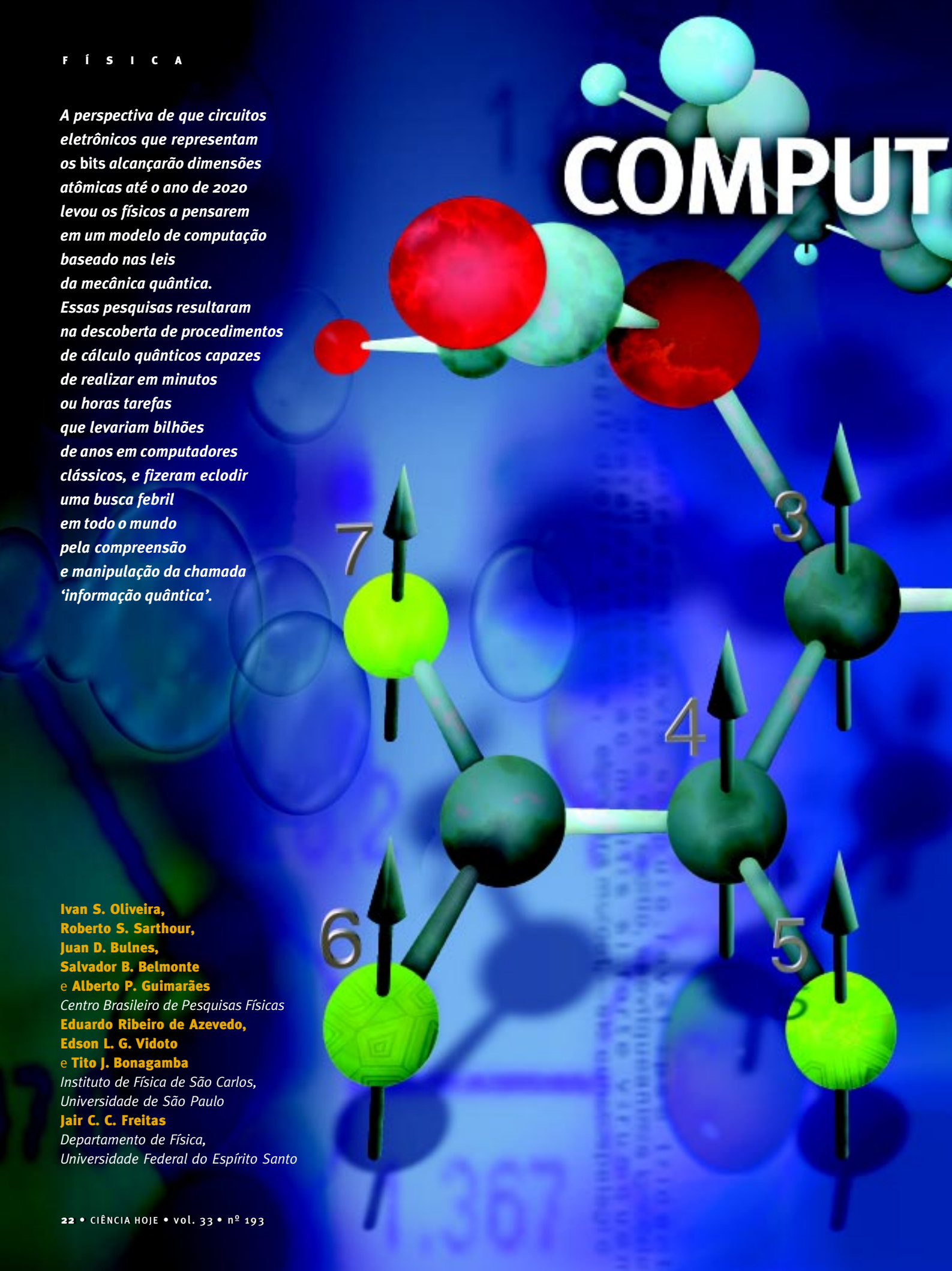
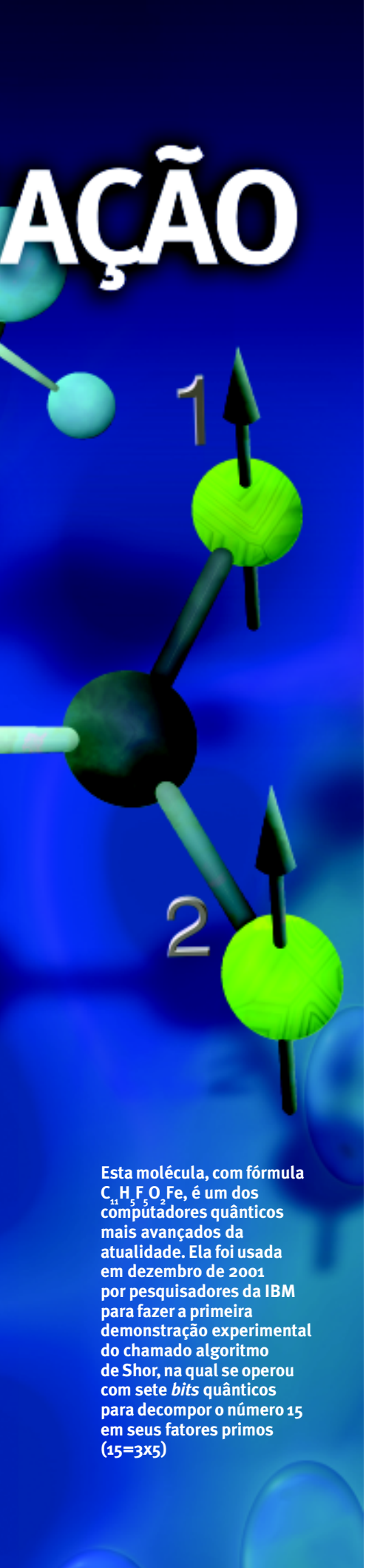
COMPUT

