithm:

- Build an initial state $|\Psi_i >= \sum_{i=0}^{N-1} a_i |i >$. Example: $1/\sqrt{N} \sum_{i=0}^{N-1} |i >$ (uniform superposition) can be build from $|00..00\rangle$ by application of $n$ Hadamard gates.
- Transform it $|\Psi_i > \longrightarrow |\Psi_f >= \sum_{i=0}^{N-1} b_i |i >$ through a sequence of elementary (local) quantum gates
- Extract information by quantum measurement of $|\Psi_f >$

The result is usually **probabilistic**: quantum measurement gives the right result with a certain probability. The algorithm works if 1) one can **recognize** the right result when it comes and 2) the probability of success is **significant** (especially when $n$ increases).

**Complexity** of the algorithm is measured by the number of quantum gates needed, taking into account that the process may have to be **iterated** since the result is probabilistic.

# Example: adding numbers

**Problem**: add all numbers between 0 and N-1=$2^n$-1; needs **three registers** of n, n+1 and n-1 qubits

- **start** from $|000...000\rangle$
- Apply $2n$ Hadamard gates $\Rightarrow 1/N \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} |i\rangle|j\rangle|0...000\rangle$
- Apply sequence of CNOT (addition mod 2 of bits) and Toffoli gates (putting the carries on the third register), put the sum most significant bit on the second register, then reverse the gates to put the third register to 0 while building the sum on the second register.
- The result is $1/N \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} |i\rangle|i+j\rangle|0...000\rangle$

$\longrightarrow$ Needs only $\approx 8n$ quantum gates to perform $N^2$ additions

$\longrightarrow$ The third (workspace) register is reset to 0 at the end

$\longrightarrow$ Everything is reversible

$\longrightarrow$ Multiplications and exponentiations can be done in the same way, by using binary decomposition $\Rightarrow$ need $\sim n^2$ (multiplication) and $\sim n^3$ quantum gates (exponentiation).

# Quantum addition

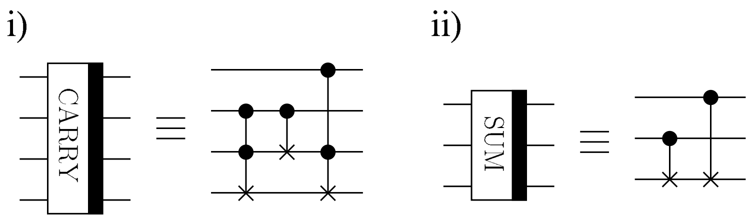



Figure 3)

V. Vedral, A. Barenco and A. Ekert

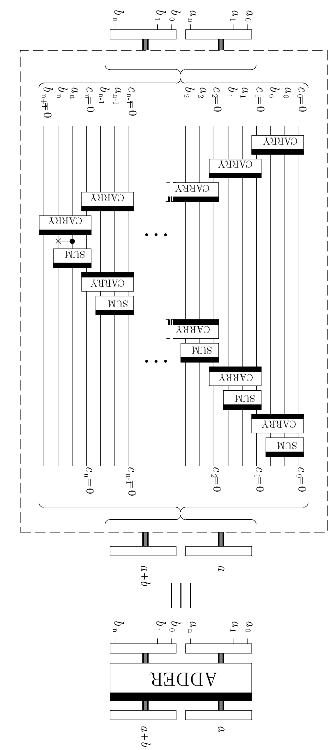



Figure 2)

V. Vedral, A. Barenco and A. Ekert

# Quantum multiplication and exponentiation

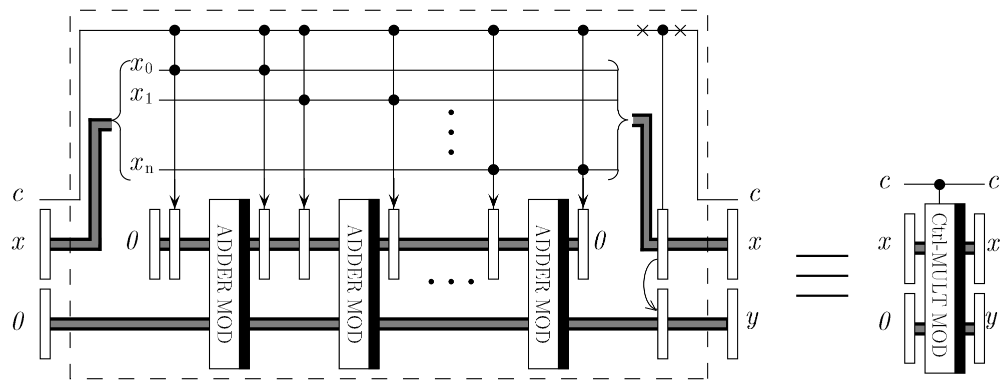



Figure 5)

