Il “Computer quantistico”

Prefazione

Nell’incontro del 21-11-2016 Rita Casadio ha posto la questione se la computazione quantistica potrebbe risolvere le situazioni di non calcolabilità algoritmica (l’*halting problem* di Turing e corrispondentemente le indecidibilità gödelliane). Risposi allora esprimendo dubbio e azzardando un “forse”.

Ho fatto una ricerca per approfondire la mia conoscenza sulla computazione quantistica e provo a fare a continuazione un riassunto dei principi fondamentali del calcolo quantistico (CQ nel seguito) nei confronti di quello classico (CC), e riporterò alcune conclusioni rilevanti per noi. I non interessati ai particolari matematici possono saltare le prossime sezioni e andare direttamente alle conclusioni e commenti finali.

Bit e Qubit

Il CC implementato nei computer traduce i comuni numeri di base decimale nel codice binario, dove il **bit** elementare d’informazione (b) può prendere i valori (0) e (1). Il bit si realizza fisicamente con transistor in circuiti elettrici che possono essere aperti (0) o chiusi (1), con materiali che possono essere smagnetizzati o magnetizzati, ecc. Una stringa di n bit può rappresentare 2^n numeri binari diversi (con corrispondenti numeri in base decimale). Il “byte” usato nei calcolatori è una stringa di $n = 8$ bit e può rappresentare 256 numeri diversi. Come aiuto utile per gli esempi posteriori presentiamo la corrispondenza tra i primi numeri interi, fermandoci a 4 bit:

Decimali:	0	1	2	3	4	5	6	7	8	9	10	11
Binari:	0	1	10	11	100	101	110	111	1000	1001	1010	1011

In entrambi i casi si possono aggiungere a convenienza zeri non significativi a sinistra per riempire le stringhe di lunghezza fissa facenti parte dei dati nello standard “doppia precisione - formato binary64” (totale di 64 bit tra il segno, l’esponente e la frazione) comunemente usati nelle memorie dei computer.

Il CQ adotta come elemento basico d’informazione il “**qubit**” (**q**), che sfrutta la proprietà prettamente quantistica della **sovrapposizione** degli **stati quantistici** (**0**) e (**1**). Qui non si tratta più di sistemi fisici macroscopici (quindi “classici”) come un transistor o un dominio magnetico, ma di oggetti, spesso microscopici, che obbediscono alla meccanica quantistica (MQ): può essere un atomo il cui *spin* (momento angolare quantizzato) abbia, nell’atto della sua misurazione, due valori, *up* (che chiamiamo **0**) e *down* (**1**), o un atomo con due livelli di energia (quantizzata) corrispondenti a uno stato fondamentale **0** e uno eccitato **1**, o un circuito superconduttore integrato (dispositivi “squid” miniaturizzati) il cui flusso magnetico è quantizzato (e di conseguenza l’intensità della corrente elettrica che circola in esso), ecc.

Il tratto caratteristico della MQ è che, prima della operazione di misurazione, il sistema può esistere in una sovrapposizione degli stati (**0**) e (**1**), cioè come una combinazione lineare

$$(\mathbf{q}) = q_0\,(\mathbf{0}) + q_1\,(\mathbf{1})$$

dove i coefficienti q_0 e q_1 sono numeri complessi (un numero complesso q si scrive come $q = a + \mathrm{i}\,b$ dove a è la parte reale e i b la immaginaria, cioè un altro numero reale b moltiplicato per l’unità immaginaria $\mathrm{i} = \sqrt{-1}$). La teoria quantistica stabilisce che questi coefficienti sono “ampiezze di

probabilità" il cui modulo al quadrato (definizione: $|q|^2 = a^2 + b^2$) rappresenta la probabilità di trovarsi nel corrispondente stato quando viene effettuata la misurazione. La probabilità totale delle possibilità **0** e **1** deve sommare 1 (cioè certezza), quindi imponiamo la condizione $|q_0|^2 + |q_1|^2 = 1$. Inoltre la "fase globale" (un fattore moltiplicativo di modulo 1) degli stati quantistici è fisicamente inosservabile, quindi arbitraria e ignorabile. Nel caso dello stato (**q**) abbiamo allora in partenza 4 parametri reali descrittivi (le parti reali e immaginarie di q_0 e q_1). La condizione del modulo lascia tre parametri liberi ma costretti a prendere valori nell'intervallo continuo tra 0 e 1, e la fase arbitraria ne elimina finalmente un altro. Riassumendo, un **qubit** viene descritto da due parametri reali, ciascuno dei quali può prendere gli **infiniti** valori numerici intermedi che esistono tra 0 e 1, codesti compresi. La differenza con il bit classico è un vero salto concettuale e qualitativo: il primo codifica due sole possibilità (i valori 0 e 1), mentre il qubit ne codifica "infinite al quadrato".

"Numeri" a più qubit

La differenza diventa ancora più drammatica quando andiamo su con le cifre. Nel CC, con due bit abbiamo $2^2 = 4$ possibilità (che corrispondono ai numeri decimali 0, 1, 2 e 3 come abbiamo visto sopra):

00 01 10 11

Un 2-qubit consiste nella sovrapposizione dei corrispondenti stati quantistici, cioè

$$(\mathbf{q}) = q_0\,(\mathbf{00}) + q_1\,(\mathbf{01}) + q_2\,(\mathbf{10}) + q_3\,(\mathbf{11})$$

e viene descritto da 6 parametri reali, ciascuno dei quali a valori nell'intervallo tra 0 e 1, e codifica quindi "infinito alla sesta" possibilità. Un *n*-qubit contiene $2^{(n+1)}$-2 tali parametri (per *n* grande e sottintendendo parametri complessi, si usa dire che abbiamo 2^n parametri).

