Università "Federico II"
SICSI – VIII Ciclo – Tecnologico

S.I.C.S.I
VIII ciclo - Tecnologico

STORIA DEL QUANTUM COMPUTER

dall'Informazione Classica (bit) all'Infomazione Quantistica (Qubit)

Specializzando:

Antonio Panaggio

Sommario

- Introduzione
- Breve storia dei calcolatori quantistici
- Dal Bit al Quantum Bit
- La potenza dei computer quantistici
- Algoritmi quantistici
- Linguaggi di programmazione quantistici
- Ostacoli ai Calcolatori Quantistici
- Dove e chi ci sta lavorando
- Cosa ci riserva il futuro
- Bibligrafia

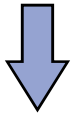
Secondo l'astrofisico Michio Kaku (è tra i padri della teoria delle stringhe) Il Pc quantico rappresenta "*the ultimate computer*", il computer definitivo: come a dire, dopo di esso nulla di più immensamente potente potrà essere creato.

Pensate ai Pc della Celera Genomics di Craig Venter, che hanno impiegato 4 anni a mappare il genoma di un moscerino: Un pc quantico ci metterebbe 10 minuti.

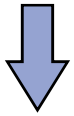
Riuscite ad immaginare quali cambiamenti potrebbe apportare questa scoperta?

Introduzione

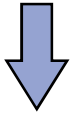
I calcolatori attuali sono milioni di volte più potenti dei loro antenati.



la tecnologia dei circuiti integrati sta raggiungendo i propri limiti fisici (della meccanica classica).

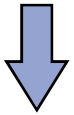


In accordo con la Legge di Moore degli anni sessanta, le capacità di integrazione di transistor su singolo chip stanno crescendo con legge esponenziale, raddoppiando ogni 18 mesi circa.

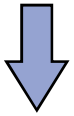


Introduzione

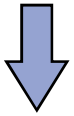
Incremento non infinito, si fermerà nei prossimi dieci anni



la materia comincia a comportarsi come un aggregato di singoli atomi e il funzionamento dei circuiti diventa problematico.



necessario sostituire o affiancare nuove tecnologie alle attuali.



Questa nuova tecnologia prende il nome di
"**Quantum Computing**".

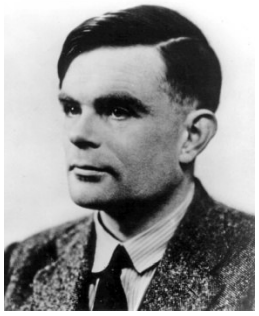
Introduzione

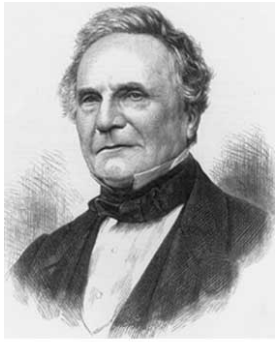
- Sul piano degli atomi, la materia obbedisce alle regole della meccanica quantistica.
- Il computer quantistico non è un'evoluzione di quello classico ma una macchina del tutto diversa, può offrire molto di più della diminuzione delle dimensioni e dell'aumento della velocità di clock dei calcolatori.
  - Dai tempi di Turing, fino ad oggi nessun cambiamento sostanziale ha avuto luogo nell'idea di che cosa sia e come operi un computer. I computer non sono altro che realizzazioni fisiche della macchina di Turing universale. Pur con delle sostanziali differenze, anche il più semplice PC può affrontare, seppur più lentamente, qualsivoglia problema risolubile da un supercomputer.
- **L'introduzione della computazione quantistica stravolgerà completamente l'informatica, e il trattamento dell'informazione, in quanto permetterà di risolvere problemi scientifici che sono attualmente irrisolvibili.**

Un po' di storia

PADRI DELL'INFORMATICA CLASSICA

- Il padre dell'Informatica è probabilmente Alan Turing (1912-1954), ed il suo profeta è Charles Babbage (1791-1871).
- Babbage, infatti, ha concepito gli elementi essenziali di un calcolatore moderno, nonostante ai suoi tempi non esistesse la tecnologia necessaria a realizzare praticamente le sue idee.
- È dovuto passare un intero secolo prima che l'Analytical Engine di Babbage fosse migliorata in quello che Turing ha descritto come la Universal Turing Machine, verso la metà degli anni Trenta.





Library of Congress

Un po' di storia

PADRI DELL'INFORMATICA CLASSICA

- La computazione classica si basa sul modello astratto della Macchina di Turing, definito nel 1936 dal matematico inglese A. Turing e successivamente rielaborato da John von Neumann negli anni '40.

- La macchina di Turing (MT) utilizza gli assiomi della fisica classica, ossia lo stato del nastro e della testina sono sempre univocamente identificabili, gli spostamenti sono sempre regolati dalle leggi del moto, etc. Quindi la MT è totalmente deterministica (MTD).

Un po' di storia

- Per lungo tempo non si è data molta importanza alle modalità fisiche secondo le quali un dispositivo di calcolo viene realizzato.
- A questa seconda possibilità cominciò subito a riflettere Richard Feynman, tentando di concepire una macchina funzionante sulla base dei principi della fisica quantistica.

