Informação quântica

DO TELETRANSPORTE AO COMPUTADOR

Há 50 anos, muitos físicos nem mesmo ousariam mencionar a possibilidade de se fazerem experimentos com átomos ou partículas de luz individuais. Hoje, porém, essas diminutas entidades já são corriqueiramente isoladas em vários laboratórios do mundo, inclusive no Brasil. E mais: a exploração das estranhas propriedades desse microuniverso promete levar ao desenvolvimento de tecnologias que, havia pouco, só habitavam o cenário da ficção científica.

Luiz Davidovich
Instituto de Física,
Universidade Federal do Rio de Janeiro

Para quem está acostumado a observar os fenômenos naturais que se revelam no dia-a-dia, o diminuto universo das dimensões atômicas ou moleculares, regido pela chamada teoria quântica, pode parecer, no mínimo, estranho. Nele, entidades quânticas, como um elétron, podem ora se comportar como ondas, ora como corpúsculos, dependendo de como são observadas.

Segundo a física clássica, uma partícula tem seu estado bem determinado por sua posição e seu momento (o produto de sua massa por sua velocidade). Com base apenas nessas duas grandezas, é possível prever, em um determinado instante, os resultados de qualquer medida efetuada sobre ela. Mas, para uma entidade quântica (elétron, próton, nêutron, fóton etc.), não é possível prever com certeza o resultado de qualquer medida realizada sobre ela. Na verdade, o que se obtêm são apenas probabilidades de a medida fornecer os vários valores possíveis para as grandezas relevantes. Essas probabilidades podem ser inferidas a partir de uma onda associada à entidade quântica, a mesma onda que descreve as suas propriedades ondulatórias. Por exemplo, se a onda associada à partícula tiver uma grande amplitude em uma certa região do espaço, isso significa que é grande a probabilidade de se encontrar a partícula nessa região.

Mais ainda: nem mesmo é possível medir o estado de uma única entidade quântica, pois as leis da física nos obrigam a ter um conjunto muito grande delas, idealmente infinito, preparadas da mesma forma para que o estado quântico possa ser medido. Isso tem relação com uma propriedade sutil: é proibido 'clonar' uma única entidade quântica. Se pudéssemos fazer isso, poderíamos produzir um conjunto muito grande de réplicas, todas com o mesmo estado, o que permitiria medir esse estado. Além disso, qualquer medida feita sobre um sistema quântico necessariamente perturba seu estado e, portanto, o altera. No mundo clás-

QUÂNTICO

sico (ou macroscópico), porém, sempre podemos supor que é possível medir um sistema de modo que a perturbação causada seja desprezível.

Essas propriedades levaram muitos físicos a considerar, há apenas 50 anos, que a idéia de realizar experimentos com átomos ou fótons individuais era absurda, consistentemente com o fato de que a física quântica deveria ser aplicada sempre a conjuntos de sistemas – em virtude de envolver a idéia de probabilidade – e jamais a sistemas individuais. No entanto, hoje, isolar essas entidades e estudá-las individualmente passou a ser um experimento rotineiro em vários laboratórios de diversos países, inclusive do Brasil.

Informação quântica

Na última década, foram desenvolvidas, em diversos laboratórios, técnicas que permitem a manipulação individual de átomos, moléculas e fótons (figura 1). Por exemplo, através de campos eletromagnéticos, já é possível aprisionar e manipular um único átomo e fazê-lo interagir com um outro, também aprisionado, ou ainda com um único fóton, armazenado em uma 'armadilha' formada por espelhos de alta reflexão.