A perspectiva de que circuitos eletrônicos que representam os* bits *alcançarão dimensões atômicas até o ano de 2020 levou os físicos a pensarem em um modelo de computação baseado nas leis da mecânica quântica. Essas pesquisas resultaram na descoberta de procedimentos de cálculo quânticos capazes de realizar em minutos ou horas tarefas que levariam bilhões de anos em computadores clássicos, e fizeram eclodir uma busca febril em todo o mundo pela compreensão e manipulação da chamada 'informação quântica'.



Ivan S. Oliveira,
Roberto S. Sarthour,
Juan D. Bulnes,
Salvador B. Belmonte
e **Alberto P. Guimarães**
Centro Brasileiro de Pesquisas Físicas
Eduardo Ribeiro de Azevedo,
Edson L. G. Vidoto
e **Tito J. Bonagamba**
Instituto de Física de São Carlos, Universidade de São Paulo
Jair C. C. Freitas
Departamento de Física, Universidade Federal do Espírito Santo



Esta molécula, com fórmula $C_{11}H_5F_5O_2Fe$, é um dos computadores quânticos mais avançados da atualidade. Ela foi usada em dezembro de 2001 por pesquisadores da IBM para fazer a primeira demonstração experimental do chamado algoritmo de Shor, na qual se operou com sete *bits* quânticos para decompor o número 15 em seus fatores primos (15=3x5)

QUÂNTICA

Manipulando a informação oculta do mundo quântico

A mecânica quântica é uma teoria física que surgiu durante o primeiro quarto do século 20 para explicar fenômenos que ocorrem com átomos e moléculas. Ela revolucionou a maneira como os físicos explicam os fenômenos naturais.

Paralelamente ao desenvolvimento da mecânica quântica, outra revolução tomou corpo na década de 1930, através principalmente do trabalho do matemático inglês Alan Turing (1912-1954). Ele criou um modelo computacional abstrato conhecido como máquina de Turing. Trata-se de um aparato idealizado que opera com seqüências lógicas de unidades de informação chamadas *bits* (do inglês, *binary digit*), que podem adquirir um entre dois valores: '0' ou '1'. Um computador atual é uma realização física de uma máquina de Turing. Toda informação fornecida a ele é lida, processada e retornada sob a forma de seqüências de *bits*.

Máquinas de Turing independem de quais objetos físicos irão representar os *bits*. Nos computadores, esses objetos são componentes eletrônicos que existem dentro dos *chips*. Com o avanço na tecnologia de fabricação de *chips*, o número de componentes dentro deles dobra a cada ano e meio (ver 'A Lei de Moore'). Traduzindo em números de átomos necessários para representar um *bit* de informação, uma análise da Lei de Moore leva à espantosa conclusão de que, em 2020, um *bit* será representado por apenas um único átomo!

Isso significaria o limite físico natural dos computadores, pois, a partir daí, não haveria mais como aumentar a densidade de *bits* por *chip*. No entanto, na escala atômica, o paradigma clássico da máquina de Turing deixa de ser válido, pois quem governa os fenômenos nessas dimensões é a mecânica quântica.

