# QUANTUM COMPUTING

## *Part II*

Jean V. Bellissard

*Georgia Institute of Technology*
*&*
*Institut Universitaire de France*

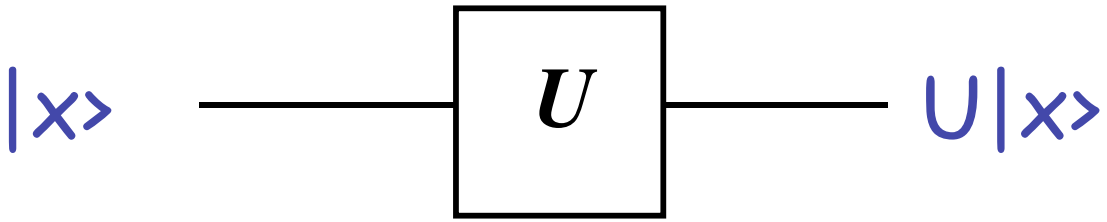
# Hello again everyone !

# QUANTUM GATES:

*a reminder*

# Quantum gates:

*1-qubit gates*



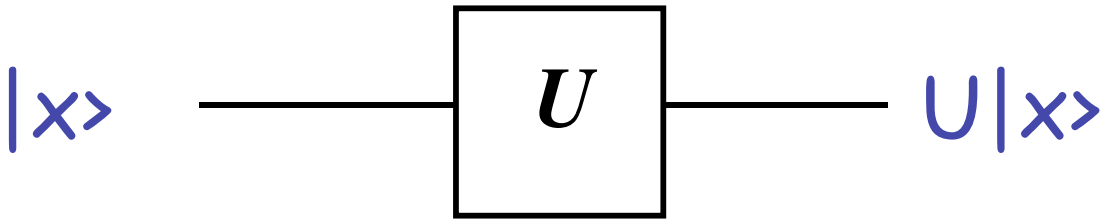

U is unitary in $M_2(\mathbb{C})$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Pauli basis in $M_2(\mathbb{C})$

# Quantum gates:

*1-qubit gates*



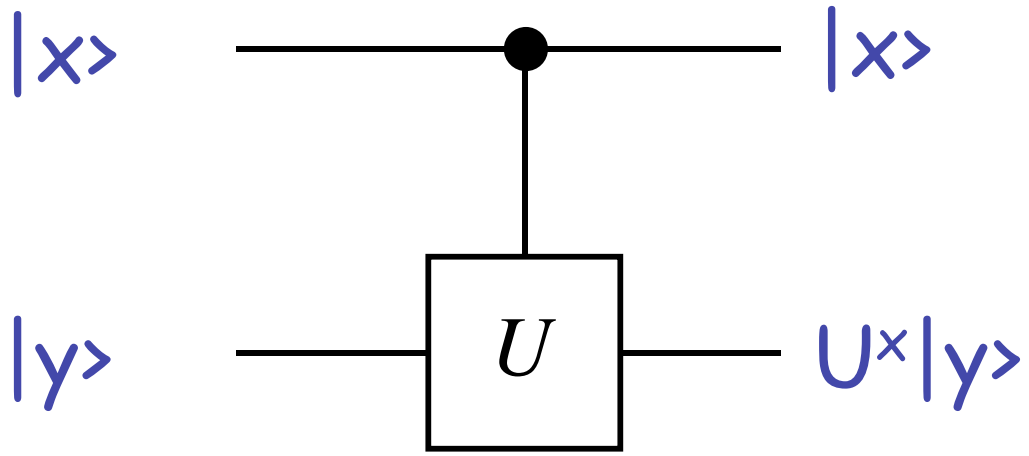

U is unitary in $M_2(\mathbb{C})$

$$H = 2^{-1/2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Hadamard, phase and $\pi/8$ gates

# Quantum gates:

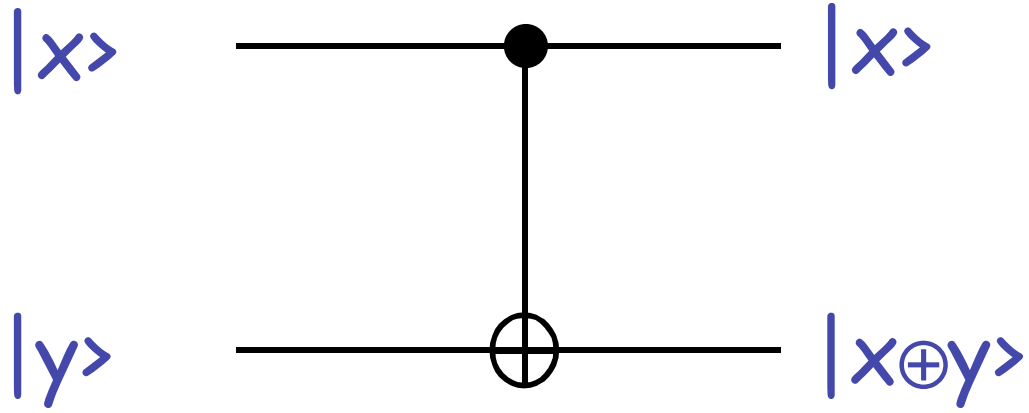
*controlled gates*




U is unitary in $M_2(\mathbb{C})$

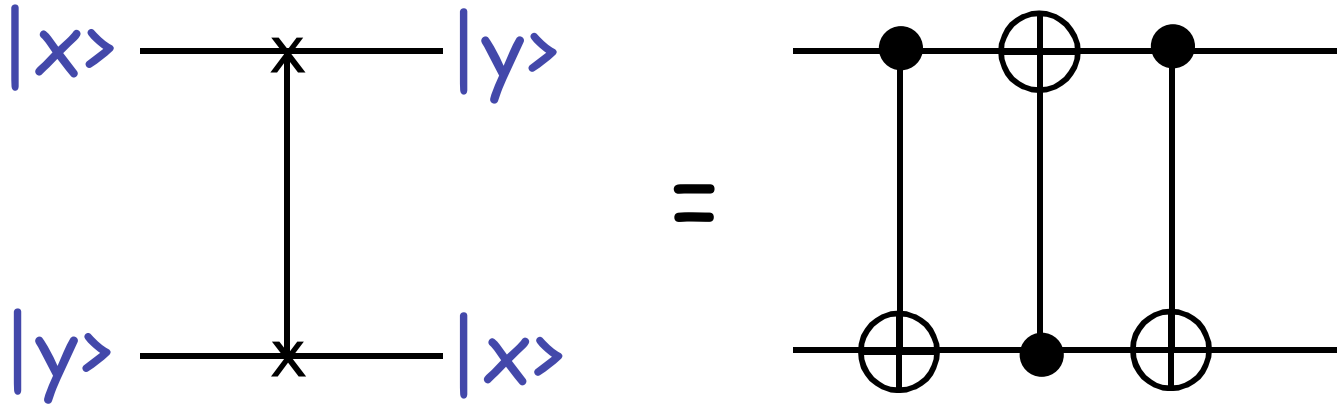
# Quantum gates:

