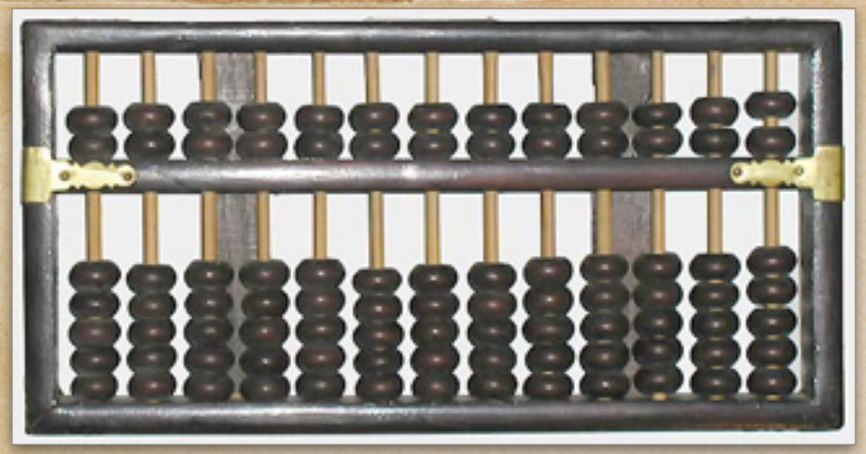
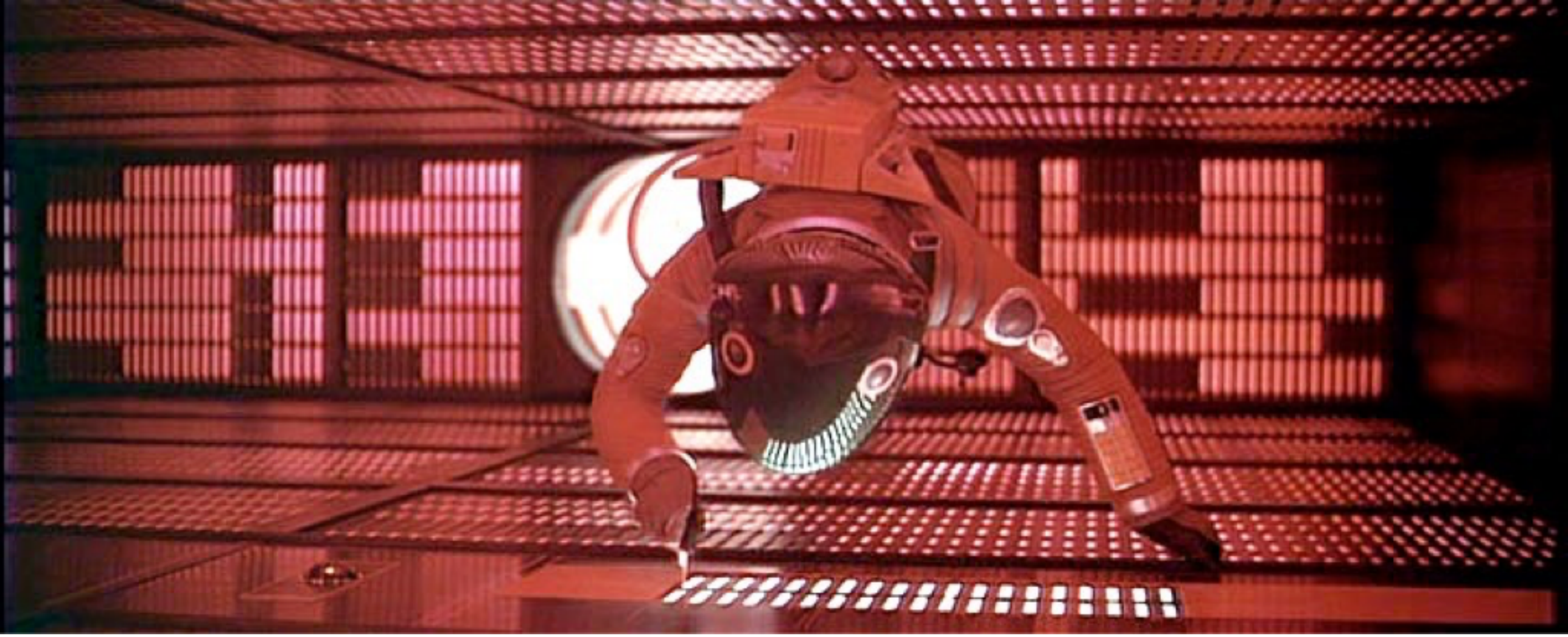
Preparandosi al Quantum Computing

Saverio Pascazio
Dipartimento di Fisica, Universita' di Bari, Italy
Istituto Nazionale di Fisica Nucleare, Bari, Italy

