Uma breve apresentação dos fundamentos de computação quântica

Guilherme R. Ribeiro

1 de julho de 2018

Resumo

Neste trabalho será feita uma breve explicação sobre conceitos básicos de computação quântica, seguida de dois exemplos: o interferômetro simples e o controlado de Mach-Zehnder. Ainda, apresentam-se gráficos obtidos com o uso do *Quantum Information Science Kit* para simulação dos circuitos quânticos, e seus formatos no *Composer*, ambos da IBM. Os códigos usados nestas simulações estão disponíveis no *GitHub*.

1 Introdução

Uma das maiores revoluções tecnológicas da humanidade definitivamente foi o surgimento do computador, que com o passar dos anos tornou-se cada vez mais avançado e permitiu a solução de problemas que a princípio nunca poderião ser resolvidos: exemplos incluem equações diferenciais sem solução analítica, e simulações de macromoléculas.

Entretanto, diferentemente do que se imaginava há algum tempo atrás, não é possível resolver toda sorte de problemas com o uso de um computador, por mais potente que seja. Isso ocorre pois há um limite para o quão rápidas estas máquinas podem ser, que além de proporcional ao número de bits que possuem, é limitado pelos computadores serem capazes apenas de estar em um único estado de cada vez. O exemplo clássico para mostrar o quão grande essa limitação é é a busca pelos fatores primos de um número: pelo Teorema Fundamental da Aritmética, todo número pode ser escrito como um produto entre números primos, ou seja, $15 = 3 \cdot 5$, $30 = 5 \cdot 3 \cdot 2$, etc. O método usual para se calcular esses fatores é por, colocando grosseiramente, "tentiva e erro": o computador testa várias combinações de fatores uma por uma até obter a resposta correta. Conforme o número aumenta, a quantidade de combinações a serem testadas também cresce rapidamente, tal que o processo torna-se cada vez mais demorado até mesmo para os computadores mais refinados atualmente.

Caso fosse possível o computador avaliar várias combinações de uma só vez, ou seja, estar em mais de um estado simultaneamente, seria possível encontrar os fatores muito mais rapidamente. Esse é o caso para os computadores quânticos, que recentemente estão ganhando cada vez mais interesse devido a serem capazes de resolver problemas que um computador clássico possui dificuldade em resolver. No restante desse trabalho, primeiramente se dará uma breve explicação sobre conceitos fundamentais de computação quântica, como o *qubit*; em seguida, se apresentarão algumas portas quânticas (equivalentes quânticos às portas lógicas clássicas); e por fim, dois circuitos quânticos a fim de mostrar aplicações.

Ainda, se mostrarão alguns gráficos incluindo os resultados dos testes realizados. Eles foram obtidos usando programas em Python junto da biblioteca *QISKit* (*Quantum Information Science Kit*) desenvolvida pela IBM. Os programas usados possuem código aberto pela licensa MIT, e estão disponíveis no GitHub na seguinte URL:

`https://github.com/Keyband/dsp003-quantum_interferometers`

2 Conceitos fundamentais para Computação Quântica

Primeiramente, deve-se esclarecer ao leitor que para uma compreensão mais adequada dos conceitos aqui apresentados, é indispensável uma apresentação mais formal e séria à Álgebra Linear, o que não está no escopo deste trabalho. Não obstante, se procurará apresentar as ideias necessárias para o entendimento do texto conforme necessário. Caso se procure uma referência para se estudar Álgebra Linear, recomenda-se [2]e, para uma apresentação mais profunda e detalhada à Computação Quântica, recomenda-se [4].

Prosseguindo, classicamente computadores funcionam a partir de bits: um bit pode estar em um de dois estados, que são 0 e 1. A partir de grupos de bits (*e.g.* bytes, megabytes, gigabytes), toda a computação é feita.

Um computador quântico funciona de modo análogo, possuindo *qubits* no lugar de bits. A diferença entre os dois tipos de computação vem da diferença entre suas unidades básicas de informação: enquanto o bit está em um de dois estados possíveis, o qubit pode ser configurado de modo a ficar em *mais* de um estado ao mesmo tempo. Isso ocorre pelo fenômeno de superposição de estados, presente na Mecânica Quântica.

Entretanto, este estado de superposição não é permanente, e desaparece assim que se mensura o estado do qubit, dando lugar a um estado de 0 ou 1, assim como o bit.