*the CNOT gate*



# Quantum gates:

*the swap gate*



# FOURIER TRANSFORM:

*quantum computers are fast !*

# Fourier Transform:

- Digital basis given by qubits

$$|x_1 x_2 \ldots x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_n\rangle = |y\rangle$$

If

$$y = 2^{(n-1)} x_1 + 2^{(n-2)} x_2 + \ldots + x_n := x_1 x_2 \ldots x_n$$

# Fourier Transform :

- Fourier transform:

$$F\,|j\rangle = \frac{1}{N^{1/2}} \sum_{k=0} e^{2i\pi jk/N}\ |k\rangle$$

$$N=2^n,$$

# Fourier Transform :

- Binary decomposition:

$$jk/2^n = (0.j_n)k_1 + (0.j_{n-1}j_n)k_2 + \ldots + (0.j_1j_2\ldots j_n)k_n$$

(*modulo* 1) where

$$0.j_1j_2\ldots j_r = j_1/2 + j_2/2^2 \ldots + j_r/2^r$$

# Fourier Transform :

- Binary decomposition:

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

$$F|j\rangle = \frac{(|0\rangle + e^{2i\pi(0.j_n)}\,|1\rangle)\otimes\cdots\otimes(|0\rangle + e^{2i\pi(0.j_1\ldots j_n)}\,|1\rangle)}{2^{n/2}}$$

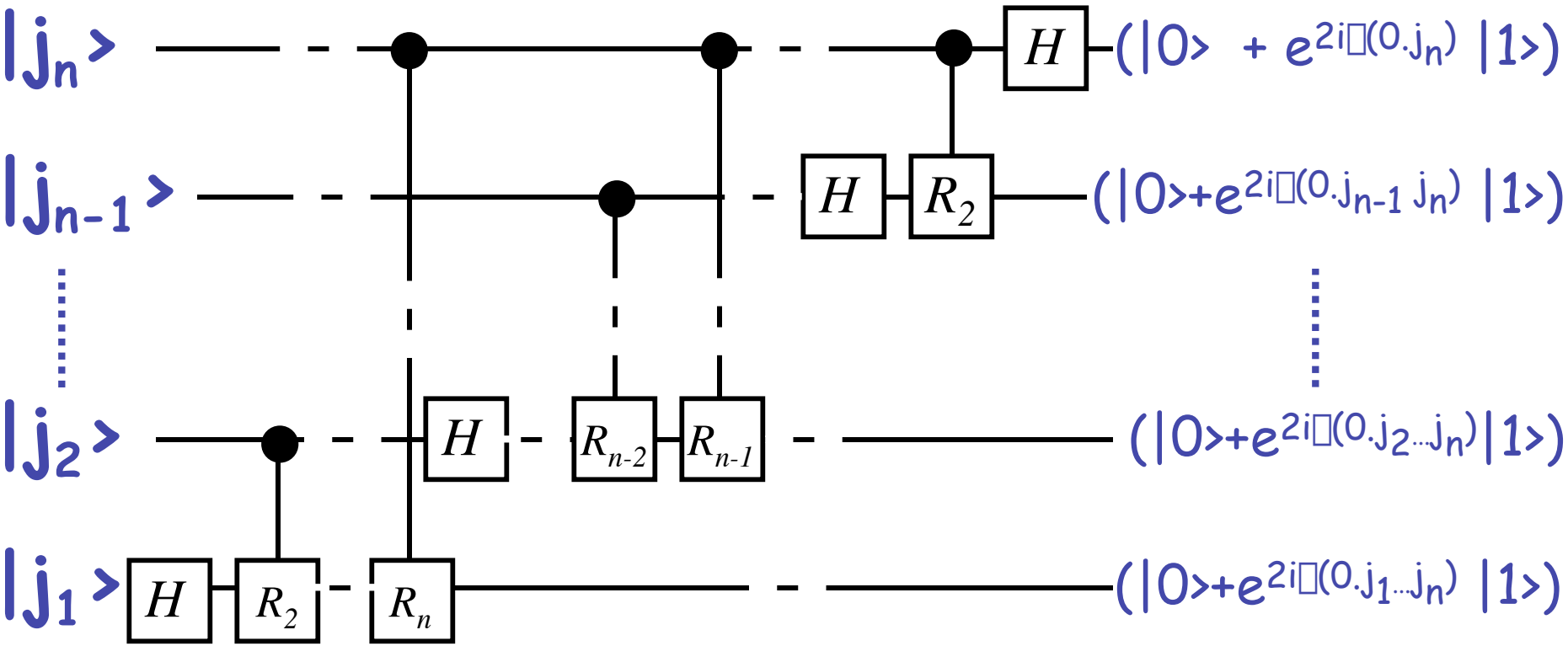
# Fourier Transform :

- Digital phase gate (1 qubit):

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2i\pi}{2^k}} \end{bmatrix}$$

