Quantum Computing

Alessandra Di Pierro

Appunti del corso - A.A. 2001-2002

1 Esercitazione 4: Un esempio di fattorizzazione mediante l'algoritmo di Shor

Illustriamo l'esecuzione dell'algoritmo quantistico per la fattorizzazione descritto a lezione, applicandolo per trovare i fattori di $N = 15$.

Passo 1 Supponiamo di scegliere il numero casuale $x = 7$.

Passo 2 Con l'algoritmo di Euclide otteniamo $MCD(7, 15) = 1$. Quindi procediamo con il passo 3.

Passo 3 Calcoliamo l'ordine di 7 modulo 15 usando l'algoritmo quantistico studiato a lezione.

- Fissiamo $\epsilon = 1/4$ e $n = 2L + 1 = 2 \cdot 4 + 1 = 9$, ottenendo $t = 2L + 1 + \log 2 + 1/2\epsilon = 9 + \log 4 = 11$.
- Prepariamo il primo registro nello stato $|0\rangle^{\otimes t}$ e il secondo registro nello stato $|1\rangle$, ottenendo lo stato iniziale $|\psi_0\rangle = |0\rangle |1\rangle$.
- Applichiamo la trasformata di Hadamard al primo registro ottenendo
$$|\psi_1\rangle = \frac{1}{\sqrt{2048}} \sum_{k=0}^{2047} |k\rangle |1\rangle$$
- Applichiamo la sequenza di operazioni controlled-U, dove $U|y\rangle = |7y(mod 15)\rangle$ a $|\psi_1\rangle$, ottenendo
$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{2048}} \sum_{k=0}^{2047} |k\rangle \left|7^k(mod 15)\right\rangle \\ &= \frac{1}{\sqrt{2048}} [|0\rangle |1\rangle + |1\rangle |7\rangle + |2\rangle |4\rangle + |3\rangle |13\rangle + \\ &= \quad + |4\rangle |1\rangle + |5\rangle |7\rangle + |6\rangle |4\rangle + \dots] . \end{aligned}$$

- Applichiamo la trasformata di Fourier inversa $FT^\dagger$ al primo registro e misuriamolo per ottenere φ. Un modo per analizzare la distribuzione dei risultati ottenuti é quello di applicare il principio della misurazione implicita, secondo il quale ogni qubit che al termine di un circuito non é stato misurato si puó assumere come terminato da un'operazione di misurazione. Nel nostro caso, poiché sul secondo registro non verranno applicate ulteriori operazioni, possiamo assumere che il secondo registro venga misurato ottenendo un risultato random tra 1, 7, 4 0 13 (Notare la periodicitá della funzione $x^k(modN)$. Supponiamo di ottenere 4. Allora lo stato del primo registro collassa a

  $$\frac{1}{\sqrt{2048/4}}\left[|2\rangle + |6\rangle + |10\rangle + |14\rangle + \ldots\right].$$

  A questo stato viene applicata la $FT^\dagger$ risultando in un certo stato $\sum_l \alpha_l |l\rangle$. Analizzando la distribuzione di probabilitá dei risulati sull'intervallo da 0 a 2048 ottenuti dalla misurazione finale, si vede che i risultati con la probabilitá piú alta (e molto vicina a 1/4) corrispondono a 0, 512, 1024 o 1536. Supponiamo di ottenere il risultato 1536. Allora otteniamo $\varphi = 1536/2048$.

- Calcoliamo l'espansione a frazioni continuate di φ: $1536/2048 = 1/(1 + (1/3))$, da cui risulta che 3/4 é un convergente di φ. Verifichiamo quindi che $r = 4$ é effettivamente l'ordine di 7 modulo 15.

Passo 4 r é pari e $7^2 = 4(mod15) \neq -1(mod15)$. Quindi possiamo proseguire con il passo successivo.

Passo 5 Calcoliamo infine i massimi comun divisori $MCD(x^2 - 1, 15) = 3$ e $MCD(x^2+1, 15) = 5$, e concludiamo che sono due fattori non banali di 15.