V. Vedral, A. Barenco and A. Ekert

multiplication

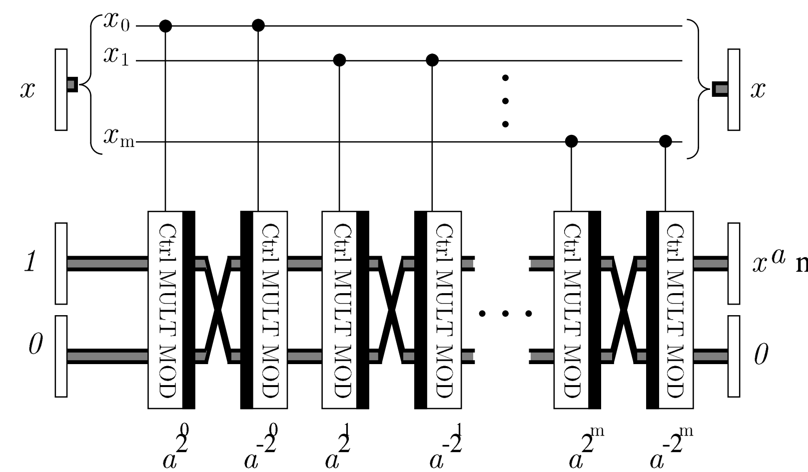



Figure 6)

V. Vedral, A. Barenco and A. Ekert

exponentiation

# Quantum Fourier Transform

Uses $n$ qubits to transform a vector of size $2^n$ by:

$$\sum_{k=0}^{2^n-1} a_k|k\rangle \longrightarrow \sum_{l=0}^{2^n-1}(\sum_{k=0}^{2^n-1} e^{2\pi ikl/2^n} a_k)|l\rangle = \sum_{l=0}^{2^n-1} \tilde{a}_l|l\rangle \ .$$

Can be written through elementary transformations:

- $H_j$ : **Hadamard gate** applied to qubit $j$
- $B_{jk}$: **two-qubit gate** applied to the qubits $j$ and $k$, characterised by $|00\rangle \longrightarrow |00\rangle$; $|01\rangle \longrightarrow |01\rangle$;$|10\rangle \longrightarrow |10\rangle$; $|11\rangle \longrightarrow \exp(i\pi/2^{k-j})|11\rangle$).

One can verify that the sequence: $\Pi_{j=1}^{n}[(\Pi_{k=j+1}^{n} B_{jk})H_j]$

gives the Fourier transform of a vector of size $2^n$ in $n(n+1)/2$ operations.