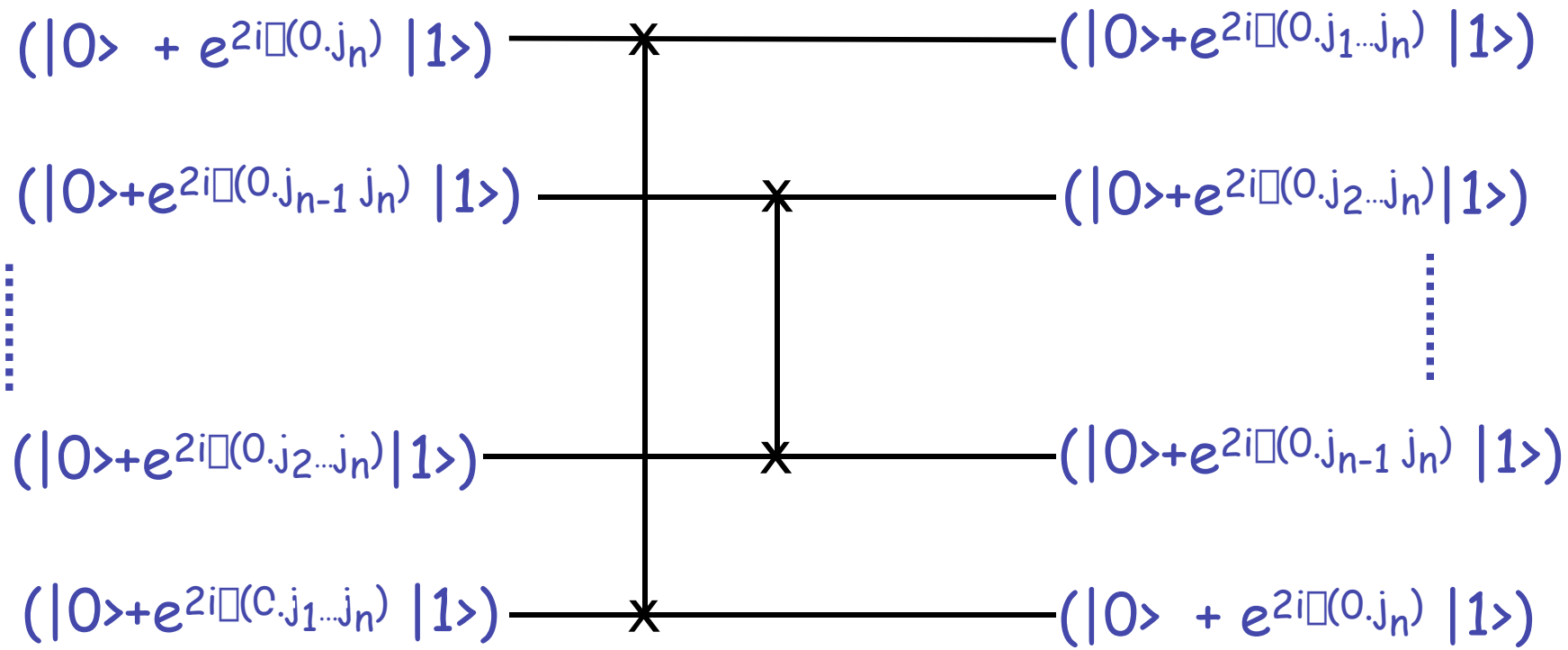
$$R_k|x\rangle = e^{\frac{2i\pi x}{2^k}}|x\rangle$$

# Fourier Transform :




Circuit producing the quantum Fourier transform

# Fourier Transform :




Swap gates arrange final qubits in right order

# Fourier Transform :

- Fourier transform

$$F \sum_j f(j)|j\rangle = \sum_k \tilde{f}(k)|k\rangle$$

$$\tilde{f}(k) = 2^{-n/2} \sum_j f(j)\, e^{2i\pi jk/2^n}$$

- the Fourier transform of f is given by the coordinates of the outcome.
- It can then be *measured*

# Fourier Transform :

- The usual FFT requires a time

$$O(N\, Ln N)$$

- The number of gates needed is

$$n^2/2 + 2n$$

- Since the $N=2^n$, the algorithm gives the result in a time (1 time unit/gate)

$$O((Ln N)^2) \text{ !!}$$

# PHASE ESTIMATION

*a key subroutine*

# Phase estimation

- U is a unitary with an eigenvalue

$$U|u\rangle = e^{i\theta}|u\rangle$$

- *Goal: compute* $\theta$.
- Set-up: two registers, one with t-qubits, the other one for representing U.

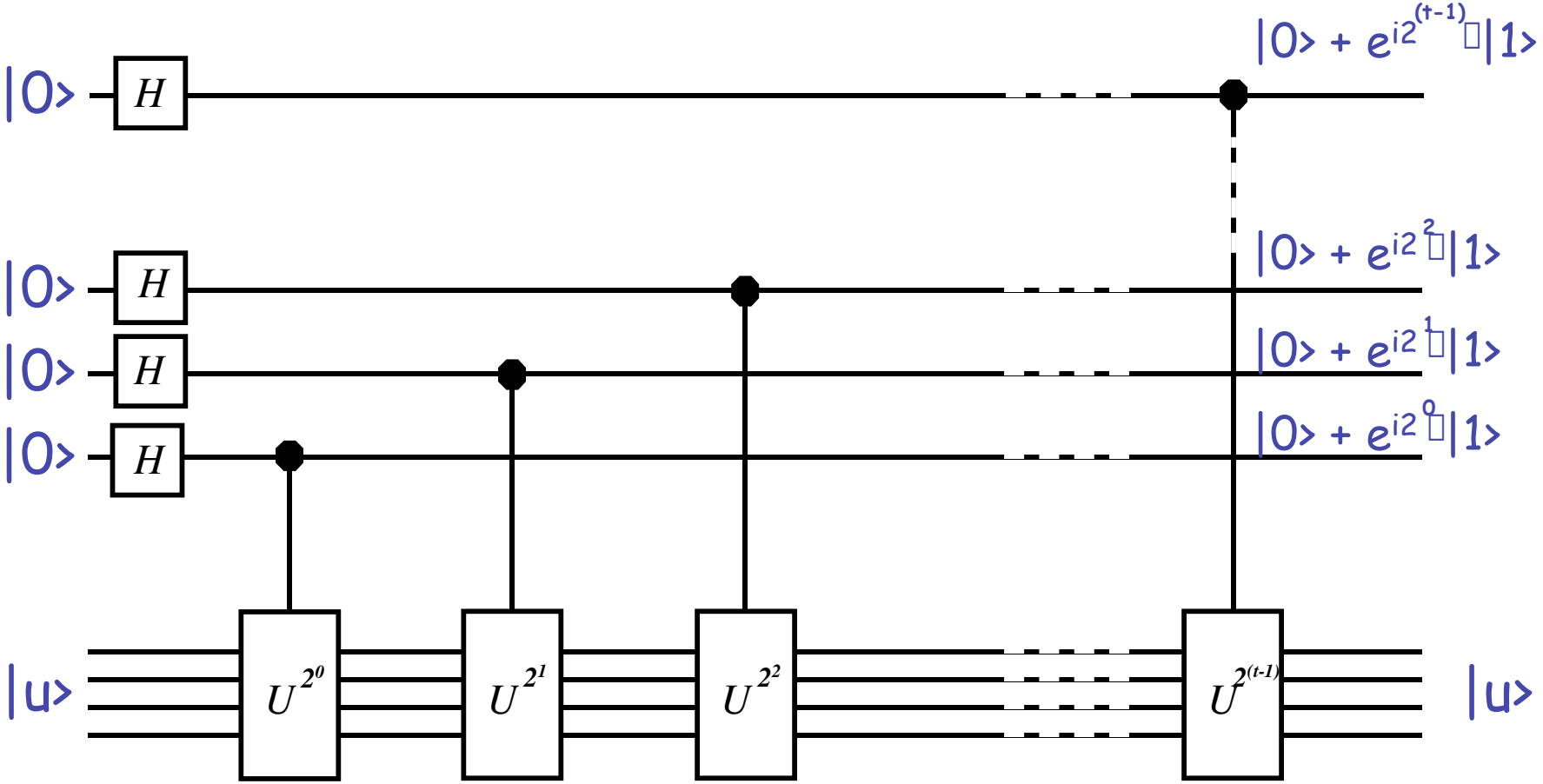
# Phase estimation

- a controlled $U^n$-gate $G_{U^n}$ gives

$$G_{U^n}|x\rangle\otimes|u\rangle = e^{inx\square}|x\rangle\otimes|u\rangle$$

- It transfers the phase of $|u\rangle$ on the component $|1\rangle$ of the first register.
- On the first register one uses a rotated state $H|0\rangle = (|0\rangle+|1\rangle)/\sqrt{2}$ instead of $|x\rangle$.

