Computação Quântica para Cientistas da Computação

Ana Silva, Breno Pimenta, Caio Caldeira, Gean dos Santos e Roberto Rosmaninho

1. Introdução

Analogamente a um computador clássico, que funciona a partir de circuitos elétricos e portas lógicas manipulando bits, o computador quântico opera a partir de circuitos quânticos baseados em portas lógicas quânticas, manipulando sua unidade fundamental, o qbit. A principal diferença entre bit e o qbit reside no fato de que o bits assumem ou o valor 0 ou o valor 1, enquanto o qbit está numa sobreposição de zeros e uns até ser medido e colapsar para um desses valores.

Neste trabalho apresentaremos os fundamentos da computação quântica sob a ótica da computação, explicando as representações e operações de álgebra linear que permitem que um computador quântico funcione.

2. *Cbits*

Iniciaremos nossa explicação por meio dos *cbits*, que nada mais são que um caso especial de *qbits*. Na computação quântica, os bits são representados como vetores:

- Bit 0, representação vetorial: $\begin{pmatrix}1\\0\end{pmatrix}$, notação de Dirac: $\mid 0\rangle$
- Bit 1, representação: $\begin{pmatrix}0\\1\end{pmatrix}$, notação de Dirac: $\mid 1\rangle$

Na computação clássica temos 4 operações unárias sobre bits: identidade, negação, *reset* e *set*. De forma análoga, conseguimos reproduzir essas 4 operações sobre *cbits* utilizando produto de matrizes. Dentre estas operações, identidade e negação são reversíveis, isto é, conhecendo-se a operação e sua saída, é possível inferir qual entrada foi fornecida à operação. Computadores quânticos utilizam somente operações reversíveis, mais especificamente, eles utilizam somente operadores que são o seu próprio reverso: se aplicarmos o operador duas vezes sobre uma dada entrada, a saída será igual à entrada.

$$\text{Identidade} \quad f(x) = x \quad \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}, \quad \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}$$

$$\text{Negação} \quad f(x) = \neg x \quad \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}, \quad \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}$$

Para representarmos *cbits múltiplos* utilizamos produto tensorial de vetores.

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_0 & \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \\ x_1 & \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} x_0 y_0 \\ x_0 y_1 \\ x_1 y_0 \\ x_1 y_1 \end{pmatrix}$$

$$| 00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad | 01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$| 10\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad | 11\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

A operação *Conditional Not (CNOT)* opera sobre sobre pares de bits. O bit mais significativo é chamado de "controle" enquanto o menos significativo é o "target". Se o bit "controle" for igual a 1, o bit "target" é negado, isto é, seu valor é invertido, caso o bit "controle" seja 0, o bit "target" não é alterado. O bit "controle" nunca é alterado.

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

$$C \mid 10\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \mid 11\rangle \quad C \mid 11\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \mid 10\rangle$$

3. Qbits e Interpolation

Os qbits são na verdade um caso geral dos cbits, ou seja, todas as propriedades e operações apresentadas acima também se aplicam aos qbits.

Uma diferença importante entre os cbits e os qbits são os valores que compõe os vetores. Qbits são representados por um $\begin{pmatrix} a \\ b \end{pmatrix}$ onde a e b são números complexos e $||a||^2 + ||b||^2 = 1$. Observe que os cbits $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ e $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ estão dentro dessa definição, bem como os exemplos abaixo:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} \begin{pmatrix} -1 \\ 0 \end{pmatrix}$$

Os qbits, diferentemente dos bits, podem representar mais que um estado. Na verdade, eles podem representar a combinação linear de 2 estados, esse fenômeno é chamado

de superposição. Um exemplo de superposição seria a representação de 2 bits pelo produto de tensores: $\begin{pmatrix} a \\ b \end{pmatrix} \bigotimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$.

Note que a restrição da soma das normas ao quadrado segue válida em $||ac||^2 + ||ad||^2 + ||bc||^2 + ||bd||^2 = 1$.

