Computação Quântica: desde Demócrito até o ACM Prize 2020

Franklin de Lima Marquezino
Professor Associado, PESC/COPPE/UFRJ
franklin@cos.ufrj.br

ACM Prize

- Não confundir com ACM A. M. Turing Award
- ACM Prize é concedido a pesquisadores em fase intermediária de suas carreiras
- Prêmio de US$250.000, patrocinado por Infosys Ltd.
- Ganhadores participam do Heidelberg Laureate Forum juntamente com ganhadores do Turing Award, Abel Prize, Fields Medal e Nevanlinna Prize

Scott Aaronson

Foto de
https://www.scottaaronson.com

- Nascido em 1981, EUA
- Graduação em Cornell, 1997-2000
- Doutorado em UC Berkeley, 2000-2004, sob orientação de Umesh Vazirani
- Postdoc em Princeton e em Waterloo, 2004-2007
- Professor, MIT, 2007-2016
- Professor, The University of Texas at Austin, 2016-hoje

Citação do prêmio

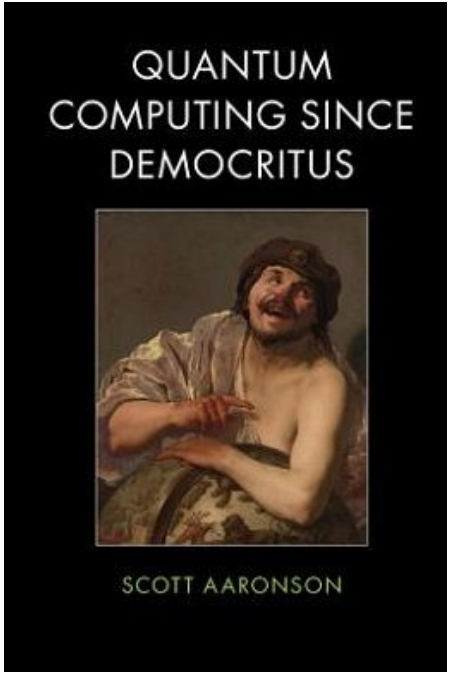
Contribuições inovadoras em computação quântica, com destaque para:

1. Tornar a computação quântica acessível: livro, blog, entrevistas, participações em TED Talks etc.
2. Limites fundamentais de computadores quânticos: prova de lower bound não trivial para problema da colisão
3. Complexidade computacional clássica: técnica de algebrização, lança luz ao problema P vs NP
4. Boson Sampling: uma proposta para comprovação da supremacia quântica

Destaque #1
Shtetl-Optimized,
Demócrito
etc

Shtetl-Optimized /ˈʃtɛtəl/

- Blog famoso sobre ciência da computação teórica (clássica e quântica)
- “Computadores quânticos não vão resolver problemas difíceis instantaneamente simplesmente tentando todas as soluções em paralelo”
- https://www.scottaaronson.com/blog/



Capa: Brugghen, 1628

Quantum Computing Since Democritus

- Demócrito (c. 460 a.C. - c. 370 a.C.), conhecido como “o filósofo que ri”, dizia que a matéria era formada por partículas indivisíveis (átomos)
- Filosofia ao longo de todo o livro:
  - trabalho de faxina intelectual, limpando a bagunça deixada pelos cientistas
    ou
  - exploração, mapeando o terreno intelectual para depois os cientistas avançarem

Dossi, 1540

Rembrandt, 1628-29

O que é a mecânica quântica?

- Cuidado: as pessoas abusam do termo!
- MQ é teoria muito bem sucedida para descrever o comportamento de coisas muito pequenas
- “MQ é o sistema operacional onde todas as outras teorias (exceto relatividade geral) rodam como aplicações”

Não sou físico! E agora?

- Existem duas formas de ensinar MQ: abordagem mais comum nos livros de Física segue ordem cronológica das descobertas; outra abordagem é matemática e vai direto ao núcleo conceitual
- MQ resumida a poucas regras, como no xadrez
- Para quem quer iniciar: base sólida em Álgebra Linear é mais importante do que em Física

Como representar os estados?

