Algoritmi 'Order-finding' e 'Factoring'

L'algoritmo di Quantum Phase Estimation trova una delle sue principali applicazioni per la soluzione del problema dell'*order-finding* e del *factoring*. Questi due problemi e la loro soluzione sono due routine centrali dell'algoritmo di Shor.

L'algoritmo di Shor è interessante perchè prova che i computer quantistici:

- siano intrinsecamente più potenti dei computer classici.
- siano in grado di rompere il cryptosystema a chiave pubblica di tipo RSA

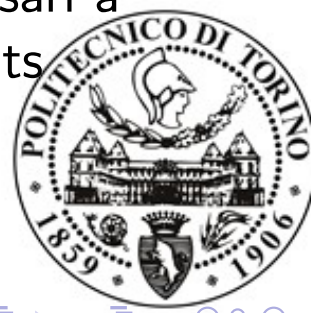
Order-finding: ricerca dell'ordine r di x modulo N

Consideriamo due interi positivi x and N con $x < N$ non aventi fattori in comune, l' *ordine* r di x modulo N è definito come il minimo intero positivo r tale che $x^r = 1 (\mathrm{mod}\, N)$.

Il problema di *order-finding* consiste nella determinazione dell'ordine r per valori assegnati di x e di N.

L'esponente r è anche chiamato periodo x^r mod N, perchè il risultato di x^r mod N si ripete con periodo r.

L' *order-finding* è un problema di difficile soluzione nell'informatica classica, nel senso che nessun algoritmo conosciuto risolve il problema utilizzando risorse polinomiali dell'ordine di $O(L)$ bits necessari a specificare il problema, dove $L \equiv \lceil \log(N) \rceil$ è il numero di bits necessari a definire N.



Ordine r di x modulo N: Esempio 1

Esempio 1: Si consideri $x = 3$ and $N = 5$. Si trovi il valore dell'ordine di $x^r (\mathrm{mod}\, N)$. I valori di 3^r e $3^r (\mathrm{mod} 5)$ sono mostrati in tabella. Il valore di r è 4.

r	3^r	$3^r (\mathrm{mod} 5)$
0	1	1
1	3	3
2	9	4
3	27	2
4	81	1
5	243	3
6	729	4
7	2187	2
8	6561	1

Order-finding: Esempio 2

Esempio 2: Si consideri $x = 5$ ed $N = 21$ Si trovi il valore dell'ordine di $x^r (\mathrm{mod}\, N)$. I valori di 5^r e $5^r (\mathrm{mod} 21)$ sono mostrati in tabella. Il valore di r è 6.

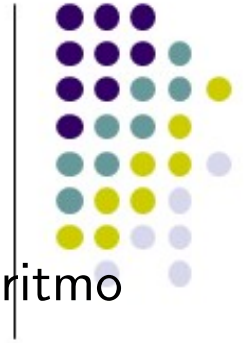
r	5^r	$5^r (\mathrm{mod} 21)$
0	1	1
1	5	5
2	25	4
3	125	20
4	625	16
5	3125	17
6	15625	1
7	78125	5
8	390625	4

Order-finding: Esempio 3

Esempio 3: Si consideri $x = 9$ ed $N = 35$ Si trovi il valore dell'ordine di $x^r (\mathrm{mod}\, N)$. I valori di 5^r e $5^r (\mathrm{mod} 21)$ sono mostrati in tabella. Il valore di r è 6.

r	9^r	$9^r (\mathrm{mod} 35)$
0	1	1
1	9	9
2	81	11
3	729	29
4	625	16
5	6561	4
6	59.049	1
7	531441	9
8	4782969	11

Order-finding



L'algoritmo di order-finding è basato sull'applicazione dell'algoritmo di stima della fase all'operatore unitario:

$$U|y\rangle \equiv |xy(\mathrm{mod}\, N)\rangle \tag{1}$$

con $y \in \{0,1\}^L$.

Si noti che quando $N \leq y \leq 2^L - 1$, la convenzione stabilita è che $xy(\mathrm{mod}\, N)$ è pari a y.

Quindi U opera in modo non triviale quando $0 \leq y \leq N-1$.

Si può verificare che gli stati definiti da:

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^k \bmod N\rangle \tag{2}$$

per i valori $0 \leq s \leq r-1$ sono autostati di U.

Order-finding

Poichè

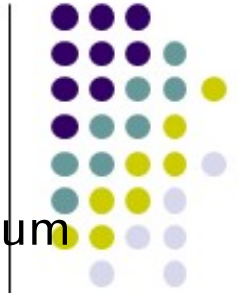
$$U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi isk}{r}\right] |x^{k+1} \bmod N\rangle \tag{3}$$
$$= \exp\left[\frac{2\pi is}{r}\right] |u_s\rangle$$

Quindi usando la procedura di stima della fase (Quantum Phase Estimation Algorithm) si può ottenere il corrispondente autovalore:

$$\exp\left[\frac{2\pi is}{r}\right] \tag{4}$$

e quindi il valore della fase $\varphi = s/r$ e quindi l'ordine r.

