Neste trabalho, terá de responder a perguntas e simular circuitos quânticos.

As respostas às perguntas devem ser entregues num documento PDF, que pode escrito a computador (utilizando Microsoft Word, LaTeX, ou semelhantes) ou escrito à mão e digitalizado.

Para escrever os circuitos, deve preencher o notebook Jupyter disponibilizado (também disponível em https://tinyurl.com/quc-avaliacao2) e entregar uma cópia do ficheiro `.ipynb` resolvido. Em alternativa, poderá implementar os circuitos utilizando o IBM Quantum Composer. Nesse caso, terá de mostrar uma cópia da imagem do circuito e do código OpenQASM/Qiskit que é gerado automaticamente. Inclua estes elementos no PDF a entregar.

O trabalho deverá ser submetido usando a opção do Inforestudante "Submissão de Trabalhos". Terão um prazo de uma semana para entregar o trabalho, com início a 23 de Dezembro e final a 4 de Janeiro.

O objetivo desta avaliação é a implementação do Algoritmo de Grover, estudado durante as aulas. No algoritmo de Grover, um oráculo marca um estado secreto da base computacional invertendo o sinal da sua amplitude, mas mantendo todos os outros estados da base computacional inalterados. O objetivo do algoritmo é encontrar o estado secreto com o menor número de chamadas ao oráculo possível.

(1) Implemente o circuito do oráculo da Figura 1. Este circuito marca um estado secreto que irá descobrir.

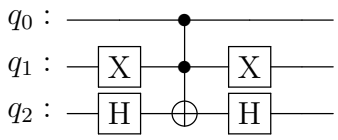


Figura 1. Circuito para o Oráculo de Grover

Nota: no IBM Quantum Composer, após desenhar o circuito, pode agregar as portas do circuito num só grupo, e dar um nome ao grupo. Para isso, selecione as portas simultaneamente e utilize a opção apropriada do menu que surge em baixo. Isto facilitará a alínea (3).

(2) Implemente o circuito do operador de difusão da Figura 2.

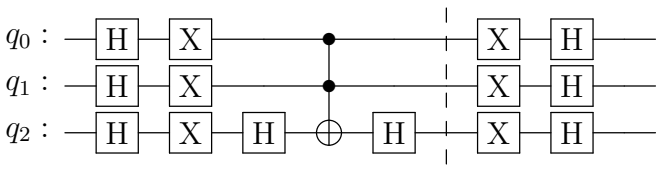
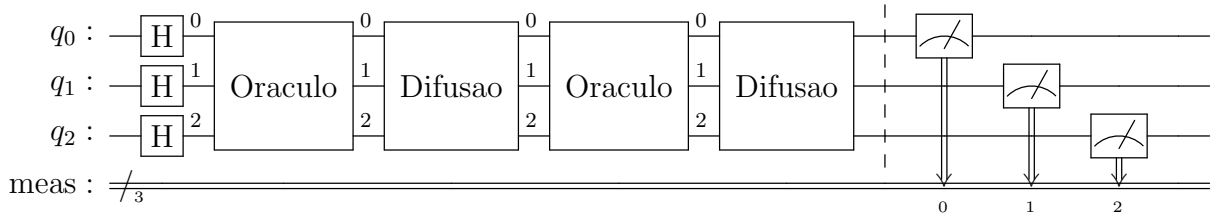


Figura 2. Circuito para o operador de difusão

(3) Implemente e simule o circuito do algoritmo de Grover. Deve aplicar, em primeiro lugar, portas de Hadamard em todos os qubits, seguido de dois ciclos de Grover, como na Figura 3. Cada ciclo de Grover é constituído por uma aplicação do Oráculo, seguido do operador de difusão. Não se esqueça de medir os qubits, com o método `.measure_all()`.

Simule e corra o circuito para 1024 *shots*. Qual é o estado secreto marcado pelo oráculo?



Nota: tendo definido os circuitos das alíneas anteriores, poderá aplicá-los facilmente utilizando, por exemplo, `QuantumCircuit.append(qc_oracle, qubits)`.

(4) Qual é o estado quântico em que o circuito se encontra após a aplicação inicial de portas de Hadamard? Nesse ponto do circuito, qual é a probabilidade de medir o estado secreto?

(5) Para n qubits, o oráculo marca apenas um estado dos $N = 2^n$ estados da base computacional. Para obter o estado marcado com probabilidade acima de 50%, é típico utilizarem-se k aplicações do ciclo de Grover, sendo $k \approx \frac{\pi}{4}\sqrt{N}$. Qual deverá ser o k para um sistema de 3 qubits (arredonde para o inteiro mais próximo)? Qual a relação com o número de ciclos utilizados neste problema?

(6) Num computador clássico, só podemos dar ao oráculo um estado $|a\rangle$ de cada vez. Por sua vez, o oráculo só pode dar uma de duas respostas: "Sim, $|a\rangle$ é o estado secreto" ou "Não, o $|a\rangle$ não é o estado secreto". Na pior das hipóteses, para três bits (como neste problema), quantas perguntas teríamos de fazer até encontrar o estado secreto utilizando um oráculo clássico? E em média?

(7) No geral, a amplitude associada ao estado secreto antes de se aplicarem os ciclos de grover é de $1/\sqrt{N}$, sendo $N = 2^n$ e n o número de qubits. Podemos definir o ângulo θ como $\sin\theta = 1/\sqrt{N}$. Com k aplicações do ciclo de Grover, a probabilidade de medir o estado secreto é $|\sin((2k+1)\theta)|^2$. Mostre que, para $n = 2$ qubits, a probabilidade de medir o estado secreto é de 100% aplicando apenas um ciclo de Grover.