#culturadigitale AICA

Facciamo luce sul
Quantum Computing

Seminario Divulgativo

Milano, 18 marzo 2014, dalle 17.30 alle 19.30
p.le Morandi 2 Milano, presso FAST (www.fast.mi.it)

Programma:

- Presentazione semplificata di meccanica quantistica
- Origine del Quantum Computing
- Vantaggi del Quantum Computing
- Sfatiamo alcuni miti
- Stato dell’arte: ricerca e realizzazioni

Relatore: Joseph D. Horing

La partecipazione è gratuita *previa iscrizione inviando mail a elisabetta.peroni@arch.aicanet.net*

E' possibile partecipare alla sessione via web facendone richiesta via mail a elisabetta.peroni@arch.aicanet.net

Facciamo Luce sul Quantum Computing

AICA – Joseph D. Horing

18 Marzo 2014

Sommario

- Presentazione del relatore
- Scopo della presentazione
- Presentazione semplificata di Meccanica Quantistica
- Origine del Quantum Computing
- Perchè il Quantum Computing?
- Smitizzazione di alcuni concetti
- Stato dell’arte: ricerca e realizzazioni
- La controversia D-wave
- Per saperne di più…
- Q&A

Presentazione del relatore

- Joseph D. Horing, 48 anni
- Ha studiato informatica all'Università degli Studi di Milano
- Si occupa di informatica finanziaria e consulenza di direzione bancaria da quasi 30 anni
- Ha seguito un corso di Quantum Computing presso l'Università della California a Berkeley via edX.

edX | BerkeleyX

CERTIFICATE

Issued October 24th, 2013

This is to certify that

Joseph D Horing

successfully completed

CS191x: Quantum Mechanics and Quantum Computation

a course of study offered by **BerkeleyX**, an online learning initiative of **The University of California At Berkeley** through **edX**.

Armando Fox
Academic Director for Online Education
Professor In Residence
UC Berkeley

Diana Wu
Executive Director for Online Education
UC Berkeley

Umesh Vazirani
Roger A. Strauch Professor of EECS
UC Berkeley

HONOR CODE CERTIFICATE

*Authenticity of this certificate can be verified at https://verify.edx.org/cert/10819f8397bf44fa85eb8022a455ed3d

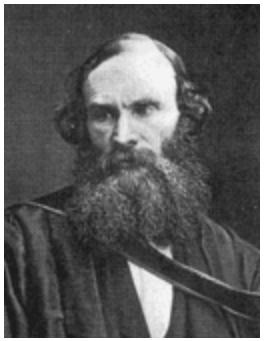
Scopo della presentazione

- Meccanica quantistica è materia ostica e poco conosciuta e il quantum computing è ancora meno conosciuto, anche tra gli informatici professionisti
- Grandi promesse, roboanti annunci e articoli di stampa
- Tutto ciò genera grande curiosità
- Questa presentazione intende dare ad un'audience di informatici un orientamento sufficiente ad inquadrare cosa si può fare, cosa si potrebbe fare e cosa invece è fantascienza.

Presentazione Semplificata di Meccanica Quantistica

- Cenni Storici
- Osservabili e Qubit
- L'universo privato e natura statistica del Qubit
- Effetto dell'osservazione su un Qubit
- Proprietà stupefacenti ed utilissime:
  - Sovrapposizione e Interferenza
  - Entanglement
- Per maggiori informazioni:
  - **Lezione di Feynman** sull'esperimento di Young, di grande interesse storico http://www.youtube.com/watch?v=hUJfjRoxCbk
  - **Cartone animato** sull'esperimento di Young, per studenti http://www.youtube.com/watch?v=DfPeprQ7oGc

Meccanica Quantistica
Cenni Storici



Le “ultime parole famose” di Sir William Thomson, Lord Kelvin, (1900): "There is nothing new to be discovered in physics now, All that remains is more and more precise measurement."

