

# Mini-Introdução à Teoria da Complexidade Quântica

Rafael Castro

[rafaelcgs10@gmail.com](mailto:rafaelcgs10@gmail.com)

Departamento de Ciência da Computação  
Centro de Ciências e Tecnológicas  
Universidade do Estado de Santa Catarina

03 de Abril de 2019

Betina



# Motivação

A Computação Quântica é o assunto do momento

<https://cio.com.br/a-computacao-que-e>

porque são construídas a partir dos princípios da mecânica quântica. Ou seja, exploram leis complexas da natureza. Ao se aproveitar disso, a computação quântica pode executar novos tipos de algoritmos para processar informações de forma mais holística.

Mas em que tudo isso poderá nos ajudar? Os sistemas quânticos podem desencadear a complexidade das interações moleculares e químicas que levam à descoberta de novos medicamentos e materiais. Eles podem permitir cadeias de logística e de abastecimento ultraeficientes, como aprimorar as operações de uma frota para entregas durante uma temporada de grande demanda. Além disso, podem nos ajudar a encontrar novas maneiras de modelar os dados financeiros e isolar os principais fatores de risco para fazer melhores investimentos. E eles podem criar máquinas muito mais poderosas. A ideia é que seja uma chave potente para abrir portas que nunca havíamos aberto antes.

Imagine, por exemplo, que você esteja planejando um mochilão, e queira saber a melhor maneira de viajar: como pagar mais barato em todas as passagens, como pegar o melhor tempo em cada lugar, como estar presente no maior número possível de festas, como evitar o máximo de dias chuvosos, etc. São, óbviamente, inúmeras as possibilidades e as variáveis que precisam ser ponderadas, e um computador tradicional precisaria calcular cada uma delas individualmente.

Um computador quântico, por sua vez, poderia calculá-las todas ao mesmo tempo. Isso permitiria não apenas responder de forma muito mais rápida perguntas complexas como essa, mas permitiria também que perguntas que levariam muito tempo para ser calculada mesmo pelos supercomputadores atuais se tornassem facilmente resolvíveis.

Outra característica diferente: quando um algoritmo quântico age sobre variáveis, o faz sobre todos os valores possíveis simultaneamente —não é preciso processar valores um depois do outro, como na computação clássica.



# Superposição

- A **Superposição quântica**: uma partícula pode assumir proporções entre dois estados.  
Ex: A polarização de um fóton (vertical ou horizontal).
- A superposição quântica pode ser utilizada para representar informação binária: **qubit**.
- A computação quântica utiliza dados armazenados em qubits: 0 - 1 (qualquer proporção de ambos estados).



## Representação dos Qubits

- Os dois estados base de um qubit são representados pelos vetores

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ e } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (1)$$

Isso é conhecido como a notação de *Dirac Ket* para vetores.

- Para completamente representar o estado de um qubit são necessários dois números  $(a, b)$  **complexos** para descrever as duas proporções das duas bases:

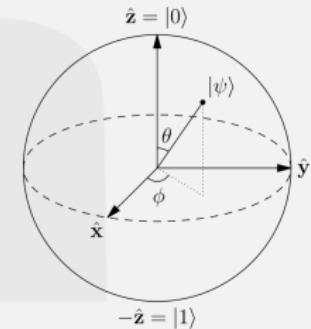
$$\Psi = a|0\rangle + b|1\rangle. \quad (2)$$

# Espaço de Estado de um Qubit

- Utiliza-se a 2-norma:

$$|a|^2 + |b|^2 = 1 \quad (3)$$

- Devido a restrição da equação 3 os possíveis valores de um qubit se limitam uma equação de uma esfera de três dimensões.



# Operações em Qubits

- Operações em qubit são feitas por produtos de matrizes unitárias, também chamado de transformação unitária.
- Uma transformação de um qubit é uma translação no espaço de estado.
- O qubit  $|0\rangle$  está no polo norte da Esfera de Bloch é levado para o seu equador, um estado de superposição, pelo produto na Equação 4.