ReCaS, Bari, 12 July 2019

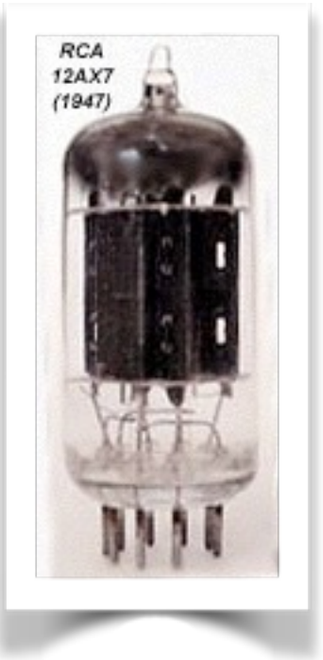




HAL 9000
2001 Odissea nello spazio

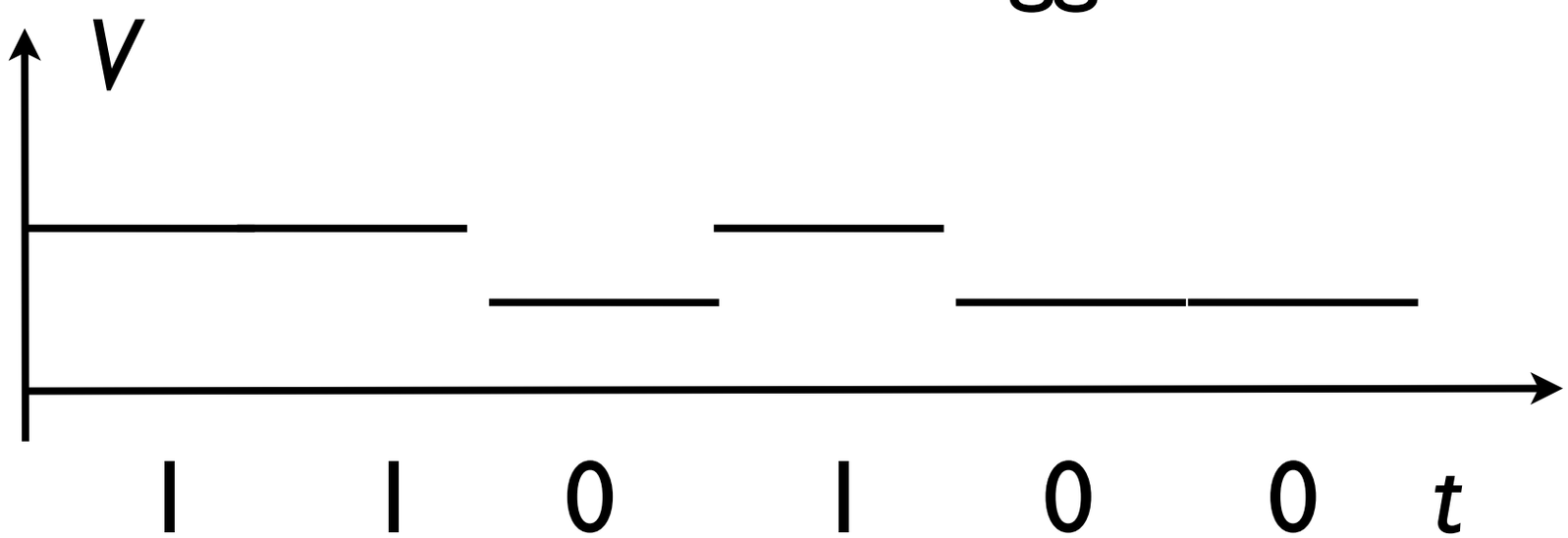
(1968)

I primi calcolatori a valvole



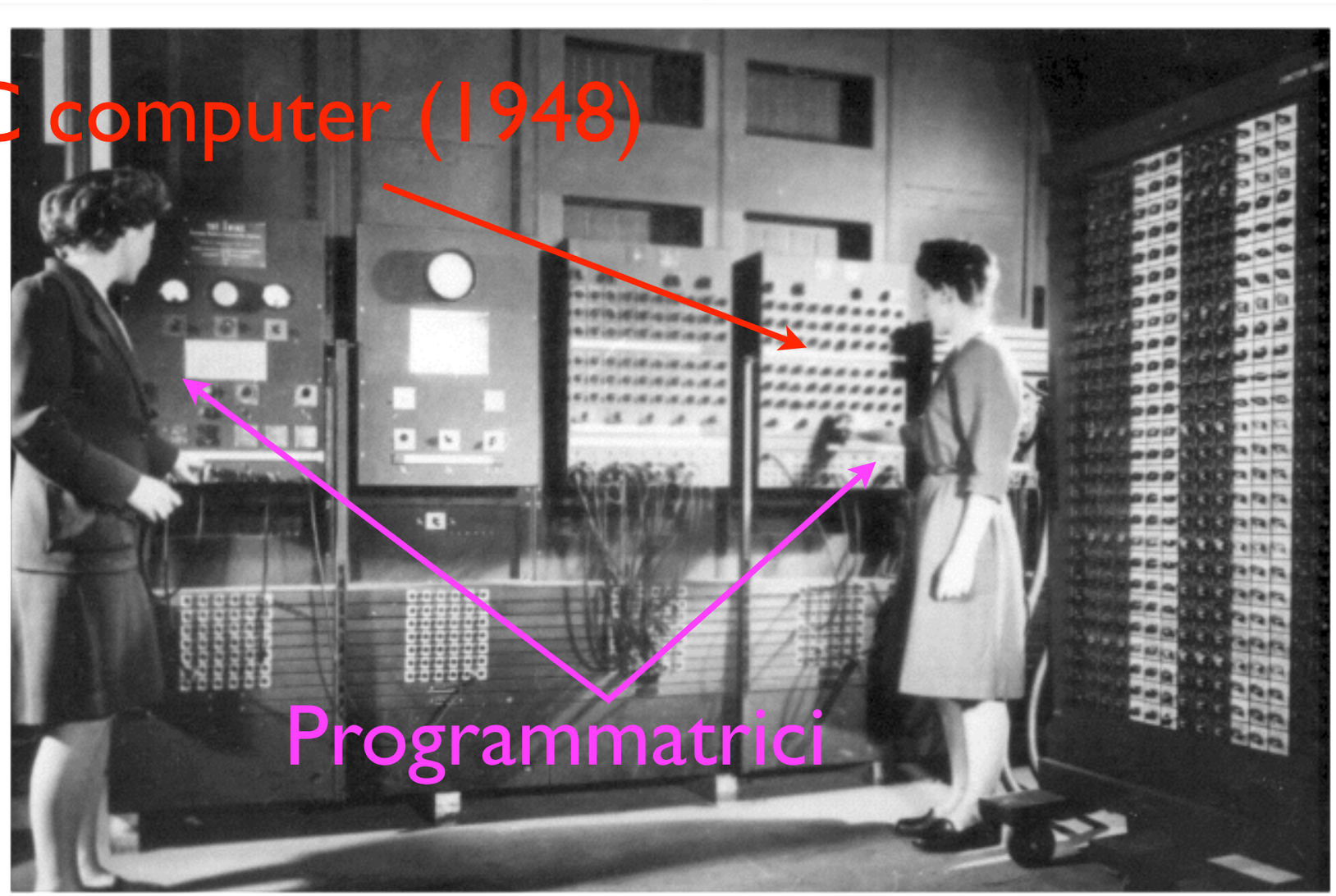
Tramite le valvole e' possibile controllare i livelli di voltaggio nel circuito

