

## **Caderno de Atividades no Qiskit**

Guilherme Penello Temporão

## Atividade 1: Operadores Unitários e a Esfera de Bloch

Nessa atividade, cada aluno (ou dupla de alunos) irá projetar um circuito quântico que transforma um qubit inicial  $|0\rangle$  em um qubit final  $|\mathbf{target}\rangle$ , utilizando no máximo 2 portas lógicas quânticas.

O qubit  $|\mathbf{target}\rangle$  a ser usado é dado pela expressão (a menos de um fator de normalização):

$$|\mathbf{target}\rangle = \frac{2}{3}(N_5 + 1) |0\rangle + \frac{3}{4}(N_6 + 1)e^{i2(N_7+1)\pi/11} |1\rangle$$

onde os números  $N_j$  correspondem ao  $j$ -ésimo dígito da matrícula do aluno (em caso de dupla, do primeiro aluno em ordem alfabética).

1. Calcule o vetor de Bloch associado ao estado  $|\mathbf{target}\rangle$  e utilize o Qiskit para visualizá-lo na Esfera de Bloch. Comente a respeito da localização do estado.
2. Crie um circuito quântico de 2 qubits, inicialmente ignorando o 2o qubit. Na linha do 1o qubit, projete um circuito composto de, no máximo, 2 portas lógicas, que seja capaz de gerar em sua saída o estado  $|\mathbf{target}\rangle$ . Considere que o qubit é inicializado no estado  $|0\rangle$ . Interprete geometricamente a ação das portas lógicas utilizadas.
3. Inicialize o 2o qubit no estado  $|1\rangle$  utilizando uma porta lógica adequada. Em seguida, aplique nesse qubit as mesmas portas lógicas do primeiro qubit e visualize os estados finais de ambos os qubits na Esfera de Bloch. Interprete o resultado obtido.
4. Realize 10.000 medidas (na base computacional) em ambos os qubits e interprete os resultados, comparando-os com o previsto pela teoria.

Lista de portas lógicas permitidas nos circuitos:

- |       |         |
|-------|---------|
| • $X$ | • $R_X$ |
| • $Y$ | • $R_Y$ |
| • $Z$ | • $R_Z$ |

Para maiores informações, consulte a documentação do Qiskit:

[https://qiskit.org/documentation/tutorials/circuits/3\\_summary-of-quantum-operations.html](https://qiskit.org/documentation/tutorials/circuits/3_summary-of-quantum-operations.html)

Os relatórios devem ter no máximo 3 páginas e devem conter o diagrama final do circuito, os resultados das medidas, as figuras das representações dos qubits na Esfera de Bloch, os cálculos utilizados e o código do Qiskit.

### Apêndice: código básico no Qiskit

1. Para visualizar um estado na Esfera de Bloch, primeiramente obtenha o vetor de Bloch associado (de 3 dimensões) e utilize o código:

```
from qiskit.visualization import plot_bloch_vector
%matplotlib inline
bloch_vector = [1,0,0] # substituir pelo vetor correspondente ao Target
plot_bloch_vector(bloch_vector, title="Target")
```

2. Para a criação do circuito no item 2 e visualização do estado na Esfera de Bloch, utilize o backend "statevector\_simulator" como no exemplo abaixo. Nesse exemplo as operações estão sendo realizadas no qubit "0" e, apenas como exemplos, as portas  $Z$  e  $R_X$  estão sendo usadas.

```
import math
from qiskit.tools.visualization import plot_bloch_multivector
circuit = QuantumCircuit(2)
circuit.z(0) # substituir pelo operador unitário adequado
circuit.rx(math.pi/2,0) # idem
simulator = Aer.get_backend('statevector_simulator')
result = execute(circuit, simulator).result()
statevector = result.get_statevector()
plot_bloch_multivector(statevector)
```

(observe que o qubit 1 não é afetado e permanece no estado inicial  $|0\rangle$ )

3. Para realizar as medidas no item 4, utilize o backend "qasm\_simulator" conforme o código abaixo:

```
circuit.measure([0,1], [0,1])
backend = Aer.get_backend('qasm_simulator')
result2 = execute(circuit, backend, shots=10000).result()
counts = result2.get_counts()
from qiskit.tools.visualization import plot_histogram
plot_histogram(counts)
```

