Computação Quântica
Aula 09

Murilo V. G. da Silva

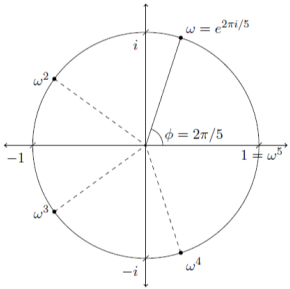
DINF/UFPR

Preliminares: A n-ésima raiz da unidade

Exemplo: Para $n = 5$, quais as raízes de $x^5 = 1$?

- Uma raíz é $x = 1$, pois $(1)^5 = 1$
- Outra raíz é $x = e^{2\pi i/5}$, pois $(e^{2\pi i/5})^5 = (e^{\pi i})^2 = (-1)^2 = 1$

Antes de procurar outras raízes, vamos entender por que $e^{2\pi i/5}$ é uma raíz. (Lembre que $e^{i\theta} \cdot e^{i\theta'} = e^{i(\theta+\theta')}$)

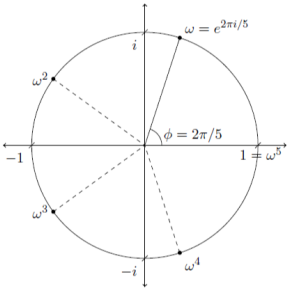


Seja $\omega = e^{2\pi i/5}$.

- Ao multiplicarmos ω consigo mesmo 5 vezes vamos somando o ângulo $2\pi/5$ até que o ângulo chegue a 2π, ou seja, o vetor chegue até 1.
- Note ao elevarmos ω^2 a quinta potência o vetor (depois de "duas voltas no círculo") também chega a 1.
- O que acontece com ω^3 e ω^4? Observe que as 5 raízes são $1, \omega, \omega^2, \omega^3$ e ω^4?

Preliminares: A n-ésima raiz da unidade

Para $n = 5$, as raízes de $x^5 = 1$ são 1, ω, ω^2, ω^3 e ω^4:



Para n em geral, sendo $\omega = e^{2\pi i/n}$, quais são as raízes de $x^n = 1$? Resp.: ω^i, $i = 0, \ldots, n-1$

- Pergunta: qual o valor de ω^n? Resposta: 1
- Pergunta: Qual o valor de $(\omega^2)^n$? Resposta: 1
- Pergunta: Para $m > n$, qual o valor de ω^m? Resp.: ω^r, tal que $r = m$ (mod n)
- Exercício 1: Calcule $1 + \omega + \omega^2 + \ldots + \omega^{n-1}$
- Exercício 2: Calcule $1 + \omega^j + \omega^{2j} + \ldots + \omega^{n-1j}$
- Exercício 3: Calcule $|1|^2 + |\omega^j|^2 + |\omega^{2j}|^2 + \ldots + |\omega^{(n-1)j}|^2$

A transformada discreta de Fourier (DFT)

Considere a seguinte matriz $M \times M$

$$\frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

sendo que $\omega = e^{2\pi i/M}$

- **Note: posição (j,k) tem o valor ω^{jk}**
- Para $M = 2$, qual a matriz correspondente? Você conhece essa matriz?
- Calcule agora a matriz para $M = 4$.

DFT *vs* QFT

Voltando a matriz $M \times M$

$$\frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

Lembrando que $\omega = e^{2\pi i/M}$

- Exercício 4: Calcule a QFT para $M = 8$.
- Exercício 5: Prove que matriz, para qualquer M, é unitária (Dica: Exercícios 1, 2, 3)
- Afirmação: É possível implementar com um número polinomial de portas (provaremos separadamente)

Qual a vantagem e a desvantagem da versão quântica da DFT?