Il calcolo quantistico

Prendiamo un problema nel quale i valori numerici coinvolti possano stare in un striga di tre bit. In tale caso nel CC abbiamo a disposizione gli otto numeri

binari	000	001	010	011	100	101	110	111	che corrispondono ai
decimali	0	1	2	3	4	5	6	7	

Il problema che abbiamo scelto è il calcolo della superficie di un quadrato di lato L, che sappiamo risulta essere $S = L^2$. Per fissare le idee con un calcolo numerico concreto prendiamo per esempio il valore L = 2, sicchè il risultato è S = 4. Il CC, che lavora in binario, prende L = 010, lo manipola con i protocolli del suo programma (algorimo) binario e ottiene il risultato binario S = 100. Finalmente ce lo rende sullo schermo nella base decimale come S = 4.

Il CQ parte dall'input L = 2 traducendolo in uno stato quantistico (**q**), concretamente nella sovrapposizione

$$(\mathbf{q}) = q_0\,(\mathbf{000}) + q_1\,(\mathbf{001}) + q_2\,(\mathbf{010}) + q_3\,(\mathbf{011}) + q_4\,(\mathbf{100}) + q_5\,(\mathbf{101}) + q_6\,(\mathbf{110}) + q_7\,(\mathbf{111})$$

dove tutti i coefficienti q_i sono nulli eccetto q_2 che vale 1. Poi lo manipola con l'algoritmo quantistico con cui è configurato il calcolatore concreto e ottiene il risultato nella forma di uno stato finale (**q'**),

in cui i coefficienti complessi sono q'_0 , ….. , q'_7 . Qui subentra la natura statistica dell'operazione di misurazione nel formalismo quantistico, che suppone si abbia a disposizione un "insieme statistico", cioè un numero elevato, di stati identici (**q'**): nell'effettuare la misurazione su ciascuno di essi, la probabilità di ottenere il risultato, mettiamo, (110) viene data da $|q'_6|^2$. In corrispondenza con il risultato S = 100 del CC, ciò che succederà con il nostro CQ è che, dopo molte misurazioni su (**q'**) otterremo una distribuzione di probabilità "piccata" su $|q'_4|^2 = 1$ piuttosto che un netto $q'_4 = 1$ e tutti gli altri coefficienti q'_i nulli.

Nell'atto pratico, l'insieme statistico (**q'**) si dovrebbe ottenere facendo molte volte lo stesso calcolo partendo dallo stesso (**q**) iniziale, ma il protocollo quantistico si può congegnare in maniera che ciò avvenga automaticamente in maniera da produrre un numeroso insieme di (**q'**) identici, provveda poi a effettuare la misurazione su ciascuno di essi e ci dia finalmente la distribuzione di probabilità. Sottolineiamo qui solamente il fatto che gli algoritmi e i risultati del CQ sono di natura probabilistica, la cui precisione si può aumentare solo a base di crescenti ripetizioni del calcolo.

Commenti e conclusioni

Nella descrizione precedente abbiamo tralasciato le procedure, fondamentali, di registro e lettura dell'informazione nei qubit, che creano profondi problemi concettuali e pratici. Il CQ è un campo in piena esplorazione, con molto variegati tentativi, approcci e interpretazioni oggetto di attiva ricerca.

L'implementazione fisica di quanto descritto sopra fa uso di un altro fenomeno esclusivamente quantistico qual è l'esistenza di stati "intrecciati" (*entangled*). Una difficoltà pratica immensa è quella di mantenere "puri" gli stati quantistici e le loro sovrapposizioni (mantenimento della "coerenza") per causa delle difficilmente evitabili interazioni con il resto del mondo: è difficilissimo mantenere i supporti dei qubit (atomi o circuiti) isolati a lungo dall'impatto di fotoni, altre particelle elementari o perturbazioni provenienti dall'ambiente, che ne alterino lo stato. In questo senso, i più pessimisti pensano che il CQ, come possibilità pratica, rimarrà sempre "il computer del futuro".

Dall'abbondante letteratura in questo campo riportiamo alcune conclusioni che si capiscono meglio in vista delle sezioni precedenti. Ne elenchiamo alcune:

Data la natura probabilistica delle procedure e dell'informazione manipolata, il CQ può prestarsi in maniera naturale a implementare la "logica diffusa" (*fuzzy logic*). Ci sono studi in questa direzione.

Il CQ, manipolando distribuzioni di probabilità di possibilità compresenti (le sovrapposizioni), esegue una sorta di calcolo classico parallelo con elevato grado di "parallelismo". In maniera *gedanken*, disponendo sequenzialmente questi calcoli paralleli (sempre in numero finito), non si ottiene concettualmente niente di nuovo rispetto ad una macchina universale di Turing. In particolare non si risolve l'*halting problem*. Ciò risponde negativamente alla questione posta da Casadio: le indecidibilità algoritmiche rimangono tali.

Nella prospettiva di oggi (la cautela è d'obbligo), il CQ, con algoritmi specializzati, potrà tutt'al più accelerare certi calcoli in cui si cerca di discriminare tra molte possibilità compresenti (tipo la fattorizzazione degli interi in numeri primi -spesso usata come test-, il problema del commesso viaggiatore, il piegamento delle proteine, e chissà se soppiantare Deep Blue come giocatore di scacchi), ma non risolvere problemi che non possa affrontare una macchina di Turing classica in tempi molto più lunghi.