Quando fallisce OF?

1. Se la procedura ritorna una cattiva stima di $\frac{s}{r}$.

2. Se $\gcd(s,r) \neq 1$ in questo caso $r'$ ottenuto con lo sviluppo in frazioni continue è un fattore di $r$.

---

① Può succedere con probabilità al più $\varepsilon$ e basta aumentare un pò la grandezza del circuito

$$t = n + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right) \right\rceil$$

② Possiamo ripetere la stima di $\varphi$ la ricostruzione con le frazioni continue 2 volte supponiamo di ottenere $\frac{s_1'}{r'} = \frac{s_1}{r}$

$\frac{s_2}{r} = \frac{s_2'}{r_2'}$ - Se $(s_1, s_2) = 1 \Rightarrow$

$\text{mcm}(r_1', r_2') = r$.

—

Quale è la probabilità che $(s_1, s_2) = 1$ ?

$$P = 1 - \sum_q P(q|s_1) P(q|s_2) \geq 1 - \sum_q \frac{1}{q^2}$$

D'altra parte se $x \geq 2$

vale $$\frac{1}{x^2} \leq \frac{3}{2} \int_x^{x+1} \frac{1}{y^2} dx$$

e quindi

$$\sum_{q} \frac{1}{q^2} \leq \sum_{x=2}^{\infty} \frac{1}{x^2} \leq \frac{3}{2} \int_{2}^{\infty} \frac{1}{y^2}\, dy = \frac{3}{4}$$

e quindi $\boxed{\theta \geq \frac{1}{4}}$

Per concludere l'analisi di OF

- Servono $O(L)$ Hadamard
- e' inversa FT $O(L^2)$ gates
- esponenziazione $O(L^3)$
- frazioni continue $O(L^3)$ ($t'$)
- Dobbiamo poi ripetere per trovare $t$.

$\Rightarrow$ costo totale $\underline{O(L^3)}$

In conclusione

OF

Input: 1. $U_{x,N}$ black box

$U_{x,N} : |j\rangle|k\rangle \to |j\rangle|x^k \bmod N\rangle$

$((N,x)=1 \quad L=\lceil \log_2(N) \rceil)$

2. $t = 2L+1+\left\lceil \log\left(2+\frac{1}{2\varepsilon}\right)\right\rceil$ qbits $|0\rangle$

3. L qbits $|1\rangle$

Output: $r>0$ t.c. $O_N(x)=r$

Runtime: $\Theta(L^3)$ operazioni

probabilità di successo $\Theta(1)$

Per finire la stima di Shor (fattorizzazione) dobbiamo stimare $P(r \equiv 0 \ (2) \wedge x^{r/2} \not\equiv -1 \ (N))$

Vogliamo vedere che $\geq \frac{1}{2}$.

Intanto osserviamo che:

<u>Lemma</u> Sia $p$ primo $\neq 2$ e sia $2^d \| \varphi(p^\alpha)$ (max pot di 2 che divide $\varphi(p^\alpha)$). Allora se $x \in \mathbb{Z}^*_{p^\alpha}$ è scelto random

$$P\left(2^d \mid \mathcal{O}_{p^\alpha}(x)\right) = \frac{1}{2}$$

( $\mathcal{O}_{p^\alpha}(x)$ = ordine di $x$ mod $p^\alpha$ ).

Dim. Certamente $d \geq 1$.

Sia $\langle g \rangle = \mathbb{Z}^*_{p^\alpha}$, esiste $\forall x \; \exists k$

$x = g^k$, $1 \leq k \leq \varphi(p^\alpha)$.

Sia $r = \Theta_{p^\alpha}(x)$.

Se $k \equiv 1 \; (2)$ $\quad g^{kr} \equiv 1 \; (p^\alpha) \Rightarrow$

$\varphi(p^\alpha) \mid kr \Rightarrow 2^d \mid r$

Se $k \equiv 0 \; (2)$ $\quad g^{k\varphi(p^\alpha)/2} \equiv \left(g^{\varphi(p^\alpha)}\right)^{k/2} \equiv 1 \; (p^\alpha)$

$\Rightarrow r \mid \dfrac{\varphi(p^\alpha)}{2} \Rightarrow 2^d \nmid r$

Concludendo $\mathbb{Z}^*_{p^\alpha} = \{x = g^k, \; k \equiv 1 \; (2)\} \cup \{x \equiv g^k \; k \equiv 0 \; (2)\}$

$2^d \mid r$ $\qquad$ $2^d \nmid r$

$\Rightarrow$ Tesi

**Teorema** $N = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$, $p_i \neq 2$ $\forall i$

e sia $x \in \mathbb{Z}^*_N$ random., $\theta_N(x) = r$.

Allora

$$P\left(r \equiv 0 \,(2) \wedge x^{r/2} \not\equiv -1 \,(N)\right) \geq 1 - \frac{1}{2^m}$$

**Dim.** Dimostriamo che

$$P\left(r \equiv 1 \,(2) \vee x^{r/2} \equiv -1 \,(N)\right) \leq \frac{1}{2^m}$$

Per il teorema cinese del resto

scegliere $x$ random in $\mathbb{Z}^*_N$ equivale

a scegliere $x_1, \dots, x_m$ random

in $\mathbb{Z}^*_{p^{\alpha_1}}, \dots, \mathbb{Z}^*_{p^{\alpha_m}}$ t.c. $x \equiv x_i \,(p^{\alpha_i})$

Indichiamo con $r_j = o_{p_j}(x_j)$

e siano $2^{d_j} \| r_j$, $2^d \| r$.

Proviamo che se $r \equiv 1 \ (2)$

o $x^{r/2} \equiv -1 \ (N)$ allora $d_j = d_i \ \forall i,j$

quindi dal lemma la probabilità

che questo succeda $\geq \frac{1}{2m}$

Caso 1 $r \equiv 1 \ (2)$. Dato che $r_j | r \ \forall j$

si ha che $r_j \equiv 1 \ (2) \ \forall j$ e quindi

$d_j = 0 \ \forall j$

Caso 2 $x^{r/2} \equiv -1 \ (N)$.

Allora $x^{r/2} \equiv -1 \ (p^{\alpha_j})$ e $r_j \nmid r/2$

Dal momento che $r_j \mid r$, $d_j = d \; \forall j$

Quindi concludendo

## Shor

Input: $N$ composto

output: $p \mid N$, $p \neq 1$

$L = \lceil \log_2 N \rceil$

Runtime: $\Theta(L^3)$ operazioni. Probabilità di successo $\Theta(1)$.

1. $N \equiv 0 \,(2) \Rightarrow 2$ $\quad \Theta(1)$ op
2. if $N = a^b \Rightarrow a$ $\quad O(L^3)$ op
3. $x$ random in $\mathbb{Z}/N$ . if $d = \gcd(x, N) \neq 1 \Rightarrow d$ $\quad \Theta(L^2)$
4. OF: $r = \theta_{x(N)}$ $\quad \Theta(L^3)$ $\quad \Theta(1)$ successo
5. if $r \equiv 0 \,(2) \wedge x^{r/2} \not\equiv -1 \,(N) \Rightarrow \gcd(x^{r/2} \pm 1, N)$

$\Theta(L^3), \Theta(1)$