Pense em “generalização” das leis das probabilidades para permitir números negativos (ou até complexos)

- Bit clássico (probabilístico):
  b = (p, 1-p) tal que $0 \leq p \leq 1$

- Bit quântico (qubit):
  q = (α,β) tal que $|\alpha|^2 + |\beta|^2 = 1$

Como o estado evolui?

- Estado representados por vetor, logo evolução representada por matriz
- Norma do vetor deve ser preservada

- Classicamente: matrizes estocásticas

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p \\ 1-p \end{pmatrix} = \begin{pmatrix} 1-p \\ p \end{pmatrix}$$

- Quanticamente: matrizes unitárias

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

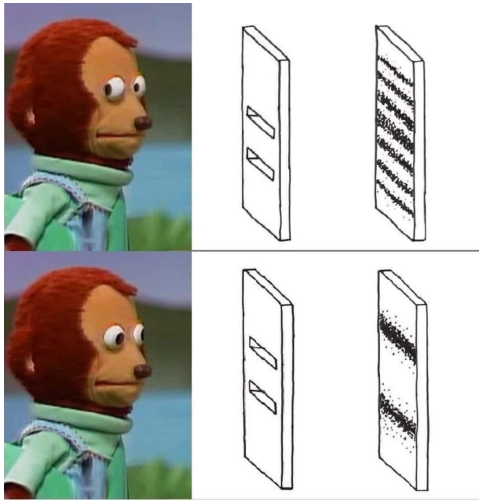
O que acontece se eu olhar?

Se você medir o valor de um bit (probabilístico ou quântico), o resultado só pode ser 0 ou 1!

- Bit probabilístico:
  0 com probabilidade p,
  1 com probabilidade 1-p

- Bit quântico:
  0 com probabilidade $|\alpha|^2$,
  1 com probabilidade $|\beta|^2$

O que acontece se eu não olhar?



- Generalização que fizemos das probabilidades não foi mero capricho
- Einstein: “Deus não joga dados” (o problema dele não com as probabilidades)
- Emaranhamento, interferência etc
- Interpretações da MQ

Máquina de Turing

- Máquina teórica, lê e escreve símbolos em uma fita, modifica seu estado interno, e eventualmente para
- Existe uma máquina universal, programável
- Existem problemas não computáveis