4. Para visualização do circuito, use o comando `circuit.draw(output='mpl')`

## Atividade 2: Estados de Bell

Essa é uma atividade voltada para o estudo das propriedades dos Estados de Bell. Cada aluno(a) ou dupla irá realizar medidas em estados de Bell em diferentes bases usando o Qiskit. Nesta atividade específica, utilizaremos os seguintes estados de Bell:

$$\begin{aligned} |\phi^+\rangle &= \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle \\ |\psi^-\rangle &= \frac{1}{\sqrt{2}} |01\rangle - \frac{1}{\sqrt{2}} |10\rangle \end{aligned}$$

Em todas as instâncias dessa atividade, o primeiro qubit (à esquerda) e o segundo qubit (à direita) representam, respectivamente, os qubits "q0" e "q1" do Qiskit.

O qubit  $|0'\rangle$  a ser usado é dado pela expressão (a menos de um fator de normalização):

$$|0'\rangle = (N_7 + 1) |0\rangle + (N_6 + 1) e^{i2(N_5+1)\pi/11} |1\rangle$$

onde os números  $N_j$  correspondem ao  $j$ -ésimo dígito da matrícula do aluno (em caso de dupla, do primeiro aluno em ordem alfabética). O qubit  $|1'\rangle$  é o estado ortogonal a  $|0'\rangle$ .

### Parte 1: Medidas em bases arbitrárias

- 1.1 Projete um circuito quântico capaz de medir um qubit na base  $\{|0'\rangle, |1'\rangle\}$ . Use as operações unitárias que desejar dentro da lista de portas quânticas permitidas (ver próxima página).
- 1.2 Realize um número grande de medidas dos qubits  $|0\rangle$  e  $|1\rangle$  nessa base e verifique se os resultados estão de acordo com o esperado.

### Parte 2: Estudo dos Estados de Bell

- 2.1 Crie um circuito quântico de 2 qubits e 2 bits clássicos. Utilize as portas quânticas necessárias para se obter o estado de Bell  $|\phi^+\rangle$ .
- 2.2 Faça um número grande de medidas nesse estado (i) na base computacional e (ii) na base dada por  $\{|0'\rangle, |1'\rangle\}$ . O que você observa? Os resultados obtidos estão de acordo com o esperado?
- 2.3 Crie um novo circuito quântico de 2 qubits e 2 bits clássicos. Dessa vez, utilize as portas quânticas necessárias para se obter o estado de Bell  $|\psi^-\rangle$ .
- 2.4 Repita o item **2.2** para esse novo estado.

2.5 Agora realize uma nova medida em  $|\psi\rangle$  da seguinte forma: o qubit "q0" deve ser medido na base computacional, enquanto o qubit "q1" deve ser medido na base  $\{|0'\rangle, |1'\rangle\}$ . O que você observa nos resultados das medidas? Compare com os valores esperados pela teoria.

Lista de portas lógicas permitidas nos circuitos:

- |       |         |              |
|-------|---------|--------------|
| • $X$ | • $R_X$ | • $H$        |
| • $Y$ | • $R_Y$ | • $T$        |
| • $Z$ | • $R_Z$ | • $Cx(CNOT)$ |

Para maiores informações, consulte a documentação do Qiskit:

[https://qiskit.org/documentation/tutorials/circuits/3\\_summary\\_of\\_quantum\\_operations.html](https://qiskit.org/documentation/tutorials/circuits/3_summary_of_quantum_operations.html)

Os relatórios devem ter no máximo 4 páginas e devem conter o diagrama final do circuito, os resultados das medidas, os cálculos utilizados e o código do Qiskit.

### Atividade 3: Teletransporte Quântico

Nessa atividade vocês implementarão o protocolo "Quantum Teleportation" descrito originalmente por C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres e W. Wootters (1993).

Considerem o cenário tradicional onde Alice e Bob compartilham, inicialmente, um estado de Bell  $|\Phi^+\rangle$ ; posteriormente, Alice deseja "teleportar" um qubit qualquer (desconhecido)  $|\phi_A\rangle$  para Bob. Esse qubit é dado pela expressão (a menos de um fator de normalização):

$$|\phi_A\rangle = (N_5 + 1) |0\rangle + (N_6 + 1)e^{i2(N_7+1)\pi/11} |1\rangle$$

onde os números  $N_j$  correspondem ao  $j$ -ésimo dígito da matrícula do aluno (em caso de dupla, do primeiro aluno em ordem alfabética).

