Ser e não ser - eis a nova questão
A computação quântica e o futuro da tecnologia

Elloá B. Guedes, Bernardo Lula Júnior

IQuanta - Instituto de Estudos em Computação e Informação Quânticas
Universidade Federal de Campina Grande
E-mail: elloa@iquanta.org.br, lula@dsc.ufcg.edu.br

A cada dia vemos os computadores se tornarem mais rápidos, os celulares ficarem menores, eletroeletrônicos estarem por toda parte e ficamos impressionados e nos perguntando que rumos a tecnologia há de tomar.

Há 50 anos, a computação ainda estava engatinhando. Os computadores, que eram verdadeiros emaranhados de fios e pesavam várias toneladas, tinham saído das mesas dos engenheiros e passaram a ser utilizados para várias operações importantes, a maioria de caráter bélico. À medida que a Física e a Química foram evoluindo, novas descobertas de materiais e de propriedades destes fizeram não somente que os computadores se tornassem menores, mas que também processassem mais rápido, ou seja, realizassem operações em menos tempo. Gordon Moore, co-fundador da Intel, conseguiu estabelecer uma lei, que recebe seu nome, baseada na observação. A lei de Moore afirma que a cada um ano e meio dobra-se a capacidade de processamento e o espaço para armazenar uma informação torna-se cada vez menor, mais especificamente, metade do espaço ocupado antes. Apesar de parecer um disparate quando enunciada 42 anos atrás, as conseqüências dessa lei são observadas ainda nos dias de hoje e é através dela que podemos justificar a existência das maravilhas tecnológicas que usufruímos.

Até aí tudo bem, temos um celular que cabe na palma da mão, um computador que podemos carregar na mochila, mas eventualmente nos esquecemos que o tempo corre e com ele a Lei de Moore insiste em se manter válida. Um ponto em particular é que ela diz que ocupamos cada vez menos espaço para armazenar informações. Antigamente, a menor unidade de informação (o bit) ocupava o equivalente à superfície de uma caixa de fósforos, hoje ocupa, em média, 0,2 μm^2. E daqui a dez anos?

A resposta a essa pergunta promove tremenda inquietação! Em meados de 2020 teremos que um bit ocupará o mesmo espaço que um átomo. E essa, apesar de parecer fantasiosa, é a realidade que provavelmente nos depararemos.

Seria fantástico alcançarmos essa possibilidade: basta lembrar a abundância de átomos que existem no universo! O preço que hoje pagamos por alguns gigas de informação talvez dê pra comprar milhões de vezes mais espaço e você já pensa que poderá armazenar sem peso na consciência a discografia completa do Elvis Presley. A lei de Moore, olhada desse ponto de vista, certamente é bastante agradável.

Porém as coisas não são tão óbvias quando estamos num mundo tão pequeno, ao nível de átomos. É como se mergulhássemos num novo universo, cheio de regras que não são visíveis no "*nosso*"mundo. Essas regras, ou melhor, leis físicas, descobertas ao longo da história por muitos físicos importantes, descrevem o comportamento das partículas quando olhadas por uma perspectiva muito próxima. Este comportamento, porém, não é tão trivial de ser compreendido, e é chamado de caráter quântico.

Vamos utilizar um exemplo prático para mostrar uma das diferenças existentes entre o mundo quântico e o que conhecemos. Veja a figura ao lado. Dependendo de qual distância ou perspectiva você olhe, é possível reconhecer imagens diferentes? Sim, existe a imagem de dois rostos que se olham e ao mesmo tempo um vaso no centro da imagem na cor branca. Ela é uma boa abstração de uma das propriedades, chamada superposição. Todas as imagens estão lá o tempo inteiro, mas caso uma ilustração dessas lhe for mostrada ao acaso, é possível prever qual delas você verá? Ou ainda, você consegue ver as duas imagens presentes ao mesmo tempo? As partículas quânticas também se comportam de modo similar, e mesmo sendo paradoxal pensar em uma partícula que se comporta dessa forma, este é apenas uma das características que as diferenciam do "*mundo*"ao qual estamos acostumados.

Os cientistas estudam como tirar proveito desse caráter para pensar em como realizar a computação, como planejar o "*computador quântico*"que a Lei de Moore prevê para daqui a alguns anos. Por exemplo, já temos uma breve noção de como será o software, a parte equivalente aos programas desse novo computador. Teoricamente, ele já consegue realizar algumas operações, inclusive mais econômicas que o computador "*clássico*".

Não somente, a computação quântica já começa a se mostrar uma preocupação em relação à computação clássica. Um exemplo interessante é a criptografia. A criptografia é a parte da computação que têm por objetivo promover a troca de mensagens sigilosas, ou seja, cujo conteúdo só possa ser entendido pelos participantes da comunicação. O método de criptografia mais utilizado atualmente se baseia na dificuldade existente em fatorar números primos muito grandes. Essa dificuldade não significa impossibilidade, mas o custo para realizá-la é tão alto, que hoje em dia utilizamos esse método de criptografia sem preocupação alguma. A computação quântica, por sua vez, possui um procedimento capaz de fatorar esses números com um custo drasticamente menor, pondo em risco toda a segurança utilizada nos dias de hoje. Não precisa se preocupar, apesar disso ser possível ainda não se conseguiu construir a parte física capaz de implementar esse procedimento a ponto de destruir a criptografia atual. Algo que vale ser citado é que também já existem soluções quânticas para a criptografia.

A tecnologia atual ainda não dispõe de meios para construir um computador quântico, mais esforços de outras áreas do conhecimento são necessários, tais como Física, Química, Engenharia de Materiais, etc. Estamos num patamar onde temos a idéia de como fazer as coisas, mas não conseguimos fazê-las na prática. Isso será um salto similar à da computação com válvulas quando houve o aparecimento do transistor, dispositivo eletrônico que permitiu que o computador se tornasse o que é hoje. Apesar de algumas empresas já terem proposto soluções para a construção do computador quântico, a comunidade científica ainda está dividida sobre a validade destas soluções.

Ah, vale lembrar que nós falamos apenas em tamanho! A lei de Moore fala também em poder de processamento e isso é um caminho que ainda é largamente estudado. Já sabemos que o computador quântico é mais econômico em alguns aspectos, a ciência se pergunta agora se ele é mais poderoso. Isso certamente tomará um pouco mais de tempo para ser respondido.

Caso a computação quântica se torne viável, acredita-se que haverá muita mudança em relação ao que temos atualmente: desde as características físicas até a forma que vamos pensar na computação. Poderemos pensar em computadores clássicos e computadores quânticos processando dados de pesquisas científicas de modo mais eficiente, fazendo com que obtenhamos resultados mais rápido, consumindo menos recursos, enfim, uma série de vantagens parece desabrochar com a computação quântica. Um novo paradigma da computação começa a engatinhar, o caráter quântico, esse "*ser e não ser*"das partículas quânticas ditando o futuro da tecnologia não só confirmará as previsões da Lei de Moore mas também trará vantagens até então dignas apenas de obras de ficção.