Considere então um qubit $|\Psi\rangle$. Considerando os estados $|0\rangle$ e $|1\rangle$ como a *base* do sistema, é possível preparar $|\Psi\rangle$ tal que:

$|\Psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$

Enquanto não mensurado, $|\Psi\rangle$ está em ambos os estados simultaneamente. Entretanto, quando mensurado, há probabilidade α^2 de o estado descoberto ser $|0\rangle$, e probabilidade β^2 de se encontrar $|1\rangle$. Note que α e β são números complexos, e $\alpha^2 + \beta^2 = 1$, por se tratarem de probabilidades.

Note também que a *base* escolhida foi $|0\rangle, |1\rangle$, e portanto os resultados da mensuração são $|0\rangle$ e $|1\rangle$: a Mecânica Quântica permite a escolha de uma base para ser feita a mensuração, e a base por sua vez altera os resultados da medida. Chama-se a base $|0\rangle, |1\rangle$ de base computacional, por relembrar os bits clássicos. Uma outra base seria $|+\rangle, |-\rangle$, que corresponde *à base computacional no eixo X da esfera de Bloch.*

Para se compreender o que isso quer dizer, deve-se saber que na Mecânica Quântica um estado, como por exemplo o qubit $|\Psi\rangle$, é um vetor, e a base são vetores com os quais pode-se escrever qualquer outro vetor, ou colocando mais rigorosamente, todos os outros vetores podem ser escritos como combinação linear dos vetores da base. A escolha da base não é única, e dependendo da base escolhida, os resultados da mensuração serão diferentes (como mencionado).

Ainda, se lembre que os coeficientes dos vetores da base, i.e. α e β, são complexos, o que dificulta a visualização de um estado do qubit dados os vetores da base. Entretanto, ainda é possível se visualizar o estado de um qubit com o uso da Esfera de Bloch: ela é uma esfera de raio unitário, e cada ponto em sua superfície representa um estado possível. Além de permitir uma maneira de se visualizar o estado de um qubit, o uso dessa ferramenta também auxilia na compreensão das operações possíveis de serem feitas em um qubit, que aparecem na forma de *quantum gates*, ou portas quânticas, análogas às portas lógicas clássicas.

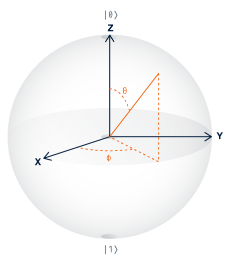


Figura 1: Esfera de Bloch. Imagem retirada de [3].

Por exemplo, a base computacional são os seguintes vetores orientados ao longo do eixo Z da Esfera de Bloch:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Enquanto que os vetores $|+\rangle$ e $|-\rangle$ possuem o mesmo formato, mas ao longo do eixo X da Esfera de Bloch. É possível escrever $|0\rangle, |1\rangle$ em termos de $|+\rangle, |-\rangle$, como se verá em breve.

3 O *Quantum Composer*

Para se programar um computador quântico, existem duas maneiras atualmente: pode-se usar o QISKit, que permite a criação de algoritmos via programação, ou pode-se usar um *Composer* (compositor), que permite a criação de algoritmos com o auxílio de uma interface gráfica. Ambos são capazes de levar aos mesmos resultados, mas o Composer permite ser mais fácil de visualizar as operações sendo realizadas, enquanto o QISKit torna mais fácil realizar vários testes em sequência, como será o caso nos exemplos apresentados. Guias para o composer estão disponíveis em [6] e [3], e para o QISKit existe sua documentação[5].

4 *Quantum gates*

Enquanto que classicamente existem portas lógicas para realizar operações entre bits, como as portas NOT, OR, XOR, AND, NAND, etc, quanticamente existem portas quânticas, ou *quantum gates*: na Mecânica Quântica, estas portas são operadores que atuam nos qubits, alterando seu estado. Por não mudarem seu módulo, são ditos operadores unitários, e para entender como funcionam convém levar em conta a mudança do estado do qubit com o uso da Esfera de Bloch. Abaixo serão apresentados alguns *quantum gates* de maior importância, junto de suas formas matriciais.

4.1 *X gate*

A porta quântica mais simples é a X ou *bit-flip*, que é uma rotação de π ao redor do eixo X: portanto, é equivalente à porta lógica clássica NOT, pois faz $X \cdot |0\rangle = |1\rangle$ e $X \cdot |1\rangle = |0\rangle$. Sua forma matricial é:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Existem ainda os gates menos usados Y e Z, que equivalem a rotações de π ao redor dos eixos Y e Z respectivamente.