Un po' di storia

PADRI DELL'INFORMATICA QUANTISTICA

- Nel 1982 R. Feynman pubblica il suo famoso lavoro sul Computer Quantistico. In esso, dimostrò che:
  - che nessuna Macchina di Turing classica poteva simulare certi fenomeni fisici senza incorrere in un rallentamento esponenziale delle sue prestazioni *(nel senso della teoria della complessità algoritmica).*
  - Al contrario, un "simulatore quantistico universale" avrebbe potuto effettuare la simulazione in maniera più efficiente.

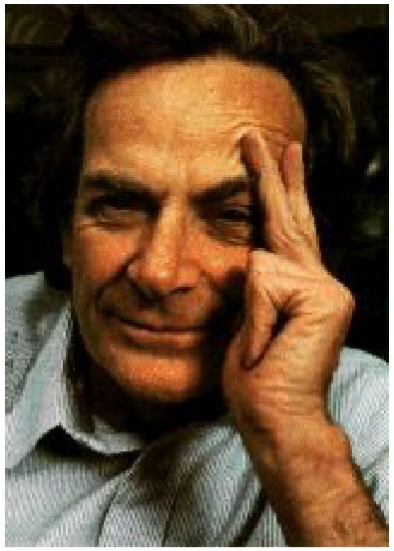


Figura 1: R. Feynman

Un po' di storia

- Finalmente, nel 1985, David Deutsch dell'Università di Oxford descrive la prima vera MTQ.
- Formalizzò le idee di Feynman nella sua Macchina di Turing Quantistica Universale, che rappresenta in teoria della calcolabilità quantistica esattamente quello che la Macchina di Turing Universale rappresenta per la calcolabilità classica e ha portato alla concezione moderna di *computazione quantistica.*
- Poco dopo david deutsch dell'istituto di matematica dell'universita' di oxford e altri scienziati statunitensi costruirono modelli di calcolatori quantistici per studiarne le differenze rispetto a quelli classici.

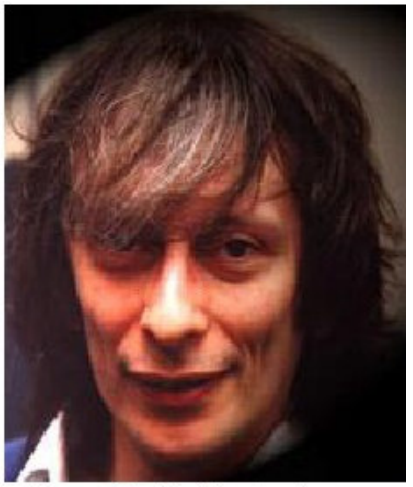


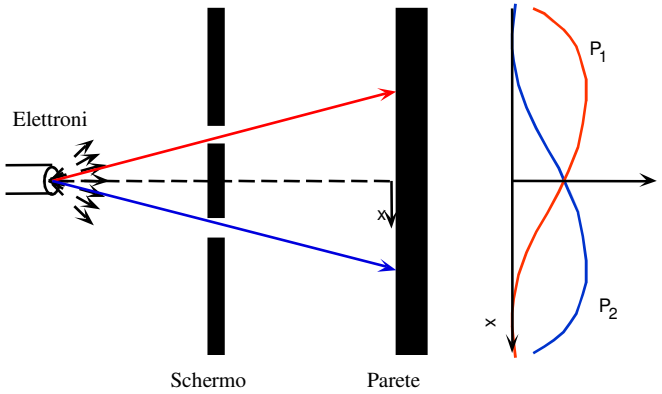
Figura 2: D. Deutsch

A questo punto fermiamoci con la storia e cerchiamo di capire su che principi di funzionamento di basa il computer quantico….

- La meccanica quantistica si è sviluppata nel corso dei primi trent'anni del '900 portando a compimento una trasformazione nella visione delle cose nel mondo fisico.
- A questa rivoluzione parteciparono alcune delle più grandi menti del secolo scorso: Plank, De Broglie, Bohr, Heinsenberg, Shrodinger, Dirac e, naturalmente Einstein, il quale, fatto forse poco noto, ha vinto il nobel per la sua spiegazione quantistica ante litteram dell'effetto fotoelettrico e non per la teoria della relatività generale.

Concetto base del QC: Interferenza di particelle e stati sovrapposti

- La luce è costituita da particelle dette fotoni.



- Consideriamo una sorgente di luce monocromatica S e uno schermo che lascia passare fotoni solo tra due sottili fori F_1 e F_2 praticati su di sesso.
- Supponiamo di misurare il numero di fotoni emessi che in media arrivano alla parete quando solo uno dei fori è aperto:
  - scopriamo che questa percentuale è pressoché identica per i due fori e supponiamo che questa percentuale sia dell'1%.

Cosa succede invece se i fori sono entrambi aperti?

- La risposta "macroscopica" è banale:

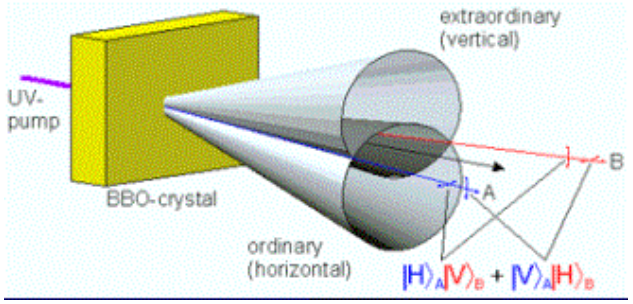
se con un foro alla volta arriva in P l'1% dei fotoni, con entrambi i fori aperti arriverà circa il 2% dei fotoni.

