REVISTA DE CIÊNCIA ELEMENTAR

Computadores Quânticos

Ariel Guerreiro

DFA/ Universidade do Porto

asguerre@fc.up.pt

CITAÇÃO

Guerreiro, A. (2018) Computadores Quânticos, *Rev. Ciência Elem.*, V6(03):057. doi.org/10.24927/rce2018.057

EDITOR

José Ferreira Gomes, Universidade do Porto

EDITOR CONVIDADO

João Lopes dos Santos, Universidade do Porto

RECEBIDO EM

20 de setembro de 2018

ACEITE EM

22 de setembro de 2018

PUBLICADO EM

04 de outubro de 2018

rce.casadasciencias.org

O computador quântico é um dispositivo que utiliza os fenómenos quânticos para armazenar e processar informação. Enquanto num computador clássico os registos de memória podem assumir apenas um de dois estados, num computador quântico cada registo está num estado aparentemente estranho que contém simultaneamente propriedades de ambos estados clássicos. Também a forma como a informação é processada num computador quântico é completamente diferente e exige um controlo muito fino da matéria e das interações que ocorrem entre os seus constituintes. Se é certo que as capacidades dos primeiros protótipos sejam ainda muito limitadas, espera-se que estas venham rapidamente a ultrapassar as dos computadores atuais, quer em velocidade quer por permitirem realizar tarefas até agora inacessíveis.

O estado de um computador quântico evolui de acordo com as leis da Mecânica Quântica, o que implica que qualquer registo (*bit*), que num computador clássico só pode estar, ou no estado 0, ou no estado 1, pode encontrar-se, num computador quântico, nestes dois estados ao mesmo tempo, de um modo semelhante ao proverbial eletrão da experiência das duas fendas, que passa por ambas. Mais precisamente, desde que a interação dos registos do computador (*qubits*) com o resto do mundo seja finamente controlada, os *qubits* podem encontrar-se em estados de sobreposição dos valores 0 e 1 tempo suficiente para realizar tarefas computacionais que são inacessíveis em tempo útil a computadores clássicos.

Em 1965, Gordon E. Moore profetizou que o custo de produção por transístor num circuito impresso cairia para metade a cada 18 meses. Esta afirmação é conhecida como a lei de Moore e constitui uma descrição não só da evolução do custo de produção, mas também do poder de cálculo dos computadores, que viria a verificar-se válida por mais de 50 anos. Porém, em 2014, a IBM anunciou que esta lei estocástica deixará de ser válida brevemente e que a tecnologia baseada em microeletrónica havia entrado em estagnação, devido essencialmente ao aumento da frequência de operação dos microprocessadores e consequente incremento do consumo de energia e dissipação de calor para além dos limites físicos desta tecnologia. Assim, e para dar resposta ao aumento contínuo das necessidades de processamento de informação, os engenheiros

e cientistas procuram atualmente desenvolver novas tecnologias, sendo que uma das mais promissoras é a computação quântica.

A computação quântica é já uma realidade pois diferentes empresas desenvolveram nos últimos anos protótipos de dispositivos que se baseiam em aplicações da mecânica quântica para realizar computação de forma mais eficiente. Entre estas destacam-se o sistema da empresa D-Wave, cujo funcionamento se baseia numa combinação de processos estatísticos e térmicos num sistema quântico complexo para efetuar cálculos numéricos, e que já vende a utilização deste recurso a outras empresas. Seguindo uma abordagem tecnológica distinta, empresas como a INTEL e a IBM, disponibilizam atualmente a utilização dos seus protótipos de computadores quânticos à comunidade científica. Por outro lado, a Google e a Microsoft lançaram também os seus próprios programas de desenvolvimento de computadores quânticos. Se o século XX foi o século da construção da teoria da mecânica quântica, o século XXI inicia-se com uma verdadeira corrida tecnológica no desenvolvimento de aplicações desta teoria. Obviamente, a teoria quântica é a descrição fundamental do comportamento da matéria e da energia e qualquer tecnologia pode ser explicada com recurso a esta teoria. No fundo, desde o átomo até à maçã que cai da árvore (e os físicos adoram utilizar maçãs para explicar o Universo), tudo pode ser descrito e compreendido de uma perspetiva quântica. Porém, o que verdadeiramente distingue as chamadas tecnologias quânticas é que o seu funcionamento apenas pode ser justificado pela teoria quântica.