4.2 *Hadamard Gate*

Uma das mais importantes portas quânticas é a *Hadamard*, que equivale a uma rotação de π ao redor do eixo $X+Z$, e que portanto faz $Z \rightarrow X$ e $X \rightarrow Z$:

$$H = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Sua importância vem do fato de poder ser usada para criar estados de superposição, uma vez que ao atuar na base computacional, que é ao longo do eixo Z da esfera de Bloch, leva a uma outra base, ao longo do eixo X e formada por $|+\rangle, |-\rangle$:

$$H \cdot |0\rangle = |+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

$$H \cdot |1\rangle = |-\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

4.3 *Phase shift gates* R_ϕ

Esta porta não altera as probabilidades de se mensurar um estado ou outro quando usada sozinha, meramente adicionando um termo de fase a $|1\rangle$ enquanto mantém $|0\rangle$ inalterado:

$$R_\phi = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

Note entretanto que a fase aplicada não é ϕ, mas sim $\frac{\phi}{2}$; isso ficará mais claro no primeiro exemplo a ser estudado, o do interferômetro simples.

Perceba que no composer do IBM Q Experience, este gate é chamado de *U1* e está disponível marcando a opção para portas avançadas de dentro do compositor.

4.4 *C(X) gate*

Além das portas que atuam somente em 1 qubit, existem *Multi-Qubit Gates*, que atuam em mais de um qubit simultaneamente. Possivelmente o mais simples e importante desse tipo de gate é o *C(X)*, também chamado de *CNOT* ou *Controlled NOT*: de acordo com o estado de um qubit (chamado de controle), aplica-se ou não um X gate em um outro qubit (chamado de alvo). Sua forma matricial é:

$$C(X) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Tal que:

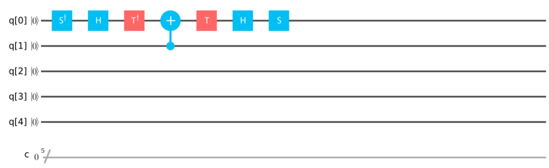
$$\begin{aligned} C(X)|00\rangle &= |00\rangle \\ C(X)|01\rangle &= |00\rangle \\ C(X)|10\rangle &= |11\rangle \\ C(X)|11\rangle &= |10\rangle \end{aligned} \tag{1}$$

4.5 *C(H) gate*

Um outro tipo de Multi-Qubit Gate é o *C(H)*, ou *Controlled Hadamard*. De acordo com o qubit de controle, aplica-se ou não a operação de Hadamard no qubit alvo:

$$C(H) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Convém se observar que usualmente não se fornece a operação de $C(H)$ para o usuário, como ocorre no composer do *IBM Q Experience*. Entretanto, ainda é possível obter o mesmo efeito observando-se que é possível aplicar variadas portas quânticas em sequência. Em particular, o circuito quântico abaixo possui o mesmo efeito de $C(H)$:



5 Interferômetro simples

Com o uso de um computador quântico é possível reproduzir um interferômetro de Mach–Zehnder. Nele, o fóton passa por um divisor de feixe, onde para um dos caminhos ganha uma fase adicional em relação ao outro: dessa forma, há uma superposição entre em fase e defasado. Passando o fóton novamente por um divisor de feixe e ao se mensurar o estado do fóton, as probabilidades de se encontrar um comportamento de partícula ou onda serão dadas por $cos^2(\alpha)$ e $sin^2(\alpha)$, onde α é a fase adicionada.

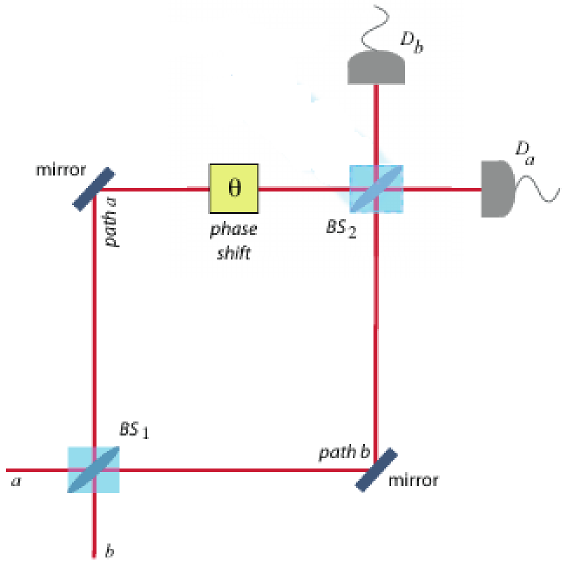
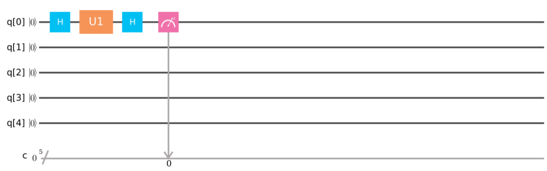


Figura 2: Interferômetro de Mach-Zehnder. Imagem retirada e editada de [1]

.