Por fim, é importante para nossas operações que quando requisitarmos o valor de um qbit apenas um valor nos seja fornecido. A isso damos o nome de colapsar um qbit. Ao colapsarmos um qbit temos a probabilidade de cada posição ser igual a 1 e todas as outras iguais a 0. Por exemplo:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \bigotimes \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$$

Dessa forma, dizemos que há uma probabilidade de $\frac{1}{4}$ do qbit colapsar para $\mid 00\rangle$ $\mid 01\rangle$ $\mid 10\rangle$ $\mid 11\rangle$

4. Hadamard gate

Da mesma forma que existem portas lógicas para a programação clássica, para a computação quântica existem portas quânticas ou *quantum gates*. Existem vários *quantum gates*, como o *Toffoli gate* e o *Fredkin gate*, no entanto, neste tópico o foco será no *Hadamard gate*, também conhecido como porta H e segundo Meng e Pian (2016) essa é uma das portas mais utilizadas em computação quântica. A primeira transição gerada por essa porta é ao receber 0- ou 1-bit, retorna uma superposição exatamente igual, como demostrado nas operações abaixo.

$$\text{H}\mid 0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \quad H \mid 1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix}$$

Repare que um dos valores da matriz que representa a porta quântica é negativo, o que permite a operação oposta ser verdadeira. Ou seja, a partir de uma superposição exatamente igual, utilizando o *Hadamard gate* é possível retornar a 1- ou 0-bit.

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Portanto, o *Hadamard gate* permite que o processo gerado pela computação quântica forneça resultados determinísticos ao invés de somente probabilísticos. Através das transformações realizada por essa porta fica claro a possibilidade da transição da computação clássica para a quântica e vice-versa. É importante ressaltar que a possibilidade de o resultado ser determinístico depende da modelagem do algoritmo, logo, não são todos os algoritmos quânticos que vão poder gerar esse tipo de resultado.

A partir dos conceitos apresentados é possível construir uma máquina de estados utilizando o *Hadamard gate*(H) e o *Not gate* (X). São estabelecidos oito estados com val-

ores para o qbits e a partir das operações das portas são estabelecidas as transições desses estados. Como os estados estão sendo apresentados com valores reais é possível representá-los em um gráfico cartesiano e a localização deles formará círculo, dando assim o nome de *unit circle* para essa máquina de estados. Vale ressaltar que a gama de valores possíveis para o qbits é muito maior do que o apresentado abaixo e para a representação correta dos estados possíveis seria uma esfera e não um círculo, no entanto, mesmo com essas limitações a máquina de estados descrita fornece uma clara representação do poder computacional gerado pelos conceitos apresentados.

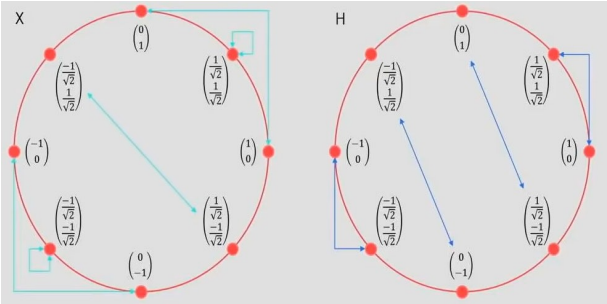


Figure 1. Máquina de estados *unit circle* para as portas *Hadamard*(H) e *Not*(X)

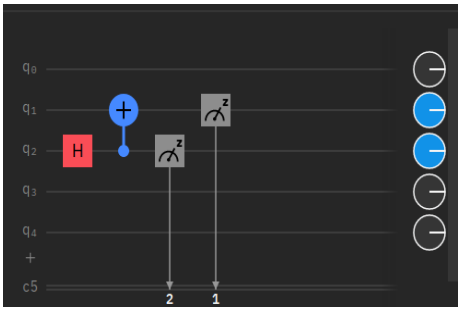
5. Entanglement

Quantum Entanglement, ou entrelaçamento quântico, ocorre quando um grupo de partículas é gerado, ou interage entre si, de tal modo que não é possível determinar o estado quântico de cada partícula independentemente. O estado quântico de um sistema entrelaçado não é capaz de ser fatorado como um produto das suas partes, isto dito, não pode ser descrito como um conjunto de partes individuais, mas sim como um sistema inseparável e uno.

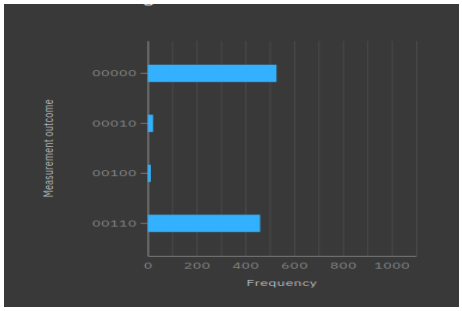
Um sistema entrelaçado quânticamente não possui solução, e portanto não podemos fatorar seu estado quântico. Isto faz com que o sistema possua uma probabilidade de 50% de colapsar para 0 ou 1. O sistema colapsa a partir do momento que nós medimos ele, e o resultado, seja 0 ou 1, é dado como aleatório, sem que possamos interferir nele.