**Compare** with $\sim N\log N$ for the classical Fast Fourier Transform!

# Period of a function

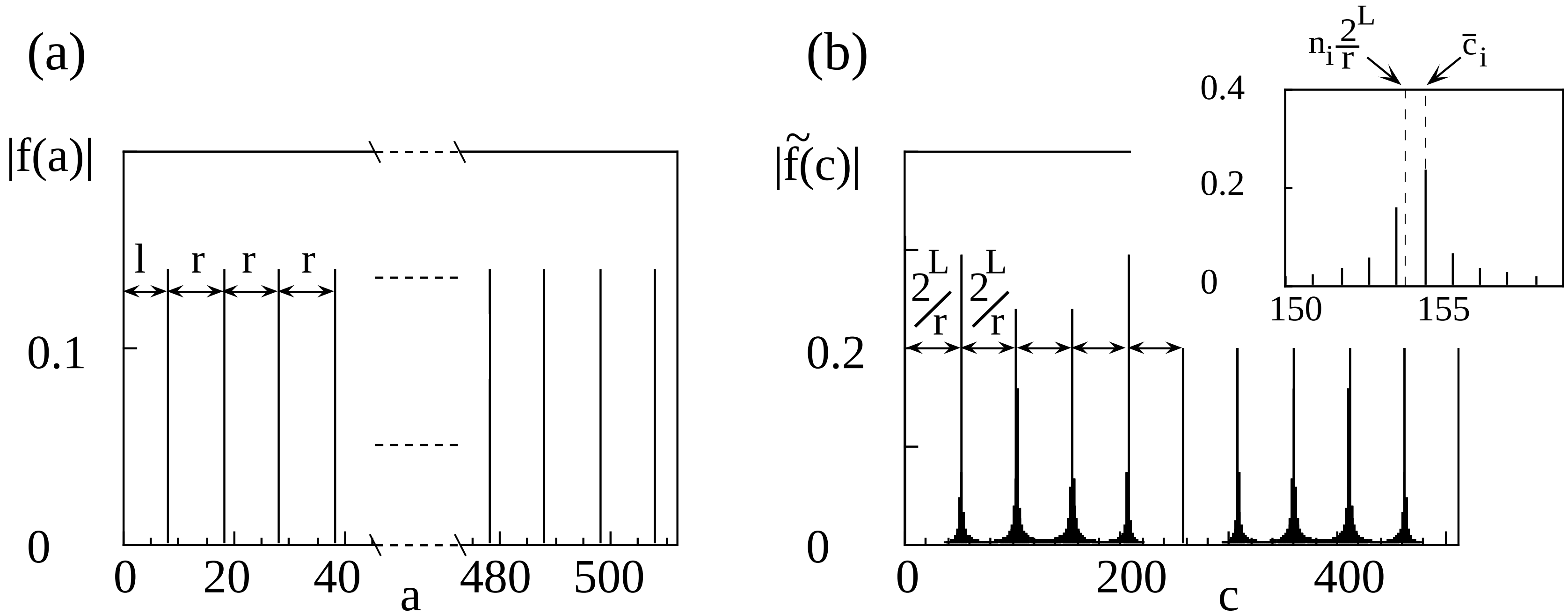
Simon (1994), Shor (1994)

$f$ function on $Z$ periodic period $r$: $f(x) = f(x + r)$, where $N/2 < r < N$

Two registers $a$ and $b$ with $\sim 2 \log N$ qubits each

- build the state $2^{-n/2}\Sigma_{x=0}^{2^n-1}|x>|0>$
- transform this state in $2^{-n/2}\Sigma_{x=0}^{2^n-1}|x>|f(x)>$
- measure the $b$ register. Result: $|u>$. Total state: $M^{-1/2}\Sigma_{j=0}^{M-1}|x_j>|u>$ where $x_j$ are all $x$ such that $f(x_j) = u$, and $M \approx 2^n/r$.
- apply a Fourier transform, and measure the $a$ register $\Rightarrow$ multiple of $M \approx 2^n/r$.

## Period of a function




From Barenco et al., Phys Rev A **54**, 139 (1996)

# Large numbers factorization

**Algorithm of Shor (1994)**: factorize $N$ in prime factors

- choose $a < N$ randomly
- find the period $r$ of $f(x) = a^x mod(N)$
- for most $a$, $r$ is even and $a^{r/2} \pm 1$ shares a common factor with $N$, can be found rapidly

**advantages:**

$\Rightarrow$ Requires $\sim 300(\log N)^3$ logical operations (classically $\sim \exp(2(\log N)^{1/3}(\log \ln N)^{2/3}))$

$\Rightarrow$ current limit with classical computers: $N \sim 10^{130} \Rightarrow \sim 2 \times 10^{10}$ operations with $\sim 1000$ qubits. For $N \sim 10^{260} \Rightarrow \times 10^7$ classically but $\times 8$ quantum mechanically!

$\Rightarrow$ Quantum computing may change the complexity class!

# Other views of Shor's algorithm

**Hidden subgroup problem**: $f$ function from group $G$ to set $X$, **constant** on cosets of a subgroup $K \Rightarrow$ find $K$.

period-finding: $G$=integers, $K$=multiples of the period.

**Phase estimation**: Given a unitary operator $U$ and an eigenvector $|u\rangle$, find efficiently the eigenvalue $e^{i\omega u}$ associated.