La smentita non si è fatta attendere: un impiegato dell’ufficio brevetti di Berna pubblica nel 1905 la scoperta della spiegazione dell’effetto foto-elettrico

Meccanica Quantistica
Cenni Storici

- Einstein scopre che la luce è fatta di particelle discrete. Questo, e non la più famosa teoria della relatività, gli è valso il Nobel.
- Tale scoperta, unita ad embrionali studi di Planck, da inizio ad una furiosa attività di ricerca a livello planetario, che produce risultati importantissimi e pone alcuni problemi filosofici di non facile soluzione.
- Tale attività è ancora in corso (si pensi al bosone di Higgs) e non ha ancora dato una spiegazione consistente a tutti i fenomeni naturali sin qui osservati (in special modo, la gravità).

Meccanica Quantistica
Cenni Storici

- Proiezione dell'animazione.
- Quanto emerge sulla natura dell'estremamente piccolo è che si comporta in modo completamente nuovo; nulla, nell'esperienza umana, si comporta così: per alcuni versi, come palline; per altri versi, come onde.

Comportamento di	Natura	Misurazione	Additività	Interferenza
Palline	Discrete	Probabilità di arrivo	Si	No
Onde d'acqua	Continue	Intensità	No	Si
Particelle subatomiche	Discrete	Probabilità di arrivo	No	Si

Esperienza diretta dei fenomeni quantistici

- Questi fenomeni, che esistono nella scala microscopica e sono solitamente estranei all'esperienza umana, determinano tutto l'universo (scala macroscopica).
- Anche se in alcuni casi si può osservare qualche fenomeno quantistico anche al nostro livello mesoscopico: basta fare una prova con due o tre filtri polarizzatori da macchina fotografica.

Esperienza diretta dei fenomeni quantistici – un semplice esperimento

- Dotarsi di tre filtri polarizzatori e di un tubo a cui adattarne due, ai due estremi del tubo
- Partire con un filtro solo. Ruotando il filtro, non cambia niente.
- Aggiungere un secondo filtro:
  - quando i filtri hanno la stessa inclinazione, non c'è differenza rispetto ad un filtro solo;
  - Quando i filtri sono perpendicolari tra loro, non passa luce
- Aggiungere un terzo filtro in mezzo ai primi due
  - Con certe angolazioni del terzo filtro posto in mezzo a due filtri tra loro perpendicolari, una parte della luce passa.

Spiegazione

- La luce ha una caratteristica: la polarizzazione
- Il flusso luminoso è costituito da particelle luminose (fotoni), ognuna polarizzata con un suo "angolo"
- Il primo filtro polarizzatore effettua una misurazione sui fotoni in arrivo:
  - elimina fotoni con probabilià crescente man mano che l'"angolo" di polarizzazione di ciascun fotone si avvicina alla perpendicolare dell'asse caratteristico del filtro
  - Cambia l'angolo di polarizzazione di tutti i fotoni che passano in quello dell'asse caratteristico del filtro
- Primo Risultato:
  - Se l'asse caratteristico del secondo filtro è parallelo a quello del primo, allora la luce passa indisturbata
  - Se l'asse caratteristico del secondo filtro è perpendicolare a quello del primo, allora la luce viene fermata
- Porre un terzo filtro in mezzo ai due filtri con angoli caratteristici tra loro perpendicolari e con il proprio a 45 gradi da ciascuno degli altri

  Secondo risultato:
  - Elimina parte della luce trasmessa dal primo filtro
  - Ne cambia l'"angolo" di polarizzazione, quindi quando la luce colpice il secondo, la polarizzazione della luce e quella del filtro non sono più perpendicolari: quindi passa un po' di luce
- **Morale: la misurazione cambia lo stato delle cose!**

Origine del Quantum Computing

Dichiarazione di

Richard Feynman

del 1982,

anno in cui la rivista Time nominava il Personal Computer “Machine of the Year”:

“I want to talk about the problem of simulating physics with computers”

Osservabili e Qubit

- Un osservabile è una proprietà <u>misurabile</u> di (ad es.) un oggetto fisico.
  - Ad esempio la mia posizione, la mia velocità o il mio peso.
- Un Qubit è un qualsiasi osservabile che possa assumere solo due valori (che chiameremo Vero e Falso).
  - Ad esempio la caratteristica di un elettrone in movimento di essere attratto o respinto da un magnete (spin).