- Ma la risposta a livello microscopico non è questa.

dietro lo schermo si creano zone di buio e massima intensità luminosa che si alternano in modo regolare: queste corrispondono alle zone in cui le onde sferiche luminose che escono dalle due fenditure si rinforzano (interferenza costruttiva) o si annullano (interferenza distruttiva).

Si trova che la percentuale di fotoni emessi che arriva in P, varia da 0 e il 4% !!!

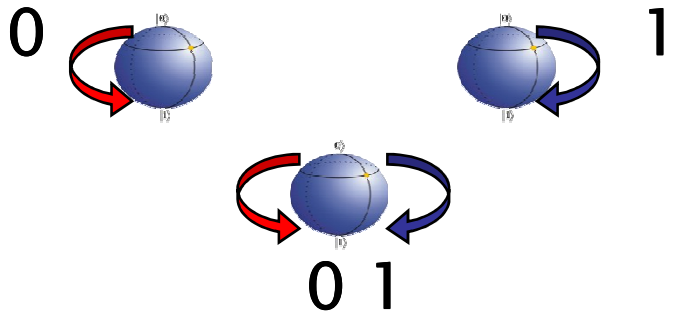
- Questo porta in realtà a pensare che i fotoni emessi da S e che arrivano in P siano ben rappresentati dalla sovrapposizione di due stati possibili: quello in cui il fotone è arrivato ad P passando da F_1 e quello in cui il fotone è arrivato ad P passando da F_2.
- Se noi cercassimo di scoprire da quale fenditura è passato il fotone, misurando in qualche modo il suo passaggio attraverso i fori, ciò comporta di far "collassare" il sistema in uno stato ben preciso cancellando la sovrapposizione (questo è uno dei postulati della meccanica quantistica).
- L'idea di costruire dei dispositivi che implementino la sovrapposizione degli stati e che permettano di fare delle operazioni sugli stati sovrapposti senza "distruggerli" sta alla base di quella che sarà la futura tecnologia dei computer quantistici.



Dal bit al Qubit

- I computer classici che tutti conosciamo utilizzano come unità di informazione di base il cosiddetto bit.
- Da un punto di vista prettamente fisico il bit è un sistema a 2 stati: - no o sì, falso o vero, o semplicemente 0 o 1.

- Il Computer Quantico utilizza un "**Qubit**" (Quantum bit), una particella che esiste in due stati nello stesso istante — come consentono le bizzarre regole della fisica quantistica — sia 1 che 0 contemporaneamente.
  - Per esempio un Qubit può essere rappresentato come lo spin di un elettrone, dove l'elettrone non sia in uno stato definito, ma in sovrapposizione di stati 0 (Spin "su ") e 1 (Spin "giù ").



Il Quantum bit

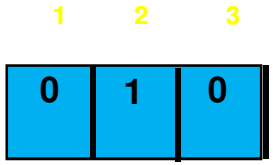
- Un qubit è una "sovrapposizione" di 0 e 1 e può essere definito dalla notazione matematica

a |0> + b |1>

- intendendo con ciò che se misurato esso potrà valere 0 con probabilità a e 1 con probabilità b
  - Non si vuole, per semplicità, approfondire la natura matematica degli stati rappresentati dal simbolo |>, ma è bene comunque ricordare che tale simbolo sta a rappresentare un vettore, per sua natura orientato. Lo stato |1 >+|0> è diverso dallo stato |0 >+|1>
  - Quando misuriamo lo stato del qubit lo facciamo collassare dalla sua sovrapposizione di |0 e 1.
  - Si è lungamente riflettuto sul significato di una simile concettualizzazione: che cosa significa affermare che lo stato di una particella è un insieme di possibili stati? Un elettrone è qui o là?
  - Nel mondo quantistico l'elettrone è sia qui sia là, ma con diverse probabilità di essere qui e là. Soltanto dopo una misura si può dire se sia qui. Otteniamo un valore preciso per una quantità che prima era semplicemente una delle tante possibilità. È proprio l'osservazione che provoca la "scelta " di quel particolare valore fra tutti quelli possibili.

Il Quantum bit

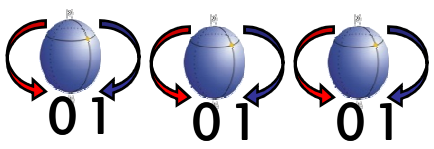
- Si consideri un registro composto da 3 bit.



Registro classico

Possiamo rappresentare fino a 8 diversi numeri possibili, cioè esso può trovarsi in una delle otto possibili configurazioni 000, 001, 010, ..., 111.

