A revolução dos q-bits

Ivan S. Oliveira
Cássio Leite Vieira

A revolução dos q-bits

O admirável mundo da computação quântica

ZAHAR
Rio de Janeiro

Projeto gráfico e composição: Mari Taboada
Capa: Sérgio Campante
Créditos das figuras: p.24, © Corbis;
p.19, 21, 28, 40 e 42, © Bettmann/Corbis.

CIP-Brasil. Catalogação-na-fonte
Sindicato Nacional dos Editores de Livros, RJ.

Oliveira, Ivan S.
O45r A revolução dos q-bits: o admirável mundo da computação quântica / Ivan S. Oliveira, Cássio Leite Vieira. — Rio de Janeiro: J. Zahar, 2009.

ISBN 978-85-378-0127-7
1. Computadores quânticos. I. Vieira, Cássio Leite, 1960-. II. Título.

CDD: 004.1
09-0528 CDU: 004.38

SUMÁRIO

Prólogo

"No futuro, os computadores se parecerão mais com as xícaras de café que costumamos esquecer ao lado do teclado." Essa estranha frase podia ser lida em uma pequena placa de bronze logo abaixo do enigmático quadro do sr. Chuang, avô de um rico empresário da computação da segunda metade do século XXI. O sr. Chuang dedicara a vida à física em um importante instituto tecnológico e fora um dos pioneiros da computação quântica, com outros cientistas de sua época.

O quadro com a foto sorridente (e a frase já não tão profética) ornamentavam a sala do sr. Lao, neto do sr. Chuang e presidente da Quantum Chips, multinacional que dominava o mercado de microprocessadores para computadores quânticos. De fato, a aparência externa dos computadores não havia mudado muito. Afinal, os usuários continuavam a pertencer ao "mundo clássico", aquele dos objetos macroscópicos, e a interface com um chip liliputiano, contendo poucas centenas de bits quânticos, ou abreviadamente q-bits, ainda devia ser feita com um tipo de teclado e monitor. Havia muito outras interfaces já estavam disponíveis no mercado, mas ainda não tinham conseguido superar esses dois resquícios quase fósseis do século XX.

Sempre que contemplava aquele quadro, o sr. Lao lembrava-se da primeira vez em que ouvira falar de q-bits, ainda nos

primeiros anos de escola. Sim, porque, ao lado da Grande Revolução Quântica — que ocorrera pouco antes da metade do século XXI, com o desenvolvimento do primeiro chip quântico —, uma profunda mudança tivera lugar também no ensino das ciências básicas, em particular no da física. Muito esforço governamental, por parte de vários países, foi feito para popularizar a mecânica quântica, tornando-a, em muitos casos, disciplina obrigatória no ensino fundamental. Contudo, várias noções desse campo ainda pareciam, para os estudantes e profissionais de outras áreas, um tanto vagas, como há 100 anos, pois continuavam a ser não intuitivas, a desafiar o bom senso.

Mas, naquela segunda metade do século XXI, a computação quântica já permitia que o processamento da informação fosse feito com uma velocidade considerada impossível para os agora extintos computadores clássicos.

No entanto (a portas fechadas, pois não era um tipo de comentário que pesquisadores sérios ousassem fazer em público), costumava-se repetir o que havia sido dito por alguns dos mais brilhantes físicos do século XX: a mecânica quântica continuava a ser aquela "receita de bolo" perfeita, que sempre funcionava, mas com ingredientes ainda um tanto bizarros.

Era estranho ser o presidente da maior fábrica de chips quânticos do planeta. De certa forma, isso não teria acontecido se o sr. Chuang e uma multidão de outros cientistas do final do século XX não tivessem acreditado na ideia. O sr. Chuang costumava contar histórias divertidas sobre debates (muitos deles acalorados) que ocorriam em conferências e nas páginas das publicações especializadas da época.

Para quem escutava essas histórias, parecia que a comunidade de físicos do final do século XX estava dividida. De um lado, estavam aqueles que acreditavam, com um sentimento quase religioso, na viabilidade da computação quântica; de outro, os

incrédulos. Inúmeras foram as publicações em que se havia demonstrado a "impossibilidade" da realização prática dessa ideia. Manter uns poucos q-bits em um ambiente isolado já parecia impossível, o que dizer então sobre controlar uma centena deles? Para a ala "pessimista" dos cientistas, a computação quântica não passava de uma ideia matemática — bela, certamente — que jamais teria qualquer uso prático. Acreditando nisso, vários países ficaram à margem dessa tecnologia, pela mera decisão de seus governos em não apoiar a pesquisa na área. Desse modo, naquela segunda metade do século XXI, o quadro geopolítico mundial podia ser resumido assim: países exportadores de chips quânticos e países que importavam tanto esse dispositivo quanto as muitas tecnologias dele decorrentes.

