Still a bit short of the Qubit – A Promessa da Computação Quântica

Carlos Herdeiro
Departamento de Matemática, Universidade de Aveiro
herdeiro@ua.pt

Corria o ano de 1981 quando Richard Feynman, sempre irreverente e provocador, lançou um desafio: simular a física quântica com computadores clássicos é ineficiente. Por que não usar as próprias regras da mecânica quântica para construir computadores? "Nature isn't classical, damn it," disse ele. "And if you want to make a simulation of nature, you'd better make it quantum mechanical." [1]. Esta foi a semente de uma ideia que demoraria décadas a germinar.

Mas eventualmente germinou. Em laboratórios do século XXI, partículas "dançam". Estão emaranhados, ocupando estados indefinidos, desafiando a lógica binária que governou o mundo digital desde os primórdios da era da informação. A computação quântica, antes um conceito de ficção científica, é agora uma corrida tecnológica, filosófica e até geopolítica. Como chegámos aqui?

Ao contrário do bit clássico, que pode ser 0 ou 1, o bit quântico ou qubit vive em superposição — pode ser 0 e 1 ao mesmo tempo. Além disso, pode estar entrelaçado com outros qubits, uma ligação quase mística onde o estado de um influencia o outro, mesmo a grandes distâncias e sem parecer colocar em causa a causalidade como a física moderna a concebe. A computação quântica promete aproveitar o paralelismo massivo na computação examinando muitos estados quânticos emaranhados simultaneamente, em vez de estados clássicos individuais sequencialmente. Esta ideia abre portas para algoritmos mais eficientes, como o de Shor [2], que promete quebrar em segundos os sistemas de criptografia que hoje protegem bancos e governos.

Empresas como IBM, Google, e startups como Rigetti e IonQ lideram a corrida para construir máquinas de qubits cada vez mais estáveis. Em 2019, a Google anunciou ter alcançado a chamada "supremacia quântica", resolvendo em 200 segundos um problema que levaria 10 mil anos num supercomputador clássico [3] — embora a relevância prática do feito tenha sido contestada.

Há avanços promissores mas a maioria dos computadores quânticos atuais ainda sofre de ruído, erro e instabilidade. A promessa é real, como se percebeu a caminhar nos corredores do March Meeting 2025 da American Physical Society (APS) - ver figura,

Mostra de computadores quânticos no March Meeting da APS 2025. Cortesia de J. F. F. Mendes.

mas ainda estamos a atravessar a adolescência da tecnologia.

As aplicações potenciais são fascinantes: medicamentos simulados a nível molecular, materiais exóticos, previsão precisa de reações químicas, ou soluções para problemas de logística e finanças atualmente insolúveis. No entanto, com grande poder vem grande responsabilidade — e risco. A computação quântica poderá tornar obsoletos os sistemas de segurança atuais, levando à necessidade urgente de criptografia pós-quântica [4]. Além disso, é preciso refletir: que tipo de sociedade estamos a construir com essa capacidade? Quem controlará essas máquinas? Quais os impactos éticos?

A computação quântica vive, por enquanto, num estado estranho — como o gato de Schrödinger: viva e morta, concreta e teórica, limitada e poderosa. Meio século antes da proposta de Feynman, Aldous Huxley escrevia o Admirável Mundo Novo. Se a inteligência artificial torna tanto da nossa sociedade obsoleto e básico, adicionada à computação quântica o Futuro parace um emaranhado de realidades distópicas, infinitamente mais admirável, e preocupante, que a visão de Huxley.

Referências
[1] Feynman, R. P. (1982). *Simulating Physics with Computers*. International Journal of Theoretical Physics, 21(6), 467–488.
[2] Shor, P. W. (1994). *Algorithms for quantum computation: discrete logarithms and factoring*. Proceedings 35th Annual Symposium on Foundations of Computer
Science.
[3] Arute, F. et al. (2019). *Quantum supremacy using a programmable superconducting processor*. Nature 574, 505–510.
[4] Mosca, M. (2018). *Cybersecurity in an era with quantum computers: Will we be ready?* IEEE Security & Privacy, 16(5), 38–41.