Due livelli di voltaggio: bit



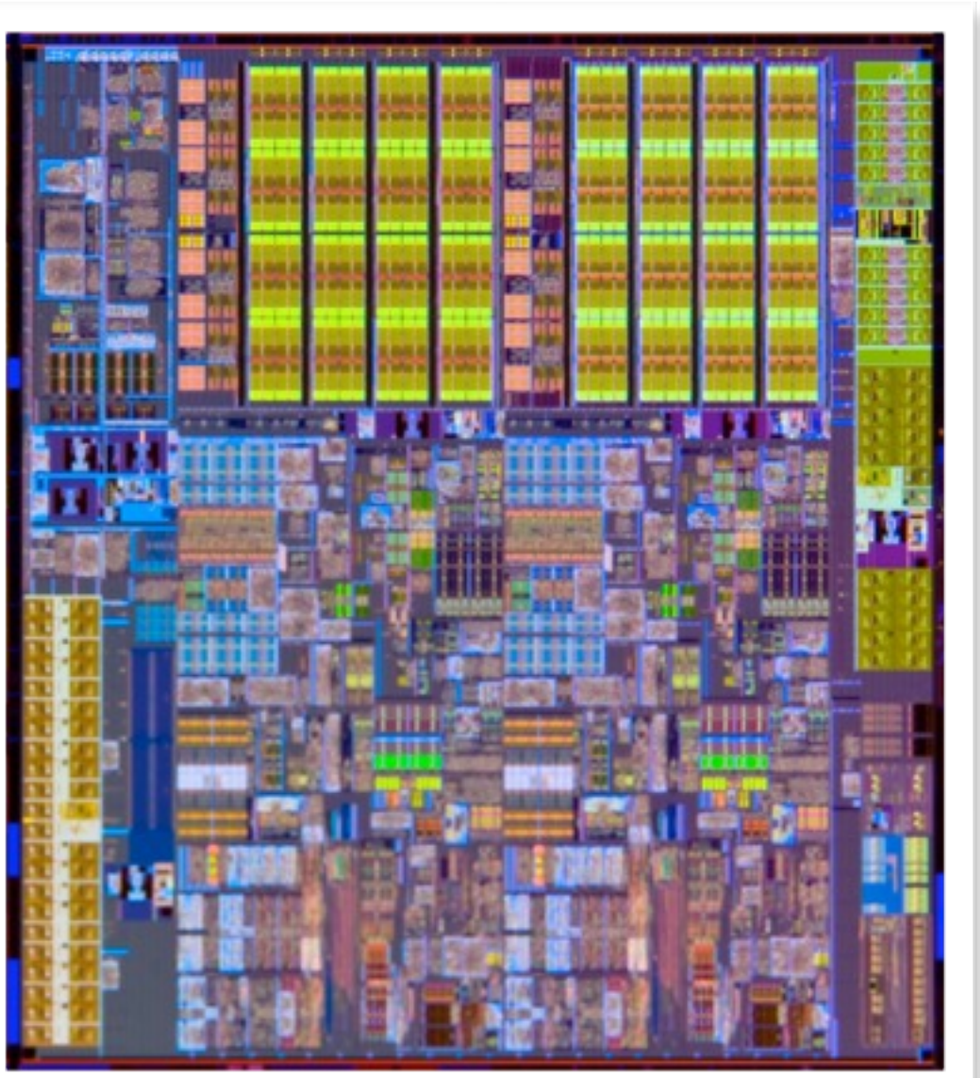
I primi calcolatori a valvole

Manipolando appropriatamente i due livelli di voltaggio si puo' creare una macchina di Turing universale

