# 94-quantum-shor-discrete-fourier-transform-properties-03

## Quantum Computing

Proprietà della QFT





## ricordiamo che

- se applichiamo la QFT (DFT) ad uno stato qualunque otteniamo

$$\frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix}\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{N-1} \end{pmatrix}$$

  - e se misuriamo l'output otteniamo un valore $j$ con probabilità $|\beta_j|^2$
- ad esempio: $\beta_1 = \alpha_0 + \omega\alpha_1 + \cdots + \omega^{N-1}\alpha_{N-1}$
  - e la probabilità di ottenere in output il valore $1$ è $|\beta_1|^2$

# 94-quantum-shor-discrete-fourier-transform-properties-03

## proprietà di convoluzione

- supponiamo sia

$$\frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix}\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{N-1} \end{pmatrix}$$

- se *ruotiamo* le ampiezze dell'input otteniamo

$$\frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix}\begin{pmatrix} \alpha_{N-1} \\ \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-2} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \omega\beta_1 \\ \omega^2\beta_2 \\ \vdots \\ \omega^{N-1}\beta_{N-1} \end{pmatrix}$$

  – e se misuriamo l'output otteniamo lo stesso un valore $j$ con probabilità $|\beta_j|^2$

3

3

## convoluzione – dimostrazione

- se ruotiamo le ampiezze dell'input otteniamo

$$\frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix}\begin{pmatrix} \alpha_{N-1} \\ \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-2} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \omega\beta_1 \\ \omega^2\beta_2 \\ \vdots \\ \omega^{N-1}\beta_{N-1} \end{pmatrix}$$

- guardiamo la seconda riga (la prima è facile, le altre sono analoghe)
  – ricordiamo che $\beta_1 = \alpha_0 + \omega\alpha_1 + \cdots + \omega^{N-1}\alpha_{N-1}$
  – dato che $\omega^N = 1$, abbiamo: $\alpha_{N-1} + \omega\alpha_0 + \cdots + \omega^{N-1}\alpha_{N-2} = \omega\alpha_0 + \cdots + \omega^{N-1}\alpha_{N-2} + \omega^N\alpha_{N-1} = \omega(\alpha_0 + \omega\alpha_1 + \cdots + \omega^{N-1}\alpha_{N-1}) = \omega\beta_1$

4

4

94-quantum-shor-discrete-fourier-transform-properties-03

## convoluzione – misura

- se ruotiamo le ampiezze dell'input otteniamo

$$\frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix} \begin{pmatrix} \alpha_{N-1} \\ \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-2} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \omega\beta_1 \\ \omega^2\beta_2 \\ \vdots \\ \omega^{N-1}\beta_{N-1} \end{pmatrix}$$

  - e se misuriamo l'output otteniamo lo stesso un valore $j$ con probabilità $|\beta_j|^2$
  - ciò dipende dal fatto che il modulo al quadrato di $\omega^k$ è $1$ per ogni valore di $k$

5

5

## convoluzione – sintesi

- quindi se applichiamo una primitiva *rotate* (o *shift*) alle ampiezze dell'input, dal punto di vista della misura dell'output le cose non cambiano

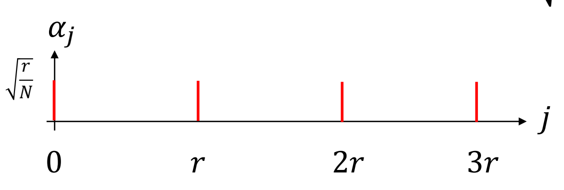
6

6

# 94-quantum-shor-discrete-fourier-transform-properties-03

## QFT e periodicità

- supponiamo che gli $\alpha_j$ in input abbiano un andamento periodico con periodo $r$ (per semplicità, con $N$ multiplo di $r$)
  - in particolare supponiamo che tutti gli $\alpha_j$ abbiano valore $0$ salvo $\alpha_0$, $\alpha_r$, $\alpha_{2r}$, …., $\alpha_{\left(\frac{N}{r}-1\right)r}$ ($\frac{N}{r}$ ampiezze), che invece hanno valore $\sqrt{\frac{r}{N}}$