- Consideriamo ora un registro quantistico composto da 3 qubit (Quantum Bit)



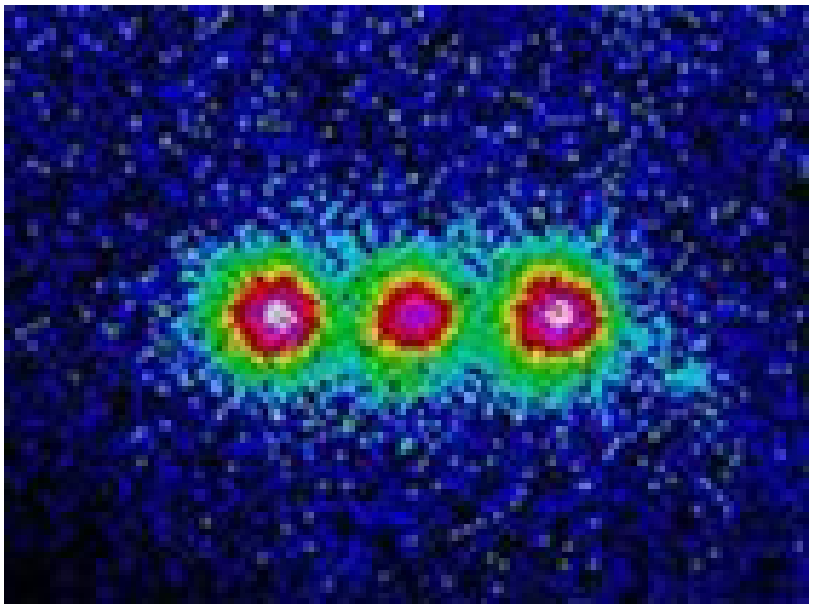
Registro quantistico

Esso sarà in grado di contenere fino a tutti gli 8 numeri contemporaneamente in una sovrapposizione quantistica, cioè tramite una *sovrapposizione coerente di stati.*

Il qubit esiste sia come 0 che 1.

- E' proprio grazie a questa *caratteristica del qubit* che un elaboratore quantistico sarebbe in grado di fare calcoli infinitamente più complessi di quelli consentiti con un computer tradizionale, perché invece di operare in modo seriale, sarebbe in grado di elaborare l'informazione in parallelo, come fa il cervello.

Il Quantum bit



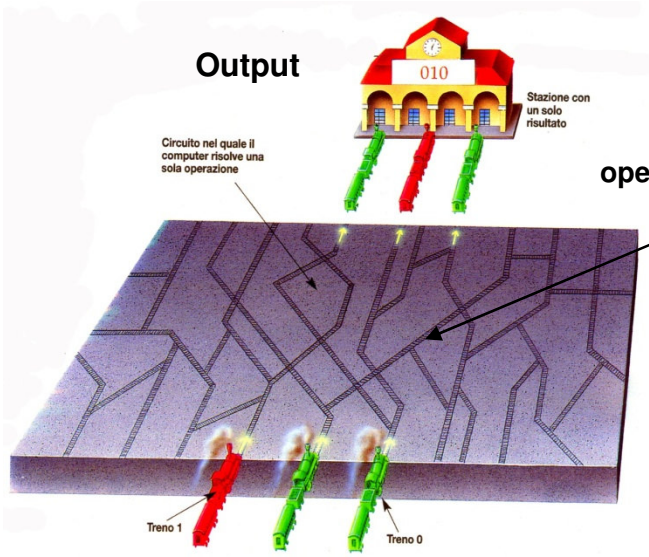
Un registro di qubit realizzato con ioni di berillio

Il Quantum bit

Calcolo classico

Ogni (treno)bit di input vale 0 o 1

Dato un input x ho solo l'output per quel valore di x

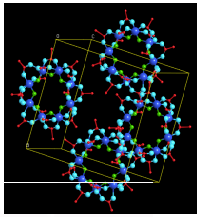


Input: x

Calcolo parallelo quantistico

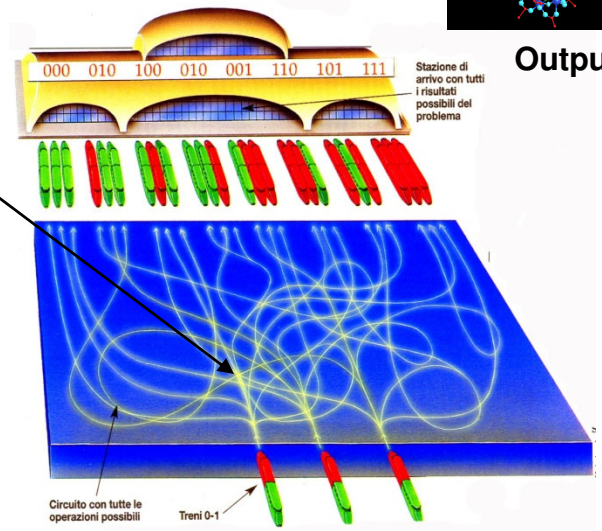
Ogni (treno)qubit di input vale contemporaneamente sia 0 che 1

In un singolo calcolo ho l'output per tutti i possibili valori di x



Output

operazione logica elementare



Input

Il Quantum bit

- Su un computer quantistico, con 3 qbit, le otto combinazioni possono essere memorizzate e manipolate contemporaneamente.
- Questo meccanismo realizza una "parallelizzazione" della elaborazione le cui potenzialità crescono in modo esponenziale rispetto al numero di qbit coinvolti.
- Se aggiungessimo più qubit al registro la sua capacità di memorizzare informazioni crescerebbe in maniera esponenziale:

in generale L qubit sono in grado di conservare 2^L numeri contemporaneamente.

- Un registro di 250-qubit, per capirci, composto essenzialmente di 250 atomi, sarebbe capace di memorizzare più numeri contemporaneamente di quanti siano gli atomi presenti nell'universo conosciuto.

Un dato senza dubbio scioccante.