(idea: compute $1/\sqrt{N}\sum_{x=0}^{N-1}|t>|U^t u\rangle = 1/\sqrt{N}\sum_{x=0}^{N-1} e^{i\omega u t}|t>|u\rangle$, then Fourier transforming the first register gives a peak at the eigenvalue)

period-finding: $U_y|f(x)\rangle = |f(x+y)\rangle$

# Grover's search algorithm

**Problem**: given an unstructured list of items $i$, find a particular item $i = j$

**Classically**: best solution is going through the list $\Rightarrow \sim N/2$ on average for $N$ items

**Quantum**: needs an operator $S$ which recognizes $i = j$ $(S(|j\rangle = -|j\rangle)$ ("oracle")

- Start from $|\Psi_i >= 1/\sqrt{N}\sum_{i=0}^{N-1}|i>$ (uniform superposition) $= \sin\theta_0|j\rangle + \cos\theta_0/\sqrt{N-1}\sum_{i\neq j}|i>$ with $\sin\theta_0 = 1/\sqrt{N}$
- Apply $S \Rightarrow -\sin\theta_0|j\rangle + \cos\theta_0/\sqrt{N-1}\sum_{i\neq j}|i>$
- Apply Fourier Transform + reverse all signs but for $|0\rangle$ + Fourier transform again
- Result: $= \sin(\theta_0+\phi)|j\rangle + \cos(\theta_0+\phi)/\sqrt{N-1}\sum_{i\neq j}|i>$
- Iterate $\approx \sqrt{N}$ times $\Rightarrow \sin\theta \approx 1 \Rightarrow$ **quantum** $\sim \sqrt{N}$. Note: **gain proven** ($\neq$ Shor)

can be used to solve problems where finding solutions is hard, but testing a candidate is easy

# Cryptographic applications

**RSA scheme**: public-key cryptography (equivalent to a mailbox)

$\longrightarrow$ rests on the fact that some mathematical operations are **non symmetric**: multiplying two numbers is easy, factoring is hard.

$\longrightarrow$ RSA uses the easy direction to **encode**; the hard inverse operation makes it impossible to decode by someone who has not the key.

**Shor's algorithm destroys RSA**

Grover's algorithm can also be used in cryptographic applications

Note that **quantum cryptography** is an alternative to classical cryptography

# Simulation of quantum physical systems

- Many quantum mechanical problems require **large** Hilbert spaces
- Examples: many-body systems ($n$ particles, $m$ orbitals $\Rightarrow m^n$ states), semiclassical limit...
- Feynman (1982): Use quantum mechanical systems to simulate quantum mechanics
- Lloyd (1996): Algorithm to simulate many-body systems with local interactions.

# Quantum maps

**Simple** evolution operators, but **complex** behaviour. Simplest maps have one degree of freedom, and evolution operator = product of position operator and momentum operator. Typically, one iteration $\Rightarrow N \log N$ classical operations. **Economical in qubits and gates**.

- Baker's map (Schack 1998); fully chaotic map. Essentially partial Quantum Fourier Transforms. Requires $n^2$ quantum gates per map iteration. Experimentally **implemented** on a NMR quantum computer with 3 qubits (Weinstein et al., 2002)
- Kicked rotator (Georgeot and Shepelyansky, 2001) $\bar{\psi} = \hat{U}\psi = e^{-ik\cos\hat{\theta}} e^{-iT\hat{n}^2/2}\psi$ **Paradigmatic** model of quantum chaos. Can simulate **Rydberg atoms** and **Anderson localization** of electrons in solids. Requires $O(n^3)$ quantum gates per map iteration.
- Sawtooth map (Benenti et al, 2001) $\bar{\psi} = \hat{U}\psi = e^{ik(\hat{\theta}-\pi)^2/2} e^{-iT\hat{n}^2/2}\psi$ Requires $3n^2 + n$ quantum gates per map iteration.
- Intermediate map (Giraud and Georgeot, 2005) $\bar{\psi} = \hat{U}\psi = e^{i\alpha\theta} e^{-iT\hat{n}^2/2}\psi$ Requires $2n^2 + 2n$ quantum gates per map iteration.

# Quantum maps: example of quantum simulation

$\hat{U} = e^{-2i\pi\hat{p}^2/N} e^{2i\pi\alpha\hat{q}}$ on a $N$-dimensional wave function, $N = 2^n$. Needs $n$ qubits.

