No, non siamo ancora all'Elaboratore Quantistico

di Andrea Pasquinucci

L'elaboratore presentato da D-Wave Systems nel cuore della Silicon Valley promette risultati senza precedenti ed è l'inizio di un percorso ancora lungo, irto di ostacoli. Ma l'interesse è alle stelle, ecco perché.

Roma - Un anno e mezzo fa su Punto Informatico scrivemmo della scommessa di D-Wave Systems: presentare entro la fine del 2006 il primo prototipo del proprio Elaboratore Quantistico ed entro il 2008 la prima versione completa. Con solo un mese e mezzo di ritardo sulla prima scadenza, il 13 febbraio D-Wave ha presentato al pubblico il suo prototipo.

Possiamo dire che D-Wave ha vinto la scommessa? Non è chiaro, ma di sicuro hanno avuto molto coraggio, come risulterà evidente da quanto segue.

Prima di tutto, il luogo scelto da D-Wave per mostrare al pubblico per la prima volta "Orion", il nome in codice del prototipo, è il Museo di Storia dei Computer in Silicon Valley, ovvero nel cuore della tana del lupo. A prima vista questa scelta potrebbe sembrare una sfida all'industria consolidata dell'informatica, proponendo un nuovo elaboratore che potrebbe, in teoria, rendere obsoleto tutto quanto viene fatto dall'industria attuale.

In realtà la scelta del luogo e del formato dell'evento, una dimostrazione durata quasi 2 ore alla presenza di quasi 400 persone, la franchezza ed onestà che i presenti hanno riconosciuto al CEO Herb Martin ed al CTO Geordie Rose, potrebbero avere lo scopo parzialmente dichiarato di trovare alleati, sostenitori e potenziali clienti in grado di aiutare D-Wave a proseguire nel proprio progetto.

Infatti D-Wave è riuscita a passare in due anni da un primissimo prototipo con 2 soli qubit, ad Orion che di qubit ne ha 16. Ma D-Wave ammette che il peggio potrebbe ancora arrivare. Nella dimostrazione effettuata il 13 Febbraio scorso, Orion ha risolto tre problemi: il matching di molecole farmaceutiche, un caso semplice del problema del Commesso Viaggiatore ed un puzzle Sudoku, troppo poco per lasciare una impronta nella storia. Il problema è che 16 qubit sono troppo pochi, ed infatti D-Wave si propone di arrivare a 32 qubit entro la fine dell'anno, 512 qubit all'inizio del 2008 e 1024 qubit alla fine del 2008.

Questo progetto però ha una grave incognita, la "decoerenza". Come avevamo già spiegato in un precedente articolo le particelle elementari utilizzate come qubit rischiano di interagire con le particelle del mondo circostante e trasformarsi in modo praticamente casuale. Questo ovviamente porterebbe a risultati praticamente casuali per i calcoli. D-Wave ammette di non essere sicura di riuscire a mettere insieme più di 16 qubit e mantenerli isolati e controllati come dovrebbero. Se questa paura si rivelasse realtà, Orion rimarrebbe non solo il prototipo ma anche l'ultimo della sua

specie.

Ma un dubbio più rilevante è stato sollevato da molti scienziati che si occupano di Elaboratori Quantistici. Come avevamo scritto, D-Wave ha scelto di realizzare il proprio Elaboratore usando dei sistemi a superconduttori a temperature vicine allo zero assoluto. Inoltre la struttura interna dell'elaboratore quantistico di D-Wave segue un modello semplificato introdotto nel 1999 che non è in grado di implementare l'algoritmo di Shor, ma solo quello di Grover. L'algoritmo di Shor è, tra gli algoritmi per elaboratori quantistici, quello più famoso poiché è in grado di fattorizzare il prodotto di numeri primi, con possibili conseguenze sia per la sicurezza informatica (gli algoritmi crittografici asimmetrici quali RSA sono basati su problemi matematici di questo tipo) che per la teoria dei numeri. L'algoritmo di Grover invece permette solamente di risolvere alcune equazioni particolarmente complesse nella fisica delle particelle elementari o delle interazioni molecolari, ed il famoso problema del "Commesso Viaggiatore" che ha moltissime applicazioni pratiche, dalla organizzazione di merci e magazzini ai portafogli finanziari.

Il problema con l'implementazione di D-Wave è che non è chiaro se Orion sia veramente un elaboratore quantistico o solamente un elaboratore superconduttore.

La differenza fra questi due tipi di elaboratori è sostanziale: il primo adotta la logica quantistica ed è in grado di fare operazioni in modo impossibile altrimenti, il secondo adotta l'usuale logica digitale ma raggiunge velocità impossibili altrimenti grazie alla superconduttività. D-Wave afferma di avere "compelling evidence" che Orion si comporta come un elaboratore quantistico, e che presto renderà pubbliche queste prove. D'altra parte il dubbio è legittimo in quanto in Orion la componente quantistica è così ridotta che è lecito dubitare se abbia veramente un qualche effetto sull'esecuzione dei calcoli.

In conclusione, la scommessa di D-Wave rimane aperta ed anche se D-Wave la vincesse non è chiaro quali reali conseguenze potrebbe avere. Infatti è ormai abbastanza chiaro cosa potrebbe fare un vero elaboratore quantistico il giorno che questo sarà costruito. Non è invece molto chiaro cosa potrebbe essere in grado di fare l'ibrido che D-Wave sta cercando di costruire, e forse anche per questo D-Wave cerca dei partner che l'affianchino nello sviluppo dell'Elaboratore Quantistico.

In ogni caso rimane l'interesse scientifico e commerciale per la realizzazione di un elaboratore superconduttore, sia che sia quantistico sia che non lo sia.

Andrea Pasquinucci

Ucci.it

A.P. E' libero professionista in Sicurezza Informatica, PhD in Fisica Teorica, esperto di crittografia, di sicurezza delle reti e dei sistemi operativi. Socio fondatore e membro del Comitato Direttivo AIPSI, insegna presso l'Università degli Studi di Milano.

Andrea Pasquinucci e collaboratori si occupano di Crittografia Quantistica a livello di ricerca universitaria sin dal 1997 e partecipano tramite l'Università di Pavia al progetto SECOQC.