La potenza del Qubit

Bisogna però comprendere bene un aspetto della questione:

- I computer quantistici possono sfruttare la sovrapposizione degli stati per fare calcoli in parallelo, un calcolatore quantistico è in grado di effettuare operazioni matematiche su tutti i dati contemporaneamente, allo stesso costo in termini computazionali dell'operazione eseguita su uno solo dei numeri, ma la lettura dei dati è possibile solo alla fine di un ciclo di elaborazioni perché, come abbiamo già detto, la lettura fa scomparire lo stato di sovrapposizione e dal registro posso leggere un solo numero.

- Questa tecnica può risultare enormemente vantaggiosa qualora si debba utilizzare il computer per valutare una serie di dati numerosissima.

…. ritorniamo alla storia

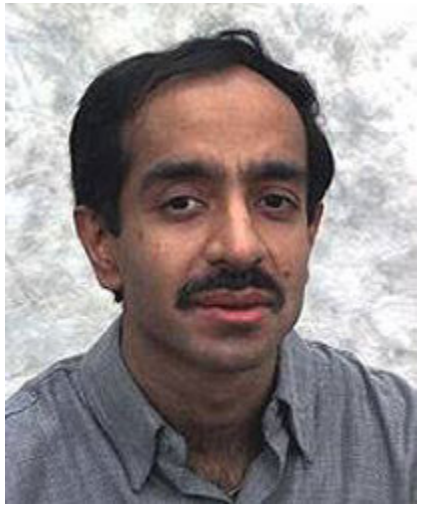
Un po' di storia

- Nella seconda metà degli anni ottanta, per diversi motivi, le ricerche languirono.
- Tuttavia nell'ultimo decennio il quadro e' cambiato.
- Molti studiosi hanno cercato quindi di sviluppare algoritmi per risolvere compiti complessi per questa tipologia di macchina.

Algoritmi quantistici

Algoritmo di Grover

- Nel 1996, Lov Grover dei Bell Labs della AT&T, introdusse un metodo quantistico per risolvere problemi di ricerca non strutturati dove il miglior algoritmo classico che si possa applicare è quello di scandire tutti gli elementi dello spazio di ricerca finché non si è trovata la soluzione.



Dr Lov K. Grover, physcien aux Bell Labs/Lucent Technologies

Algoritmi quantistici

Conseguenze dell'algoritmo di Grover

- Pensiamo, ad esempio, di dover ricercare un numero di telefono specifico all'interno di un elenco contenente 1 milione di elementi, ordinati alfabeticamente: è ovvio che nessun algoritmo classico più migliorare il metodo di ricerca a forza bruta che consiste nella semplice scansione degli elementi fino a quando non si trova quello che ci interessa. Gli accessi alla memoria richiesti nel caso medio saranno pertanto 500.000!!!
- Un computer quantistico è invece in grado di esaminare tutti gli elementi simultaneamente in un sol colpo!!!

Osservazione

- Se fosse programmato per stampare semplicemente il risultato a questo punto, però, non costituirebbe un miglioramento rispetto all'algoritmo classico, perché solamente uno sul milione dei percorsi di calcolo effettuati conterrà l'elemento a cui siamo interessati, e per conoscerlo dovremo per forza di cose ispezionarli tutti.

Algoritmi quantistici

- Un'altra importantissima applicazione dell'algoritmo di Grover è nel campo della crittanalisi, per attaccare schemi crittografici classici come il Data Encryption Standard (DES) con un approccio a forza bruta.
- Crackare il DES fondamentalmente richiede una ricerca tra tutte le $2^{56} = 7 \times 10^6$ possibili chiavi.

- Un computer classico,impiegherebbe migliaia di anni a scoprire quella corretta; un computer quantistico che utilizzi l'algoritmo di Grover, invece, ci metterebbe pochissimi secondi.

Algoritmi quantistici

Algoritmo di Shor

- Nel 1994 Peter W. Shor (AT&T Labs) dimostra che il problema della fattorizzazione dei numeri primi (classicamente considerato intrattabile perché cresce esponenzialmente con N) si può risolvere efficientemente (cioè in tempo polinomiale) con un algoritmo quantistico.

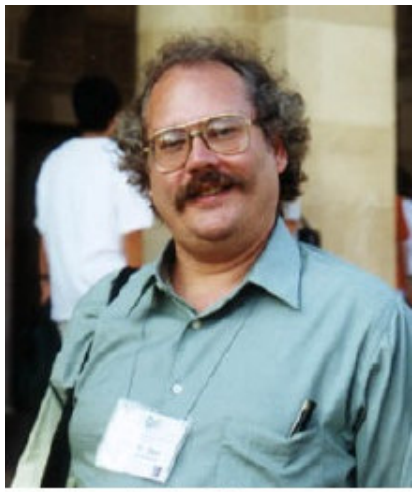


Figura 3: P. Shor

Algoritmi quantistici

Conseguenze dell'algoritmo di Shor

- Ricavarne i fattori di un numero primo non è altrettanto facile, e tutti i sistemi crittografici più diffusi, come ad esempio RSA, (tale algoritmo crittografico è al momento largamente impiegato per proteggere le comunicazioni più riservate e le transazioni bancarie) sfruttano la credenza di molto scienziati che non esista un algoritmo polinomiale per la fattorizzazione, o che se esista sia computazionalmente difficile.
- L'algoritmo di Shor ha aperto nuove problematiche legate alla crittografia.
- Con queste nuove scoperte tutto questo potrebbe decadere e rendere completamente inutili gli esistenti sistemi crittografici, resi vulnerabili da attacchi crittoanalitici di tipo quantistico.