- In $q$ representation: $e^{2i\pi\alpha\hat{q}}$ is diagonal. $q = \sum_{j=0}^{n-1} q_j 2^j$ (binary decomposition) $\Rightarrow$ $\exp(2i\pi\alpha\hat{q})$ corresponds to the application of the $n$ one-qubit gates $|0\rangle \longrightarrow |0\rangle$, $|1\rangle \longrightarrow \exp(2i\pi\alpha 2^j)|1\rangle$.
- Quantum Fourier Transform $\Rightarrow$ shift from $q$ to $p$ representation, using $n(n+1)/2$ gates.
- In $p$ representation, the second operator $e^{-2i\pi\hat{p}^2/N}$ is diagonal. $p = \sum_{j=0}^{n-1} p_j 2^j$ $\Rightarrow$ $\exp(-2i\pi p^2/N) = \prod_{j_1,j_2} \exp(-2i\pi p_{j_1} p_{j_2} 2^{j_1+j_2}/N)$ $\Rightarrow$ $n^2$ two-qubit gates applied to each qubit pair $(j_1, j_2)$, keeping the states $|00\rangle, |01\rangle, |10\rangle$ unchanged while $|11\rangle \longrightarrow \exp(-2i\pi 2^{j_1+j_2}/N)|11\rangle$.
- Quantum Fourier Transform $\Rightarrow$ shift from $q$ to $p$ representation.

In total, one iteration requires $2n^2 + 2n$ gates to be implemented ($N \log N$ classically).

# Extraction of information

One map iteration is exponentially fast. Extracting information may require many measurements $\Rightarrow$ Total efficiency of the complete algorithm?

- **Localization length** (Benenti et al, 2003): Direct measurement of the final wavefunction for localized systems $\longrightarrow$ **polynomial gain**.
- **Form factor** (D. Poulin et al, 2003): Use additional circuit to compute $\mathrm{Tr}U^n$, gives spectral correlations $\longrightarrow$ **polynomial gain**.
- **Fidelity decay** (Emerson et al, 2002): Measure the sensitivity to perturbation of the quantum system $\longrightarrow$ **possibility of exponential gain**.
- **Spectrum** (Abrams and Lloyd, 1999): Measure eigenvalues through versions of phase estimation algorithm $\longrightarrow$ **possibility of exponential gain**.
- **Wigner function** (Miquel et al, 2002, Terraneo et al, 2004): Use additional circuit and/or Quantum Fourier Transform to measure Wigner or Husimi distributions $\longrightarrow$ **polynomial gain**.

# Quantum simulators

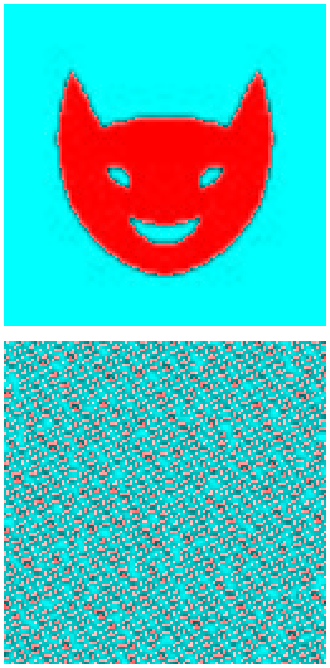
- **Bose-Einstein condensate** of cold atoms in **optical lattice**
- When lattice parameters are changed, **quantum phase transition** from superfluid to Mott insulator (Bose-Hubbard model) (observed in Greiner et al, Nature 2002).
- Adding electric fields and magnetic fields and changing the parameters of the optical lattice $\Rightarrow$ Possibility to simulate **many different many-body Hamiltonians**, in a controllable way.

$\longrightarrow$ "quantum analog computer": not universal, but easier to use than a general-purpose quantum computer

$\longrightarrow$ Other physical implementations possible

# Simulation of classical physical systems

- Less explored, since less natural than quantum systems. Still, factoring is a classical problem...
- Simulation of **classical spin systems** possible (Lidar and Biham, 1997).
- **Classical maps** can be simulated on a quantum computer. Example: cat map (Georgeot and Shepelyansky, 2001) $\bar{y} = y + x \pmod 1$ , $\bar{x} = y + 2x \pmod 1$ **Discretized classical phase space density** $\longrightarrow$ exponential number of points can be iterated in polynomial time.



