Calcolo della fase.

Assumiamo $M = 2^t$

e consideriamo la base

$|0\rangle, \dots, |M-1\rangle$.

Abbiamo visto che se $|j\rangle = |j_1 \cdots j_t\rangle$

$$F : |j\rangle \longrightarrow \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} e^{\frac{2\pi i j k}{M}} |k\rangle$$

ossia

$$|j_1 \dots j_t\rangle \longrightarrow \frac{\left(|0\rangle + e^{2\pi i 0.j_t} |1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_1 \cdots j_t} |1\rangle\right)}{\sqrt{N}}$$

dove $.j_l \cdots j_m = \frac{j_l}{2} + \frac{j_{l+1}}{4} + \dots + \frac{j_m}{2^{m-l+1}}$

Vogliamo applicare QFT per definire una procedura, la <u>STIMA della FASE</u>, che è alla base di molti algoritmi quantistici.

Supponiamo di avere uno stato

$$|\psi\rangle = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} e^{2\pi i \varphi k} |k\rangle$$

Vogliamo stimare φ.

Applichiamo a $|\psi\rangle$ l'inversa di QFF

$$\rightarrow \bullet \quad F^{-1}|\psi\rangle = \frac{1}{M} \sum_{k,j=0}^{M-1} e^{-\frac{2\pi i k j}{M}} \cdot e^{2\pi i \varphi k} |j\rangle$$

se φ può essere espresso esattamente con t bits come $\varphi = 0.\varphi_1 \dots \varphi_t$ (ad es se $\varphi = \frac{j}{2^t}$) allora

$$|\psi\rangle = \sum_{k=0}^{M-1} e^{2\pi i \varphi} |k\rangle = \qquad M = 2^t$$

$$= \frac{1}{\sqrt{M}} \left(|0\rangle + e^{2\pi i 0.\varphi_t} |1\rangle\right) \dots \left(|0\rangle + e^{2\pi i 0.\varphi_1 \dots \varphi_t} |1\rangle\right)$$

e quindi applicando l'inversa della QFT misuriamo esattamente

$$|\varphi_1 \dots \varphi_t\rangle = |\varphi\rangle \quad !$$

ma se φ non ha un'espansione binaria con t bits?

Vogliamo vedere che riusciamo a ottenere una buona approssimazione di φ.

Sia $0 \le b \le 2^t - 1$ t.c.

$\frac{b}{2^t} = 0.b_1 \dots b_t$ sia la

migliore approssimazione di φ

per difetto ($\le \varphi$).

In questo caso $\delta = \varphi - \frac{b}{2^t}$

è tale che

$$0 \le \delta \le \frac{1}{2^t}$$

Vogliamo vedere che la misura

di $*$ produce un risultato

"vicino" a b che quindi permette

di stimare φ con alta probabilità.

Dopo aver applicato F^{-1} abbiamo lo stato

$$F^{-1}|\psi\rangle = \frac{1}{M}\sum_{k=0}^{M-1}\sum_{l=0}^{M-1} e^{-\frac{2\pi i k l}{M}} \cdot e^{2\pi i \varphi k} |l\rangle$$

Allora l'ampiezza dello stato $|b+l \pmod{2^t}\rangle$ è

$$\gamma_l = \frac{1}{M}\sum_{k=0}^{M-1}\left(e^{2\pi i\left(\varphi - \frac{(b+l)}{M}\right)}\right)^k$$

$$= \frac{1}{M}\;\frac{1-e^{2\pi i (M\varphi-(b+l))}}{1-e^{2\pi i\left(\varphi - \frac{b+l}{M}\right)}}$$

$$= \frac{1}{M}\;\frac{1-e^{2\pi i (M\delta - l)}}{1-e^{2\pi i (\delta - l/M)}}$$

dato che $M\varphi = M\delta + b$.

Supponiamo di misurare $\underline{\underline{m}}$

Vogliamo limitare la probabilità

di ottenere un valore di m

t.c. $|m-b|>e$, con $e \in \mathbb{N}_+$

(che caratterizzerà la tolleranza

che vogliamo) Per come abbiamo def. γ_e si ha:

$$P(|m-b|>e) = \sum_{-M/2 < l \leq -(e+1)} |\gamma_l|^2 + \sum_{e+1 \leq l \leq M/2} |\gamma_l|^2$$

Vediamo cosa possiamo dire

di $|\gamma_l|$.

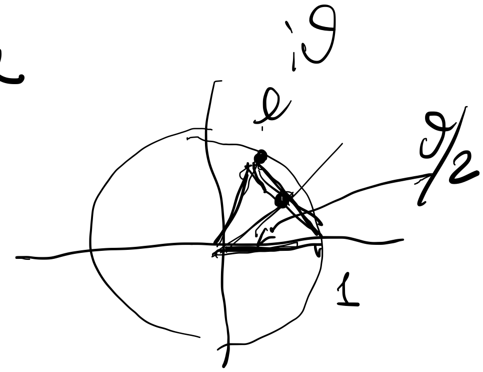
innanzitutto, dato che $\forall \vartheta \in \mathbb{R}$

$|1-e^{i\vartheta}| \leq 2$ vale

$$|\gamma_\ell| \le \frac{2}{M\left|1-e^{2\pi i(\delta-\ell/M)}\right|}.$$

Poi se $-\pi \le \vartheta \le \pi$ vale

$$|1-e^{i\vartheta}| \ge \frac{2|\vartheta|}{\pi}$$



e quindi, dato che se $-\frac{M}{2} \le \ell \le M/2$

$$-\pi \le 2\pi\left(\delta - \frac{\ell}{M}\right) \le \pi$$

vale anche

$$|\gamma_\ell| \le \frac{1}{2M\left(\delta-\frac{\ell}{M}\right)}$$

Combinando

$$P(|m-b|>\varepsilon) \leq \frac{1}{4}\left[\sum_{-\frac{M}{2}+1}^{-(e+1)} \frac{1}{(\ell - M\delta)^2} + \frac{1}{4}\sum_{e+1}^{M/2} \frac{1}{(\ell - M\delta)^2}\right]$$

e dal momento che $0 \leq M\delta \leq 1$

$$P(|m-b|>\varepsilon) \leq \frac{1}{4}\left[\sum_{-M/2+1}^{-(e+1)} \frac{1}{\ell^2} + \sum_{e+1}^{M/2} \frac{1}{(\ell-1)^2}\right]$$

$$\leq \frac{1}{2} \sum_{e}^{M/2-1} \frac{1}{\ell^2} \leq \frac{1}{2}\int_{e-1}^{M/2-1} \frac{1}{\ell^2}\, d\ell$$

$$= \frac{1}{2(e-1)} .$$

Supponiamo allora di volere approssimare φ con un'accuratezza $\underline{2^{-n}}$ se scegliamo $e = 2^{t-n} - 1$ usando $t = n+p$ bits la probabilità di ottenere un'approssimazione corretta è almeno $1 - \frac{1}{2(2^p - 2)}$

Allora otteniamo φ accurato a $\underline{\underline{n}}$ bits con probabilità di successo almeno $1-\varepsilon$ se scegliamo

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