O sr. Lao imaginava qual teria sido a reação de seu avô ao ver o primeiro chip quântico entrar em funcionamento, fazendo desmoronar de uma só vez todos os argumentos teóricos contra a viabilidade desse diminuto artefato. Talvez, aquele sorriso irônico da foto...

Particularmente interessante era a história da criptografia quântica que se contava na escola. De fato, essa havia sido a primeira área da informação quântica a se desenvolver comercialmente. No início do século XXI, um método de transmitir informação, denominado BB84, já era empregado em larga escala por governos e empresas privadas. Toda e qualquer transmissão de dados feita com base no BB84 passou a ser 100% segura, inviolável. Foi o início do fim dos piratas da rede, os chamados *hackers*.

A velha forma de criptografar dados, baseada no centenário protocolo RSA, tivera um final dramático, mas fora enterrada com todas as honras. Peter Shor, então pesquisador dos Laboratórios AT&T, nos Estados Unidos, era lembrado nas escolas como o precursor de toda a "confusão" que se seguiu. A primeira aplicação séria do então recém-lançado chip quântico fora justamente com

o algoritmo de Shor. Naquele dia, a ansiedade tomara conta de cientistas do mundo inteiro, bem como de chefes de Estado, oficiais dos serviços de inteligência, banqueiros, donos de cassinos, investidores do mercado financeiro, empresários, terroristas, políticos corruptos etc. — por sinal, estas duas últimas categorias ainda existiam na segunda metade do século XXI; para muitos, uma prova de que progresso tecnológico e avanço moral não costumavam caminhar lado a lado.

O velho RSA havia resistido até então a todos os testes. Ele consistia em gerar, a partir da informação que se queria enviar, um código que tornava a informação secreta. Preocupadas com o rápido desenvolvimento da computação quântica, várias empresas de segurança de redes, na década de 2020, haviam se juntado às centenárias empresas de computação (clássica) para financiar a construção de um supercomputador cuja exclusiva tarefa seria tentar quebrar um código gerado pelo RSA.

A previsão era de que 100 milhões de anos seriam necessários para completar a tarefa. O supercomputador rodou ininterruptamente por dez anos, sem sucesso. Mas, por volta dessa época, surgiria o que foi classificado como o mais importante desenvolvimento da computação quântica: o chip quântico, contendo apenas duas centenas de q-bits. Era a chance de se testar o que, cerca de três décadas antes, ficara conhecido como algoritmo de Shor, um tipo de primeiro programa para computadores quânticos.

O binômio chip quântico-algoritmo de Shor estava pronto para quebrar o código gerado pelo protocolo RSA. Duas centenas de q-bits contra os muitos milhões de megabytes (e de dólares!) do supercomputador. A previsão, nesse caso, era de que o tempo necessário para quebrar o RSA seria de cerca de... 4,5 minutos. Mas apenas em 3,95 minutos estava tudo terminado.

Era o insólito se concretizando diante dos olhos de todos: uma tarefa que deveria levar 100 milhões de anos para ser executada por um computador clássico fora finalizada em menos de quatro minutos por um chip quântico! Essas poucas dezenas de

segundos foram suficientes para tornar obsoleto todo o então sistema de segurança em redes de computadores, bem como fechar gradualmente as portas das megacorporações que sobreviveram durante os quase 200 anos da computação clássica. A computação clássica estava perto do fim. E começava o que ficou conhecido como a Segunda Revolução Quântica.

O supercomputador milionário foi desligado e vendido como sucata para um ferro-velho. Sua tecnologia pouco depois foi esquecida. As antigas empresas de segurança que não haviam acreditado na nova proposta faliram. Muitos anos foram necessários para a adaptação da rede mundial de computadores à nova realidade.

O sr. Lao pensou como, no início do século XXI, todos esses conceitos (computação quântica, criptografia quântica, q-bits, protocolo BB84 e RSA etc.) eram ainda restritos a uma minoria da população mundial. E, no entanto, agora, crianças já lidavam com computadores quânticos desde os primeiros anos de escola. Infelizmente, os computadores — acreditava o sr. Lao — continuavam sendo caixas-pretas como 100 anos atrás.

Era uma manhã ensolarada de primavera. O sr. Lao olhou pela janela, apanhou a xícara de café que esquecera ao lado do teclado, recostou-se na poltrona que ficava embaixo do quadro de seu avô e rememorou toda a história, como gostava de fazer nos raros momentos de folga.

E sonhou como seria a computação quântica nos próximos 100 anos...