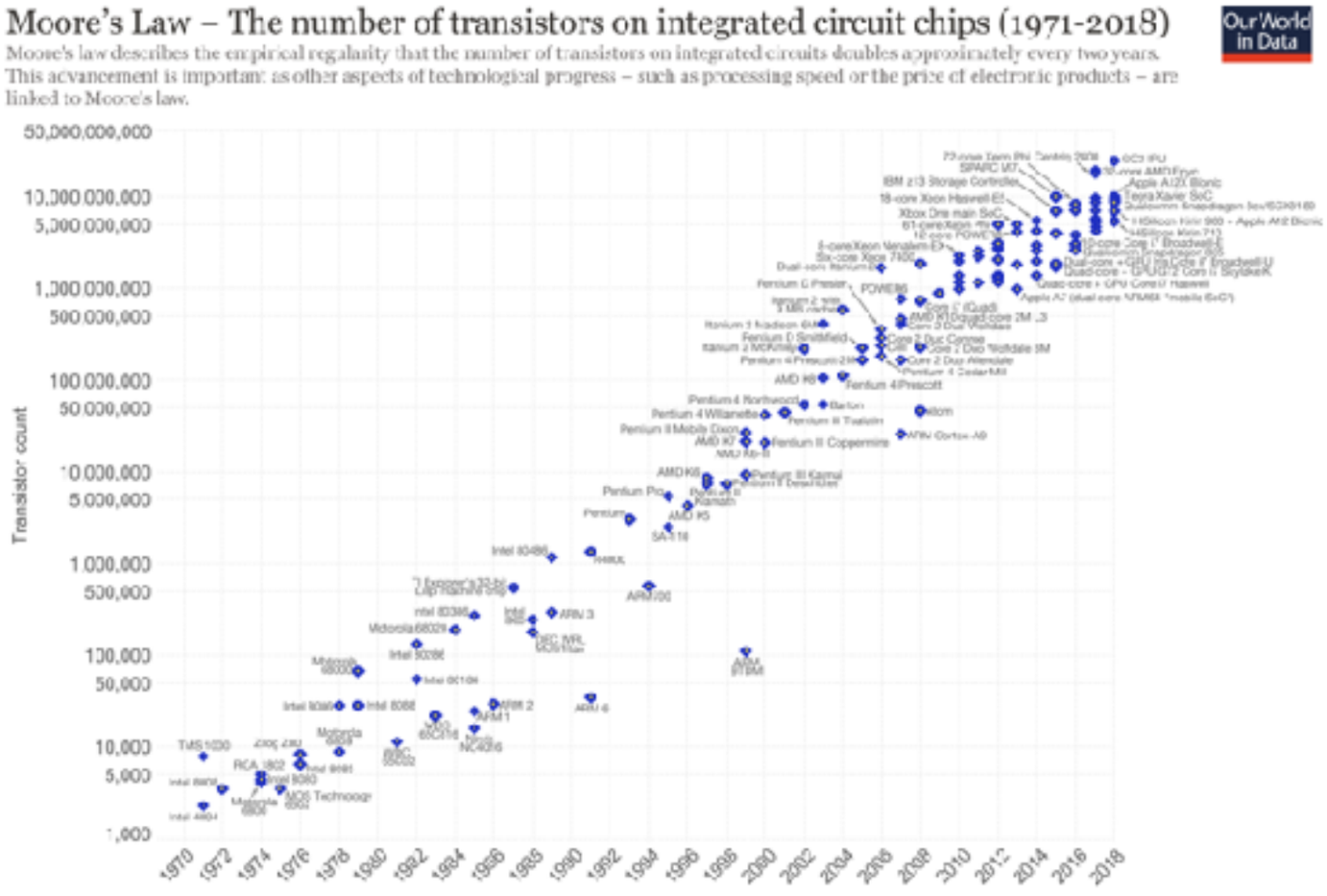


Il transistor

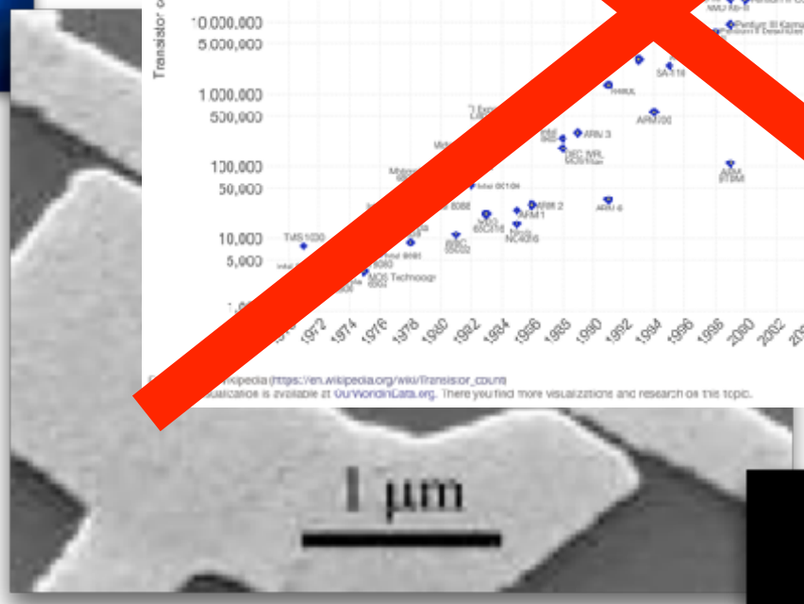
I transistor possono essere miniaturizzati