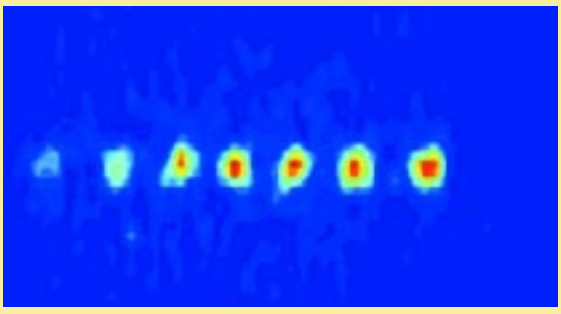


FOTO DE RAINER BLATT/UNIVERSIDADE DE INNSBRUCK (ÁUSTRIA)

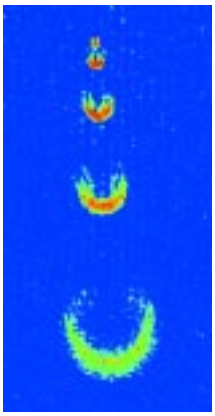
Figura 1. Íons presos por campos magnéticos poderão ser usados no desenvolvimento da computação quântica

Esses avanços possibilitaram o desenvolvimento de uma nova área de pesquisa, a chamada informação quântica, que estuda métodos para caracterizar, transmitir, armazenar, compactar e utilizar computacionalmente a informação contida em estados quânticos. Trata-se de um tema amplo e multidisciplinar que teve um desenvolvimento acelerado nos últimos anos, motivado tanto pelo interesse fundamental dos fenômenos naturais que explora quanto pelas perspectivas de aplicação em computação quântica, telecomunicação e criptografia.

Pinças e condensados

As técnicas de aprisionamento e manipulação têm permitido a investigação de propriedades sutis do mundo quântico e podem levar ao desenvolvimento de novos materiais, à construção de instrumentos de medida de altíssima sensibilidade, à implementação de computadores quânticos e à análise de moléculas biológicas. Em relação a esse último tema, feixes de *laser* – em configurações denominadas pinças ópticas – já permitem prender, mover e até mesmo esticar moléculas biológicas, como o DNA, e estudar suas propriedades mecânicas.

O aprisionamento de átomos em armadilhas eletromagnéticas levou recentemente à investigação detalhada de um fenômeno previsto ainda na



WOLFGANG KETTERLE/MIT (ESTADOS UNIDOS)

Figura 2. Pulsos de átomos oriundos de um condensado de Bose-Einstein formam o chamado 'laser de átomos'

década de 1920 por Albert Einstein (1879-1955), que o desenvolveu com base nas idéias de seu colega indiano Satyendra Bose (1894-1974). O chamado condensado de Bose-Einstein é um aglomerado de átomos que ocupa um único estado quântico e, assim, se comporta como se fosse um 'átomo gigante'.

É interessante destacar que o condensado de Bose-Einstein, de certa forma, pertence aos dois mundos: é um sistema macroscópico que exibe notáveis propriedades quânticas. Através da aplicação de feixes de ondas eletromagnéticas – na freqüência de ondas de rádio –, força-se a saída ordenada dos átomos que formam o condensado da armadilha em que estão aprisionados, formando-se então um feixe com propriedades análogas às de um *laser* e que, por isso mesmo, tem sido chamado '*laser* de átomos' (figura 2).

'*Lasers* de átomos' poderiam ser aplicados, por exemplo, em técnicas litográficas de altíssima resolução – a litografia consiste em imprimir informação sobre um substrato, resultando, por exemplo, naqueles intricados desenhos vistos em circuitos impressos. Essa nova litografia levaria a um aumento substancial da capacidade de armazenamento de informação com relação àquela feita com luz ou com elétrons. Esse aumento resulta do fato de a onda associada aos átomos ter um comprimento de onda (distância entre dois máximos sucessivos da onda) muito menor que a quantidade correspondente para fótons de luz ou elétrons que tenham a mesma velocidade dos átomos. Quanto menor o comprimento de onda, maior a resolução com a qual se pode 'escrever' sobre um substrato e, assim, maior a capacidade de armazenamento de informação.

