Capitolo 7: Algoritmi quantistici

§.35 Il parallelismo quantistico

Il grande vantaggio della computazione quantistica consiste nella possibilità di svolgere calcoli in parallelo quindi in maniera estremamente efficiente.

Il parallelismo quantistico è la caratteristica fondamentale di molti algoritmi quantistici. Rischiando un'eccessiva semplificazione, diremo che il parallelismo quantistico consente di calcolare simultaneamente i valori assunti da una funzione $f(x)$ per differenti valori di x.

Supponiamo che $f(x):\{0,1\}\to\{0,1\}$ sia una funzione booleana di $B_{1,1}$ della quale non è noto l'effetto. Un modo per implementare una funzione booleana su un computer quantistico consiste nel definire un circuito che lavora su due qubit inizialmente nello stato $|x,y\rangle$. Con un'opportuna sequenza di porte logiche è possibile trasformarlo nello stato $|x,y\oplus f(x)\rangle$ dove, al solito, il simbolo $\oplus$ rappresenta la somma modulo 2. Il primo qubit verrà chiamato *registro dati* ed il secondo *registro target*. Chiamiamo U_f la trasformazione definita da $|x,y\rangle\to|x,y\oplus f(x)\rangle$ di cui è facile verificare l'unitarietà. Se $y=0$ allora lo stato finale del secondo qubit è proprio il valore di $f(x)$.

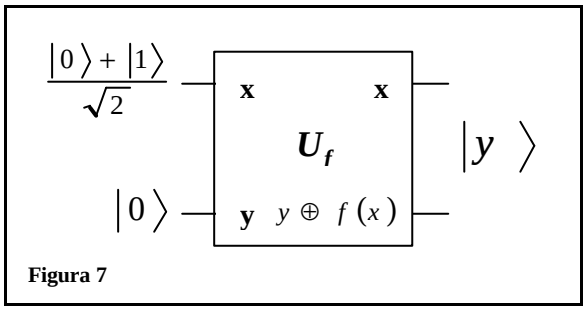


Figura 7

In fig.7 è rappresentato il circuito applicato ad un input non nella base computazionale. Invece, il registro dati è predisposto in uno stato di sovrapposizione che può essere ottenuto con l'azione della porta di Hadamard sullo stato $|0\rangle$. Applicando U_f lo stato risultante sarà:

(128) $$|y\rangle=\frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}}$$

Tale stato contiene informazioni in merito sia a $f(0)$ che a $f(1)$; è come se avessimo valutato $f(x)$ per due valori di x contemporaneamente, caratteristica nota, appunto, come parallelismo quantistico.

A differenza del parallelismo classico, in cui più circuiti identici vengono utilizzati simultaneamente, qui viene utilizzato un unico circuito sfruttando la caratteristica di un qubit di essere in sovrapposizione di differenti stati.

La valutazione in parallelo di una funzione $f(x) \in B_{n,1}$, cioè definita su n bit e a valori su un solo bit, può essere svolta preparando $n+1$ qubit nello stato $|0\rangle^{\otimes n}|0\rangle$, applicando la trasformata di Hadamard sui primi n qubit seguita dal circuito che realizza U_f arrivando al risultato:

(129) $$|y\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle .$$

In un certo senso, il parallelismo quantistico rende possibile la valutazione simultanea di tutti i possibili valori della funzione f.
Ma è anche vero che tale caratteristica da sola non ci è di aiuto a causa del postulato sulla misurazione che non solo ci impedisce di "estrarre" più di un risultato alla volta ma, addirittura, "distrugge" tutti gli altri rendendo la computazione quantistica esattamente identica a quella tradizionale.

Quindi la computazione quantistica richiede qualcosa di più che il solo parallelismo quantistico per risultare utile ovvero più efficiente della computazione classica.

§.36 La trasformata di Fourier quantistica QFT

Uno dei metodi più utili per la risoluzione di un problema in ambito scientifico consiste nel trasformarlo in un altro più semplice.

La trasformata di Fourier è un tipico esempio di uso frequentissimo. La teoria generale delle trasformate di Fourier, che affonda le sue radici nella teoria dei gruppi finiti, non verrà affrontata in questa sede. Ai nostri scopi basterà sapere che la *trasformata discreta di Fourier modulo q* (DFT_q) è usualmente descritta come la trasformazione che manda q-uple di numeri complessi $x_0, \ldots, x_{q-1}$ in q-uple di numeri complessi $y_0, \ldots, y_{q-1}$ definita da

(130) $$y_j = \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} e^{2\pi ijk/q} x_k .$$

E' importante, invece, notare che la trasformata di Hadamard introdotta precedentemente è un esempio di questa classe di trasformazioni di Fourier generalizzate e che, inoltre, molti dei principali algoritmi quantistici, come l'algoritmo veloce di Shor per la fattorizzazione, fanno uso di un qualche tipo di trasformata di Fourier.