Para perceber o que é um computador quântico e em que difere dos computadores atuais, é importante constatar que na sua essência um computador armazena e manipula informação codificada sob a forma de dados. Informação por sua vez não é mais que uma representação das propriedades de algo. Por exemplo, podemos falar da informação sobre o estado de maturação de uma maçã (e cá temos mais uma vez uma maçã no centro de uma explicação): uma maçã pode estar verde ou madura. A informação sobre o estado de maturação permite saber essa propriedade sem ter de a medir ou observar diretamente a maçã. Para inscrever essa informação num computador é necessário codificá-la sob a forma de um estado de memória da máquina. Num computador clássico, cada registo de memória designa-se por *bit* e pode tomar um de dois estados, que por tradição chamamos de “0” e “1”. Este estado pode corresponder à orientação do momento magnético de um conjunto de átomos ou à carga elétrica acumulada num condensador, mas corresponde sempre ao estado físico de um componente da máquina. Nos computadores atuais cada registo de memória é composto por vários átomos à temperatura ambiente pelo que o seu comportamento físico é adequadamente descrido pelos modelos da física clássica.

Ocorre que, se em vez de um componente microscópico do computador, o registo de memória é algo como um único átomo, o seu comportamento tem de ser descrito pelas leis da mecânica quântica. Neste caso, o registo de memória não tem apenas dois estados “0” e “1” mas uma infinidade de estados que possuem propriedades híbridas entre os estados “0” e “1”, graças a uma propriedade conhecida com sobreposição quântica. Um computador quântico baseia-se neste tipo de registos de memória governados pelas leis quânticas, os chamados *qubits*. Notar que os eletrões que percorrem os circuitos de um computador clássico são partículas com propriedades quânticas, e nesse aspeto em nada distintas das utilizadas nos computadores quânticos. Contudo,

um impulso elétrico resulta do movimento de muitos eletrões, cada um interagindo de forma diferente com os restantes e com os átomos que vai encontrando no caminho, pelo que no final o seu estado quântico é parecido, mas não é igual. Essa variabilidade implica que o resultado não pode ser codificado no estado quântico dos eletrões, mas nas propriedades médias do seu conjunto, as quais são descritas pela teoria clássica. Num computador quântico, o controlo da evolução do estado quântico das várias partículas envolvidas é de tal forma cuidadoso que essa variabilidade é praticamente nula ou pelo menos bem conhecida, e é possível utilizar esses estados para codificar e processar informação.

Por se basear em registos de memória quânticos, um computador quântico tem necessariamente mecanismos de operação diferentes. Por exemplo, num computador clássico para operar um cálculo é necessário destruir a informação contida nos dados, aumentando a entropia do sistema e levando à produção de calor. Num computador quântico cada cálculo elementar corresponde a uma transformação quântica e reversível, pelo que o processo não gera calor. Por outro lado, as leis da mecânica quântica permitem efetuar operações e algoritmos sobre *qubits* que não são possíveis num computador clássico, assim e em princípio o poder de cálculo de um computador quântico é superior.

Note-se que num computador as operações correspondem a transformações físicas que relacionam o estado inicial com o estado final do registo de memória. Como num computador quântico os registos de memória podem assumir uma gama maior de estados do que num computador clássico, é fácil perceber que o tipo de operações permitido pelo primeiro tipo de computador é mais rico. Por outro lado, foi sugerido que a sobreposição quântica possa ser utilizada para implementar computação paralela, que permitiria em princípio codificar simultaneamente os dados correspondentes a diversos casos no mesmo registo de memória e ao efetuar sobre este as operações quânticas, processá-los de forma simultânea no mesmo circuito quântico. Infelizmente, existem ainda desafios práticos quanto à forma como os resultados obtidos via este paralelismo quântico podem ser medidos, e as vantagens desta abordagem não são ainda claras.