# Phase estimation



# Phase estimation

- If $\theta = 2\pi .j_1 j_2 \ldots j_t \ldots$, the outcome is

$$\frac{(|0\rangle + e^{2i\pi(0.j_t)}\,|1\rangle) \otimes \cdots \otimes (|0\rangle + e^{2i\pi(0.j_1 \ldots j_t)}\,|1\rangle)}{2^{n/2}}$$

- Then use a Fourier transform back to get $|j\rangle = |\, j_1 j_2 \ldots j_t \,\rangle$, giving the value of the phase modulo $O(2\pi/2^t)$.

# Phase estimation

- To get n digit of $\theta$ accurate, with probability of success $(1-\varepsilon)$, it can be shown that t must be chosen as

$$t=n+\log(2+1/2\varepsilon)$$

# SHOR'S ALGORITHM:

*factorizing integer into primes*

# Shor's algorithm

- *Input*: a composite integer N
- *Output*: a non trivial factor of N
- *Runtime*: $O((\log N)^3)$ operations, succeeds with *probability* $O(1)$.

# Shor's algorithm

- *First step: order finding.*
- If $x<N$ are integers with no common factors, the *order* of $x$ *modulo* $N$ is the least $0<r$ such that $x^r \equiv 1 (mod\ N)$.
- Use the unitary $U|y\rangle = |xy (mod\ N)\rangle$. If $y \in \{0,1\}^L$, $N<2^L$, and $N \le y<2^L$, set $U|y\rangle = |y\rangle$.

# Shor's algorithm

- Then

$|u_s\rangle = r^{-1/2} \sum_{k=0}^{r} \exp(-2i\pi sk/r)|x^r (\mathrm{mod}\ N)\rangle$

is an eigenvector of U with phase

$\phi = 2\pi s/r$

- *A phase-finding* computes s/r. *A* continuous fraction expansion gives r.

# Shor's algorithm

- It may not be possible to prepare the initial state of the second register in the state $|u_s\rangle$. But any initial state is a linear combination of the $|u_s\rangle$ 's.
- The outcome will be $s/r$ for some $s$. A continuous fraction expansion will give $r$ anyway.

# Shor's algorithm

- *Factoring procedure*

(i) If N is even, return the factor m=2

(ii) Find if $N=a^b$, for $a>1$, $b\geq 2$, integers (special subroutine)

(iii) Choose randomly $x \in [1,N-1]$. If $m=\gcd(x,N) > 1$, then return m.

# Shor's algorithm

- *Factoring procedure (continued)*:

(iv) Find the order r of x *mod* N.

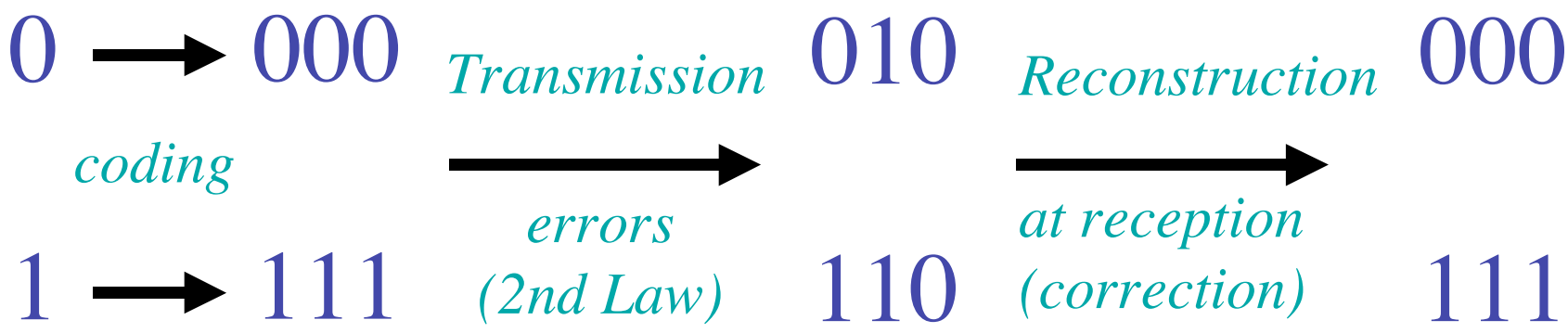
(v) If r is *even* & $x^{r/2}-1 \neq -1 \pmod{N}$, compute $\gcd(x^{r/2}-1,N)$ & $\gcd(x^{r/2}=1,N)$, check if one is a nontrivial factor m. If so return m.