Applicata all'ambito quantistico la trasformata discreta di Fourier modulo q viene chiamata *trasformata di Fourier quantistica*. Vediamo che in realtà sono la stessa cosa e, allo scopo, immaginiamo di definire una trasformazione lineare U su n qubit attraverso la sua azione sugli stati $|j\rangle$ della base computazionale, dove $0 \le j \le q-1$:

(131) $$QFT : |j\rangle \to \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} e^{2\pi ijk/q} |k\rangle \quad \forall j = 0, \ldots, q-1 .$$

dove i è l'unità immaginaria.
Si può verificare che questa trasformazione è unitaria e, quindi, ben si presta ad essere implementata con un circuito quantistico.

Di più, se scriviamo la sua azione su uno stato di sovrapposizione

(132) $$\sum_{j=0}^{q-1} x_j \left| j \right\rangle \to \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} \left[\sum_{j=0}^{q-1} e^{2\pi ijk/q} x_j \right] \left| k \right\rangle = \sum_{k=0}^{q-1} y_k \left| k \right\rangle ,$$

vediamo che questa corrisponde proprio all'equazione (130) in notazione vettoriale.

§.37 L'algoritmo di Shor

Nel 1993 *Peter Shor* ha mostrato che, in linea di principio, un computer quantistico può scomporre in fattori numeri grandi molto più rapidamente dei computer tradizionali.

Egli sfrutta il fatto che la ricerca di un fattore primo p di un numero composito N può essere ricondotta alla ricerca del periodo della funzione $f_{y,N} : \{0,1,2,3,\ldots,N-1\} \to \{0,1,2,3,\ldots,N-1\}$ data da:

(133) $$f_{y,N}(a) = y^a \bmod N$$

dove y è un qualsiasi numero intero più piccolo di N che sia *coprimo* con N ovvero che non abbia fattori in comune con N. Naturalmente se y non è coprimo con N, il massimo comun divisore tra y ed N fornisce già di per sè un fattore di N.

Per capire il legame tra la periodicità della funzione $f_{y,N}(a)$ e la fattorizzazione di N consideriamo l'equazione

(134) $$x^2 \equiv 1 \bmod N$$

che ammette sempre le due soluzioni banali $x \equiv \pm 1 \bmod N$. Se N è un numero primo $p \neq 2$ allora queste sono anche uniche. Viceversa, se N non è primo l'equazione (134) avrà anche coppie di soluzioni non banali della forma $x \equiv \pm a \bmod N$.

Ad esempio l'equazione $x^2 \equiv 1 \bmod 341$ ammette due soluzioni non banali $x \equiv \pm 32 \bmod 341$ in virtù del fatto che $341 = 11 \times 31$.

In generale sia $N = n_1 n_2$ con n_1 e n_2 coprimi tra loro e consideriamo i quattro sistemi di equazioni

(135)
$$(a)\ \begin{cases} x_1 \equiv +1 \mod n_1 \\ x_1 \equiv +1 \mod n_2 \end{cases},\ (b)\ \begin{cases} x_2 \equiv -1 \mod n_1 \\ x_2 \equiv -1 \mod n_2 \end{cases}$$
$$(c)\ \begin{cases} x_3 \equiv +1 \mod n_1 \\ x_3 \equiv -1 \mod n_2 \end{cases},\ (d)\ \begin{cases} x_4 \equiv -1 \mod n_1 \\ x_4 \equiv +1 \mod n_2 \end{cases}.$$

In ogni caso è $x_i^2 \equiv 1 \mod n_j$ e quindi ogni x_i è anche soluzione dell'equazione (134).

Poiché, in virtù di un teorema noto come "Chinese reminder theorem", ognuno dei quattro sistemi ha un'unica soluzione $\mod N$, da (a) e da (b) otteniamo le due soluzioni banali dell'equazione (134) $x_1 = 1 \mod N$ e $x_2 = -1 \mod N$, mentre da (c) e da (d) otteniamo le due soluzioni non banali $x_3 = a \mod N$ e $x_4 = -a \mod N$.