Linguaggi di programmazione quantistico

- Con il passare del tempo sono state create le basi per lo sviluppo di proposte di linguaggio di programmazione d'alto livello per i computer quantistici, come ad esempio:
  - Q-gol (Greg Baker, 1996)
  - qGCL (Paolo Zuliani, 2000)
  - Quantum C Language (Stephen Blaha, 2002)
- Il più evoluto progetto si è dimostrato quello di Zuliani il quale ha proposto un formalismo astratto con rigide regole semantiche.
- L'obiettivo è quello di sviluppare un linguaggio che permetta di operare con i computer quantistici facendo uso di un formalismo simile a quello dei linguaggi esistenti (ad esempio con una sintassi simile al C).

Linguaggi di programmazione quantistico

- Nella seguente tabella vengono mostrate le principali differenze tra un linguaggio di programmazione classico ed un linguaggio quantistico

Linguaggio classico	Linguaggio quantico
Architettura classica	Architettura quantistica
Variabili	Registri quantistici
Input classico	Misurazione quantica
Espressioni booleane	Condizioni quantiche

Tabella 2: Differenze tra un linguaggio classico ed uno quantistico

Linguaggio di programmazione quantistico

- Un esempio di applicativo per un linguaggio di programmazione quantistica è qlc. Utilizza una sintassi molto simile a quella del C. Per capire meglio mostriamo alcuni comandi.

```
$ qcl --bits=5
[0/8] 1 |00000>
qcl> qureg a[1];
qcl> dump a
: SPECTRUM a: |....0>
1 |0>
```

- In questo modo abbiamo eseguito i seguenti passi:
  - utilizziamo con 5 qubits;
  - lo stato della macchina è inizializzato a zero (|00000>);
  - qureg a[1] alloca un bit per a.
  - Il comando dump a ci da informazioni su a, in particolare ci dice:
    - SPECTRUM ci dice dove i qubits per a sono stati allocati.
    - Dovremmo misurare il valore 0 con probabilità 1.

Ostacoli ai calcolatori quantistici

- Ci sono almeno due tipi di problemi che occorre risolvere:

Decoerenza

- I calcolatori quantistici operano ad un livello infinitesimale della materia. A causa del loro dominio di applicazione sono facilmente soggetti a problemi di rumore ed interferenza.
- Nella manipolazione dei qubit l'ambiente esterno va a interferire con il loro stato inquinando i risultati, dando luogo al fenomeno conosciuto come *decoerenza (decoherence).*

Collegamento

- Collegare fra loro due porte quantiche e' cosa difficilissima: il cavo deve essere in grado di smontare l'atomo per spostare a volonta' elettroni e protoni e poi di ricomporlo e tutto senza modificare lo spin delle particelle.
- Esistono pero' altre soluzioni al problema dei collegamenti: j. Ignacio cirac dell'universita' di castiglia-la mancia in spagna e peter zoller dell'universita' di innsbruck hanno proposto uno schema che isolerebbe i qbit in una trappola ionica.

Dove e chi ci sta lavorando

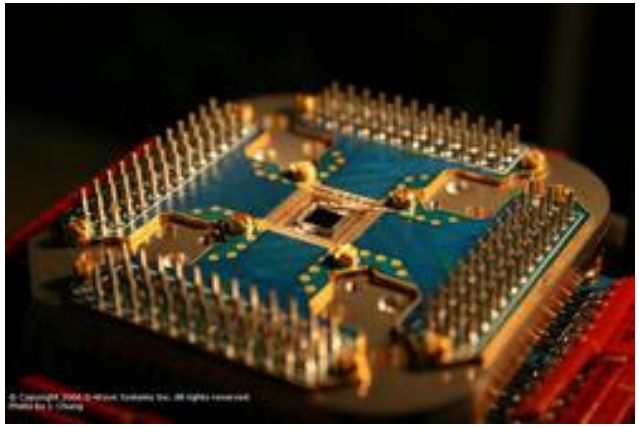
- Sono numerosi i centri di ricerca in cui si stanno sperimentando bizzarre e fantascientifiche tecniche per la messa a punto di computer quantistici (prototipi di alcuni qubit). In questo settore i laboratori più all'avanguardia si trovano negli Stati Uniti. Fra questi:
  - il National Laboratory di Los Alamos,
  - il Caltech (con il team capeggiato da Tim kimble)
  - il National Institute of Standards and Technology a Boulder, in Colorado, dove operano David Wineland e Chris Monroe

Orion

- **Il 13 febbbraio 2007,** nonostante non fosse creduto possibile prima di almeno 20 anni, il primo computer quantico, ORION (questo è il suo nome), equipaggiato con un processore quantistico a 16 qubit è stato creato, dalla canadese D-Wave Systems, bruciando sul tempo i Bell Labs, tra i più avanzati laboratori in questo campo di ricerca, insieme all'Almaden Research Center di IBM.
- Nel corso della prima dimostrazione pubblica organizzata il13 febbraio al Computer History Museum (Sylicon Valley), in una sala gremita da curiosi e addetti ai lavori, il processore quantistico messo a punto dalla canadese ***D-Wave Systems*** ha superato tre prove escogitate per testarlo con problemi di ottimizzazione, elaborazione e riconoscimento.