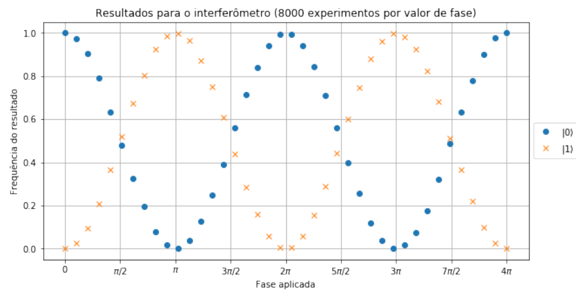
Para se reproduzir este experimento com o uso de um computador quântico, o seguinte procedimento é feito:

- Primeiramente deve-se preparar um qubit no estado de superposição, i.e. $\frac{1}{\sqrt{2}} \cdot (|0\rangle + |1\rangle)$, usando-se de um *Hadamard gate* aplicado no qubit default $|0\rangle$;
- Em seguida, uma fase $\frac{\alpha}{2}$ pode ser aplicada usando-se do gate R_α, tal que o estado do qubit será $\frac{1}{\sqrt{2}} \cdot \left(|0\rangle + e^{\frac{-i\alpha}{2}}|1\rangle\right)$, ou equivalentemente, $\frac{e^{\frac{i\phi}{2}}}{\sqrt{2}} \cdot \left(e^{-\frac{i\phi}{2}}|0\rangle + e^{\frac{i\phi}{2}}|1\rangle\right)$, uma vez que a fase global do qubit não altera as probabilidades do resultado da mensuração;
- E por fim aplica-se novamente o *Hadamard gate* para se obter o estado $\frac{e^{\frac{i\phi}{2}}}{2} \cdot \left(\left(e^{\frac{i\phi}{2}} + e^{-\frac{i\phi}{2}}\right)|0\rangle + \left(e^{\frac{i\phi}{2}} - e^{-\frac{i\phi}{2}}\right)|1\rangle\right)$, ou reescrevendo, $cos(\frac{\alpha}{2}) \cdot |0\rangle + sin(\frac{\alpha}{2}) \cdot |1\rangle$. Perceba que é por causa disso que a fase efetiva é metade da fase aplicada, como mencionado anteriormente na explicação do gate R_ϕ.



Feitas estas operações aplica-se uma porta de mensuração, onde os dois resultados possíveis ($|0\rangle$ e $|1\rangle$) possuem probabilidades $cos^2(\frac{\alpha}{2})$ e $sin^2(\frac{\alpha}{2})$ respectivamente.

Usando do *Quantum Information Science Kit* (ou *QISKit*)é possível fazer experimentos sucessivamente para diferentes valores de α rapidamente: note que se preferiu realizar simulações no lugar de usar um dos chips reais, por estes últimos serem de uso limitado para usuários do IBM Quantum Experience.



6 Interferômetro controlado

Uma outra versão do interferômetro mencionado anteriormente é o *Interferômetro controlado*, para o qual há um segundo separador de feixes que pode estar em uma superposição de aberto ou fechado. Como explorado em alguns artigos, caso o interferômetro esteja aberto o fóton é percebido como partícula, enquanto que caso fechado é percebido como onda e pode-se analisar seu padrão de interferência. Caso o interferômetro esteja em uma superposição entre aberto e fechado, é possível observar ambos os aspectos do sistema com o mesmo interferômetro (entretanto, os comportamentos de onda e partícula não podem ser percebidos simultaneamente pelo Princípio da Complementaridade de Bohr). Uma analise mais completa deste experimento está presente em [1].