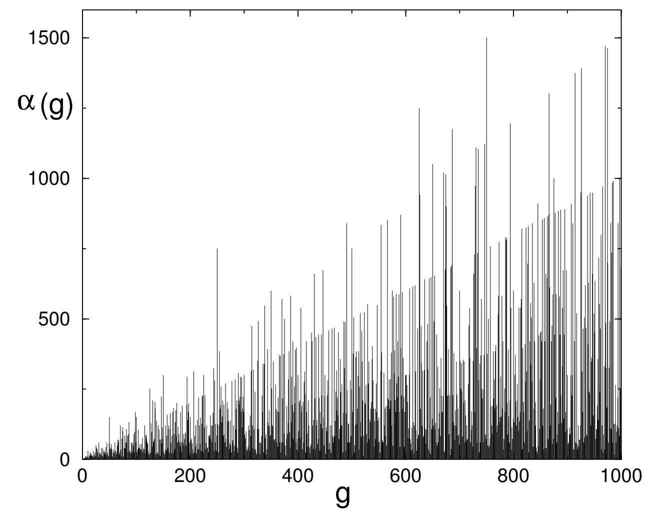
10 iterations of the cat map

# Extraction of information

- Fourier coefficients of the discretized phase space density: apply **Quantum Fourier transform** after iterating the map; possibility of exponential gain.
- Recurrence times (Georgeot 2004): apply **period-finding** algorithm or **Grover's search** as subroutines.

  $\longrightarrow$ **Exponential gain** for the cat map.

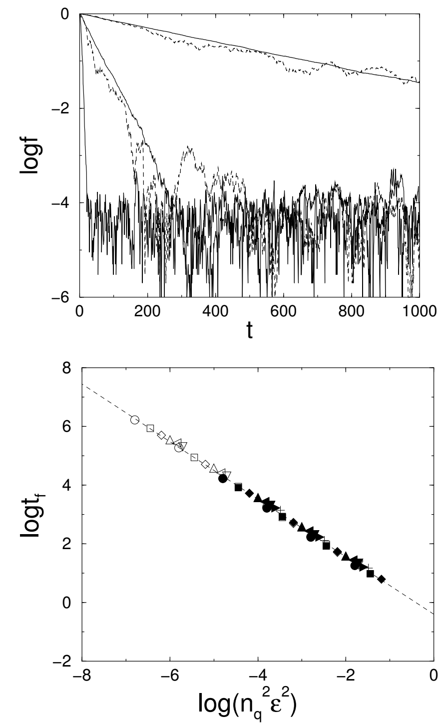
  $\longrightarrow$ For a larger class of systems, only **polynomial gain**.




Recurrence times for the cat map

# Problem: decoherence

- Interaction with the environment destroys the **coherence** of quantum states.
- The need to **manipulate** quantum states to perform the gates further complicates the problem
- Decoherence effects depend on the experimental implementation
- Can be **unitary** or **non unitary**
- Times scales are not exponentially small: in principle can be overcome




Effect of noisy gates (Lévi et al (2003))

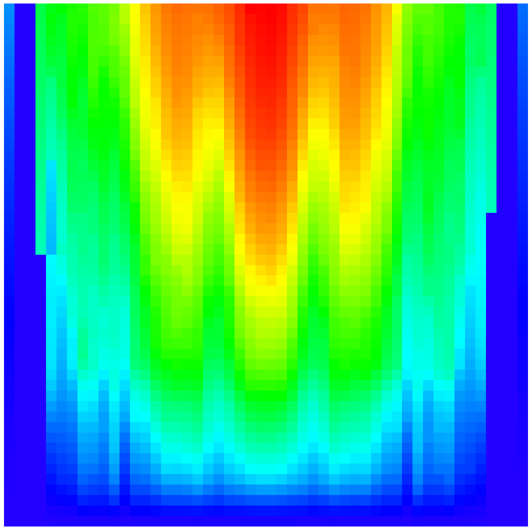
# Problem: static imperfections

**Internal imperfections**, e.g. residual coupling between qubits, fluctuations in energy difference of qubits.

Model: $H = \sum_i \Gamma_i \sigma_i^z + \sum_{i<j} J_{ij} \sigma_i^x \sigma_j^x$

2D lattice of $n$ qubits; $J_{ij}$ **nearest-neighbour** coupling random in $[-J, J]$; $\Gamma_i$ random in $[\Delta_0 - \delta/2, \Delta_0 + \delta/2]$

**Quantum chaos** sets in for $J > J_c$.
Chaos $\Rightarrow$ mixing of exponentially many multi-qubit states, ergodicity.
$\Rightarrow$ "melting" of the quantum computer.
$\Rightarrow$ **destruction** of the computer
**without coupling to the environment**