Orion

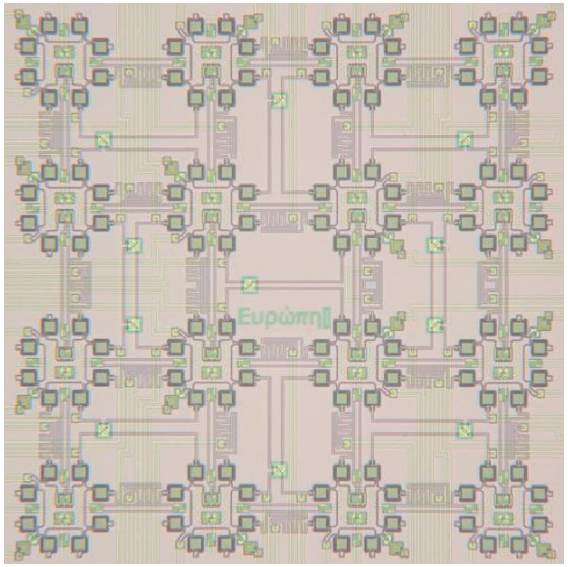
- Il nuovo processore della D-Wave sarà in grado di risolvere problemi NP-Completi quasi come bere un bicchiere d'acqua.
  - Per gli umili mortali come noi, trattasi della categoria più ostica in assoluto di problemi matematici in NP, vale a dire "problemi non deterministici a tempo polinomiale".
- Il cuore della macchina è un processore costituito da 16 bit quantistici, *qubit*,



Un'immagine del processore quantistico Orion, prosto di una capacità di calcolo di 16 qubit.

Orion

- I qubit utilizzati sono flux qubit, anelli di alluminio in fase superconduttiva interrotti da tre o più sottili strati di materiale isolante, chiamati giunzioni Josephson.
- I qubit sono arrangiati in un matrice 4x4, come illustrato in figura.



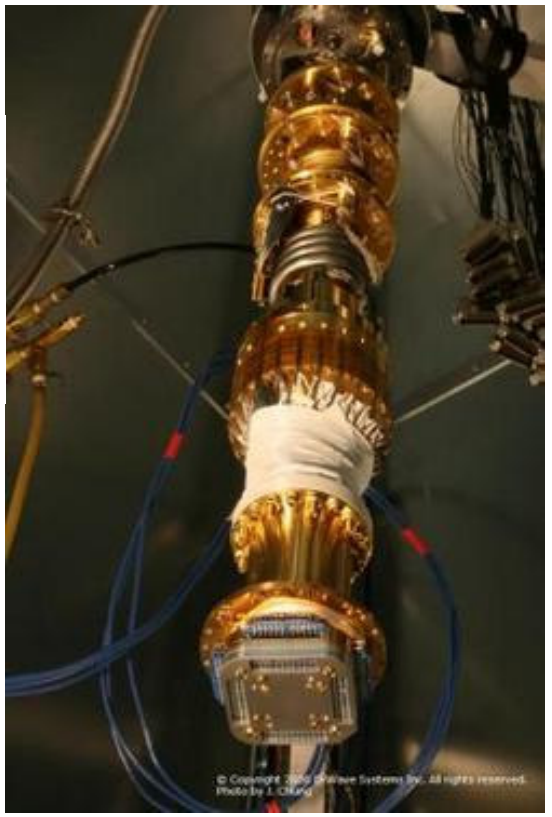
- La disposizione dei qubit permette di connetterli l'un l'altro, in modo da farli interagire.

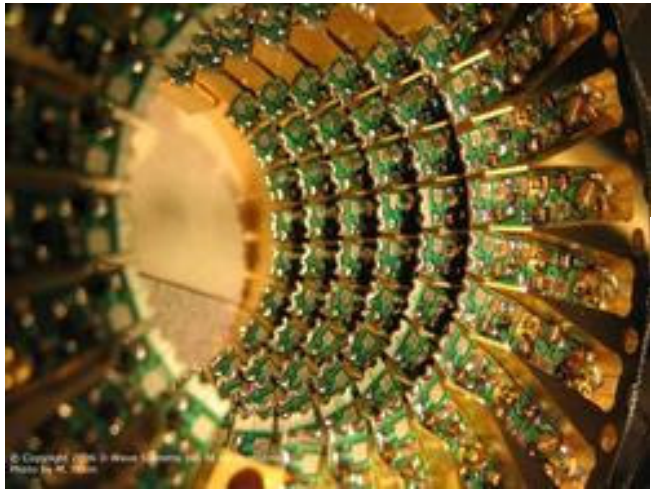
Orion

- Il dispositivo, per funzionare, deve essere portato alla temperatura critica di 5 mK, vale a dire 5 millesimi di grado al di sopra dello zero assoluto (pari a circa 273,16 gradi Celsius sotto zero).
- Opportuni stadi di prefiltraggio permettono di regolare l'accoppiamento tra i singoli qubit, limitando al minimo l'influenza del rumore.
- Il processore è progettato per operare in coppia con un chip classico che funziona da controllore e interprete e che ne invoca il funzionamento ogni qual volta si presenti un compito che lo richieda.

Orion

Particolare del sistema criogenico usato per raffreddare il chip a 16 qubit della D-Wave Systems, fino a pochi millesimi di grado sopra lo zero assoluto (-273,16 gradi Celsius).