#### Parte 1: Protocolo incompleto - comunicação mais rápida que a luz?

- 1.1 Crie um circuito quântico com 3 qubits no Qiskit, no qual  $q_0$  corresponde ao qubit de Alice a ser teleportado e os qubits  $q_1$  e  $q_2$  correspondem ao par emaranhado compartilhado por Alice e Bob, respectivamente. Prepare  $q_0$  no estado  $|\phi_A\rangle$  e os qubits  $q_1$  e  $q_2$  no estado de Bell  $|\Phi^+\rangle$ .
- 1.2 Realize uma medida de Bell nos qubits  $q_0$  e  $q_1$  um número suficientemente grande de vezes e obtenha a *matriz de densidade* do qubit  $q_2$ .
- 1.3 O que você pode concluir a respeito da informação que Bob possui a respeito de  $|\phi_A\rangle$  após a realização da Medida de Bell? Você acredita ser possível se comunicar de forma mais rápida que a luz usando esse protocolo?

#### Parte 2: Protocolo completo - implementando as operações unitárias e comunicação clássica

- 2.1 Complete o circuito anterior com as operações unitárias necessárias para implementar o protocolo original de Teletransporte Quântico.
- 2.2 Mostre que o estado final obtido por Bob corresponde a  $|\phi_A\rangle$ .
- 2.3 Esse resultado de alguma forma viola o Teorema da Não-Clonagem? Justifique.

Lista de portas lógicas permitidas nos circuitos:

- $X$
- $Y$
- $Z$
- $R_X$
- $R_Y$
- $R_Z$
- $H$
- $Cz$
- $Cx(CNOT)$

Para maiores informações, consulte a documentação do Qiskit:

[https://qiskit.org/documentation/tutorials/circuits/3-summary\\_of\\_quantum\\_operations.html](https://qiskit.org/documentation/tutorials/circuits/3-summary_of_quantum_operations.html)

Os relatórios devem ter no máximo 4 páginas e devem conter o diagrama final do circuito, os resultados das medidas, os cálculos utilizados e o código do Qiskit.

### Atividade 4: Criptografia Quântica

Nessa atividade vocês irão simular parcialmente um sistema de criptografia quântica utilizando o protocolo BB84, assim como o tipo mais simples de ataque que pode ser realizado contra um desses sistemas: o ataque "Intercept-Resend".

Nesse protocolo, Alice deseja estabelecer uma chave secreta com Bob, e para isso ela envia qubits pertencentes ao conjunto  $\{|0\rangle, |+\rangle, |1\rangle, |-\rangle\}$ . Bob, por sua vez, decide se vai realizar uma medida na base "computacional" ( $\{|0\rangle, |1\rangle\}$ ) ou na base "diagonal" ( $\{|+\rangle, |-\rangle\}$ ). Em seguida, Alice e Bob realizam uma conciliação de bases, fazem uma estimativa da taxa de erro e procedem para a etapa seguinte, de Amplificação de Privacidade.

#### Parte 1: Protocolo ideal

- 1.1 (Alice) Crie um circuito quântico de dois qubits ( $q_0$  e  $q_1$ ), e por enquanto ignore  $q_1$ . Implemente uma operação unitária  $U_A$  que seja capaz de receber como entrada dois bits clássicos. Para cada combinação possível desses 2 bits, um dos estados  $\{|0\rangle, |+\rangle, |1\rangle, |-\rangle\}$  deve ser obtido após aplicação de  $U_A$  em  $q_0$ .
- 1.2 (Bob) crie uma operação unitária  $U_B$  que receba como parâmetro um bit clássico e realize uma medida em  $q_0$ . Dependendo do bit recebido, a medida deve corresponder a uma medida projetiva na base computacional ou na base diagonal.
- 1.3 (Conciliação de bases) Implemente um algoritmo (clássico) de conciliação de bases, de modo que após a aplicação do algoritmo Alice e Bob permanecem com bits relacionados a escolhas da mesma base.
- 1.4 (Verificação da taxa de erro) Implemente um novo algoritmo que sacrifica 10% dos bits de Alice e Bob e compara seus valores, de modo a estimar a taxa de erro.
- 1.5 (Primeira rodada do protocolo BB84) Rode o protocolo para  $N = 10000$  qubits enviados por Alice, onde as escolhas de bits (tanto por Alice quanto por Bob) são aleatórias. Qual a taxa de erro encontrada no final?