# ERROR-CORRECTIONS:

*can quantum information be protected ?*

# Error-correction codes

- Classical code theory uses *redundancy* to transmit *bits* of information



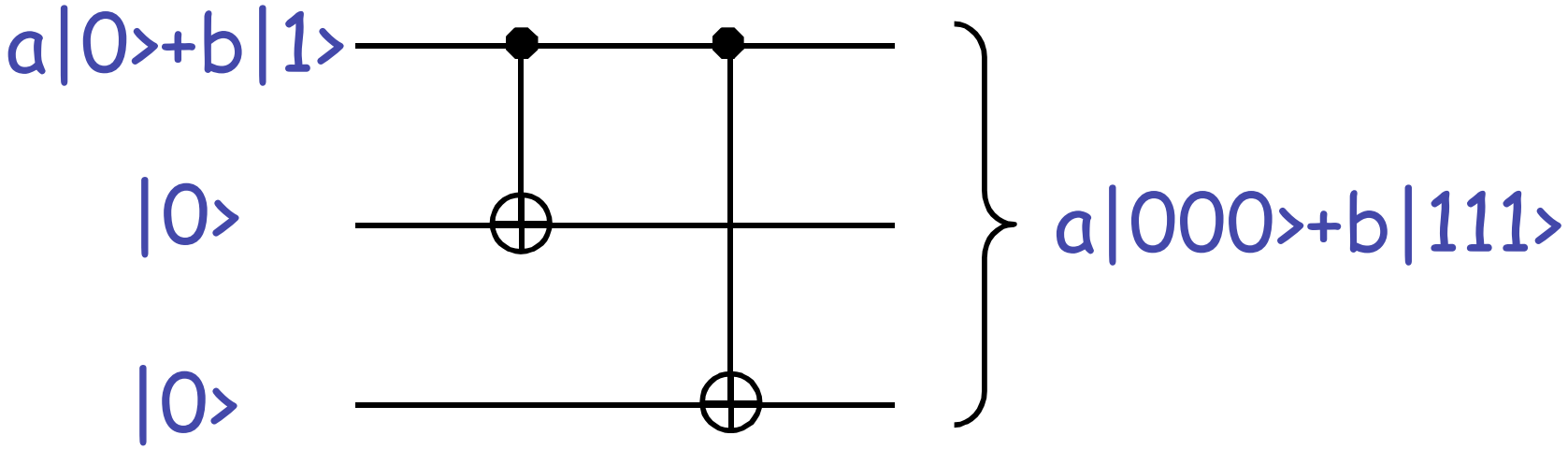
# Error-correction codes

- Quantum computer are submitted to the *no-cloning theorem*!
- there is no Hilbert space $\mathcal{H}$ neither any unitary operator U on $\mathcal{H}\otimes\mathcal{H}$ for which there is a state $|s\rangle$ such that

$$U|\psi\rangle\otimes|s\rangle = |\psi\rangle\otimes|\psi\rangle \qquad \psi \in \mathcal{H}$$

# Error-correction codes

- However it is possible to produce quantum circuits for which |0>□ |000> and |1>□ |111> for instance:



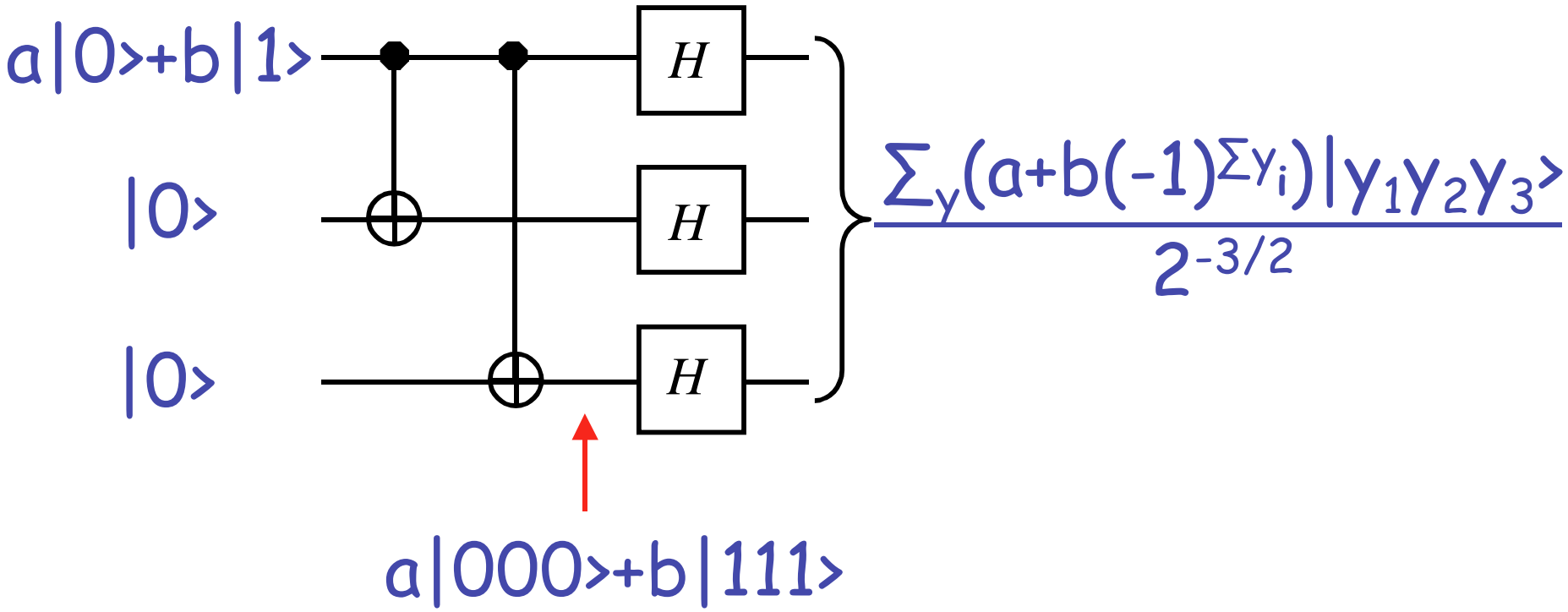
# Error-correction codes

- The previous circuit protects against *index flips*. How can one protects the signal against *phase flips* ?
- Hadamard gates transform index into a phase:

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

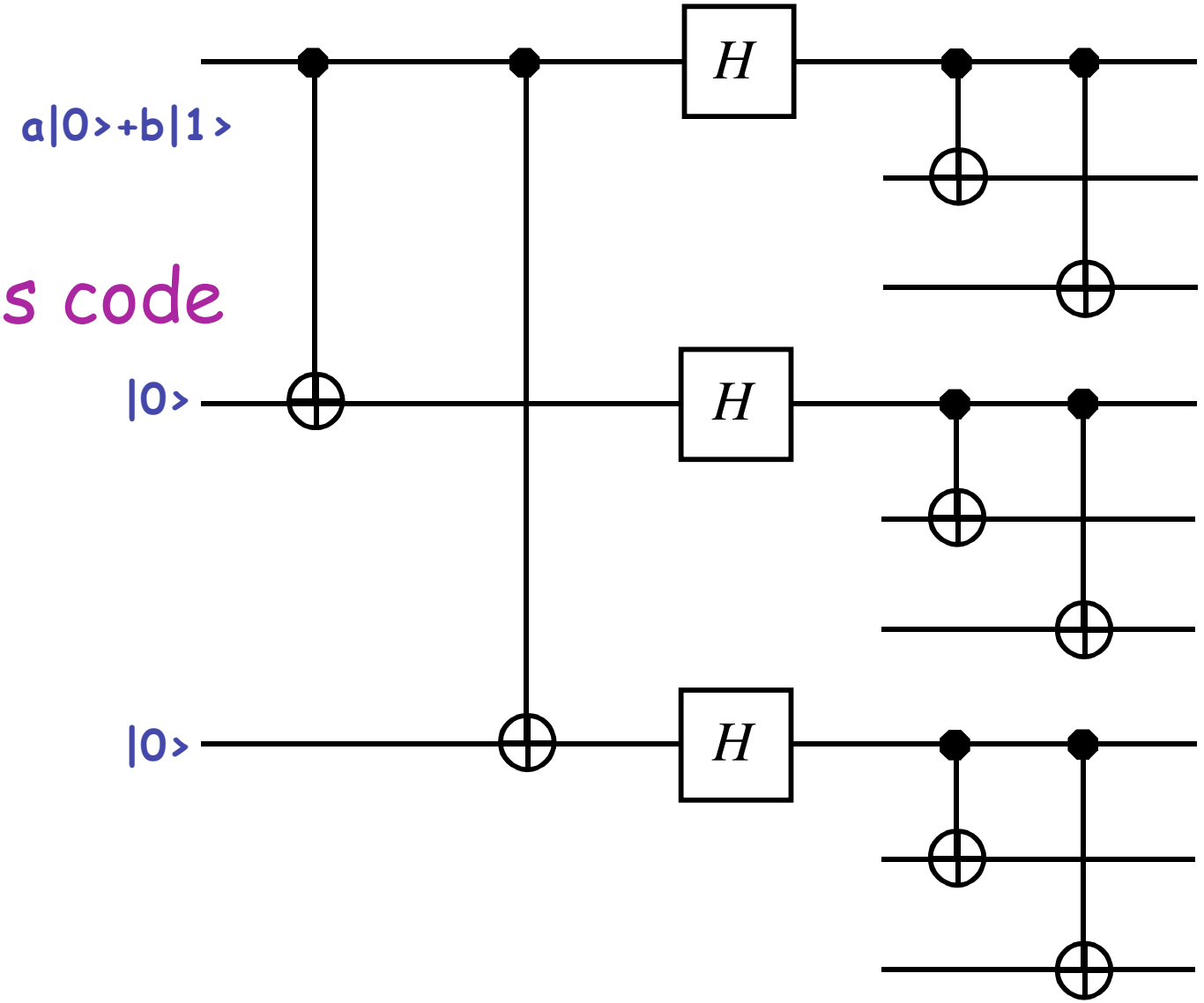
# Error-correction codes

- Phase flip protection



# Error-correction codes

- Shor's code



# Error-correction codes

- Shor's code gives $|0\rangle \rightarrow |0_L\rangle$ and $|1\rangle \rightarrow |1_L\rangle$ with:

$$|x_L\rangle = \frac{(|000\rangle + (-)^x|111\rangle)(|000\rangle + (-)^x|111\rangle)(|000\rangle + (-)^x|111\rangle)}{2\sqrt{2}}$$

# Error-correction codes

- Kitaev proposed in 1997 to replace digital degrees of freedom by topological ones.
- Tunneling effect between topological sectors is unlikely, leading to a better code protection.

# PHYSICAL REALIZATIONS

*can quantum computers be built ?*

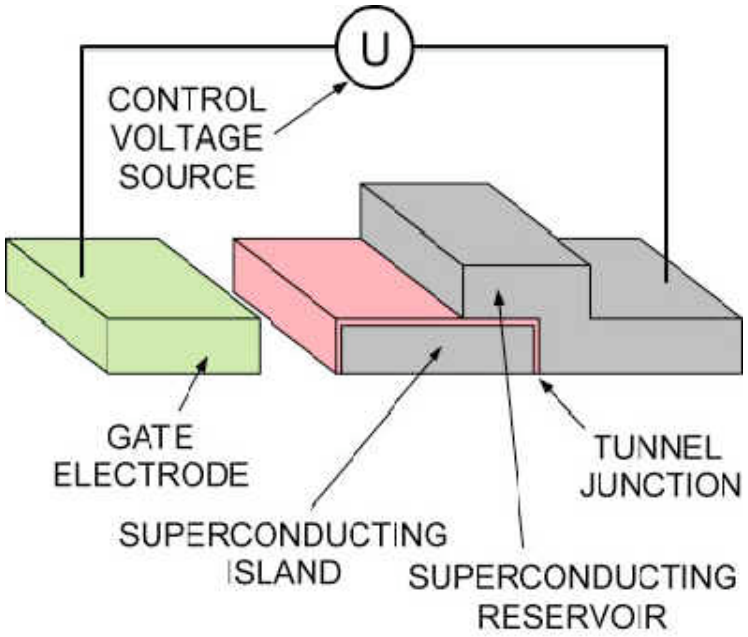
# Realizations

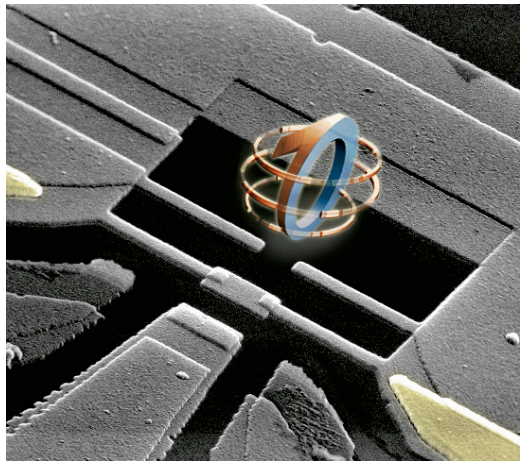
- Several devices may produce qubits:

1. Any quantum harmonic oscillator
2. Optical photons
3. Optical cavity quantum electrodynamics: coupling with 2-level atoms.
4. Ion traps
5. Nuclear magnetic resonance: computation with up to 7-qubits have permitted to test Shor's algorithm 15=3x5 !!
6. Josephson junctions: *quantronium*
7. Double well with quantum dots

# Realizations: *1-qubit, the quantronium*

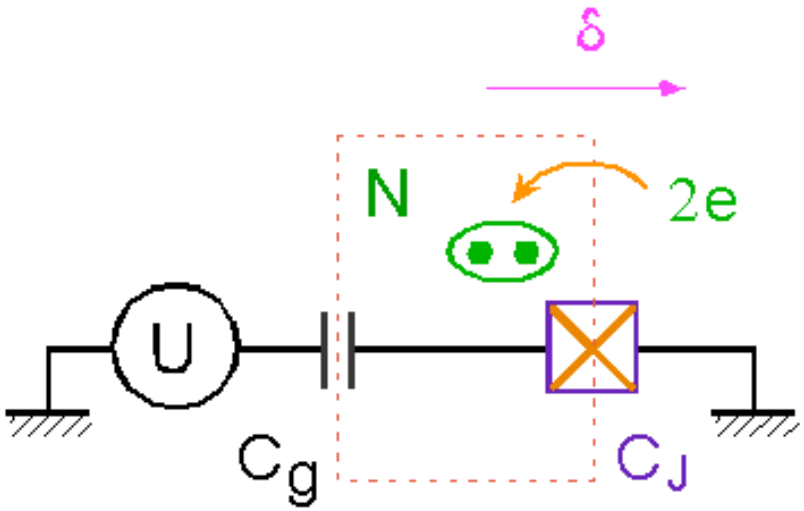
- The *quantronium* (Esteve & Devoret Saclay): a Josephson tunneling junction