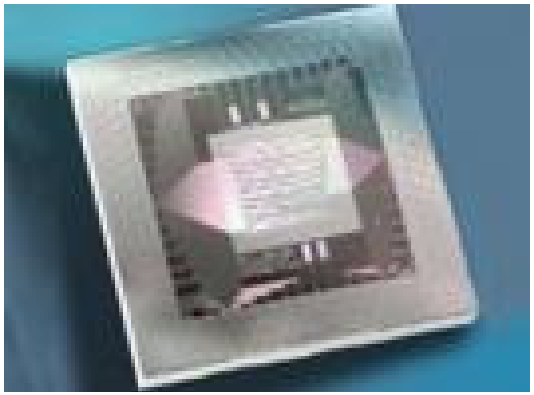




Veduta di uno degli stadi di filtraggio di Orion, indispensabile per ridurre l'effetto del rumore termico e risolvere i problemi di decoerenza che affliggono il funzionamento dei processori quantistici.

Orion

- Per quanto strabiliante, 16 qubit non possono fare miracoli!
- La D-Wave prevede ora di raggiungere presto un processore da 32 qubit, per arrivare addirittura alla soglia dei 1024 qubit (il primo *kilo-qb*) entro la fine del 2008.
- L'impresa sarebbe resa possibile dalla scalabilità della tecnologia, che dovrebbe permettere ai progettisti di interconnettere d'ora in avanti unità equivalenti al *core* usato per Orion.
- Attualmente c'e' una versione a 28-qubit presentata il 15 novembre 2007



D-Wave Demonstrates 28-Qubit Quantum Computer
Thursday, November 15, 2007 - Sarah Gingichashvili

Orion

- Attualmente non ci resta che accontentarci di un paio di dimostrazioni live della macchina.
- Il sistema realizzato dalla D-Wave è progettato per lavorare in remoto, cioè a distanza, ed è semplice da usare.
- Per raggiungere il pubblico più vasto possibile, D-Wave prevede anche di rendere disponibile il prototipo on-line gratuitamente: curiosi ed esperti potrebbero sottoporre in remoto i loro problemi a Orion, che invierebbe poi la risposta dal Canada.

Cosa ci riserva il futuro?

- D'ora in avanti una dimostrazione dovrà essere considerata come un processo (il calcolo stesso, e non una registrazione di tutti i suoi passaggi),
- In futuro è estremamente probabile che un calcolatore quantistico riesca a dimostrare teoremi attraverso metodi che un cervello umano (o un calcolatore classico) non è in grado nella maniera più assoluta di controllare, perché se la "sequenza di proposizioni" corrispondente alla dimostrazione intesa nel senso classico venisse stampata, la carta riempirebbe l'universo osservabile per molte volte.

Cosa ci riserva il futuro?

- Gli studi sull'elaboratore quantistico si incontrano con quelli sul PC molecolare con l'obiettivo di fondere l'intelligenza umana e quella della materia.
  - Il computer a base di Dna sostituisce i circuiti in silicio con le molecole organiche delle reti nervose animali.
  - Il computer quantistico, invece, opera a livello subatomico, utilizzando le particelle invisibili di cui è composta tutta la materia.
- Entrambi sono, per ora, in fase di studio e di ricerca. Ma l'obiettivo – neppure troppo lontano – è quello di fondere le due strade e arrivare alla creazione di intelligenze "postumane", in cui i codici della vita e della materia operino in modo sinergico e potente

- Se ci pensate bene…

con queste macchine noi uomini stiamo ponendo le basi per il superamento della nostra stessa specie.

Riferimenti bibliografici

- Alex Ferrara e Guido Vicino, Introduzione ai Calcolatori Quantistici, 2006
- Alessandra Di Pierro, *Quantum Computing: Appunti delle Lezioni, (2004).*
- P. W. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring, in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE* Computer Society Press (1994).
- Marco Ivaldi, *Introduzione al quantum computing, Luglio (2002).*
- Bernhard Ömer, *Structured Quantum Programming, (2003).*
- Stallings, *Cryptography and Network Security, Prentice Hall. (2003).*
- Brad Huntting, *An Introduction to Quantum Computing, University of Colorado (2001).*
- Benjamin Schumacher, *Quantum Computing, Lectures Notes, (1998).*
- Andrew M. Steane*, Quantum Error Correction, Clarendon Laboratory, Oxford OX1 3PU, England. (1996).*

Riferimenti bibliografici

- Centro di ricerca per il Quantum Computing, comprendente una grande quantità di documentazione, compresa quella sull'esperimento della riflessione dei fotoni citato nel testo. http://www.qubit.org
- QCL (Quantum Computation Language), linguaggio di programmazione architecture independent ad alto livello per computer quantistici, con una sintassi derivata dai linguaggi procedurali classici come il C e il Pascal. http://tph.tuwien.ac.at/ oemer/qcl.html
- "Heads" (1990), novella di Greg Bear. Pubblicata in Italia con il titolo di "Zero assoluto", nella raccolta "Cyberpunk" della Editrice Nord.
- Quantum Computation/Cryptography presso il Centro di Ricerca di Los Alamos. http://qso.lanl.gov/qc/
- Quantum Computing FAQ (Frequently Asked Questions) http://www.rdrop.com/cary/html/quantum_c-_faq.html
- Sito della D-Wave http://www.dwavesys.com