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \quad (4)$$

- Aplicar uma segunda vez essa transformação levaria novamente para o qubit  $|0\rangle$ .



# Emaranhamento Quântico

- Um par (ou mais) de partículas tem o seu estado associados de maneira que não é possível descrever o estado de uma delas individualmente.
- - ➊ Dois *spins* (*A* e *B*) emaranhados por seus campos magnéticos, ambos preparados no estado  $|0\rangle$ .
  - ➋ O *spin A* é colocado na superposição  $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$  por meio da aplicação de um campo magnético oscilante.
  - ➌ Aplica-se outro campo magnético no *spin B* que vai nega-lo (mudar para  $|1\rangle$ ) somente se o *spin A* estiver no estado  $|0\rangle$ .
  - ➍ O *spin B* está numa superposição de  $|0\rangle$  e  $|1\rangle$ , devido ao emaranhamento com o *spin A*.  
O sistema final é uma superposição  $\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$ .
- O emaranhamento quântico é a chave para o paralelismo quântico!  
A computação de um qubit afeta o estado de outro qubit.



# Portas Quânticas 1

- Portas quânticas são análogas as portas lógicas binárias: operam em  $n$  bits/qubits e dão algum bit/qubit de resposta.
- Portas quânticas não perdem informação: são reversíveis.
- Considera a porta AND clássica e a porta quântica C-NOT (Control-NOT):

A	B	A	A AND B
0	0	0	0
0	1	0	0
1	0	1	0
1	1	1	1

A	B	A	A CNOT B
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Figura: Portas AND e CNOT.

## Portas Quânticas 2

- Portas lógicas quânticas de  $n$  qubits são transformações unitárias representadas por matrizes de tamanho  $2^n \times 2^n$ . Por exemplo, a porta lógica quântica CNOT tem a matriz unitária da Equação 5 e a matriz da Equação 4 é a porta quântica Hadamard (H).

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (5)$$



# Circuitos Quânticos 1

- Circuitos clássicos e quânticos (com as devidas restrições) são um modelo de computação.
- Um circuito quântico é uma sequência de portas lógicas quânticas que operam sobre uma entrada de  $n$  qubits.
- [Bernstein and Vazirani, 1993] provou que Circuitos Quânticos (com as devidas restrições) representam um modelo Turing-Completo.
- Não é trivial simular primitivas simples como *looping*, *branching* e composição no contexto de Máquinas de Turing Quânticas, pois as leis da Mecânica Quântica impõem restrições difíceis, como observar uma informação implica no colapso do seu estado.

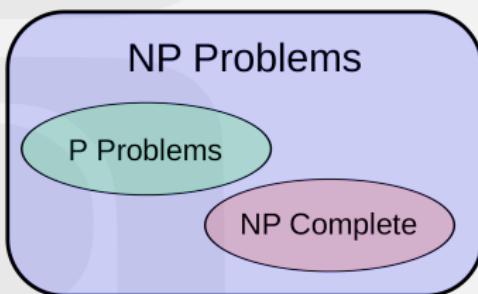


## Circuitos Quânticos 2

- *Conjunto universal de portas quânticas* (CUPQ) é um conjunto portas quânticas capaz de construir circuitos que representam tudo que um computador quântico pode fazer.
- Foi demonstrado por [Shi, 2003] que as portas Toffoli e Hadamard são um CUPQ.
- Foi demonstrado por [Dawson and Nielsen, 2006] que qualquer CUPQ pode ser simulado por outro CUPQ em tempo polinomial.

# Classe de Problemas na Computação Tradicional

- **NP (nondeterministic polynomial time)**: Problemas de decisão verificáveis em tempo polinomial.  
Eficientes no modelo computacional “Máquina de Turing Não-Determinista”.
- **P**: Problemas de decisão computáveis em tempo polinomial.  
Eficientes no modelo computacional “Máquina de Turing Determinista”.



## P vs NP

Exemplos de problemas: SAT, Caixeiro viajante...