Esses feixes atômicos poderiam também ser a base de funcionamento de um interferômetro de alta precisão. Interferômetros são aparelhos que dividem um feixe de luz em dois, reunindo os dois feixes resultantes depois que cada um deles percorre um dos 'braços' do equipamento. A divisão pode ser feita, por exemplo, com espelhos semitransparentes, que deixam passar uma parte do feixe e refletem a outra, como as vitrines onde se vê o objeto exposto e ao mesmo tempo o reflexo do observador. Após serem reunidos, os feixes interferem entre si, dando origem a franjas claras e escuras. Se um dos feixes, por alguma razão, se atrasa em relação ao outro, essas franjas se deslocam. Esse atraso pode ser provocado, por exemplo, por um movimento de rotação do aparelho ou pela presença de um campo gravitacional, com valores diferentes nos dois braços do interferômetro, devido, por exemplo, a um dos braços estar mais alto que o outro. Interferômetros podem também ser construídos com corpúsculos. Nesse caso, é a onda associada ao corpúsculo que produz interferência.

A sensibilidade de um interferômetro é tanto maior quanto menor é o comprimento de onda. Por isso, o fato de ser o comprimento de onda associado a um átomo muito menor que o de um elétron permitiria a construção de interferômetros extremamente precisos, úteis para a navegação interestelar, para a medida de constantes fundamentais e para aplicações em prospecção geológica e mineral – por exemplo, um interferômetro desse tipo permitiria a medida do campo gravitacional na superfície da Terra com precisão suficiente para detectar poços de petróleo.

TED HANSCH/UNIVERSIDADE DE MUNIQUE (ALEMANHA)

Figura 3. Possível esquema para um chip atômico: o ponto luminoso é um condensado de Bose-Einstein, mantido por campos magnéticos a uma distância de alguns mícrons da superfície do circuito integrado – a mosca dá uma idéia do grau de miniaturização

Chips atômicos

Os recentes desenvolvimentos na área de informação quântica têm permitido que uma nova geração de *chips* comece a ser investigada em vários laboratórios. Nos chamados '*chips* atômicos', em vez de elétrons, têm-se átomos individuais ou mesmo condensados de Bose-Einstein sendo conduzidos através de um circuito integrado. Diferentemente

C. MONROE/*NATURE* 21/08/97, NEWS AND VIEWS, PP. 719-720

dos *chips* eletrônicos – em que os elétrons fluem através dos fios condutores impressos em uma placa de silício –, em um *chip* atômico os átomos são mantidos 'flutuando' a alguns mícrons de uma superfície de silício, por meio de campos magnéticos criados pelo circuito integrado (figura 3).

Quando se vibra uma corda – de violão, por exemplo –, formam-se nela vales e picos que se alternam espacialmente. Uma configuração análoga, porém feita com ondas eletromagnéticas estacionárias, tem sido usada para aprisionar átomos em uma estrutura tridimensional semelhante a uma caixa de ovos (figura 4). Essa técnica tem permitido a realização de 'redes cristalinas ópticas', bem como o estudo de um fenômeno típico – porém, difícil de se obter de forma controlada – das redes cristalinas convencionais: a chamada transição de fase quântica.

Ao contrário das transições de fase usuais – que dependem da temperatura, como, por exemplo, a transformação de água em gelo –, as transições de fase quânticas dependem do valor relativo de dois tipos de efeito: a) o de interação entre as partículas; b) um efeito essencialmente quântico, o 'tunelamento', que faz com que uma partícula possa atravessar, de um 'vale' (mínimo) para outro da 'caixa de ovos', a barreira que os separa. Se os campos eletromagnéticos são fracos, predomina o efeito de tunelamento, e os átomos circulam entre as várias regiões da rede. Por outro lado, para campos suficientemente fortes, os átomos ficam presos e localizados em mínimos da rede óptica. A transição de fase corresponde precisamente à transição entre esses dois tipos de comportamento dos átomos.

Aplicações desses sistemas têm sido consideradas para a computação quântica, da qual voltaremos a falar mais adiante.