- Ideia filosófica importante: Tese de Church-Turing

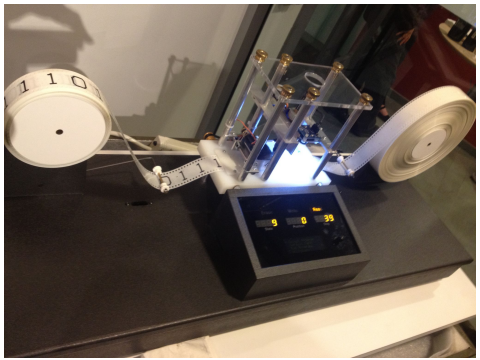
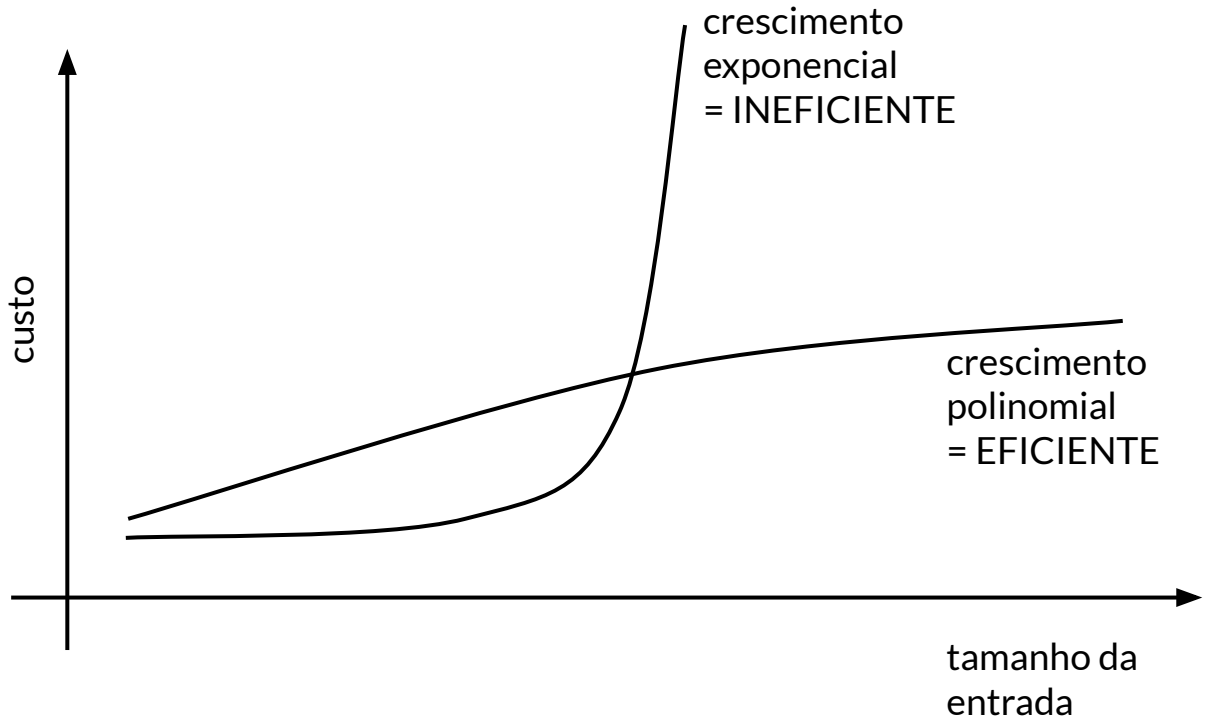
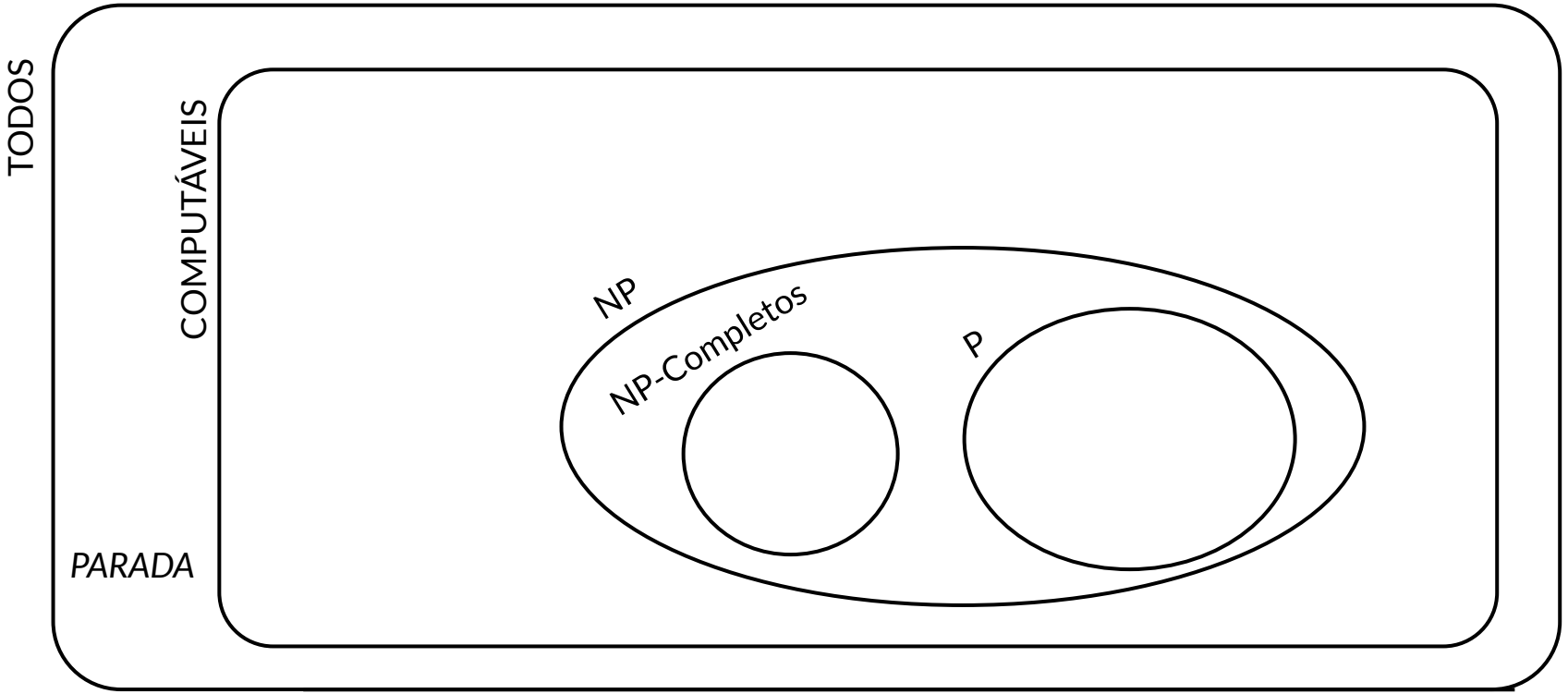