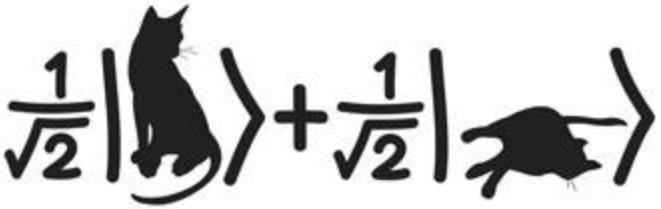
Caratteristiche del Qubit

- L'universo privato e natura statistica del Qubit
  - Lo stato del Qubit è definito da due numeri complessi (cioè quattro numeri reali)
    - Anche solo uno ci consentirebbe di rappresentare una quantità illimitata di bit)
    - Purtroppo questi numeri non si possono misurare! **Però si possono utilizzare – vedremo come.**
  - Questi numeri, insieme, definiscono la probabilità del Qubit di essere misurato come Vero o come Falso.
- Effetto dell'osservazione su un Qubit
  - La misurazione del Qubit ne <u>fissa</u> lo stato sul valore Vero oppure Falso che viene misurato. Quale che fosse il suo stato precedente e quale che sia il valore risultante dalla misurazione, <u>ogni successiva misurazione risulterà nello stesso valore.</u>

Caratteristiche del Qubit

- Proprietà stupefacenti ed utilissime:
  - Sovrapposizione
  - Interferenza
  - Entanglement

Sovrapposizione di Stati



- Ciascun Qubit può essere
  - Vero,
  - Falso
  - In parte Vero e in parte Falso – misurando il Qubit si potrà leggere Vero oppure Falso con <u>probabilità</u> dipendente da quanta parte è Vero e quanta parte è Falso.
- Le porte logiche di un computer quantistico elaborano simultaneamente anche gli stati sovrapposti.
- L'esperimento (mentale) del "Gatto di Schrödinger"
- Natura probabilistica della Meccanica Quantistica
- Generazione di numeri veramente casuali e non pseudocasuali

Interferenza

- Torniamo all'esperimento di Young: eseguiamolo con un solo fotone.
  - Il risultato è che questo fotone mostra segni di interferenza. Ma con chi?
  - **Con se stesso!**

  - È come se il fotone percorresse una sovrapposizione di tutti i possibili percorsi; e quando i percorsi si intersecano, esso interferisse con se stesso.
  - L'interpretazione moderna è che si sa dove e quando parte, si sa dove e quando arriva, ma nulla si può dire su dove si trovi nel frattempo.

Entanglement

- È possibile manipolare due (o più, ma non tantissimi) Qubit in modo tale che la misurazione di uno dei Qubit influisca (istantaneamente, anche a grande distanza!) sul risultato di una successiva misurazione dei restanti Qubit.
- Esempio ed impatto sulla privacy nella comunicazione di dati: può essere usato per comunicare rilevando eventuali intercettazioni.
- In ogni caso non consente comunicazioni più veloci della luce.
- Problema filosofico enorme sul tema della località.

Complessità della Meccanica Quantistica

Dichiarazione di
Richard Feynman
del 1965:

"I think I can safely say that nobody understands quantum mechanics."

Werner Heisenberg, citando Niels Bohr, nel 1971:

"… those who are not shocked when they first come across quantum theory cannot possibly have understood it."

Porte logiche classiche

Nome	Effetto	Note
AND	1 se entrambi gli input sono 1	
OR	1 se almeno uno degli input è 1	
NOT	Cambia il valore del bit	
NAND	Equivale a NOT (A AND B)	Rilevante perchè è universale: tutte le porte logiche classiche si possono definire in termini di porte NAND

