Computação Quântica

Luís Soares Barbosa

Mestrado em Engenharia Física
Universidade do Minho

Folha de Exercícios 3

Questão 1

O iterador de Grover corresponde ao circuito

$$G = H^{\otimes n} P H^{\otimes n} Q_f$$

onde $P = 2|0\rangle\langle 0| - I$ e $Q_f|x\rangle = (1)^{fx}|x\rangle$, i.e. a *phase query gate* obtida de um oráculo para f.

Considere um problema de procura não estruturada sobre 2^2 e suponha que o único valor para o qual f retorna 1 é $x_0 = 10$.

1. Calcule a matriz correspondente à porta Q_f.
2. Calcule a matriz correspondente a $H^{\otimes 2} P H^{\otimes 2}$.
3. Calcule a matriz correspondente a $H^{\otimes 2} P H^{\otimes 2} Q_f H^{\otimes 2}$ e aplique-a ao estado inicial $|00\rangle$.
4. Calcule o estado resultante de uma segunda execução do iterador de Grover. Medindo este estado na base computacional, qual a probabilidade de obter o valor marcado 01?

Questão 2

Mostre que o iterador de Grover é um operador unitário.

Questão 3

É objectivo deste exercício e do seguinte generalizar o algoritmo de Grover para o caso em que a procura tem um conjunto

$$s = \{x \in \Sigma^n \mid fx = 1\}$$

não necessariamente singular. Representemos por r o complementar de s. Note que $Q_f|s\rangle = -|s\rangle$ enquanto $Q_f|r\rangle = |r\rangle$e consideremos os estados em sobreposição uniforme sobre s e r, i.e.,

$$|s\rangle = \frac{1}{\sqrt{s}} \sum_{x \in s} |x\rangle \qquad |r\rangle = \frac{1}{\sqrt{r}} \sum_{x \in r} |x\rangle$$

Claramente,

$$|\phi\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \Sigma^x} |x\rangle = \sqrt{\frac{|s|}{N}}|s\rangle + \sqrt{\frac{|r|}{N}}|r\rangle$$

1. Justifique o seguinte cálculo do efeito do iterador de Grover sobre $|r\rangle$:

$$\begin{aligned}
G|r\rangle &= (2|\phi\rangle\langle\phi| - I)Q_f|r\rangle \\
&= (2|\phi\rangle\langle\phi| - I)|r\rangle \\
&= 2\sqrt{\frac{|r|}{N}}|\phi\rangle - |r\rangle \\
&= 2\sqrt{\frac{|r|}{N}}\left(\sqrt{\frac{|r|}{N}}|r\rangle + \sqrt{\frac{|s|}{N}}|s\rangle\right) - |r\rangle \\
&= \left(\frac{2|r|}{N} - 1\right)|r\rangle + \frac{2\sqrt{|r||s|}}{N}|s\rangle \\
&= \frac{|r| - |s|}{N}|r\rangle + \frac{2\sqrt{|r||s|}}{N}|s\rangle
\end{aligned}$$

2. Calcule $G|s\rangle = -\frac{2\sqrt{|r||s|}}{N}|r\rangle + \frac{|r|-|s|}{N}|s\rangle$.
3. Mostre que a acção de G pode ser expressa pelo quadrado da seguinte matriz M

$$\begin{bmatrix} \sqrt{\frac{|r|}{N}} & -\sqrt{\frac{|s|}{N}} \\ \sqrt{\frac{|s|}{N}} & \sqrt{\frac{|r|}{N}} \end{bmatrix}$$

4. A matriz M pode ser expressa como

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

   onde $\theta = \sin^{-1}\sqrt{\frac{|s|}{N}}$.
   Mostre que

$$M^2 = \begin{bmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{bmatrix}$$

   e $|\phi\rangle = \cos\theta\,|r\rangle + \sin\theta\,|s\rangle$.

Questão 4

O efeito do iterador de Grover corresponde a uma rotação de 2θ no espaço definido pelos vercotre $|r\rangle$ e $|s\rangle$. Logo,

$$\begin{aligned}
G|\phi\rangle &= \cos 3\theta\,|r\rangle + \sin 3\theta\,|s\rangle \\
G^2|\phi\rangle &= \cos 5\theta\,|r\rangle + \sin 5\theta\,|s\rangle \\
\cdots &= \cdots \\
G^k|\phi\rangle &= \cos{(2k+1)\theta}\,|r\rangle + \sin{(2k+1)\theta}\,|s\rangle
\end{aligned}$$

para determinar o valor ideal de k, i.e., do número de iterações, será necessário escolhê-lo de forma que

$$\langle s|G^k|\phi\rangle = \sin{(2k+1)\theta}$$

seja o mais possível próximo de 1 de modo a maximizar a probabilidade de obter um $x \in s$ na medição. Então, $(2k+1)\theta \approx \frac{\pi}{2}$, donde,

$$k \approx \frac{\pi}{4\theta} - \frac{1}{2}$$

em rigor, o valor inteiro mais próximo de $\frac{\pi}{4\theta}$.

1. Explique por que razão o número óptimo de iterações é dependente do número de soluções.
2. Considere $|s| = 1$ e, consequentemente, k como o inteiro mais próximo de

$$\frac{\pi}{4\sqrt{\frac{1}{N}}} = \frac{\pi}{4}\sqrt{N}$$

Note que

$$\theta = \sin^{-1}\left(\sqrt{\frac{1}{N}}\right) \approx \sqrt{\frac{1}{N}}$$

A probabilidade

$$p = sin^2(2k+1)\theta$$

de obter a (única) solução utilizando o número óptimo de iterações k calculado acima é dependente de N, como vimos. Faça uma tabela com as probabilidades calculadas para diferentes valores de N (de 2 a 2048). O que pode concluir?

O estudo que efectuar mostrará que os valores tomados pelas probabilidades não são estritamente crescentes, mas que a probabilidade de sucesso aumenta com o valor N, aproximando-se de 1 para N muito elevado.

3. Repita este estudo para o caso em que $|s| = 4$.