Foto: Wikipedia

Complexidade computacional



Classes de complexidade

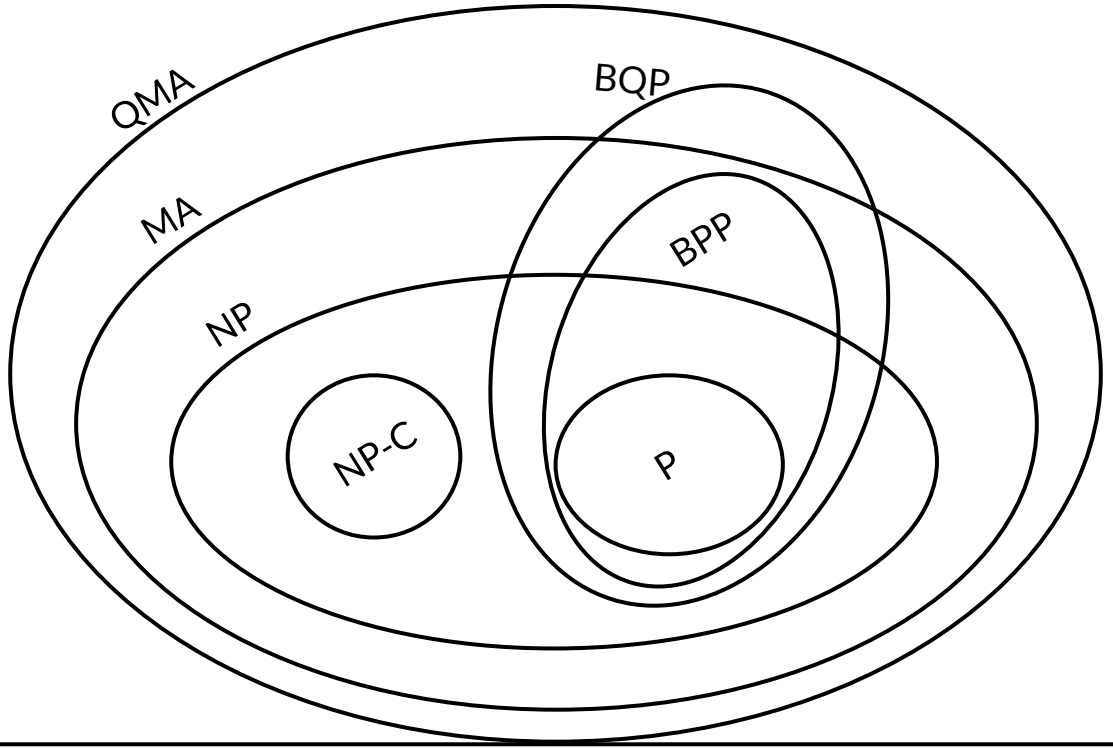


Destaque #2
Algebrização

Barreiras para o problema P vs NP

- P vs NP: resolver é mais difícil que verificar?
- Palestra de Celina: https://youtu.be/OZTYKk8RJSg
- Por que é difícil provar que P ≠ NP ou que P = NP ?
- Relativização (Baker, Gill, and Solovay, 1975)
- Provas naturais (Razborov and Rudich, 1997)
- **Algebrização** (Aaronson and Wigderson, 2009)