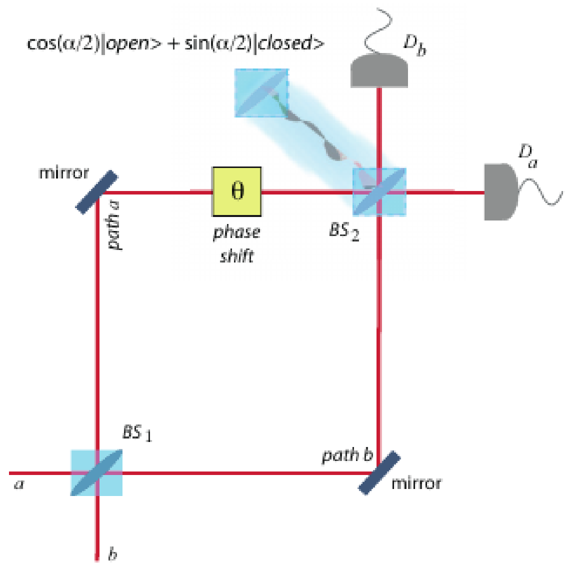
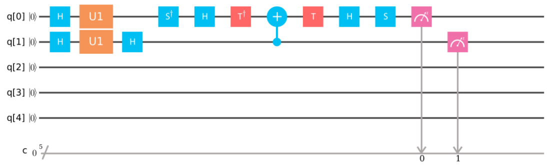


Figura 3: Interferômetro de Mach-Zehnder em um estado de superposição entre aberto e fechado. Imagem retirada de [1]

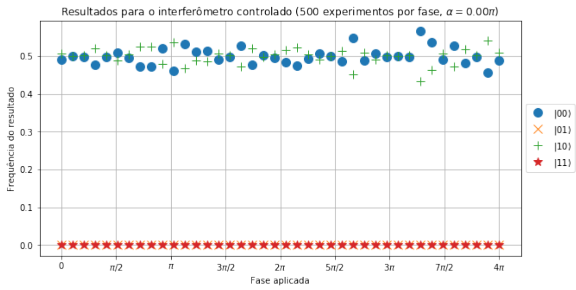
.

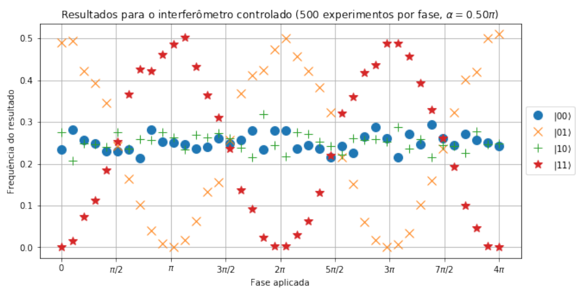
O circuito quântico para o interferômetro controlado está ilustrado abaixo. Perceba que o qubit $q[1]$ é preparado em um estado de superposição $|\Psi\rangle = cos(\frac{\alpha}{2}) \cdot |0\rangle + sin(\frac{\alpha}{2}) \cdot |1\rangle$, da mesma maneira que a mostrada no interferômetro simples. Ainda, servindo como qubit de controle para C(H), tem o papel de dar ao interferômetro a possibilidade de estar em superposição de aberto e fechado. O qubit $q[0]$ equivale portanto ao fóton do interferômetro.

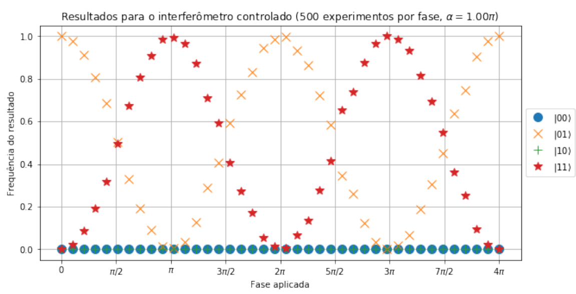


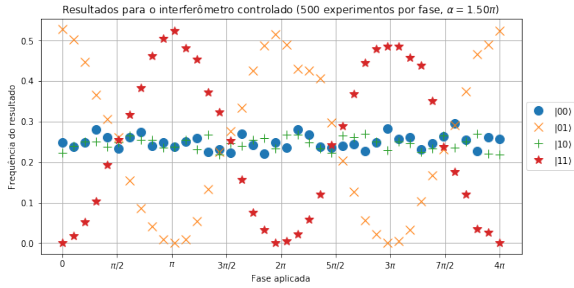
Dessa forma, para o caso de $\alpha = 0$ por exemplo, a porta $C(H)$ não aplica o gate Hadamard e portanto há igual probabilidade de se obter os estados $|0\rangle$ e $|1\rangle$ na mensuração; por outro lado, caso $\alpha = \pi$ (e portanto a fase efetiva aplicada seja de $\frac{\pi}{2}$) isso quer dizer que o gate Hadamard será aplicado, e portanto obtêm-se o Interferômetro simples novamente.