In questo Intel core i7 ci sono circa 1,000,000,000 di transistors

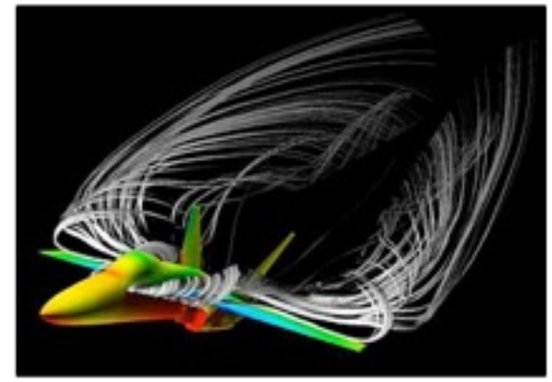


Miniaturizzazione

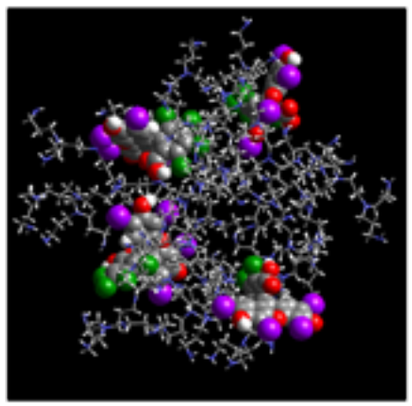


Computer moderni

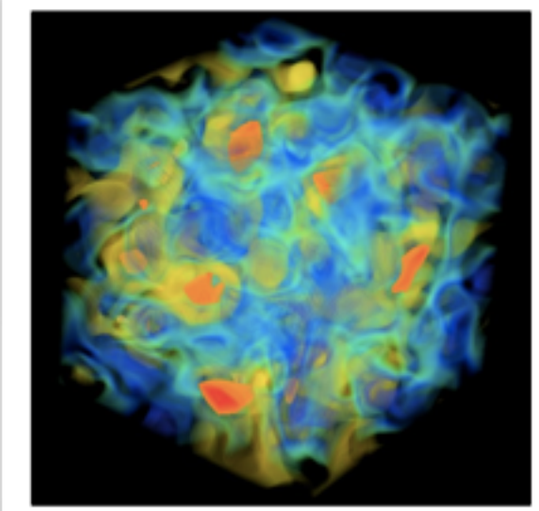
Crittografia



Progettazione: idrodinamica



Ricerca: chimica, farmaceutica

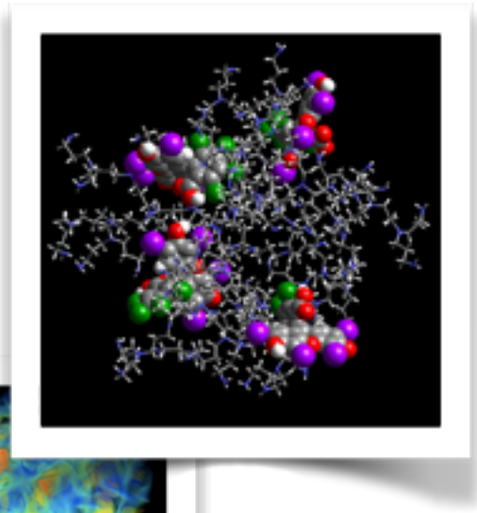


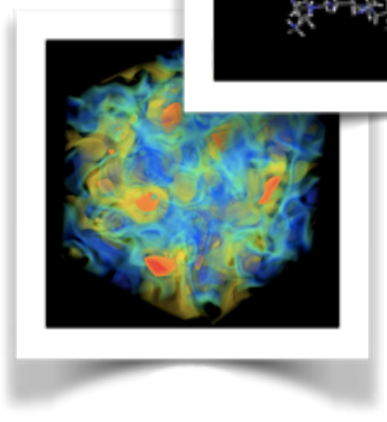
Ricerca: fisica

Sono tutti compiti difficili anche per i computer moderni!

Il computer del futuro

Un indizio su quale fenomeno fisico utilizzare viene dalla seguente osservazione





Nel mondo microscopico i fenomeni seguono le leggi della **meccanica quantistica**

Vogliamo descrivere una molecola complessa, diciamo che ha *N=100* livelli energetici e *M=40* elettroni

Tale molecola e' descritta da un vettore (funzione d'onda) con

13,746,234,145,802,811,501,267,369,720

componenti

Operation	Input	Output	Algorithm	Complexity
Addition	Two n-digit numbers N, N	One n+1-digit number	Schoolbook addition with carry	$\Theta(n)$, $\Theta(\log(N))$
Subtraction	Two n-digit numbers N, N	One n+1-digit number	Schoolbook subtraction with borrow	$\Theta(n)$, $\Theta(\log(N))$
Multiplication	Two n-digit numbers	One $2n$-digit number	Schoolbook long multiplication	$O(n^2)$
			Karatsuba algorithm	$O(n^{1.585})$
			3-way Toom–Cook multiplication	$O(n^{1.465})$
			k-way Toom–Cook multiplication	$O(n^{\log(2k-1)/\log k})$
			Mixed-level Toom–Cook (Knuth 4.3.3-T)[2]	$O(n 2^{\sqrt{2\log n}} \log n)$
			Schönhage–Strassen algorithm	$O(n \log n \log\log n)$
			Fürer's algorithm[3]	$O(n \log n\, 2^{2\log^* n})$
Division	Two n-digit numbers	One n-digit number	Schoolbook long division	$O(n^2)$
			Burnikel-Ziegler Divide-and-Conquer Division [4]	$O(M(n) \log n)$
			Newton–Raphson division	$O(M(n))$
Square root	One n-digit number	One n-digit number	Newton's method	$O(M(n))$
Modular exponentiation	Two n-digit numbers and a k-bit exponent	One n-digit number	Repeated multiplication and reduction	$O(M(n)\, 2^k)$
			Exponentiation by squaring	$O(M(n)\, k)$
			Exponentiation with Montgomery reduction	$O(M(n)\, k)$