#### Parte 2: Ataque Intercept-Resend

- 2.1 (Eva) Implemente agora a ação da espiã, Eva, no protocolo acima. Para cada qubit enviado por Alice, Eva deve "interceptar" o qubit e proceder exatamente como Bob; em seguida ela deve reenviar o resultado de sua medida projetiva para Bob. Utilize agora o qubit  $q_1$  para representar o qubit reenviado por Eva a Bob, e modifique o circuito anterior de modo que agora Bob mede  $q_1$  ao invés de  $q_0$ .
- 2.2 (Segunda rodada do protocolo BB84) Rode o protocolo para  $N = 10000$  qubits enviados por Alice. Qual a nova taxa de erro encontrada no final?.



- 2.3 (Taxa de erro máxima) Eva sabe que o protocolo é interrompido se a taxa de erro ultrapassar o limite de, digamos, 10%. Qual a maior fração de qubits de Alice que ela deve interceptar de modo a sempre manter a taxa de erro abaixo do limite? E qual a fração dos bits da chave compartilhada que Eva conhece? Simule esse caso.
- 2.4 (Amplificação de Privacidade) Efetue uma etapa de um algoritmo de Amplificação de Privacidade que realiza uma operação soma módulo 2 (XOR) entre cada 2 bits consecutivos da chave compartilhada. Qual a nova fração dos bits da chave compartilhada que Eva conhece? Com base nesse resultado, comente sobre a etapa de Amplificação de Privacidade e sua importância para o protocolo BB84.

Lista de portas lógicas permitidas nos circuitos: nessa atividade não há restrição de portas no circuito, desde que todas sejam portas de apenas 1 qubit.

Para maiores informações, consulte a documentação do Qiskit:

[https://qiskit.org/documentation/tutorials/circuits/3\\_summary\\_of\\_quantum\\_operations.html](https://qiskit.org/documentation/tutorials/circuits/3_summary_of_quantum_operations.html)

Os relatórios devem ter no máximo 4 páginas e devem conter o diagrama final do circuito, os resultados das medidas, os cálculos utilizados e o código do Qiskit.

### Atividade 5: Desigualdade de Bell

Nessa atividade vocês irão violar a Desigualdade de Bell-CHSH, demonstrando que a Mecânica Quântica é incompatível com o modelo de Realismo Local sugerido por Einstein, Podolsky e Rosen.

Considerem o cenário onde pares de qubits são gerados e enviados a Alice e Bob, que recebem um qubit de cada par. Suponha que Alice pode realizar duas medidas em seu qubit, que vamos representar pelos observáveis  $A_1$  e  $A_2$ . Os resultados das medidas (respectivamente  $a_1$  e  $a_2$ ) podem assumir os valores  $+1$  ou  $-1$ . Analogamente, Bob também pode realizar medidas em seu qubit, representadas pelos observáveis  $B_1$  e  $B_2$ , cujos resultados  $b_1$  e  $b_2$  também assumem os valores  $+1$  ou  $-1$ .

Considere agora a quantidade  $S = \langle A_1 B_1 \rangle + \langle A_2 B_1 \rangle + \langle A_2 B_2 \rangle - \langle A_1 B_2 \rangle$ , onde a notação  $\langle O \rangle$  representa o valor médio do operador  $O$ . A Desigualdade de Bell-CHSH afirma que, partindo de um modelo de Realismo Local, obtemos:

$$|S| \leq 2$$

No entanto, se Alice e Bob compartilham um estado de Bell  $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$  ("singlete") e os observáveis  $\{A_1, A_2, B_1, B_2\}$  são definidos pelas seguintes combinações dos operadores de Pauli  $X$  e  $Z$ :

$$\begin{aligned} A_1 &= Z \\ A_2 &= X \\ B_1 &= \frac{1}{\sqrt{2}}(-Z - X) \\ B_2 &= \frac{1}{\sqrt{2}}(Z - X) \end{aligned}$$

Então  $S = 2\sqrt{2}$ , uma clara violação da Desigualdade de Bell-CHSH.

