Computação Quântica
Aula 07

Murilo V. G. da Silva

DINF/UFPR

Introdução

Ponto chave em algoritmos quânticos:

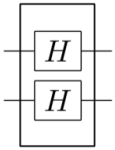
- Uma vez que temos *qubits* ao invés de *bits*, a ideia é criar manipular superposições "interessantes"
- Na aula de hoje veremos a técnica mais importante neste contexto: Amostragem de Fourier

A transformada de Hadamard

1-bit clássico na entrada

- $H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
- $H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$
- nada de novo até agora...

A transformada de Hadamard



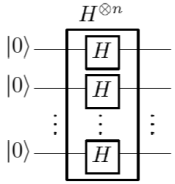
2-bits clássicos na entrada

- $H^{\otimes 2}|00\rangle = +\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$
- $H^{\otimes 2}|01\rangle = +\frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$
- $H^{\otimes 2}|10\rangle = +\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$
- $H^{\otimes 2}|11\rangle = +\frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$

Note:

- Dada uma string clássica u acima, em $H^{\otimes 2}|u\rangle$, temos que...
- ...sinal do termo $\frac{1}{2}|x\rangle$ depende de $x \cdot u$
- Especificamente, o termo é multiplicado por $(-1)^{x \cdot u}$

A transformada de Hadamard



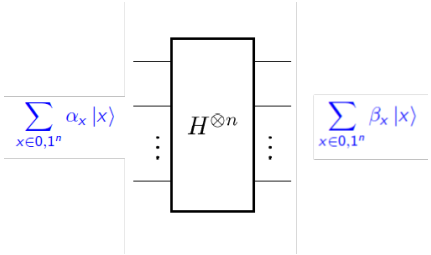
Caso geral: Seja u uma string de n bits clássica

$$H^{\otimes n}|u\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_{x}(-1)^{u\cdot x}|x\rangle$$

Obs: Notação ligeiramente diferente encontrada na literatura:

$$H^{\otimes n}|u\rangle_n = \frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{2^n-1}(-1)^{u\cdot x}|x\rangle_n$$

Amostragem de Fourier



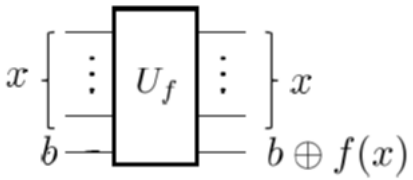
A seguinte técnica é conhecida como amostragem de Fourier:

- Aplicar a transformada de Hadamard em alguma superposição

$$\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \longrightarrow \sum_{x\in\{0,1\}^n} \beta_x |x\rangle$$

- Depois medir, obtendo obter x com probabilidade $|\beta|^2$

A técnica "phase kick-back"



Considere o circuito acima que computa a função booleana $f : \{0,1\}^n \to \{0,1\}$.

- Lembramos que a saída $f(x)$ em circuitos quânticos é um $\oplus$ com 0's de entrada.
- Em muitos casos será útil setar tais bits de entrada com qubits $b \neq 0$, o que será o caso para fazermos *phase kick-back*.
- O que faremos é setar tal qubit da entrada para $|-\rangle$.

Afirmação: $U_f |x\rangle |-\rangle = (-1)^{f(x)} |x\rangle |-\rangle$
Prova: Próximo slide.

A técnica "phase kick-back"

Seja $f : \{0,1\}^n \Rightarrow \{0,1\}$ e U_f o circuito quântico computando f. Então

$$U_f \left|x\right\rangle_n \left|-\right\rangle = (-1)^{f(x)} \left|x\right\rangle_n \left|-\right\rangle$$

Prova: $U_f \left|x\right\rangle_n \left|-\right\rangle = U_f \left|x\right\rangle_n (\frac{|0\rangle}{\sqrt{2}} - \frac{|1\rangle}{\sqrt{2}}) = U_f(\frac{\left|x\right\rangle_n|0\rangle}{\sqrt{2}} - \frac{\left|x\right\rangle_n|1\rangle}{\sqrt{2}})$

$= (\frac{U_f\left|x\right\rangle_n|0\rangle}{\sqrt{2}} - \frac{U_f\left|x\right\rangle_n|1\rangle}{\sqrt{2}})$ por linearidade

$= (\frac{\left|x\right\rangle_n|0 \oplus f(x)\rangle}{\sqrt{2}} - \frac{\left|x\right\rangle_n|1 \oplus f(x)\rangle}{\sqrt{2}})$ aplicação do circuito U_f

$= \left|x\right\rangle_n (\frac{|0 \oplus f(x)\rangle}{\sqrt{2}} - \frac{|1 \oplus f(x)\rangle}{\sqrt{2}})$

$= \left|x\right\rangle_n (\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}})$

$= \left|x\right\rangle_n (-1)^{f(x)} (\frac{|0\rangle - |1\rangle}{\sqrt{2}})$ visto em sala

$= (-1)^{f(x)} \left|x\right\rangle_n \left|-\right\rangle$

O Problema de Bernstein-Vazirani

Entrada: Uma função $f : \{0,1\}^n \to \{0,1\}$ que computa $f(x) = x \cdot a$, para string a desconhecida.

Saida: Retornar a string a

Obs: Neste problema assumimos que estamos no "modelo *black box*"

(na prática podemos pensar que a entrada é um circuito ou um algoritmo que computa f, mas não podemos "inspecioná-los", sim apenas fazer *queries*.)

Pergunta:

- Com um algoritmo clássico, quantas *queries* precisamos fazer?
- Podemos fazer melhor usando um algoritmo quântico?

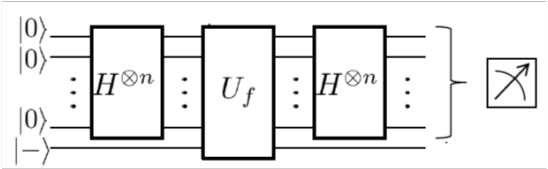
Algoritmo clássico:

- Seja $x_i \in \{0,1\}^n$, onde x_i tem o i-ésimo bit setado para 1 e os demais para 0.
- Compute $f(x_i)$, para $i = 1, ..., n$. Com isso revela-se o i-ésimo bit de a
- Note que como cada query pode revelar no máximo um bit, o algoritmo é ótimo neste modelo.

O Algoritmo de Bernstein-Vazirani

Entrada: Uma função $f : \{0,1\}^n \to \{0,1\}$ que computa $f(x) = x \cdot a$, para string a desconhecida.

Saida: Retornar a string a



- Estado dos n qubits saindo da primeira transormada de Hadamard: $\frac{1}{2^{\frac{n}{2}}} \sum |x\rangle$
- Estado dos $n+1$ qubits depois de U_f: $\frac{1}{2^{\frac{n}{2}}} \sum (-1)^{f(x)} |x\rangle |-\rangle$
- Estado dos n qubits saindo da segunda transformada de Hadamard: $|a\rangle$
- Medindo $|a\rangle$, obtém-se a com probabilidade 1.