Algebraic functions

Operation	Input	Output	Algorithm	Complexity
Polynomial evaluation	One polynomial of degree n with fixed-size polynomial coefficients	One fixed-size number	Direct evaluation	$\Theta(n)$
			Horner's method	$\Theta(n)$
Polynomial gcd (over $\mathbf{Z}[x]$ or $\mathbf{F}[x]$)	Two polynomials of degree n with fixed-size polynomial coefficients	One polynomial of degree at most n	Euclidean algorithm	$O(n^2)$
			Fast Euclidean algorithm [5]	$O(M(n) \log n)$

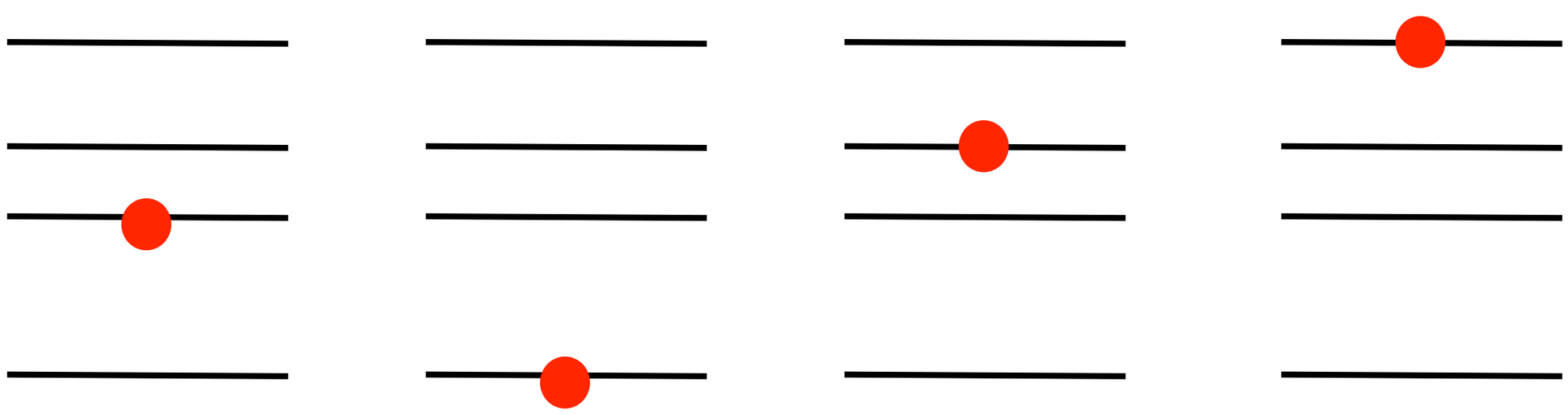
Special functions

la complessita' va legata al concetto che un calcolo e' "fisico"

La meccanica quantistica

Da dove viene questa complessita'?

Viene dal fatto che nel mondo microscopico succedono cose strane...



Un elettrone puo' stare con una certa probabilita' in ognuno di questi livelli

$$\psi = (\psi_1, \psi_2, \psi_3, \psi_4)$$

Vettore delle ampiezze di probabilita'

$$\psi_1^2 + \psi_2^2 + \psi_3^2 + \psi_4^2 = 1$$

Descrizione classica: 2 bit

"il computer quantistico e'
infinitamente piu' potente"

?

Multi-qubit Systems

2-qubit QC: $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$

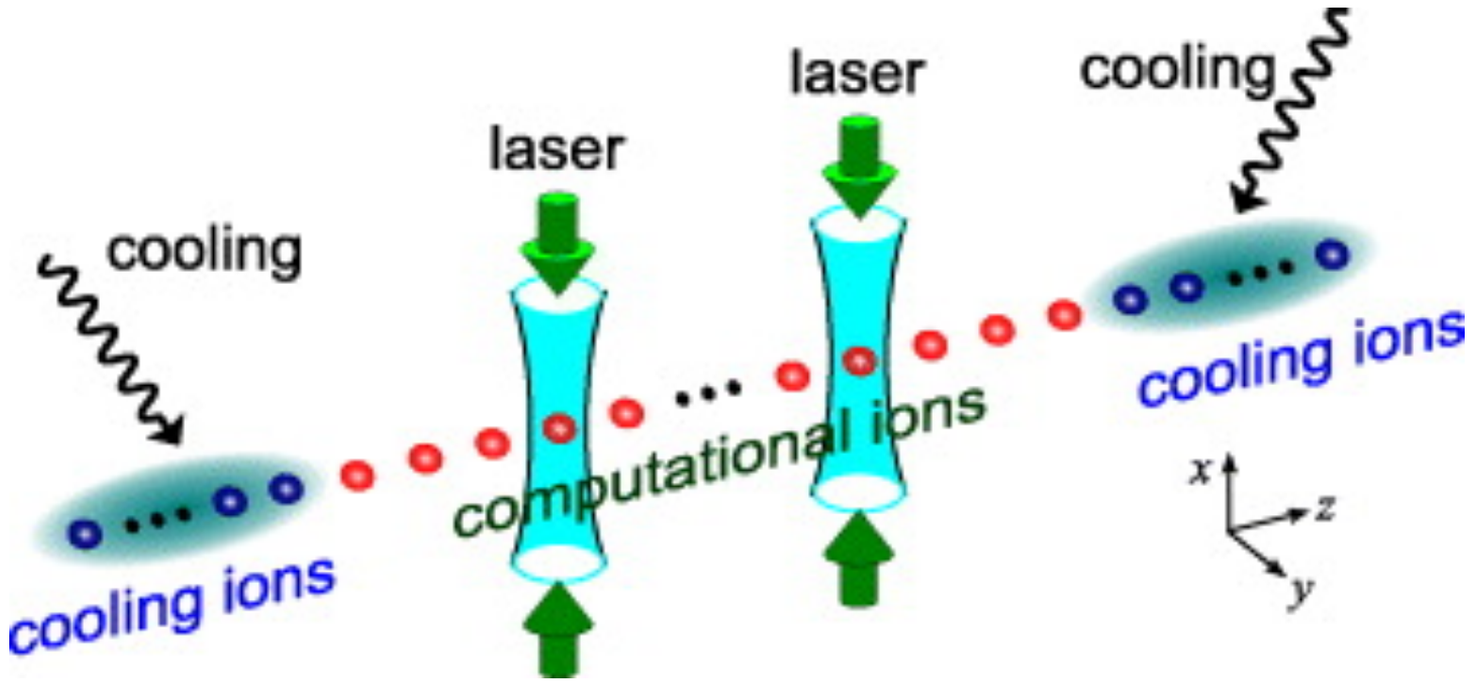
$$\Rightarrow |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle \mapsto |0\rangle, |1\rangle, |2\rangle, |3\rangle$$