#### Parte 1: Preparação dos Circuitos Quânticos

- 1.1 Crie um circuito quântico de dois qubits ( $q_0$  e  $q_1$ ) que seja capaz de gerar o estado de Bell  $|\psi^-\rangle$ . Esse circuito servirá de base para construção dos 4 circuitos quânticos que serão utilizados em seguida.
- 1.2 Calcule os operadores unitários necessários para se realizar as medidas  $\{A_1, A_2, B_1, B_2\}$ .
- 1.3 Para cada combinação de observáveis  $(A_i, B_j)$  ( $i, j = 1, 2$ ), crie um circuito quântico que realize uma medida projetiva no qubit  $q_0$  segundo o observável  $A_i$  e uma medida projetiva no qubit  $q_1$  segundo o observável  $B_j$ , utilizando os unitários calculados no item anterior.

## Parte 2: Medindo o parâmetro $S$

- 2.1 Utilizando o **qasm\_simulator**, realize 10000 medidas em cada circuito. Para cada resultado obtido, obtenha o valor médio  $\langle A_i B_j \rangle$ . (Dica: observe que o Qiskit trata os resultados das medidas como "0" e "1", enquanto os observáveis definidos acima possuem resultados possíveis +1 e -1; não esqueça de levar isso em consideração)
- 2.2 Calcule o valor de  $S$  e verifique que ele é próximo do valor teórico  $S = 2\sqrt{2}$ .

## Parte 3: Estados Separáveis

Considere agora que a espiã, Eva, tomou conta da fonte de estados emaranhados e passa a enviar estados separáveis para Alice e Bob. Ou seja, Eva envia os estados  $|01\rangle$  e  $|10\rangle$  aleatoriamente, com probabilidades iguais (50%).

- 3.1 Modifique os circuitos quânticos do item 1 de modo a refletir essa estratégia.
- 3.2 Realize um número suficientemente grande de medidas e calcule o novo valor de  $S$ . O que você observa?

Lista de portas lógicas permitidas nos circuitos: nessa atividade não há restrição de portas no circuito.

Para maiores informações, consulte a documentação do Qiskit:

[https://qiskit.org/documentation/tutorials/circuits/3\\_summary\\_of\\_quantum\\_operations.html](https://qiskit.org/documentation/tutorials/circuits/3_summary_of_quantum_operations.html)

Os relatórios devem ter no máximo 4 páginas e devem conter o diagrama final do circuito, os resultados das medidas, os cálculos utilizados e o código do Qiskit.

## Atividade 6: Algoritmo de Deutsch-Josza

Nessa atividade vocês irão primeiramente implementar o algoritmo de Deutsch, que é capaz de, com apenas uma consulta a um oráculo que implementa uma função  $f : \{0, 1\} \rightarrow \{0, 1\}$ , determinar se ela é *constante* ou *balanceada*. Em seguida, vocês implementarão uma generalização para uma função que tem como entrada sequências de  $n$  bits - o chamado Algoritmo de Deutsch-Josza.

### Parte 1: Algoritmo de Deutsch

- 1.1 Determine o circuito quântico do oráculo  $U_f$  correspondente a cada uma das 4 funções  $f$  possíveis.
- 1.2 Simule no Qiskit um circuito quântico que implemente o Algoritmo de Deutsch para cada uma das funções acima.

### Parte 2: Algoritmo de Deutsch-Josza

- 2.1 Crie circuitos quânticos para dois oráculos à sua escolha: um correspondente a uma função constante e outro correspondente a uma função balanceada, onde as funções têm como entrada sequências de 6 bits, isto é,  $f : \{0, 1\}^6 \rightarrow \{0, 1\}$ .
- 2.2 Simule no Qiskit um circuito quântico que implemente o Algoritmo de Deutsch-Josza para cada uma das funções acima.

Lista de portas lógicas permitidas nos circuitos: nessa atividade não há restrição de portas no circuito.

Para maiores informações, consulte a documentação do Qiskit:

[https://qiskit.org/documentation/tutorials/circuits/3\\_summary\\_of\\_quantum\\_operations.html](https://qiskit.org/documentation/tutorials/circuits/3_summary_of_quantum_operations.html)

Os relatórios devem ter no máximo 4 páginas e devem conter o diagrama final do circuito, os resultados das medidas, os cálculos utilizados e o código do Qiskit.