Trasformada quântica de Fourier

Primeira propriedade útil da QFT:

- Sobreposições e shits circulares

QFT e sobreposições circulares

- Seja $|\Phi\rangle \in \mathbb{C}_M$ e F_M a matriz da QFT
- Seja $|\Phi'\rangle$ o vetor obtido de "shift circular" de j posições de $|\Phi\rangle$
- Se $F_M |\Phi\rangle = |\Psi\rangle$, então $F_M |\Phi'\rangle = \omega^j |\Psi\rangle$.
- Lembre que $|\omega^j| = 1$

Ou seja, se o objetivo é fazer uma medida após a QFT, um shift circular não altera a distribuição de probabilidade dos estados resultantes

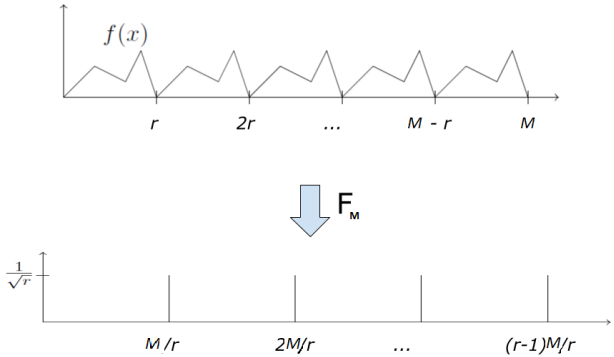
Trasformada quântica de Fourier

Segunda propriedade útil da QFT:

- Sobreposições periódicas

QFT e funções periódicas

Aplicamos a QFT F_M a um vetor de amplitudes periódico, com período r:

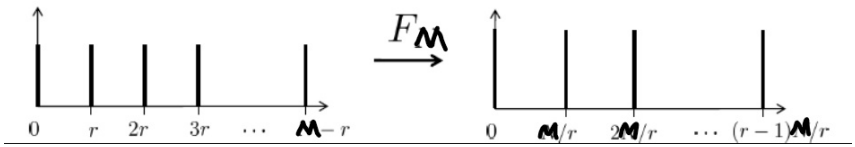


Resultado:

- Saída também é um vetor de amplitudes periódico, agora com período M/r
- Vamos ver agora um caso particular desta propriedade que nos será útil no Algoritmo de Shor.

QFT e funções periódicas

O caso particular é ilustrado pela figura abaixo:



Amplitudes de α_r entrada:

- As amplitudes α_i, para $|i\rangle$, onde $i = jr$, $j = 0, 1, 2, ..., (M/r - 1)$ são todas iguais e todas > 0.
- As demais amplitudes são todas iguais a zero.
- Pergunta: Qual o valor de cada amplitudes α_r? Resposta: $\sqrt{\frac{r}{M}}$.

Amplitudes de saída β_k devem ser:

- Para $k = 0, \frac{M}{r}, \frac{2M}{r}, \frac{3M}{r}, ..., \frac{(r-1)M}{r}$ as amplitudes devem ser iguais a $\frac{1}{\sqrt{r}}$
- iguais a zero para as demais posições do vetor de amplitudes.
- Vamos provar que a QFT tem de fato esta propriedade neste caso particular
  (não precisamos da propriedade da QFT em funções periódicas em geral no Algoritmo de Shor)

Prova:

- Vetor de entrada: $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr\rangle$
- Vamos calcular as amplitudes β_j do vetor de saída.
- Vamos olhar para os β_j, onde j é um múltiplo de $\frac{M}{r}$, ou seja, $j = \frac{kM}{r}$
- O valor $\beta_{\frac{kM}{r}}$ é o produto da $(\frac{kM}{r})$-ésima linha de F_M pelo vetor de entrada

  (Atenção, nesta notação a primeira linha é a 0-ésima linha)
- Portanto $\beta_{\frac{kM}{r}} = \sum_{j=0}^{\frac{M}{r}-1} \sqrt{\frac{r}{M}} \cdot \frac{1}{\sqrt{M}} \omega^{jr \frac{kM}{r}} = \frac{M}{r} \frac{\sqrt{r}}{M} = \frac{1}{\sqrt{r}}$

Como cada uma das r amplitudes $\beta_{\frac{kM}{r}}$ é igual a $\frac{1}{\sqrt{r}}$ e o a soma do quadrado do módulo destas r amplitudes β_j é 1, as demais amplitudes devem ser 0, e o teorema está provado.

Exercício 6: execute a QFT para um exemplo em que $M = 32$ e $r = 4$.