Criptografia quântica

A possibilidade de controlar individualmente cada fóton está na base da chamada criptografia quântica. A criptografia envolve a codificação de mensagens. Uma etapa essencial nesse processo é passar a 'chave' de decodificação para a pessoa que vai receber a mensagem. A manipulação de entidades quânticas isoladas permite que a transmissão dessas chaves seja feita fóton a fóton. Aliando isso à impossibilidade de clonagem, bem

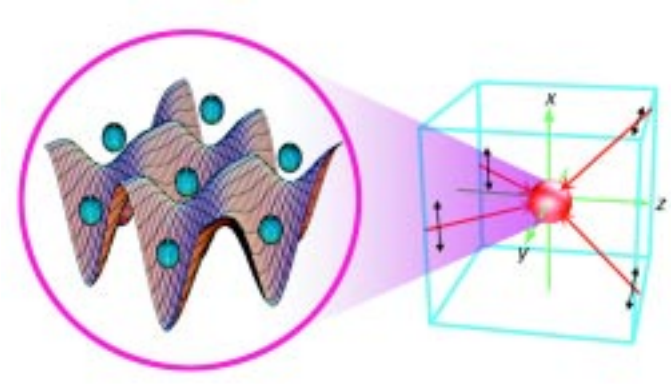


Figura 4. Esquema de uma rede óptica, com átomos aprisionados nos vales de ondas estacionárias produzidas por quatro feixes de laser

como ao fato de que qualquer medida de uma entidade quântica transforma necessariamente seu estado, tem-se uma receita ideal para tornar a transmissão de mensagens 100% seguras: se um desses fótons for interceptado, ou seja, medido, seu estado se modifica, o que pode ser verificado posteriormente pelo emissor e receptor da mensagem através da comparação, por via pública, de um subconjunto dos fótons enviados.

Se houver alguma diferença entre os fótons enviados e os recebidos, isso indica que houve tentativa de interceptação da mensagem e, portanto, a chave criptográfica transmitida deve ser descartada. Qualquer tentativa do interceptador de reproduzir o fóton interceptado, enviando a cópia ao receptor final, para que ele não desconfie da interceptação, será fadada ao fracasso, devido à impossibilidade de clonagem quântica.

Fótons gêmeos e teletransporte

Além do controle e da manipulação individual de átomos e moléculas, os pesquisadores da área de informação quântica já produzem um dos fenômenos mais intrigantes da natureza: os chamados estados emaranhados de fótons (ou 'fótons gêmeos').

Fótons gêmeos são produzidos quando se ilumina um cristal com um feixe de *laser* intenso. Existe uma certa probabilidade, que aumenta com a intensidade do *laser*, de que cada fóton do feixe incidente seja absorvido pelo cristal, ao mesmo tempo em que é produzido um par de fótons. Depois de formados, esses pares passam a ter suas propriedades fortemente correlacionadas, ou seja, qualquer medida efetuada em um deles altera as pro-

priedades do outro, mesmo que o par esteja separado por milhares de quilômetros. Daí o nome de 'fótons gêmeos' para esses pares emaranhados.

Einstein chegou a dizer que entre dois fótons emaranhados agia "uma fantasmagórica ação a distância". Porém, no início da década de 1980, foi mostrado experimentalmente que essa 'estranha' correlação existia de fato entre partículas gêmeas. Hoje, as propriedades desses estados emaranhados têm levado a aplicações em computação quântica e a demonstrações de novos processos quânticos, como o teletransporte.

Os estados emaranhados de fótons permitem uma nova forma de comunicação, baseada no envio de informação completa sobre o estado quântico de um sistema de um lugar para outro. Isso é notável, pois, para um único sistema quântico, já sabemos que não é possível medir seu estado quântico. Porém, é possível transmiti-lo, usando, para isso, um canal de comunicação quântico, formado por dois fótons gêmeos.