# Classe Probabilística BPP

- A classe BPP (*Bounded-Error Probabilistic Polynomial-Time*): Polinomial por uma Máquina de Turing Probabilística (com um mecanismo de aleatoriedade).
- Somente é aceitável no máximo  $1/3$  de chance de fornecer a resposta errada (seja sim ou não).
- A classe BPP funciona como um análogo probabilístico da classe P.
- A verificação de primalidade:  $\text{BPP} \rightarrow \text{P}$ .

## Classe Quântica BQP

- A classe de problemas resolvidos de maneira eficiente por computadores quânticos é a BQP (*Bounded-Error Quantum Polynomial-Time*).
- Assim como a classe BPP, a classe BQP requer no máximo  $1/3$  de chance de erro.
- Definida por Circuitos Quânticos.
- O número de qubits permitidos no circuito deve ser polinomial ao tamanho do problema.  
O algoritmo de Shor para fatoração de números primos de  $n$ -bits requer um circuito de  $2n$ -qubits.



# Relação Entre as Classes

- $BPP \subseteq BQP$ , pois como fonte de aleatoriedade basta utilizar a porta Hadamard.
- A classe PP é similar a BPP, mas com requisito de probabilidade difícil o suficiente para não ser possível aumentar a chance de acerto ao rodar o algoritmo várias vezes.
- A Classe PSPACE: problemas resolvidos com espaço polinomial, mas com tempo ilimitado.
- $P \subseteq BPP \subseteq BQP \subseteq PP \subseteq PSPACE$ .

## O Maior Problema da Teoria da Complexidade Quântica

Computadores quânticos são mais eficientes que computadores probabilísticos clássicos?

- $BPP \neq BQP$
- A evidência mais popular que isso é verdade é o algoritmo quântico Shor e o fato que até hoje ninguém descobriu um eficiente algoritmo probabilístico que realiza o mesmo trabalho.

## Classes com Oráculos

- Não há relação direta entre a classe NP e as classe probabilística BQP.
- Ao menos, sabe-se que a classe BPP está contida na classe  $\text{NP}^{\text{NP}}$  (NP com um oráculo NP).
- Há a classe PH (Polynomial Hierarchy) que contém todos as classes com tempo polinomial estendidas com máquinas oráculos, inclusive NP e BPP.
- O papel do oráculo é funcionar como uma espécie de medida de dificuldade do problema, quanto mais um algoritmo precisa consultar o oráculo, mais difícil é o problema.
- PH é uma generalização (e um superconjunto) da classe NP.

# BQP $\subseteq$ PH?

- BQP está contida em PH?  
Isso questiona se há problemas somente tratáveis por um computador quântico, mesmo que  $P = NP$
- Computadores quânticos são um caso a parte na Teoria da Complexidade?
- Em 2009 Aaronson introduziu o problema da “fourrelação” e demonstrou estar em BQP [Aaronson, 2009].
- Em Maio de 2018 [Ran Raz, 2018] demonstraram que esse problema não está em PH.
- Uma computador quântico precisa de apenas uma consulta a um oráculo para resolver esse problema, enquanto um computador clássico não é capaz de resolve-lo de maneira eficiente, mesmo com um número ilimitado de consultas.

# Ilha da Complexidade Quântica

## A New Island on the Complexity Map

What can a quantum computer do that any possible classical computer cannot? Computer scientists have finally found a way to separate two fundamental computational complexity classes.

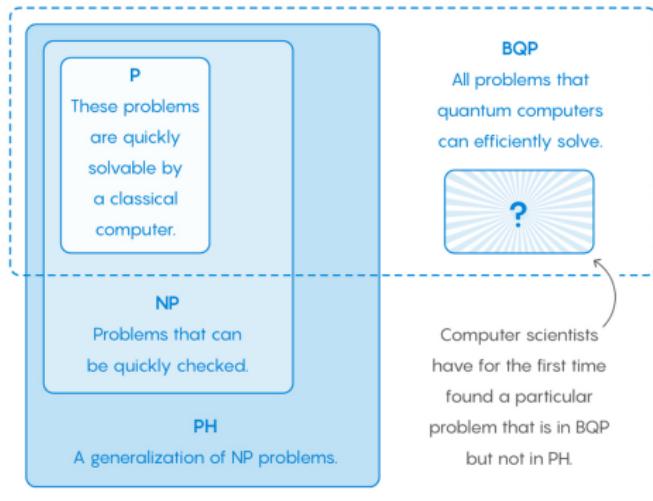


Figura: Ilha de complexidade BQP. Fonte: QuantaMagazine.org.