Partendo ad esempio dalla (c), ricaviamo $a - 1 \equiv 0 \mod n_1$ e $a + 1 \equiv 0 \mod n_2$ ovvero $a - 1 = q_1 n_1$ e $a + 1 = q_2 n_2$ che, moltiplicate tra loro, offrono $(a+1)(a-1) = q_1 q_2 n_1 n_2 = qN$ ovvero $(a+1)(a-1) \equiv 0 \mod N$ con $(a \pm 1) \neq 0$ il che equivale a dire che N divide il prodotto $(a+1)(a-1)$ ma non i singoli fattori perché $(a \pm 1) \leq N + 1$. Ciò significa che “una parte” di N deve dividere $(a+1)$ e “l’altra parte” deve dividere $(a-1)$.
Quindi se $a \neq \pm 1$, il massimo comun divisore tra N e $a \pm 1$ fornisce almeno un fattore non banale di N.

Il massimo comun divisore tra due numeri può essere calcolato in maniera efficiente usando l'algoritmo di Euclide.

Riassumendo, nota una soluzione x non banale dell'equazione (134) possiamo trovare un fattore non banale di N. La soluzione x può essere individuata come segue.

Dato N, scegliamo a caso un numero $y < N$. Se y è coprimo con N allora sia r l'ordine di $y \mod N$ (cioè la più piccola potenza di y tale per cui $y^r \equiv 0 \mod N$). Questo è esattamente il periodo di $f_{y,N}(a)$ dell'equazione (133). Perciò

(136)
$$y^r \equiv 1 \mod N.$$

Inoltre, se r è pari, ponendo

(137)
$$x = y^{r/2}$$

otteniamo proprio $x^2 \equiv 1 \mod N$ e, quindi, $x = y^{r/2}$ è candidato per essere una soluzione non banale dell'equazione (134). Questo fornisce il collegamento tra la periodicità di $f_{y,N}(a)$ e il calcolo di un fattore non banale di N.

Il procedimento appena descritto è inefficace se la scelta casuale di y ci conduce o ad un valore di r dispari o, anche se r pari, ad una soluzione banale dell'equazione (134) cioè a $y^{r/2} \equiv \pm 1 \mod N$. E' dimostrato che la probabilità di una scelta felice di y è superiore a $\frac{1}{2}$.

Illustriamo con un semplice esempio il funzionamento di questo metodo. Sia $N = 15$. Innanzi tutto scegliamo y in modo che sia $\mathrm{mcd}(y,15) = 1$. Nel caso in esame y può essere uno qualsiasi tra i numeri $\{2,4,7,8,11,13,14\}$ e, ad esempio, prendiamo $y = 7$.

I valori assunti da $f_{7,15}(a) = 7^a \mod 15$ per $a = 0,1,2,3,4,5,6,\ldots$ sono rispettivamente $1,7,4,13,1,7,4,\ldots$. A questo punto si renderebbe necessario l'utilizzo dell'algoritmo di ricerca per individuare il periodo r. L'algoritmo ci restituirebbe il valore $r = 4$, risultato che noi, nell'esempio specifico, individuiamo a vista.

Calcolando $\mathrm{mcd}\left(y^{r/2} \pm 1, N\right)$, dove $y^{r/2} = 49$, otteniamo la scomposizione cercata, ovvero $\mathrm{mcd}(48,15) = 3$ e $\mathrm{mcd}(50,15) = 5$. I periodi di f per gli altri valori di y nell'insieme $\{2,4,7,8,11,13,14\}$ sono, rispettivamente $\{4,2,4,4,2,4,2\}$ e, in questo particolare esempio, ogni scelta ad eccezione di $y = 14$ conduce al risultato corretto. Nel caso $y = 14$ otteniamo $r = 2$, da cui $y^{r/2} \equiv -1 \mod 15$ e il metodo non funziona perché le condizioni non sono entrambe soddisfatte.

Nell'algoritmo di Shor, il collo di bottiglia è rappresentato proprio dalla ricerca del periodo r della funzione f. Ma le potenzialità della computazione quantistica consentono di rimuovere tale ostacolo garantendo l'individuazione estremamente efficiente del periodo. Vediamo come.

Consideriamo la successione $f(0), f(1), \ldots, f\left(2^n - 1\right)$ dove la funzione booleana f appartiene a $B_{n,n}$ cioè $f : \{0,1\}^n \to \{0,1\}^n$. In altri termini, posto $q = 2^n$, consideriamo una qualsiasi successione di q numeri interi compresi tra 0 e $q-1$.

Obiettivo del nostro algoritmo è individuare un'eventuale periodicità negli elementi della successione. Per cui iniziamo predisponendo due registri quantistici entrambi costituiti da n qubit.
Indicheremo lo stato complessivo del sistema con $|x, y\rangle = |x\rangle \otimes |y\rangle$ dove $|x\rangle$ rappresenta lo stato del primo registro e $|y\rangle$ quello del secondo.