Uma implicação interessante do entrelaçamento quântico é que, por se tratar do resultado da interação de partes inseparáveis, é possível escolher o tempo e a distância dessa medição dentro do sistema de tal modo que seria impossível que a informação do resultado da medição em uma das partes do sistema seja comunicada à outra parte, que também está sendo medida. Mesmo assim, o sistema sempre irá se colapsar em conjunto para o mesmo resultado a partir da primeira medição, o que contradiz com o teorema da relatividade que afirma que informação não pode viajar mais rápido do que luz.

Esta implicação gera interessantes consequências sobre computação e física quântica. Uma teoria mais intuitiva sobre ela, *Hidden Variables Theory*, traz a hipótese de que estes sistemas entrelaçados quanticamente computam seu resultado previamente e armazenam esse resultado dentro de suas partes, então quando realizamos a medição não temos informação viajando mais rápido que a luz, mas sim o resultado de um pré-processamento sendo retornado. Entretanto, essa teoria possui algumas falhas, que são muito densas pro escopo trabalho. Outra dessas consequências é o conceito de não-



(a) Configuração para q-bits entrelaçados no IBM



(b) Resultado dos q-bits entrelaçado

localidade quântica se aplicar para ambos espaço e tempo, como foi provado em experimentos em 2012 e 2013.

6. Teleportation

O entrelaçamento descrito pode usado para enviar um qubit em superposição, de um lugar onde há um de dois qubits entrelaçados para onde está o outro, seguindo esse procedimento: A pessoa A quer enviar um qubit $|\phi\rangle = a\,|0\rangle + b\,|1\rangle$, em que a e b são desconhecidos,para a pessoa B, A e B cada possuem metade de um par entrelaçado $|\psi_0\rangle = \sqrt{\frac{1}{2}}(|00\rangle + |11\rangle)$.

A pessoa A começa com o estado $|\phi\rangle \otimes |\psi_0\rangle = \sqrt{\frac{1}{2}}(a\,|000\rangle + a\,|011\rangle + b\,|100\rangle + b\,|111\rangle)$ e depois aplica Cnot $\otimes I$ seguido por $H \otimes I \otimes I$ e obtém $\frac{1}{2}(|00\rangle\,(a\,|0\rangle + b\,|1\rangle) + |01\rangle\,(a\,|1\rangle + b\,|0\rangle) + |10\rangle\,(a\,|0\rangle - b\,|1\rangle) + |11\rangle\,(a\,|1\rangle - b\,|0\rangle))$ em que H é a matriz de Hadamard e I é a identidade.

Ao medir $|\phi\rangle$ e $|\psi_0\rangle$, a pessoa A obtém $|00\rangle, |01\rangle, |10\rangle, ou\, |11\rangle$ com a mesma probabilidade, e envia os resultados para a pessoa B. Esse envio de informação não supera a velocidade da luz porque esses dois bits clássicos devem ser enviados normalmente.

Quando a pessoa B recebe os dois bits clássicos da pessoa A, ele sabe como o estado de sua metade do par entrelaçado se compara ao estado original do qubit da pessoa A. B pode reconstruir o estado original do qubit de A, aplicando a transformação de decodificação apropriada ao seu qubit, originalmente parte do par entrelaçado.

Se ele receber 00, aplica I, 01 aplica X, 10 aplica Z, 11 aplica Y, sendo que I é a identidade,

X = $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ Y = $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ Z = $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Assim, B consegue reconstruir o estado $|\phi\rangle$ original.[MENG 2016]

References

[IBM 2020] IBM (2020). Quantum computing. https://quantum-computing.ibm.com/.

[Inspire 2020] Inspire, Q. (2020). What is a qubit? https://www.quantum-inspire.com/kbase/what-is-a-qubit/.

[MENG 2016] MENG, Xiangping; PIAN, Z. (2016). *Chapter 5 -Vulnerability Assessment of the Distribution Network Based on Quantum Multiagent.* Elsevier Inc.

[Microsoft 2018] Microsoft (2018). Quantum computing for computer scientists. https://www.microsoft.com/en-us/research/uploads/prod/2018/05/40655.compressed.pdf.

[Wikipedia 2020] Wikipedia (2020). Quantum entanglement. https://en.wikipedia.org/wiki/Quantum_entanglement.

[Wikipedia 2021] Wikipedia (2021). Bit quântico. https://pt.wikipedia.org/wiki/Bit_quantico.