É possível que os fãs de ficção científica notem uma certa semelhança entre a transmissão de estados quânticos e o teletransporte da série de ficção científica *Jornada nas estrelas*. Há, no entanto, diferenças importantes: no teletransporte que está sendo demonstrado atualmente em diversos laboratórios, não é a partícula que está sendo transportada, mas sim seu estado quântico. Essa 'informação quântica' não é transportada instantaneamente, mas respeita os limites impostos pela velocidade da luz. Além disso, os cientistas só conseguem teletransportar, por enquanto, o estado de uma única partícula ou estados simples de campos eletromagnéticos, a distâncias pequenas se comparadas às espaciais.

BRUCE KANE/UNIVERSIDADE DE MARYLAND (ESTADOS UNIDOS)

Figura 5. Computação quântica com átomos de fósforo implantados em um substrato de silício, conforme proposta de Bruce Kane, da Universidade de Maryland (Estados Unidos). Esse esquema está sendo posto em prática na Austrália. Nele, os eletrodos permitem manipular os elétrons dos átomos de fósforo

Computadores quânticos

Sem dúvida, a informação quântica tem encorajado novas idéias que, por sua vez, podem levar ao desenvolvimento de novas tecnologias. Talvez, entre essas promessas, a mais popular seja a do computador quântico. Essas máquinas, baseadas em uma arquitetura revolucionária de processamento de dados e no uso da física quântica para implementação de novos algoritmos, poderiam ser exponencialmente mais rápidas que os computadores atuais – podemos entender um algoritmo como um procedimento matemático para a realização de um cálculo. É um programa de computador (*software*) que executa um algoritmo, ou seja, torna prática essa idéia.

Os computadores 'clássicos', que utilizamos hoje em dia, codificam a informação através de uma seqüência de *bits* que assumem os valores 0 e 1. Esses dois dígitos formam a base binária, que permite expressar qualquer número inteiro. Esses *bits* – que podem ser associados fisicamente, por exemplo, a cargas de capacitores – são processados por dispositivos eletrônicos que permitem a realização de operações básicas, em termos das quais qualquer computação pode ser realizada.

Já os computadores quânticos codificariam a informação através de '*qbits*' (ou *bits* quânticos) que apresentam uma propriedade extremamente sutil do mundo quântico: eles podem ser colocados em uma superposição de estados correspondentes aos valores 0 e 1 – no mundo macroscópico e 'clássico' dos computadores atuais, seria como se um *bit* pudesse

representar, simultaneamente, os valores 0 e 1. Essa superposição poderia ser materializada através, por exemplo, de um átomo que poderia estar em uma superposição de dois de seus estados.

Um conjunto de N *qbits* pode ser colocado, da mesma forma, em uma superposição de 2^N estados, cada um desses estados correspondendo a certos *qbits* no estado 0 e outros no estado 1: (000... 0), (100... 0), (010... 0), (111... 0), ... (111... 1). Esses estados codificam todos os números passíveis de serem representados por N *bits*. Isso permite aplicar uma operação física – que corresponderia a um cálculo computacional – simultaneamente a todos as entradas possíveis, realizando-se, assim, uma computação em paralelo, em vez de se calcular seqüencialmente o resultado para cada uma das entradas.

Duas motivações

São duas as motivações para o desenvolvimento de computadores quânticos. Em primeiro lugar, uma observação feita, já na década de 1960, por Gordon Moore, um dos fundadores da empresa norte-americana Intel. Segundo o que ficou conhecido como 'lei de Moore', o número de transistores na unidade central de processamento (microprocessador), bem como a velocidade de processamento, dobram a cada 18 meses. Ao mesmo tempo, cai à metade o número de átomos necessários para codificar um *bit* de informação. Nessa progressão, chegaríamos ao limite de um átomo por *bit* em torno de 2015, o que implicaria a saturação da lei de Moore. Torna-se, então, natural pensar na utilização das propriedades quânticas dos átomos para a implementação de algoritmos computacionais que permitissem aumentar a velocidade de processamento, apesar da saturação dessa lei.

