Quantum Computing

Alessandra Di Pierro

1 Esercitazione 3

Esercizio 1.1 (QFT)

(i) *Scrivere la matrice per la trasformata di Fourier quantistica e il circuito che la implementa per il caso* $n = 3$ *(tre qubits).*

(ii) *Dimostrare che l'inversa della QFT é data da:*

$$F^\dagger : |j\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_k = 0^{2^n-1} e^{-2\pi ijk/2^n} |k\rangle \,.$$

(iii) *Scrivere il circuito per l'inversa della QFT.*

Soluzione

(i) L'operatore F é rappresentato in questo caso da una matrice 8×8 il cui elemento generico F_{jk} é dato dall'ampiezza del vettore $|k\rangle$ nella sovrapposizione $\sum_{k=0}^{7} e^{2\pi ijk/8} |k\rangle$ che definisce la trasformata, cioé $F_{jk} = e^{2\pi ijk/8}$. Poiché $F_{jk} = F_{kj}$ la matrice é simmetrica. Ponendo $\omega = e^{\pi i/4} = (1 + i)/2$, e osservando che $\omega^2 = i$, $\omega^3 = i\omega = (-1 + i)/2$, $\omega^4 = -1$, $\omega^5 = -\omega$, $\omega^6 = -i$, $\omega^7 = -i\omega$, si calcola ω^{jk} per ogni riga $0 \leq j \leq 7$, e colonna $0 \leq k \leq 7$ ottenendo la matrice

$$F = \frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & i & i\omega & -1 & -\omega & -i & -i\omega \\ 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & i\omega & -i & \omega & -1 & -i\omega & i & -\omega \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -\omega & i & -i\omega & -1 & \omega & -i & i\omega \\ 1 & -i & -1 & i & 1 & -i & -1 & i \\ 1 & -i\omega & -i & -\omega & -1 & i\omega & i & \omega \end{bmatrix}$$

(*ii*) Poiché F é simmetrica, il suo aggiunto é rappresentato dalla matrice complessa coniugata di F. Quindi

$$F_{kj}^{-1} = F_{kj}^{\dagger} = F_{jk}^{*} = F_{kj}^{*} = \frac{1}{\sqrt{2^n}} e^{-2\pi ijk/2^n}.$$

(*iii*) Il circuito per l'inversa della QFT si ottiene invertendo il circuito per F, cioé prendendo gli aggiunti dei vari gates composti in ordine inverso. Nota che $(AB)^{-1} = B^{-1}A^{-1}$ e che $H^{\dagger} = H$ e $R_k^{\dagger} = \begin{bmatrix} 1 & 0 \\ 0 & e^{-2\pi i/2^k} \end{bmatrix}$.

Esercizio 1.2 (Aritmetica modulare) *Dimostrare che*

(i) *se a e b sono inversi di x modulo n allora $a = b(mod n)$*

(ii) *l'ordine r di x modulo n é tale che $r \leq n.x$*

Esercizio 1.3 *Dimostra che se $0 \leq x \leq N$, $MDC(x, N) = 1$ e $L = \lceil \log N \rceil$, allora l'operazione $U : \mathbb{C}^2 \to \mathbb{C}^2$ definita da*

$$U\left|y\right\rangle = \left|xy(modN)\right\rangle$$

per $0 \leq y \leq N-1$, e $U\left|y\right\rangle = \left|y\right\rangle$ per $N \leq y \leq 2^L - 1$, é unitaria.