# Realizations *1-qubit, the quantronium*

- *Quantronium :*




2 characteristic energies

$$E_c = \frac{(2e)^2}{2(C_g + C_J)}$$

$$E_J = \frac{\Delta h}{8\, e^2 R_T}$$

Hamiltonian:

$$\hat{H} = -E_J \cos\hat{\delta} + E_c(\hat{N} - Ng)^2$$

$$\downarrow$$

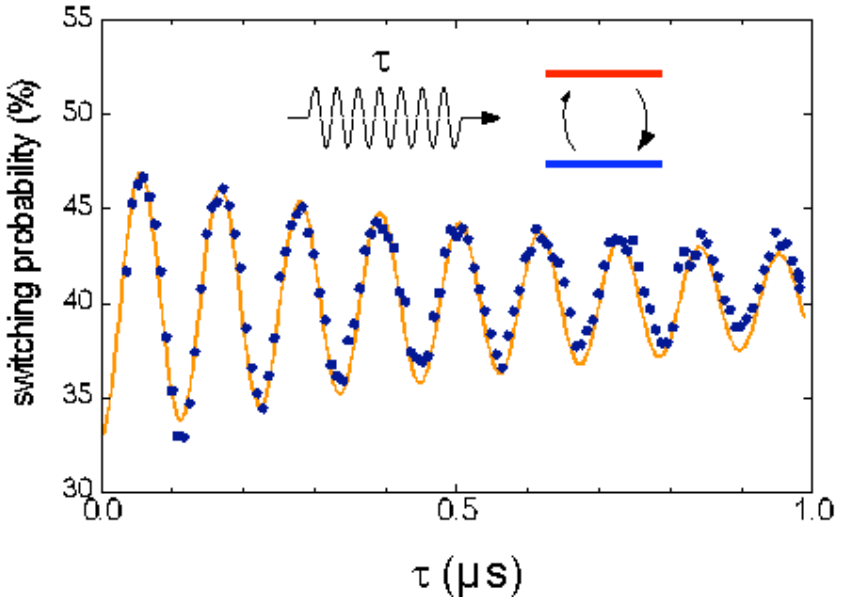
$$1/2 \sum_N{}' |N\rangle\langle N+1| + |N\rangle\langle N-1|$$

1 degree of freedom: $[\delta, N] = i$

1 control knob: U or $Ng = CgU/2e$

# Realizations

- *Quantronium* :

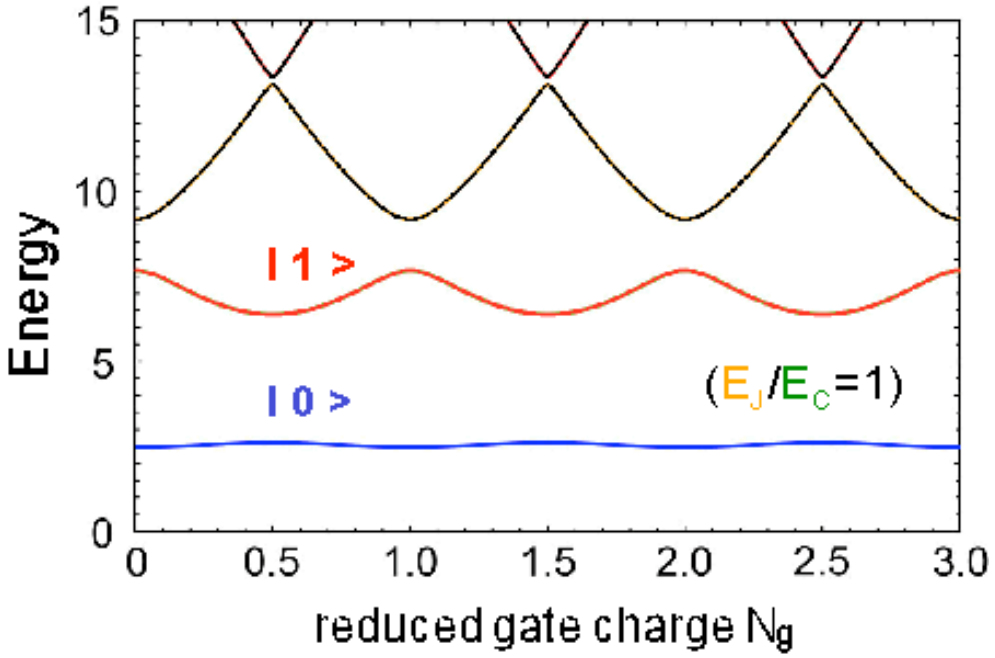



**RABI OSCILLATIONS**

Coherent manipulation of the Quantronium state: a microwave resonant pulse with duration □ and amplitude URF is applied to the gate. The Quantronium undergoes Rabi oscillations. The probability of measuring the Quantronium in its excited state, i.e. the switching probability of the measuring junction, oscillates accordingly as a function of □and URF.

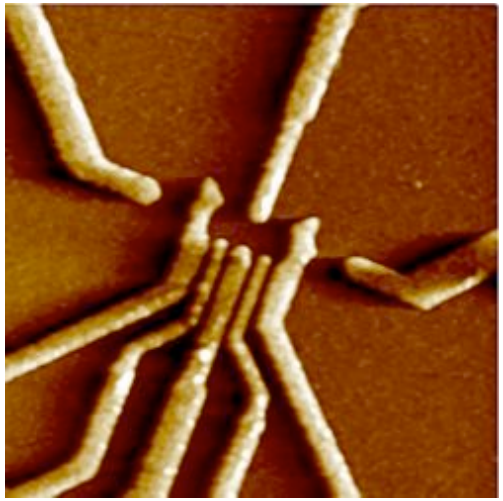
Each dot is an average over 50000 measurements.