N-qubit quantum computer $\longrightarrow$ 2^n states $|0\rangle, |1\rangle, \ldots |2^n - 1\rangle$

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

30 ioni in trappola



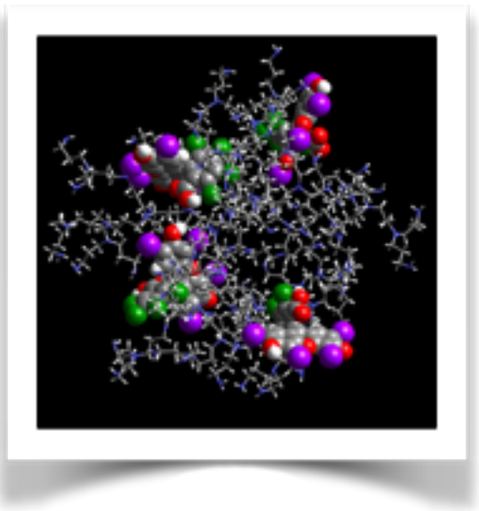
$$2^{30}(!)$$

le difficolta'

la coerenza (della fisica 2)

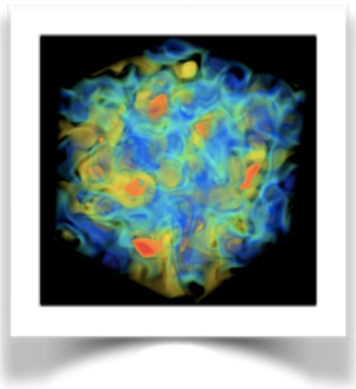
Il computer quantistico

Non abbiamo ancora realizzato un computer quantistico pero' sappiamo che, una volta realizzato, sara' piu' efficiente in molti compiti



I 100 livelli potranno essere studiati con 100 qubit, e non 800,000,000 GB

Potremo studiare con piu' successo la struttura della materia a distanze microscopiche