Porte logiche quantistiche

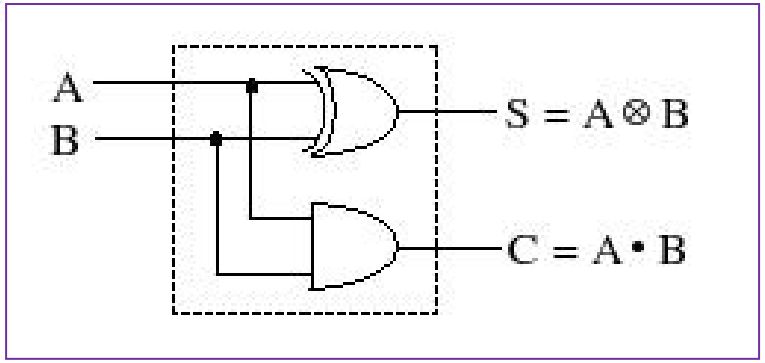
Nome	Equivalente	Effetto	Note
NOT o X	NOT	Scambia le probabilità tra Vero e Falso	
Hadamard	Trasformata di Fourier	Modifica la sovrap-posizione di stati. Nel caso di uno stato puro, risulta in un'equa sovrapposizione.	Caso particolare della trasformata di Fourier quantistica

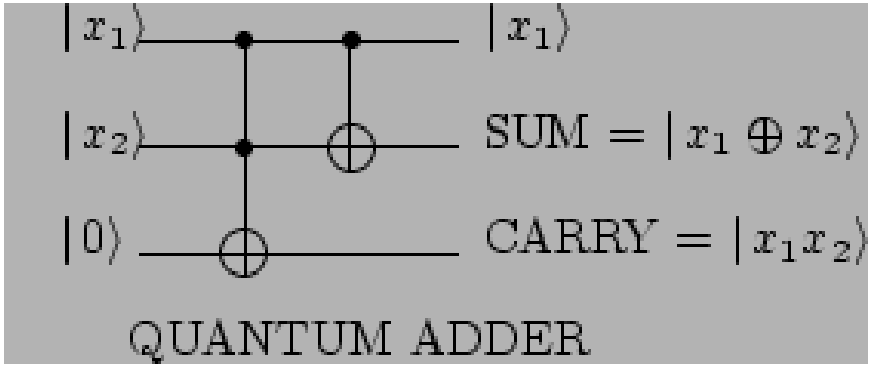
Controlled NOT o CNOT	If A then
	B :=NOT B;
	End if;
		Se il primo Qubit è Vero, allora scambia le probabilità del secondo	Unitamente all'Hadamard, si può usare per creare entanglement tra due Qubit

Toffoli (Controlled CNOT)	If A and B then
	C :=NOT C;
	End if;
		Se i primi due Qubit sono Veri, allora scambia le (ampiezze di) probabilità del terzo	Analogo alla porta NAND nel senso che è universale: tutte le porte logiche quantistiche si possono definire in termini di porte Toffoli

SWAP	C:=A; A:=B; B:=C;	Scambia gli stati di A e B	

Un esempio di circuito quantistico a confronto con un circuito classico





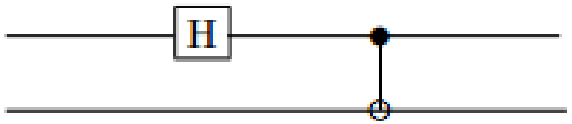
Un semisommatore binario classico (XOR + AND). S ci dice se A e B sono diversi (la somma) e C ci dice se sono entrambi veri (il riporto).

Un semisommatore binario quantistico (Toffoli + CNOT). Quando ciascuno degli input è in uno stato puro di Vero o di Falso, il risultato sarebbe lo stesso della controparte classica.
Poichè ciascun Qubit in ingresso può assumere stati sovrapposti, il meccanismo è più complesso (e potente!)

I Circuiti Quantistici a Gate Universali sono <u>reversibili</u>.

Un circuito che crea entanglement in due Qubit

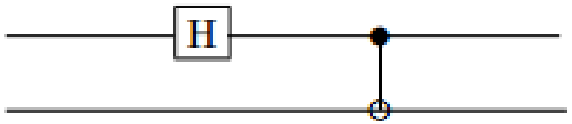
- Quando questo circuito viene applicato a due Qubit entrambi in stato Vero, il risultato è che:



  - i due Qubit si trovano in una equa sovrapposizione di stati, quindi ciascuno verrà misurato come Vero il 50% delle volte e come Falso l'altro 50% delle volte, e
  - la misurazione di uno dei due Qubit comporta SEMPRE che anche l'altro Qubit, alla successiva misurazione, risulti (in questo esempio di input Vero e Vero) sempre lo stesso stato del primo.