Entrambi i registri sono inizialmente impostati a zero. Avviamo l'elaborazione passando il primo registro per una porta di Hadamard in modo da preparare i qubit nell'ormai consueto stato di sovrapposizione

(138) $$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a,0\rangle .$$

Il passo successivo consiste nella valutazione parallela della funzione f con un operatore unitario U_f, analogo a quello presentato in precedenza ma che, questa volta, opera su n qubit e, che trasforma $|a,0\rangle$ in $|a,\ f(a)\rangle$. Dopo la sua applicazione i nostri registri saranno nello stato

(139) $$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a,\ f(a)\rangle .$$

Il passo finale consisterà nell'applicare la trasformata di Fourier quantistica al primo registro che essendo in uno stato di sovrapposizione emergerà con la forma

(140) $$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1}e^{2\pi i a f/q}|c,\ f(a)\rangle .$$

Il calcolo è ora completo e si tratta solo di estrarre i risultati effettuando la misurazione degli stati dei qubit del primo registro. Cosa otterremo come output?

Consideriamo tutti i possibili stati $|c,\ f(a)\rangle$ al variare di $c,a=0,\ldots,q-1$.

Supponiamo che la nostra successione $f(a)=y^a \bmod N$ abbia periodo r. Allora avremo che due stati $|c,\ f(a)\rangle$ e $|c,\ f(b)\rangle$ coincideranno se e solo se $f(a)=f(b)$ ovvero se e solo se $y^a=y^b$. Ma ciò capita se e solo se $b=kr+a$ ovvero se e solo se $a\equiv b \bmod r$. Dunque, fissato c, avremo interferenza tra i coefficienti ogni volta che $a\equiv b \bmod r$. Per vedere che tipo di interferenza si forma, fissiamo a e osserviamo che i coefficienti $e^{2\pi iac/q}$ giacciono sulla circonferenza unitaria con angolo $q=2\pi iac/q$.

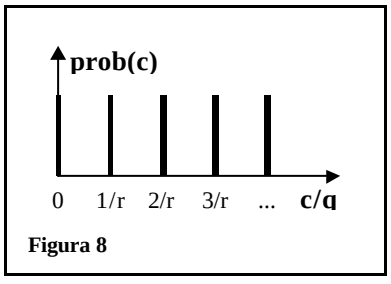


Figura 8

Dunque due vettori $|c,\ f(a)\rangle$ e $|c,\ f(b)\rangle$ coincidono ogni volta che $b\equiv a \bmod r$.

Quindi i coefficienti di tutti questi vettori $|c,\ f(b)\rangle$ andranno sommati per costituire l'unico coefficiente del vettore $|c,\ f(a)\rangle$.

Tale fatto riflette ancora una volta il fenomeno dell'interferenza che ci viene in aiuto per individuare il periodo r.

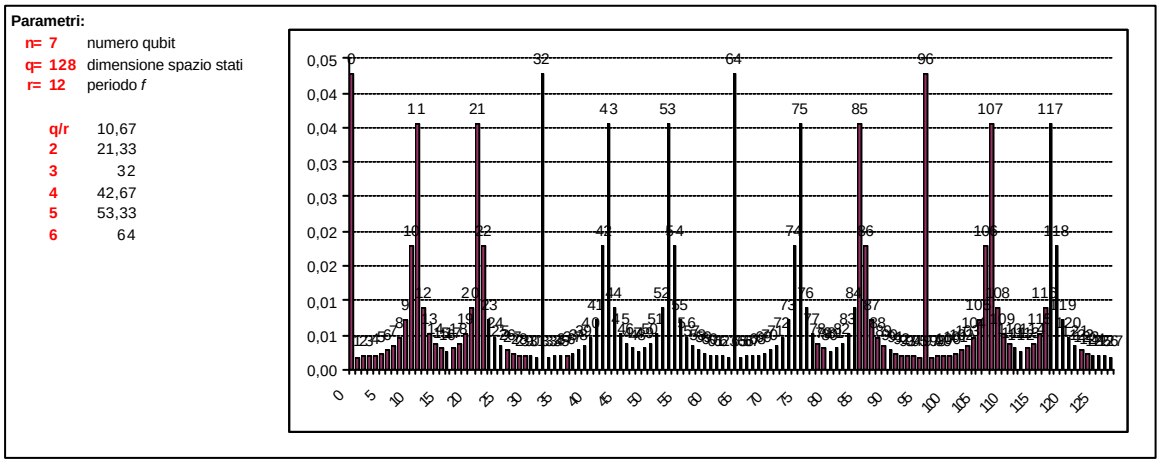
Infatti la somma estesa a tutti i valori che a può assumere genererà interferenza costruttiva tra i coefficienti $e^{2\pi i a l/q}$ soltanto quando $c/q = l/r$ cioè quando c/q è un multiplo dell'inverso del periodo $1/r$.
Tutti gli altri valori di c/q produrranno interferenza distruttiva più o meno ampia.
La distribuzione di probabilità per i differenti valori risultanti dalla misurazione del primo registro è schematicamente rappresentata in fig.8 dove si è scelto il caso particolare in cui r divide esattamente q e in cui, conseguentemente, l'interferenza distruttiva azzera completamente i coefficienti di tutti i vettori $|c,\ f(a)\rangle$ per i quali c/q non è un multiplo di $1/r$.