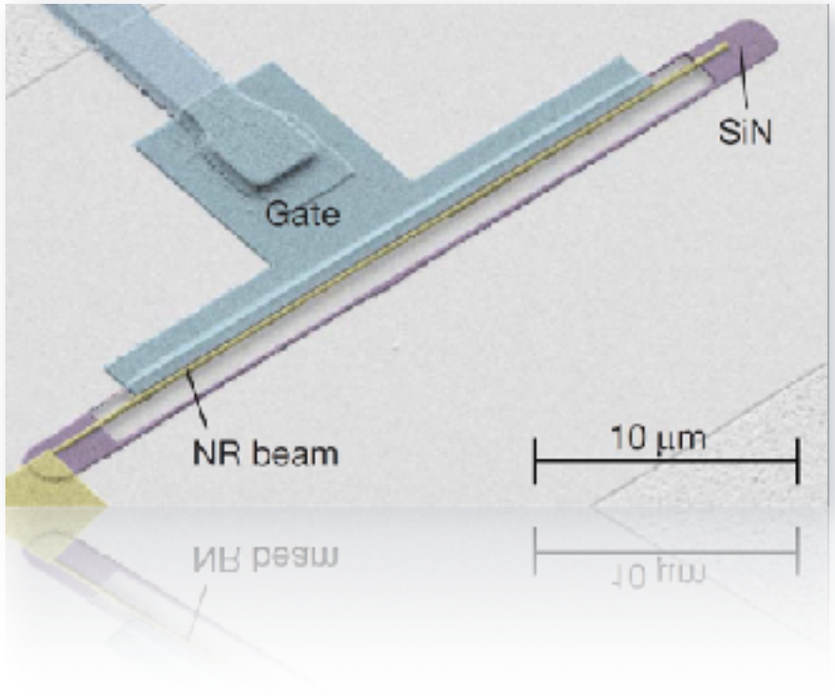


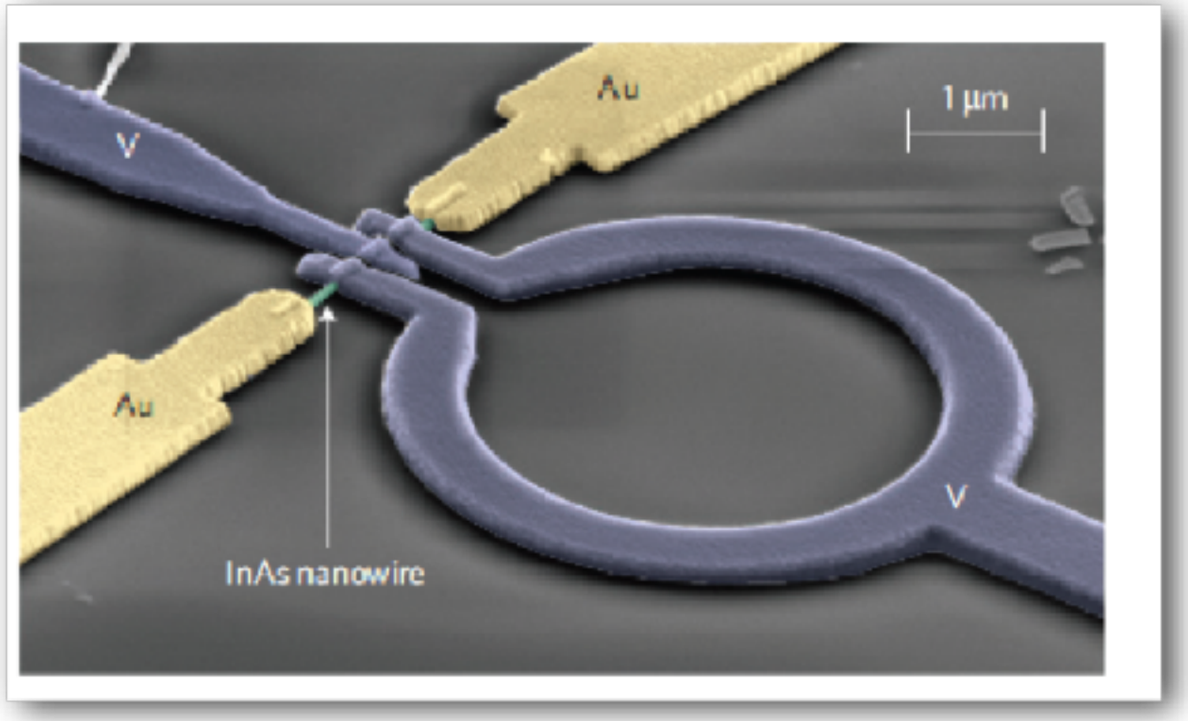
Computer Quantistici

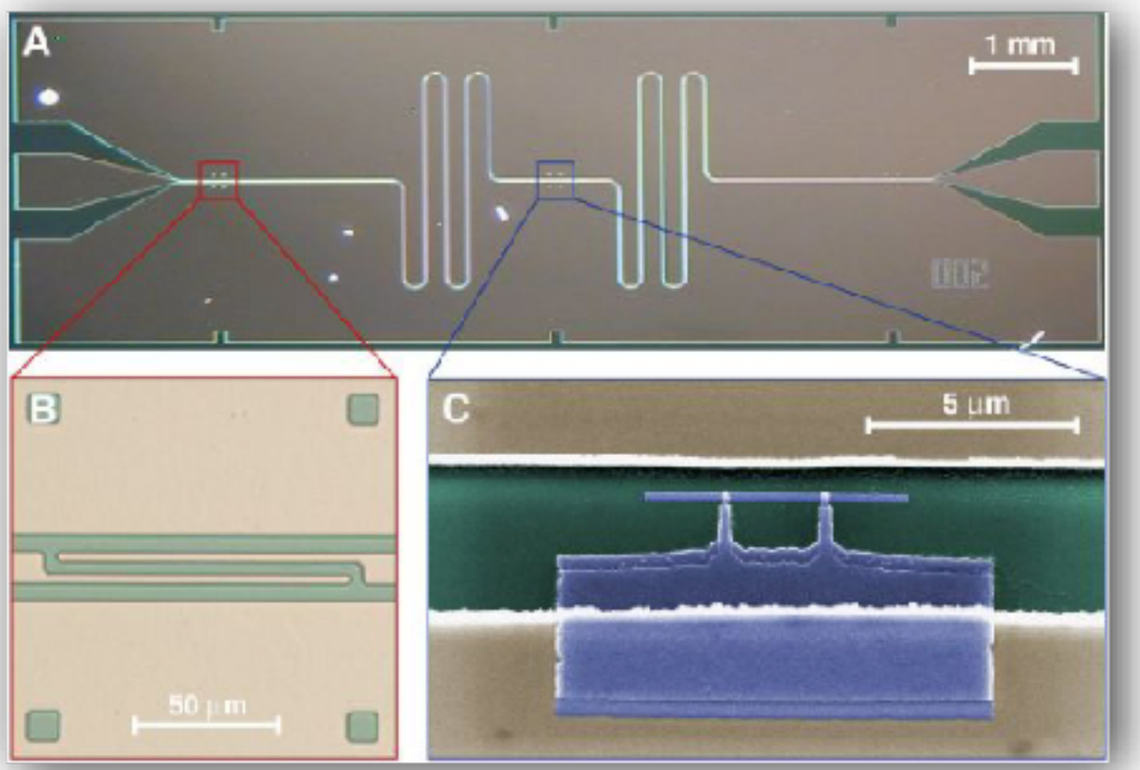
Google

rigetti

IBM Q


Gate
SiN
NR beam
10 µm


V
Au
1 µm
Au
InAs nanowire
V


A
1 mm
B
50 µm
C
5 µm