Porém, realizar um computador quântico não é fácil, e atualmente existem apenas uma mão cheia de protótipos capazes de realizar alguns tipos de operações ou cálculos sobre um pequeno número de *qubits*. De facto, controlar o estado quântico de um grande conjunto de *qubits* não é fácil. Primeiro é preciso arrefecer todo o sistema até temperaturas criogénicas pois, embora as operações quânticas não gerem calor, basta a muitos sistemas físicos aquecerem acima de um grau Kelvin para que as suas propriedades quânticas se tornem muito difíceis de identificar e controlar. Depois é preciso preparar o sistema num estado quântico inicial que corresponda à codificação adequada da informação que se quer processar sob a forma de *qubits*, bem como atuar sob este de forma a despoletar as transformações físicas que produzam os cálculos desejados. E por fim, medir o estado final dos *qubits* de forma extrair os resultados dos cálculos. Todos estes processos exigem um controlo físico muito sofisticado e que possui ainda grandes limitações.

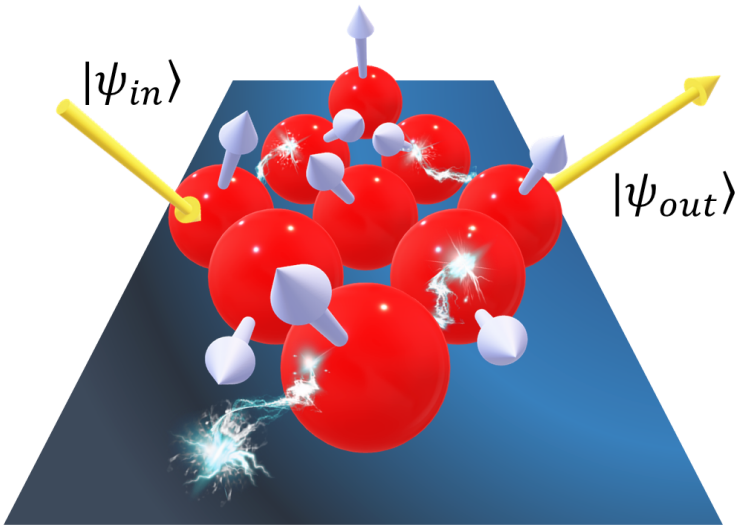

FIGURA 1. Um computador quântico é constituído por vários sistemas com propriedades marcadamente quânticas, como átomos, que ao interagirem entre si processam informação, convertendo um estado inicial, $|\psi_{in}>$ (constituído por vários *qbits*) num estado final $|\psi_{out}>$ (também ele constituído por vários *qbits*). Desenvolver um computador quântico exige um fino controlo do estado da matéria e da forma como os seus constituintes interagem entre si.

É muito provável que a transição entre a tecnologia de computadores atual e a computação quântica seja lenta e não passemos todos a ter um computador quântico de um dia para o outro. De facto, parece que a tecnologia quântica está a ter uma evolução que mimetiza a história do seu congénere clássico. Tal como o seu antepassado, os computadores quânticos ocupam hoje edifícios inteiros devido a todos os equipamentos necessários para que possam funcionar e a sua utilização está ainda limitada a cientistas e especialistas que pretendam explorar as suas capacidades. Porém, é de esperar que com o desenvolvimento desta tecnologia, o aumento do seu poder computacional e redução de tamanho, o computador quântico ganhe um papel cada vez mais importante na sociedade humana, permitindo processamento mais eficaz e rápido da informação, permitindo ao espírito e curiosidade humana espreitar onde antes não era possível.