In questo caso ogni singola esecuzione della procedura offrirà come risultato uno dei valori c/q a caso tra i soli multipli dell'inverso del periodo. Se siamo stati fortunati e l è coprimo rispetto ad r basterà ridurre c/q ad una frazione irriducibile per ottenere il periodo r.
Viceversa, poiché la probabilità che sia $\mathrm{mcd}(l,r)=1$ è maggiore di $1/\log r$, ripetendo la procedura un numero sufficiente di volte, i risultati si concentreranno su almeno uno dei multipli coprimi rispetto a r, determinando, così, il suo valore in maniera univoca.

Dunque questo algoritmo offre solo un risultato probabilistico ma, per nostra fortuna, possiamo rendere questa probabilità prossima a 1 quanto vogliamo.

Torniamo ora al caso generale in cui il periodo r non divide esattamente q. Nella seguente figura viene presentata la distribuzione di probabilità relativa ai risultati della misurazione del primo registro dopo l'esecuzione dell'algoritmo di ricerca del periodo.

Come si può notare i picchi sono in corrispondenza dei valori di c più "vicini" ai multipli di q/r.



Per rendere precisa quest'ultima affermazione cominciamo col notare che se r divide esattamente q allora $rc \mod q = 0$.
Nel caso generale dovremo, invece, accontentarci di valori c tali per cui $rc \mod q$ è piccolo.

Consideriamo, quindi l'intervallo

(141) $$-r/2 \le rc \mod q \le r/2.$$

Ci sono esattamente r valori di $c \bmod q$ che soddisfano (141) così come prima l'equazione (140) aveva, per un a fissato, solo r coefficienti non nulli.

La probabilità che una misurazione ci offra proprio un valore c che soddisfa (141) è superiore a $4/p^2$. Quindi, anche in questo caso, un numero sufficiente di misurazioni ci garantisce di individuare un valore di c "vicino" ad un multiplo di r ovvero che soddisfi la condizione (141).

Adesso non ci resta che desumere il valore di r da quello di c. Per fare ciò notiamo che la condizione (141) è equivalente a

(142) $$|rc - c'q| \le r/2$$

per qualche $0 \le c' \le r-1$. Gli r differenti valori di c' sono associati con gli r possibili valori di c per cui la probabilità di osservare un valore c' è anch'essa superiore a $4/p^2$.
L'equazione (142) può essere riscritta come

(143) $$\left|\frac{c}{q} - \frac{c'}{r}\right| \le \frac{1}{2q}$$

dove c e q sono noti, $r \le N$ e, ricordando che q è il numero di vettori della base computazionale, possiamo dotare il nostro sistema di un numero di qubit sufficiente a garantire $q \ge N^2$. Questa condizione ci garantisce l'esistenza di un'unica frazione c'/r, il cui denominatore è al più uguale a N, che soddisfa l'equazione (143).
Questa frazione può essere determinata in maniera efficiente usando il metodo dello sviluppo finito in frazioni continue per determinare un convergente di c/q.
Ricordiamo che si chiama sviluppo finito in frazioni continue la scrittura di un numero razionale nel seguente modo

(144) $$\frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots \cfrac{1}{a_n}}}$$

Ogni frazione p_k/q_k ottenuta arrestando lo sviluppo al k-esimo passo viene detta convergente di p_n/q_n. E' dimostrato che se a è un numero razionale, esiste solo un numero finito di approssimazioni razionali $\frac{p}{q}$ tali che $\left| a - \frac{p}{q} \right| < \frac{1}{q^2}$.

Ancora una volta, se $\text{mcd}(c', r) = 1$, otteniamo subito r, viceversa potremo ripetere il procedimento un numero sufficiente di volte per ottenere r e, conseguentemente, un fattore di N. Combinando tutte le probabilità otteniamo che il procedimento, nel suo complesso, garantisce il risultato per r grande, con probabilità superiore a $4/p^2 \log N$.

E questo conclude la nostra trattazione.