Order-finding



I passaggi essenziali della procedura di stima della fase (Quantum Phase Estimation Algorithm) sono:

1. implementare l'operatore U^{2^j} per qualsiasi numero intero j
2. preparare in modo efficiente l'autovettore $|u_s\rangle$ con un autovalore non banale, o almeno una sovrapposizione di tali autovettori.

Il primo requisito è soddisfatto usando una procedura nota come *esponenziazione modulare*, secondo la quale possiamo implementare l'intera sequenza di operazioni controllate U^{2^j} applicate usando $O\left(L^3\right)$ porte.

Il secondo requisito è un pò più complicato: preparare $|u_s\rangle$ richiede che si conosca r (che invece è ciò che vogliamo calcolare). Questo ostacolo può essere aggirato come segue e superare il problema di preparare $|u_s\rangle$ ricordando che:

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle \tag{5}$$

Order-finding

Nel realizzare la procedura di stima della fase, usiamo due registri.

Nel primo registro sistemiamo un numero di qubits pari a:

$$t = 2L + 1 + \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right)\right\rceil \tag{6}$$

Il secondo registro lo prepariamo con lo stato $|1\rangle$. In particolare per il secondo registro usiamo L qubits nello stato $|1\rangle$.

Lo stato iniziale complessivo dei due registri si scrive sinteticamente come:

$$|\psi\rangle = |0\rangle|1\rangle \tag{7}$$

Order-finding

Si applica poi la trasformazione di Hadamard al primo registro ottenendo lo stato:

$$|\psi\rangle = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|1\rangle \tag{8}$$

Il passo successivo è l'applicazione dell'operatore U che implementa la funzione di cui si vuole trovare la fase $\varphi = s/r$.

In questo caso quindi l'operatore U implementa l'operazione: $U|y\rangle \equiv |xy(\mathrm{mod}\, N)\rangle$ sul secondo registro, cioè:

$$|\psi\rangle = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle \left|x^j \bmod N\right\rangle \tag{9}$$

Order-finding

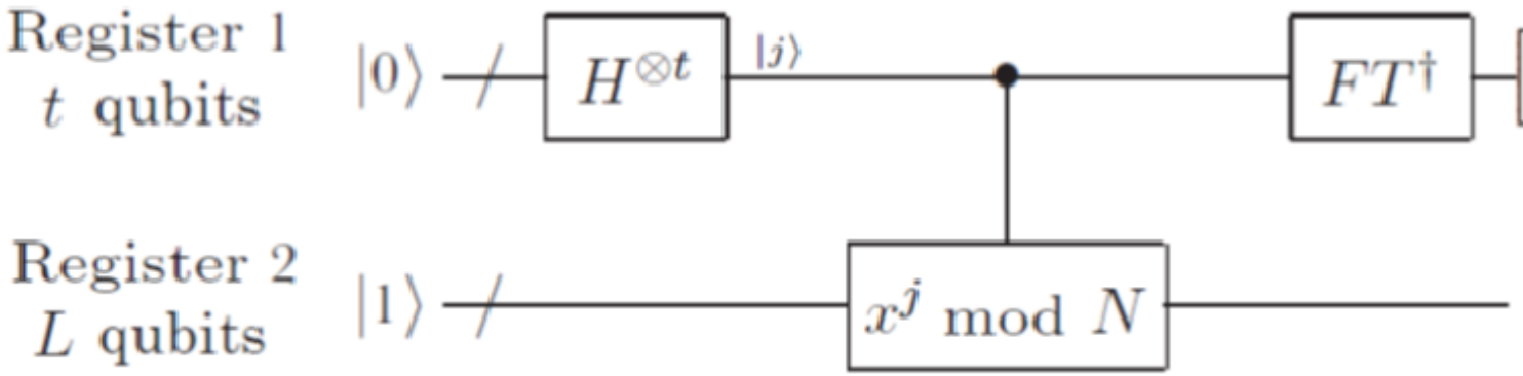


Figure 5.4. Quantum circuit for the order-finding algorithm. The second register is shown as being in the $|1\rangle$ state, but if the method of Exercise 5.14 is used, it can be initialized to $|0\rangle$ instead. This circui used for factoring, using the reduction given in Section 5.3.2.

Order-finding

In questo caso quindi l'operatore U implementa la trasformazione detta all'inizio: $U|y\rangle \equiv |xy(\mathrm{mod}\, N)\rangle$ al secondo registro cioè:

$$|\psi\rangle = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle \left|x^j \bmod N\right\rangle \tag{10}$$

$$|\psi\rangle \approx \frac{1}{\sqrt{r2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{2\pi isj/r} |j\rangle \, |u_s\rangle \tag{11}$$

Order-finding

Si applica successivamente l'operatore *QFT* inversa al primo registro:

$$|\psi\rangle \approx \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\widetilde{s/r}\rangle \, |u_s\rangle \tag{12}$$

da cui si ricava la fase:

$$\varphi \approx \widetilde{s/r} \tag{13}$$

per passare da $\widetilde{s/r}$ a r si applica un algoritmo per il calcolo delle frazioni (che non vedremo).

Order-finding