Un circuito che crea entanglement in due Qubit

- Questo semplice circuito mostra lo stupefacente fenomeno dell'entanglement:



  - La misurazione di uno dei due Qubit determina un cambiamento nel risultato della misurazione dell' altro,
  - In funzione del valore risultante dalla misurazione
  - mediante la variazione delle sue (ampiezze di) probabilità.

Perchè il Quantum Computing?

- Rende possibili elaborazioni precedentemente troppo impegnative (ma non tutte)
- Risoluzione di problemi inversi e di ottimizzazione
- Riconoscimento di oggetti
- Elaborazione di segnali
- Intelligenza artificiale

Smitizzazione di alcuni concetti

- Elaborazioni istantanee
- Elaborazioni in carenza di dati
- Teletrasporto

Stato dell’arte: ricerca e realizzazioni

- Ricerca teorica
  - Algoritmi: Shor, Grover
- Realizzazione Hardware
  - A gate universali: nulla!
  - Quantum Annealing: D-wave

Stato dell’arte: Algoritmo di Shor

- Problema: scomporre un numero in fattori primi
- Tempo di elaborazione da parte di una macchina classica: cresce **esponenzialmente** rispetto alle dimensioni del numero; con numeri relativamente piccoli (qualche centinaio di cifre decimali) si eccede facilmente la potenza di calcolo di tutti i computer del pianeta messi assieme. **È la base di un tipo di crittografia molto utilizzato (es. RSA).**
- Tempo di elaborazione da parte di una macchina quantistica: cresce solo **polinomialmente** rispetto alle dimensioni del numero; **sarà la fine della crittografia come la conosciamo oggi**.

Algoritmo di Shor: come funziona?

- Supponiamo N in input:
- a := random(); // e a < N
- se MCD(a, N) ≠ 1, end; // algoritmo di Euclide
- r := **periodo(f(a, N))**; // cioè il più piccolo numero tale che f(x)=f(x+r)
- Se r è dispari, non va bene: ricominciare.
- Se $a^{r/2}$= -1, non va bene: ricominciare.
- b := MCD($a^{r/2}$±1, N) // b è un fattore di N
- Fin qui, è tutta elaborazione classica. Vediamo ora la funzione **periodo()**.

Algoritmo di Shor: come funziona?

- Trovare un numero intero Q (potenza di 2) tale che $N \leq Q < N^2$
- Inizializzare q ($=\log_2 Q$) Qubit con un'equa sovrapposizione di Q stati diversi, ad esempio con una porta Hadamard.
- Applicare la funzione (implementata con porte quantistiche) $f(x) = a^x (\mathrm{mod} N)$.
- Applicare la Trasformata di Fourier Quantistica
- Il risultato è una sovrapposizione di stati che, quanto più si avvicinano al risultato desiderato (o, meglio, a un suo precursore), tanto più **interferiscono costruttivamente** tra di loro, amplificandosi; invece quegli stati che si allontanano dal precursore del risultato desiderato, **interferiscono distruttivamente** tra loro, minimizzandosi.
- Alla misurazione, è molto probabile che risulti un precursore del risultato desiderato. Nei casi, meno probabili, in cui viene misurato un valore che non è precursore del periodo cercato, ripetere la routine.

Algoritmo di Shor: Conclusioni

- La parte quantistica dell'algoritmo utilizza alcune tra le funzionalità più squisitamente quantistiche: sovrapposizione ed interferenza.
  - All'inizio, vediamo che occorrono Qubit in quantità non superiore a $\log_2 N^2$; ad esempio,
    - Nel caso di una delle prime implementazioni in laboratorio, per fattorizzare il numero 15 si sono impiegati 7 Qubit
    - per fattorizzare 143 dovrebbero essere serviti 14 Qubit.
    - nel caso di un numero di 2048 bit o circa 620 cifre decimali, la lunghezza della chiave attualmente raccomandata da RSA, occorrerebbero 4 MegaQubit.
  - quando crea una equa sovrapposizione di 2^q stati diversi nei q qubit, inserisce tutti (nei casi di esempio: 2, 3 e 620 cifre decimali!!!) i possibili input <u>contemporaneamente</u>, che vengono elaborati <u>nello stesso tempo</u>.
  - Alla fine, quando seleziona l'output, utilizza l'interferenza per eliminare gli output candidati indesiderati (miliardi di miliardi di … di miliardi) e potenziare quelli più plausibili.
- È un esempio di come un computer quantistico potrebbe rendere possibili, cioè computazionalmente accessibili, certe elaborazioni che, in un computer classico, impiegherebbero tempi proibitivi.