Classes quânticas



Destaque #3
Lower bound para problema da colisão

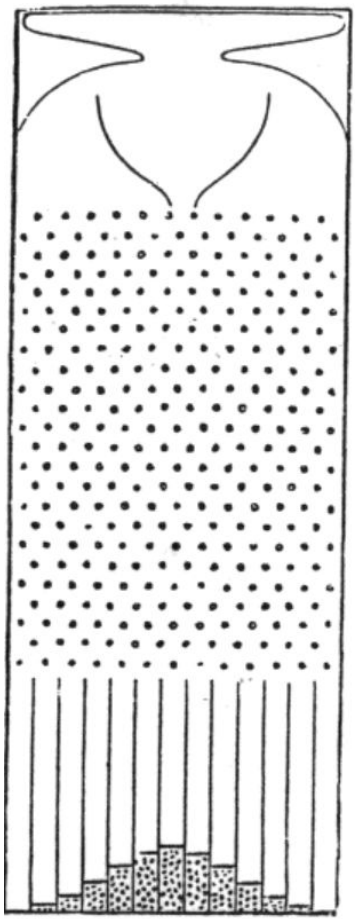
Problema da colisão

- Seja $X = \{x_1, x_2, \ldots, x_n\}$ um conjunto de elementos tirados de $\{1, 2, \ldots, n\}$, com n par.
- É prometido que X é um-para-um, ou X é dois-para-um
- Pergunta: qual dos dois é o caso?
- Aaronson provou lower bound $\Omega(n^{1/5})$ em 2002
- Era problema em aberto desde 1997 provar qualquer lower bound melhor que $\Omega(1)$
- Lower bound: “o que não podemos fazer com computadores que ainda não temos”

Destaque #4
Boson Sampling

Supremacia quântica

- Termo cunhado por John Preskill
- Computação quântica possui vantagem sobre a computação clássica? Parece que sim, mas como provar?
- Resolva algum problema que deveria levar um tempo absurdo no melhor supercomputador clássico atual
- Quais problemas são bons candidatos? Fatoração de inteiros? Não é um boa ideia…
- É possível demonstrar supremacia quântica usando equipamentos ruidosos, sem correção de erros?



Problemas de amostragem

- Qual a distribuição das bolinhas no tabuleiro ao lado?
- Substitua as bolinhas por partículas quânticas, e os pinos por dispositivos que interajam com as partículas. Qual a distribuição resultante agora?

Amostragem de bósons

- Bósons: por exemplo, fótons
- Amostragem de bósons: análogo à figura do slide anterior, faça um circuito com dispositivos ópticos muito simples, fótons entram de um lado, diga qual a distribuição na saída
- Relativamente fácil construir, porém muito difícil simular classicamente (mesmo aproximando!)
- Problema do permanente de matrizes: #P-completo

Conclusões

- Aaronson: contribuições significativas em computação clássica e quântica
- Mecânica quântica para cientistas da computação: pode-se aprender por uma abordagem matemática
- Computação quântica: importância não só prática, mas também para a teoria da computação
- Filosofia: ajuda a entender o sentido das teorias científicas, ajuda a propor novas pesquisas

Onde encontrar os artigos principais

- Sobre Boson Sampling: “The Computational Complexity of Linear Optics”, STOC 2011, https://dl.acm.org/doi/10.1145/1993636.1993682
- Sobre lower bound para problema da colisão: “Quantum Lower Bound for the Collision Problem”, STOC 2002, https://dl.acm.org/doi/10.1145/509907.509999
- Sobre algebrização: “Algebrization: A New Barrier in Complexity Theory”, ACM Trans. Comput. Theory, https://dl.acm.org/doi/10.1145/1490270.1490272
- Blog: https://www.scottaaronson.com/blog/
- Livro: https://doi.org/10.1017/CBO9780511979309

Computação Quântica: desde Demócrito até o ACM Prize 2020

Franklin de Lima Marquezino
Professor Associado, PESC/COPPE/UFRJ
franklin@cos.ufrj.br