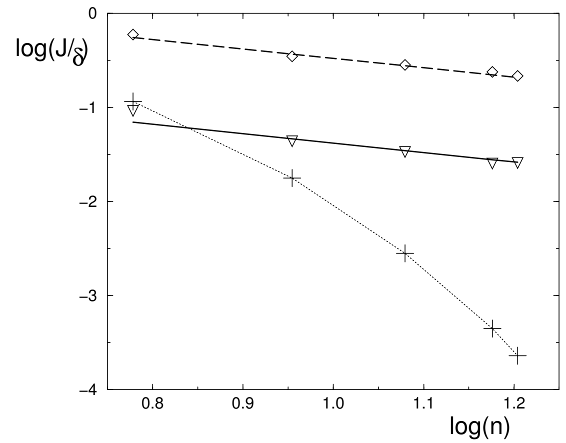


Quantum computer melting

# Problem: static imperfections

Hamiltonian: **sparse** random matrix
two-body interaction $\Rightarrow$ three energy scales:
$\Delta_0 =$ one-qubit level spacing
$\Delta_c =$ level spacing between directly coupled multi-qubit states $\sim \delta/n$
$\Delta_n =$ level spacing between multi-qubit states: $\sim n2^{-n} \ll \Delta_c$
Quantum chaos sets in for $J > J_c$.

**Theory:** (B.G. and D. Shepelyansky, 2000)
One multi-qubit state is coupled to $\approx n$ states in an energy interval $2\delta$.
$\Rightarrow J_c \approx \Delta_c \sim \delta/n$
**polynomial scaling !**




Theory confirmed
by numerical simulations

# Classical error-correcting codes

**Example : Hamming code**

$0000 \longrightarrow 0000000$; $0001 \longrightarrow 1010101$; $0010 \longrightarrow 0110011$; $0011 \longrightarrow 1100110$, etc...

$4$ bits $\longrightarrow$ $7$ bits; every codewords differs from all the others in at least $3$ places, $\Rightarrow$ any single-bit error can be corrected

**Shannon:** in general, it is possible to correct noise-induced errors at the price of longer codewords; the process is more efficient if one has information on the type of noise

# Quantum error-correcting codes

(Calderbank, Shor (1996), Steane(1996))

- Should correct both **bit errors** and **phase errors**
- add other registers which evolve coherently with the quantum computer
- measure the extra registers $\Rightarrow$ gives information on the noise operator $M$
- use this information to apply $M^{-1}$ on the computer
- the extra operations produce noise, but one can show that one can correct more noise than produced $\Rightarrow$ **fault-tolerance threshold**
- **price:** increases the number of qubits enormously to cope with usual levels of noise
- Introduces irreversibility, dissipation
- Codes can be tailored to specific types of errors (example: PAREC (Kern, Alber and Shepelyansky, 2004) for static imperfections)
- Recent development: **decoherence-free subspaces**

# So, what is a quantum computer?

A set of $n$ qubits (Hilbert space of dimension $2^n$) such that (Steane 1997):

- Each qubit can be prepared in some known state $|0>$
- Each qubit can be measured in the basis $|0>$, $|1>$
- Universal quantum gates can be applied to subsets of qubits
- The qubits do not evolve other than via the above transformations

**Experimental challenge:** Find two-level systems in physics fulfilling these requirements

Such systems should be **protected from the environment** (long decoherence time) but **easy to manipulate** $\Rightarrow$ contradictory requirements

Key issue: **scalability**

# Realization $1$: NMR (Gershenfeld and Chuang, 1997)

- **qubits:** nuclear spins in molecules
- **quantum gates:** oscillating magnetic fields are applied in pulses of controlled duration; hundreds of gates can be applied.
- **advantage**: uses techniques well developped for e.g. medical applications.
- **problems:** what is measured is the average spin state of a very large number of molecules; signal goes down exponentially with number of qubits; no global entanglement.
- best achievement: factoring 15 with $7$ qubits (Vandersypen et al, 2001).