Stato dell’arte: Algoritmo di Grover

- Problema: trovare una chiave in una lista non ordinata (o, in alternativa, data una qualsiasi funzione, dato l’output, trovare l’input).
- Tempo di elaborazione da parte di una macchina classica: mediamente, proporzionale alla **metà** del numero di elementi della lista.
- Tempo di elaborazione da parte di una macchina quantistica: mediamente proporzionale alla **radice quadrata** del numero di elementi della lista**.**

Stato dell'arte: Realizzazioni

- **Le porte logiche quantistiche ancora non esistono**, se non in implementazioni sperimentali e con numerosi e notevoli problemi che ancora ne impediscono la realizzazione industriale**. Quindi i computer quantistici universali ad oggi non esistono.**
- Ci sono delle idee su come si potrebbero fare.
- Sono stati realizzati (in laboratorio) dei computer quantistici elementari:
  - È stato implementato l'algoritmo di Shor per scomporre il numero 143 nei suoi fattori primi 11 e 13

    (http://phys.org/news/2012-04-largest-factored-quantum-algorithm.html)**.**

Stato dell'arte: Realizzazioni

- **Interessante il computer "quantistico" D-Wave 2** (http://www.dwavesys.com)
- Non è un computer quantistico a porte logiche universali. È adatto a risolvere efficientemente solo un insieme limitato di problemi – **ma sono problemi interessanti!**
- Tuttavia mostra di sfruttare almeno in parte delle proprietà quantistiche, in particolare l'entanglement.
- Dato il potenziale, il primo esemplare a 512 Qubit è stato acquistato per circa $10M nel 2013 in società da NASA, Google e un consorzio di università, con finalità di ricerca.

La controversa D-Wave

- Macchine a porte logiche universali vs. macchine a Quantum Annealing
- Simulated Annealing Classico e Quantum Annealing
- Lo studio del 2013
- Controversia da parte del mondo della ricerca
- Conclusione: la macchina D-wave 2 esibisce un embrionale utilizzo di fenomeni quantistici, ma è limitata nelle applicazioni e non implementa gli algoritmi sin qui scoperti

Cosa dice di fare D-Wave 2?