# *Computational Complexity-Theoretic Church–Turing Thesis*

- Esse novo resultado invalida a *computational complexity-theoretic Church–Turing thesis*
- Proposto por [Bernstein and Vazirani, 1993], que diz que uma Máquina de Turing Probabilística pode simular em tempo polinomial qualquer outro modelo de computação.
- Algoritmos quânticos são eficientes em tarefas que algoritmos probabilísticos não são.

# NP-Completure e Computação Quântica

- Erroneamente muitas pessoas ou sites/revistas de notícias anunciam que a computação quântica é capaz de resolver de maneira eficiente problemas NP-Completos.
- O status de  $NP \subset BQP$  é desconhecido.
- É sabido uma separação por oráculo de  $NP \not\subset BQP$ : suponha um problema com espaço de busca de tamanho  $2^n$  de possíveis soluções e um oráculo que decide se a uma possível solução é a procurada.
- Num computador normal, no pior dos casos, é necessário  $2^n$  consultas no oráculo.
- Por meio do algoritmo de Grover [Grover, 1996] é possível encontrar a resposta em até  $2^{n/2}$  consultas.

# Speed-up da Computação Quântica

- O *speed-up* da computação quântica para problemas de busca genéricos e não estruturados é quadrático. Não é conhecido como fazer *speed-up* exponencial para esse tipo de problema.
- O motivo para o *speed-up* ser quadrático é a 2-norma:
  - Classicamente, num espaço de  $N$  possíveis soluções com apenas uma correta (cada possibilidade com  $1/N$  de ser a resposta), para um número  $m$  de tentativas, tem a probabilidade de  $m/N$  de adivinhar a solução. Assim, para ter uma boa chance de adivinhar a resposta correta é necessário ter um  $m$  próximo a  $N$ .
  - Já com a computação quântica é possível aplicar transformações lineares no vetor das amplitudes, que são as raízes quadradas das probabilidades por causa da 2-norma. Logo, para  $m$  tentativas tem-se  $m/\sqrt{N}$  de probabilidade de adivinhar a resposta. Com aproximadamente  $\sqrt{N}$  tentativas a chance de encontrar a resposta já é boa o suficiente.



## Resumindo...

- Não sabemos como resolver de maneira eficiente problemas NP-Completos num computador quântico.
- Não tem essa de testar todas as possibilidades ao mesmo tempo.

## Referências I

-  Aaronson, S. (2009).  
Bqp and the polynomial hierarchy.  
In *Proceedings of the Forty-second ACM Symposium on Theory of Computing*, STOC '10, pages 141–150, New York, NY, USA. ACM.
-  Bernstein, E. and Vazirani, U. (1993).  
Quantum complexity theory.  
In *Proceedings of the Twenty-fifth Annual ACM Symposium on Theory of Computing*, STOC '93, pages 11–20, New York, NY, USA. ACM.
-  Dawson, C. M. and Nielsen, M. A. (2006).  
The solovay-kitaev algorithm.  
*Quantum Info. Comput.*, 6(1):81–95.

## Referências II

-  Grover, L. K. (1996).  
A fast quantum mechanical algorithm for database search.  
In *ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING*, pages 212–219. ACM.
-  Ran Raz, A. T. (2018).  
Oracle separation of bqp and ph contact add comment  
rss-feed.  
*Electronic Colloquim on Computation Complexity*.
-  Shi, Y. (2003).  
Both toffoli and controlled-not need little help to do universal quantum computing.  
*Quantum Info. Comput.*, 3(1):84–92.