$\longrightarrow$ **Good for demonstration purpose, but probably not the good way to build a large quantum computer.**

$\longrightarrow$ **By far the most advanced to date.**

## Realization $2$: ion trap (Cirac, Zoller (1995))

- **qubits:** $2$ internal states of cold ions in a ion trap
- **single-qubit rotation :** by laser pulse
- **two-qubit gates:** laser pulse exciting the collective quantized motion of ions $\Rightarrow$ Coulomb interaction needed
- **preparation:** optical pumping and laser cooling
- **measurement:** lasers $+$ detection of fluorescence on cameras
- **problems:** temperature: should reach microKelvin to put ions in the ground state
- Two-qubit gate realized, teleportation, entanglement of six ions (Boulder group, Innsbruck group)

# Realization $3$: Josephson junctions

Two superconducting islands (Bose-Einstein condensates of Cooper pairs) separated by thin insulating layer.

- **qubits:** charge difference between the two islands ("charge qubit") or magnetic flux through a superconducting circuit ("flux qubit").
- **quantum gates**: inductive couplings between superconducting circuits
- **advantages**: Mesoscopic size; in principle scalable.
- First qubit in 1999 (Nakamura et al), then first long-living qubit 2002 (Vion et al.). Coupling and CNOT between two qubits realized (Yamamoto et al, 2003).

# Other proposals

- **Lattice of spins** (Privman, Vagner, Kventsel (1998), Kane (1998) **qubits:** nuclear spins; **single-qubit rotation, CNOT :** electronically controlled through gate voltage (local electric fields) (the hyperfine interaction couples electrons and nuclear spins) + a magnetic field; **measurement:** currents of spin-polarized electrons; **problems:** extreme precision for placing atoms and for the electric fields; impurities, etc...
- **Optical lattices** (Jaksch et al (1999), Brennen et al (1999), Sorensen and Molmer (1999)) **qubits:** internal states of atoms; **single-qubit rotation:** by laser pulses; **two-qubit gate:** two optical lattices, one of $|0>$, one of $|1>$, are built, and displaced with respect to each other to create interaction.
- **Optical cavities:** coupling between a single atom or ion (qubit) and a mode of the electromagnetic field in the cavity.
- **Quantum dots:** qubit: spin state of single-electron quantum dot; operations effected by the gating of the tunneling barrier between neighboring dots.

# What is the situation?

- Theoretical construction of quantum logical operations: quantum Turing machines.
- Theory of Quantum information.
- Specific algorithms now exist.
- Error-correcting codes now exist.
- Experimental implementation on small systems have been realized (Shor's algorithm on $7$ qubits, enabling to factor $15$, Vandersypen, Steffen, Breyta, Yannoni, Sherwood, Chuang, *Nature* **414**, 883, (2001); technique:NMR).
- Other types of quantum computers: adiabatic quantum computation, one-way quantum computer.
- New development in quantum algorithm: quantum random walks.

## What is the prospect?

- American roadmap (http://qist.lanl.gov/)
- European roadmap (http://www.cordis.lu/ist/fet/qipc-sr.htm)
- Experimental effort is huge; but the problems are so hard that still limited to a few qubits.
- Still, **no physical reason** why it should not be possible to build a **large quantum computer**.
- If no sudden breakthrough, a really useful quantum computer (with hundreds or thousands of qubits) will not be built in the near future. In the mean time, demonstration-purpose quantum computers with a few tens of qubits may be built.
- There is a need for new quantum algorithms.

# Research organization

- American programs: intelligence and military agencies (National Security Agency and Army Research Office), DARPA (Defense Advanced Research Projects Agency) and NSF
- Europe: "Quantum Information Processing" program, included in "Future and Emerging Technologies" part of IST (Information society technologies). Budget FP7 $\approx$ 30 MEuros
- National programs in many European countries, sometimes parts of nanotechnology programs.

Tendency towards large projects integrating theoreticians and experimentalists

## More information ...


- B.Georgeot and D.L.Shepelyansky, *Les ordinateurs quantiques affrontent le chaos*, Images de la physique 2003-2004 (2004), 17 (quant-ph/0307103) **(short introduction, in French)**.
- A. Eckert and R. Josza, *Quantum computation and Shor's factoring algorithm*, Rev. Mod. Phys. **68**, 733 (1996) **(mostly factoring algorithm)**.
- A. Steane, *Quantum Computing*, Rep. Progr. Phys. **61**, 117 (1998) (quant-ph/9708022) **(very good review paper)**.
- G. Benenti, G. Casati and G. Strini, *Principles of quantum computation and information*, World Scientific (2004) **(good introduction to the field)**.
- M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, Cambridge University Press (2000) **(very complete reference)**.