A segunda motivação veio precisamente da descoberta feita, em 1994, por Peter Shor, então pesquisador da empresa AT&T (Estados Unidos), de um algoritmo quântico – para a decomposição de um número em fatores primos – exponencialmente mais rápido que o melhor algoritmo clássico conhecido. A decomposição em fatores primos (ou simplesmente fatoração) é uma operação simples para um computador – dois exemplos de decomposição em fatores primos são $18 = 2 \times 3^2$ e $30 = 2 \times 3 \times 5$. Porém, se o número for grande, o tempo consumido pelo computador para fatorar aumenta muito.

Essa dificuldade para fatorar números grandes é a base de um método criptográfico bastante utilizado hoje em dia, o método RSA – a sigla vem das iniciais de seus idealizadores, os pesquisadores Ron Rivest, Adi Shamir e Len Adleman. Porém, um computador quântico poderia fatorar um número grande – e, nesse caso, quebrar uma mensagem criptografada – em um tempo exponencialmente menor que o necessário para um computador clássico. Em outras palavras: um computador quântico poderia fazer em segundos o que o mais veloz computador atual levaria milhares de anos.

Mais tarde, outros algoritmos quânticos foram descobertos. Atualmente, há vários sistemas – ver figura 5, por exemplo – tidos como bons candidatos para tornar a computação quântica realidade. Entre esses candidatos, estão: i) íons em armadilhas magnéticas; ii) átomos e fótons em cavidades supercondutoras; iii) redes cristalinas ópticas; iv) moléculas em soluções líquidas manipuladas por ressonância nuclear magnética, a mesma técnica que permite fazer imagens do corpo humano; v) pontos quânticos (um conjunto de elétrons confinados, com poucos bilionésimos de metro de diâmetro) e impurezas em semicondutores.

No Brasil

Já há no Brasil laboratórios que realizam experiências com átomos aprisionados a baixíssimas temperaturas, fótons emaranhados, pinças ópticas, pontos quânticos e ressonância magnética nuclear. Grupos teóricos investigam propostas para a realização de operações elementares de computação quântica em diversos sistemas físicos, bem como propriedades de estados emaranhados, efeitos do ambiente em sistemas quânticos, algoritmos computacionais.

O Instituto do Milênio de Informação Quântica (IMIQ), criado no final de 2001, reúne diversos desses grupos, apoiando esforços experimentais e promovendo reuniões de trabalho e escolas sobre o tema. Procura-se, assim, realizar o potencial interdisciplinar de uma área que, em outros países, reúne físicos, químicos, matemáticos, engenheiros e cientistas da área de computação.

A complementação e modernização dos equipamentos dos laboratórios existentes, além da formação de novos grupos, aumentarão a competitividade do Brasil nessa área, na qual a inovação tecnológica é ainda incipiente, o que abre a possibilidade de ocupação de nichos por parte de países que se iniciam nesse tipo de atividade.

Na página http://omnis.if.ufrj.br/~infoquan/, podem-se obter mais informações sobre o IMIQ, incluindo a relação completa das instituições e dos pesquisadores. ■

SUGESTÕES PARA LEITURA

DAVIDOVICH, L. 'Teletransporte: uma solução em busca de um problema' (entrevista a Cássio Leite Vieira) in *Ciência Hoje* n. 137, abril de 1998.

DAVIDOVICH, L. 'O Gato de Schrödinger: do mundo quântico ao mundo clássico' in *Ciência Hoje* n. 143, outubro de 1998.

OLIVEIRA, I. S. *et al.* 'Computação Quântica – manipulando a informação oculta do mundo quântico' in *Ciência Hoje* n. 193, maio de 2003.

JOHNSON, G. *A Shortcut through Time: The Path to the Quantum Computer* (Knopf, Random House, New York, 2003).