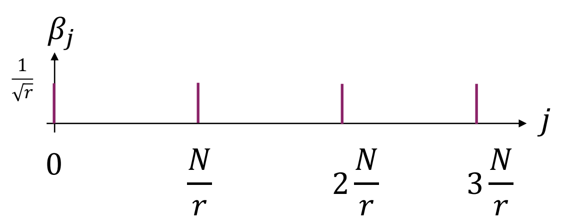



7

7

## QFT e periodicità

- allora i $\beta_i$ in output hanno un andamento periodico con periodo $\frac{N}{r}$ (con $N$ multiplo di $r$)
  - in particolare tutti i $\beta_j$ hanno valore $0$ salvo $\beta_0$, $\beta_{\frac{N}{r}}$, $\beta_{2\frac{N}{r}}$, …., $\beta_{(r-1)\frac{N}{r}}$, $\beta_N$ ($r$ ampiezze), che invece hanno valore $\frac{1}{\sqrt{r}}$




8

8

# 94-quantum-shor-discrete-fourier-transform-properties-03

## QFT e periodicità – vettori

- in termini di rappresentazione vettoriale abbiamo

$$\sqrt{\frac{r}{N}}\begin{pmatrix}1\\0\\\vdots\\0\\1\\0\\\vdots\\0\\1\\0\\\vdots\\0\end{pmatrix} \xrightarrow{\mathrm{QFT}_N} \frac{1}{\sqrt{r}}\begin{pmatrix}1\\0\\\vdots\\0\\1\\0\\\vdots\\0\end{pmatrix}$$

9

9

## QFT e periodicità – dimostrazione

- in termini di notazione ket abbiamo

$$\sqrt{\frac{r}{N}}\sum_{j=0}^{\frac{N}{r}-1}|jr\rangle \xrightarrow{\mathrm{QFT}_N} \sum_{j=0}^{N-1}\beta_j|j\rangle$$

- vediamo quanto valgono effettivamente i $\beta_j$
  - se $j$ è multiplo di $\frac{N}{r}$ scriviamo $\beta_j$ come $\beta_{k\frac{N}{r}}$ e abbiamo

$$\beta_{k\frac{N}{r}} = \sum_{j=0}^{\frac{N}{r}-1}\sqrt{\frac{r}{N}}\sqrt{\frac{1}{N}}\,\omega^{jr\cdot k\frac{N}{r}} = \sum_{j=0}^{\frac{N}{r}-1}\sqrt{\frac{r}{N}}\sqrt{\frac{1}{N}}\,\omega^{j\cdot kN} =$$

$$\sqrt{\frac{r}{N}}\sqrt{\frac{1}{N}}\sum_{j=0}^{\frac{N}{r}-1} 1 = \frac{N}{r}\cdot\frac{\sqrt{r}}{N} = \frac{1}{\sqrt{r}}$$

10

10

# 94-quantum-shor-discrete-fourier-transform-properties-03

## QFT e periodicità – dimostrazione un'occhiata alla matrice della QFT

$$\frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & \vdots & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \omega^{k\frac{N}{r}} & \vdots & \omega^{rk\frac{N}{r}} & \cdots & \omega^{(k-1)\frac{N}{r}(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \vdots & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} r = \begin{pmatrix} \beta_0 \\ \vdots \\ \beta_{k\frac{N}{r}} \\ \vdots \\ \beta_{N-1} \end{pmatrix}$$

11

11

## QFT e periodicità – dimostrazione

- in termini di notazione ket abbiamo

$$\sqrt{\frac{r}{N}}\sum_{j=0}^{\frac{N}{r}-1}|jr\rangle \xrightarrow{\text{QFT}_N} \sum_{j=0}^{N-1}\beta_j|j\rangle$$

- vediamo quanto valgono effettivamente i $\beta_j$
  – se $j$ è multiplo di $\frac{N}{r}$ scriviamo $\beta_j$ come $\beta_{k\frac{N}{r}}$ e abbiamo $\beta_{k\frac{N}{r}} = \frac{1}{\sqrt{r}}$
  – ci sono $r$ di queste ampiezze e la somma dei loro quadrati è $1$; questo implica che tutte le altre ampiezze hanno valore $0$

12

12