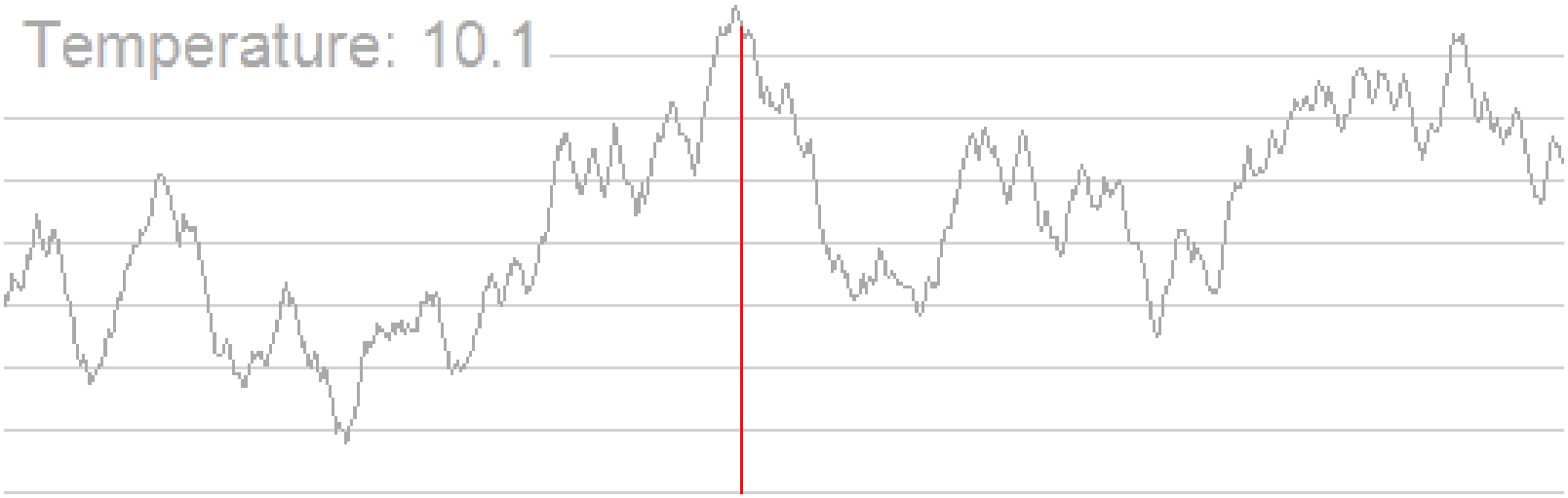
- Simulazione di proteine 3D
- Compressione video
- Intelligenza Artificiale e Machine Learning
- Creazione di video
- Riconoscimento di oggetti nelle immagini
- Ricerca di molecole in un DB
- Taggatura di articoli di stampa (AI)
- Analisi dei sentimenti (rabbia, gioia) da blog (AI)

Macchine a porte logiche universali vs. macchine a Quantum Annealing

- Macchine a porte logiche universali
  - Circuiti combinatori reversibili composti con porte come NOT (X), NOT Condizionato, SWAP, Y, Z (phase flip), Hadamard, Toffoli…
- Macchine a Quantum Annealing
  - Si assegna una funzione “energia” e la macchina trova lo stato in cui l’”energia” assume il valore minimo ➔adatta a problemi di ottimizzazione

Simulated Annealing Classico e Quantum Annealing

- L'annealing (=ricottura, termine preso a prestito dalla metallurgia) si simula anche con algoritmi che girano su macchine classiche.
  (cfr. http://it.wikipedia.org/wiki/Simulated_annealing)



D-Wave: La controversia e lo studio del 2013

- Il mondo della ricerca non condivide l'entusiasmo e la risonanza generati dagli annunci di D-Wave
- D-Wave ha commisisonato e pagato uno studio per confrontare le prestazioni di una sua macchina con quelle di una macchina classica. Il risultato è stato un'accelerazione di un fattore 3600!
- Tuttavia, il mondo della ricerca è rimasto scettico, in quanto lo studio è stato condizionato dal tipo di problema scelto, molto adatto a quella macchina e dal fatto che la macchina classica di confronto è una normale macchina server con processore Intel Xeon, anzichè hardware ad hoc.
- **Rimane un interessante campo di R&D.**

Per saperne di più…

- Articolo su Mondo Digitale n. 48
  http://mondodigitale.aicanet.net/2013-4/articoli/01_Computer_Quantistici.pdf
  di Alessandra di Pierro e Oliver Morsch
- È possibile seguire il corso, di livello universitario, gratuitamente e online, del prof. Vazirani (quello del teorema di Vazirani e della trasformata di Fourier quantistica)
  - Si può ottenere un certificato di profitto.
  - Prerequisiti: Algebra lineare, matematica dei numeri complessi.
  - Durata: due mesi, 8 ore a settimana

Cosa abbiamo visto

- Genesi della meccanica quantistica
- Elementi fondamentali di meccanica quantistica
- Genesi del Quantum Computing
- Porte logiche e circuiti
- Algoritmi
- D-Wave 2

Ringraziamenti

- Elisabetta Peroni
  - Presidente AICA sezione Lombardia
- AICA - Gruppo di lavoro IT Systems Architect
- Prof. Alessandra di Pierro
  - Dipartimento di Informatica dell'Università di Verona
- Dott. Oliver Morsch
  - Ricercatore presso l'Istituto Nazionale di Ottica (INO-CNR) a Pisa.

Domande e Risposte