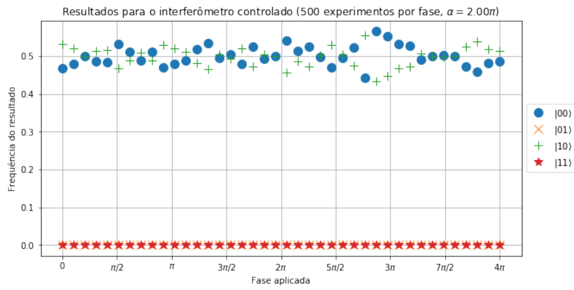
Usando novamente o QISKit, os seguintes resultados foram encontrados para valores variados de α.











7 Conclusões

Ainda que outras aplicações da Computação Quântica possam ser de maior interesse comercial, como o Algoritmo de Shor para obtenção dos fatores primos de um número (problema mencionado na introdução deste trabalho), o exemplo do interferômetro possivelmente é o que deixa mais claro o fenômeno da superposição. Ao final do primeiro exempçlo explorado, o do interferômetro simples, o estado do qubit era de $cos(\frac{\alpha}{2}) \cdot |0\rangle + sin(\frac{\alpha}{2}) \cdot |1\rangle$, o que nos dá as probabilidades de $cos^2(\frac{\alpha}{2})$ e $sin^2(\frac{\alpha}{2})$ de se encontrar respectivamente $|0\rangle$ e $|1\rangle$ em uma mensuração, e como esperado, ao serem realizadas várias medidas para diferentes valores de α os resultados obtidos corresponderam ao esperado.

No caso do Interferômetro Controlado, os resultados podem ser mais difíceis de interpretar pela presença de um outro qubit: ainda assim, cada caso corresponde ao esperado. Por exemplo, para $\alpha = 0$, a porta Hadamard não será aplicada no qubit alvo, e dessa maneira ele permanecerá orientado no plano XY, e ao se mensurar seu estado na base computacional, há 50% de chance de se obter $|0\rangle$ e 50% de chance de se obter $|1\rangle$.

Para $\alpha = \pi$, o qubit de controle possuirá probabilidade 1 de estar no estado $|1\rangle$ e portanto a porta Hadamard será aplicada sempre no qubit alvo, e assim se recupera o resultado do primeiro exemplo.

Esses dois casos, $\alpha = 0$ e $\alpha = \pi$, correspondem aos casos de o interferômetro estar aberto e fechado, tal que valores de α entre os dois correspondem à uma superposição. Isso é percebível para $\alpha = \frac{\pi}{2}$, em que o resultado encontrado é semelhante aos resultados obtidos separadamente para $\alpha = 0$ e $\alpha = \frac{\pi}{2}$. Note que a soma entre as frequências de $|00\rangle$ e $|01\rangle$ é igual à soma das frequências de $|01\rangle$ e $|11\rangle$, i.e. 0.5, pois a fase efetiva no qubit de controle, $\frac{\pi}{4}$, faz com que metade das vezes o interferômetro esteja fechado, e na outra metade, esteja aberto.

Por fim, perceba que o menor número de repetições do experimento levou a pontos ligeramente mais distantes do esperado em comparação com o Interferômetro simples, para o qual os testes foram repetidos 8000 vezes (esse número foi escolhido pois o Composer permite um máximo de aproximadamente 8000 testes, e preferiu-se tornar os resultados comparáveis com o que pode ser obtido usando-se dessa ferramenta).

Referências

[1] R. Auccaise et al. "Experimental analysis of the quantum complementarity principle". Em: 85.3, 032121 (mar. de 2012), p. 032121. DOI: 10.1103/PhysRevA.85.032121. arXiv: 1201.5951 [quant-ph].

[2] S. Axler. *Linear Algebra Done Right*. 2nd edition.

[3] *IBM Q Experience User Guide*. https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=full-user-guide&page=introduction. Acessado: 12/07/2018.

[4] Isaac L. Chuang Michael A. Nielsen. *Quantum Computation and Quantum Information: 10th Anniversary Edition*.

[5] *QISKit Documentation*. https://qiskit.org/documentation/. Acessado: 13/07/2018.

[6] A. Ramanan. *IBM Q Experience User Guide*. https://blogs.msdn.microsoft.com/uk_faculty_connection/2018/02/26/quantum-gates-and-circuits-the-crash-course/. Acessado: 13/07/2018.