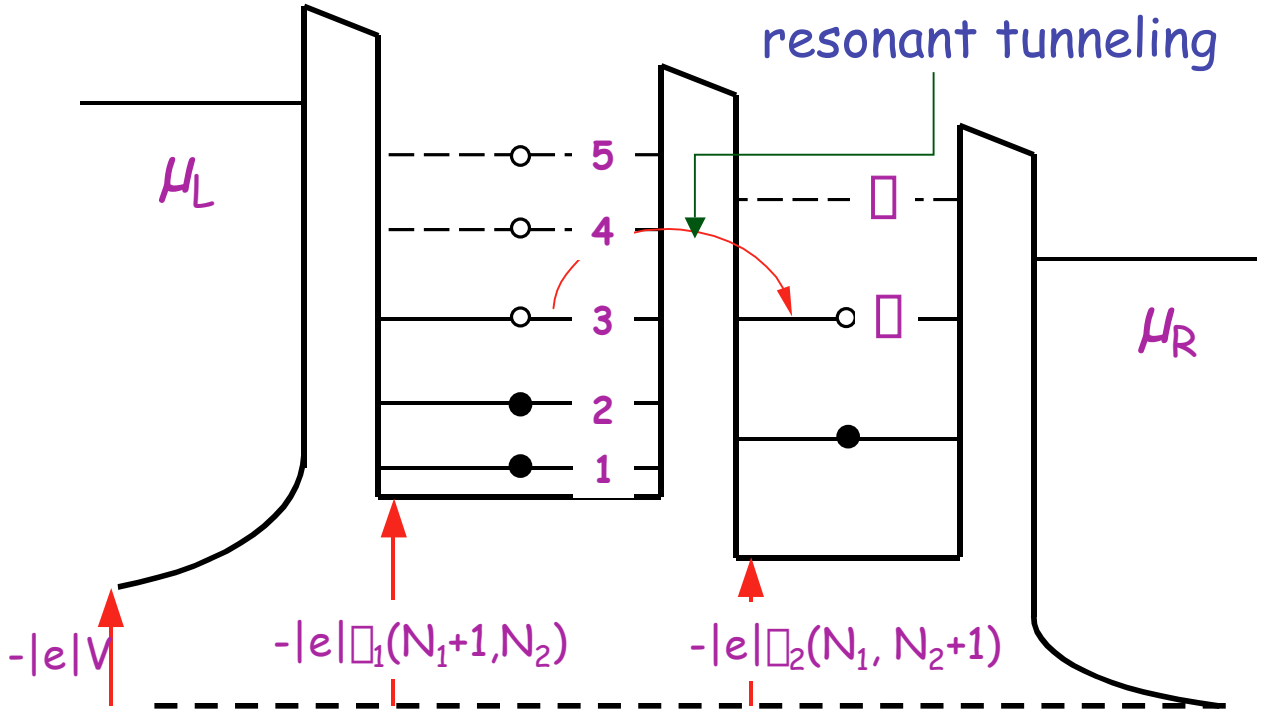
The decoherence time is about 5$\mu s$.



# Realizations *1-qubit, quantum dots*

- *Double quantum dots* : group of Kouwenhoven, (U. Delft Holland)

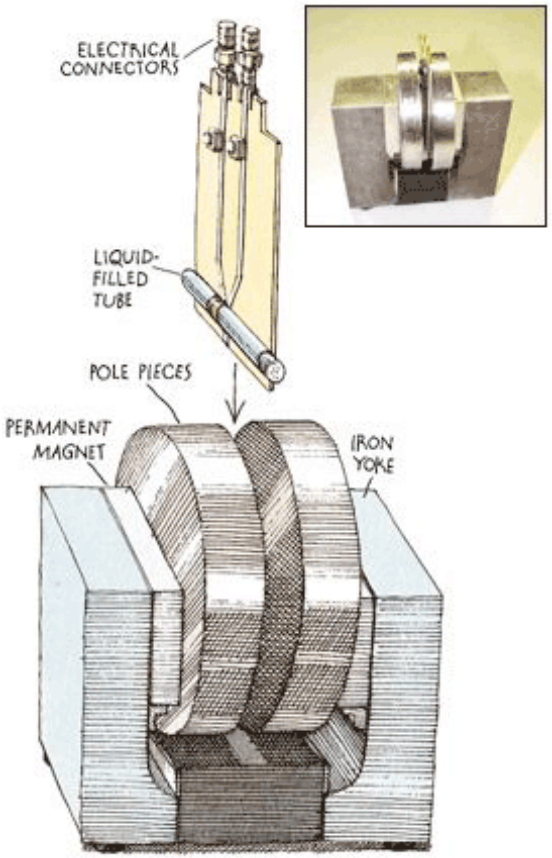


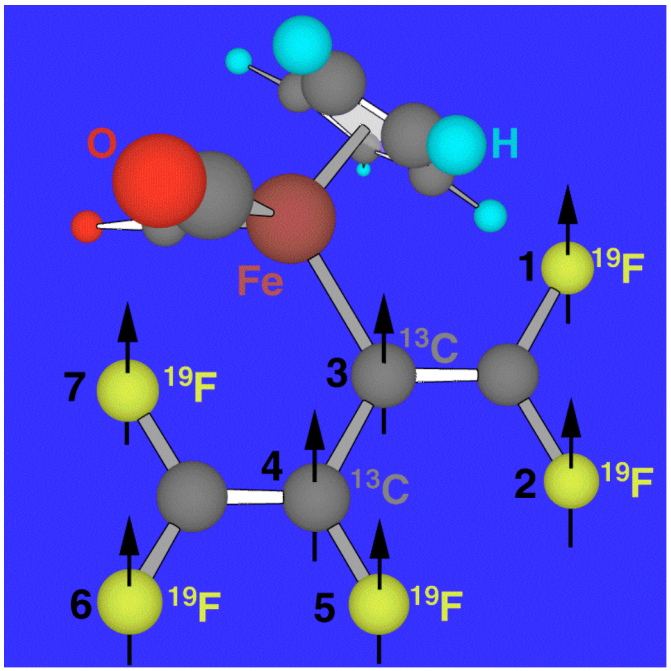


# Realizations *7-qubit, NMR*

- *Nuclear Magnetic Resonance* : IBM

15=3x5 !! (Shor's algorithm)



# CONCLUSIONS

*will quantum computers be built ?*

# To conclude (from Part I)

1. The elementary unit of quantum information is the *qubit*, with states represented by the *Bloch ball*.
2. Several qubits are given by tensor products leading to *entanglement*.
3. Quantum gates are given by unitary operators and lead to quantum circuits
4. Law of physics must be considered for a quantum computer to work: measurement, dissipation…

# To conclude (Part II)

1. Several algorithms are available: Fourier transform, phase estimation, quantum search, hidden subgroup, order-finding
2. Shor's algorithm for factoring shows enormous efficient and threaten present cryptography
3. Error-correcting codes are now available
4. Few qubits computer have been realized with NRM experiments

# To conclude (other topics)

1. A theory of quantum information and code theory is also available even though incomplete
2. Quantum cryprography exists (*Gisin*, Geneva)
3. Need for developments in quantum complexity theory: are notions of P- NP- completeness obsolete ?
4. Main problem: putting qubits together in concrete machines. Can one control entanglement and /or decoherence on a large scale ? … Not clear !!

# WILL QUANTUM COMPUTERS BE BUILT ?

**YES of course !!**