ESTADOS SUPERPOSTOS

A mecânica quântica oferece possibilidades jamais imaginadas para um computador em termos de velocidade de processamento e manipulação da informação. Podemos entender a fonte desse poder computacional com uma analogia simples. Suponha que você tenha duas moedas e que queira usá-las para representar dois *bits* de informação. Digamos que você atribua o dígito '0' ao lado 'cara' e '1' ao lado 'coroa'. Existem, então, quatro seqüências lógicas possíveis de *bits*, como mostra a figura 1.

Por ser um objeto macroscópico – portanto governado pelas leis da física clássica –, uma moeda só pode exibir uma face de cada vez. No entanto, se as moedas fossem objetos quânticos, cada uma delas poderia ser colocada em uma estranha situação, como se as duas faces estivessem visíveis ao mesmo tempo! Isso porque estados de objetos governados pelas leis da mecânica quântica podem ser colocados em combinações de outros estados – ou superposições de estados, como preferem os físicos.

Essa propriedade, que vai totalmente contra o nosso senso comum, é inteiramente quântica, ou seja, é impossível ser observada em objetos macroscópicos (ou clássicos). Qual a conseqüência desse fenômeno para a computação? Poderíamos manipular todos os estados das duas moedas – '00', '01', '10' e '11' – simultaneamente.

Contudo, estados quânticos superpostos não podem ser observados diretamente. Por exemplo, se colocássemos uma única moeda em uma superposição de 'cara' e 'coroa' e tentássemos olhar para ela, não veríamos a superposição, mas apenas uma das possibilidades clássicas, ou seja, 'cara' ou 'coroa'.

Da mesma forma, se criássemos uma superposição dos quatro estados de duas moedas, ao tentar observá-la encontraríamos apenas uma das quatro possibilidades mostradas na figura 1. Em resumo: o ato de tentar observar estados superpostos tem como conseqüência a destruição da superposição!

Vendo por outro ângulo, estados quânticos possuem mais informação do que aquilo que podemos observar. Essa 'informação oculta' é inacessível à observação direta. Como isso pode ser útil?

OS *QUBITS*

Para se realizar operações lógicas em sistemas quânticos, precisamos definir o *bit* quântico. Este é chamado *qubit* (do inglês, *quantum bit*). Um *qubit* é um objeto que pode adquirir os valores lógicos '0', '1' ou qualquer superposição deles. É a propriedade de superposição que distingue *bits* de *qubits*.

Vários sistemas físicos podem representar *qubits*, da mesma forma que muitos sistemas clássicos podem fazer o papel de *bits*

MOEDA 1	MOEDA 2	SEQÜÊNCIA BINÁRIA	EQUIVALENTE DECIMAL
cara	cara	0 0	0
cara	coroa	0 1	1
coroa	cara	1 0	2
coroa	coroa	1 1	3

Figura 1. Seqüências lógicas possíveis para duas moedas. No caso, são atribuídos os dígitos 'o' para 'cara' e '1' para 'coroa'. Na última coluna, está o equivalente decimal para cada combinação

– moedas ou circuitos eletrônicos, por exemplo. A própria luz pode servir de meio físico no qual *qubits* são codificados. Outros exemplos são correntes elétricas em anéis supercondutores – as chamadas junções Josephson; elétrons aprisionados em sistemas conhecidos como poços quânticos; íons aprisionados em armadilhas magnéticas etc.

Um sistema físico tem sido particularmente útil para demonstrar os princípios da computação quântica: os momentos magnéticos de núcleos atômicos. A manipulação da informação quântica nesses *qubits* é feita através da técnica conhecida como Ressonância Magnética Nuclear (RMN). Mas, na prática, onde estão esses *qubits*? Nesse caso, eles ocorrem naturalmente em moléculas de algumas substâncias, como nas de clorofórmio ($CHCl_3$), onde os núcleos do carbono (C) e do hidrogênio (H) formam um sistema de dois *qubits*.

A maioria dos elementos da tabela periódica possui momento magnético em seu núcleo. O momento magnético de um núcleo é uma espécie de 'bússola quântica'. Assim como a agulha das bússolas convencionais, ele interage com campos magnéticos e tende a apontar, paralela ou antiparalelamente, na direção do campo. Associamos ao estado 'paralelo' o valor lógico '0' e ao antiparalelo o valor lógico '1'. Através da RMN, podem-se criar superposições de 'paralelo' e 'antiparalelo' (ver 'A Ressonância Magnética Nuclear').

Existem outras técnicas que podem manipular a informação quântica, como, por exemplo, a óptica, na qual os possíveis planos em que os fótons (partículas de luz) vibram representam os *qubits* – quando a luz vibra em um determinado plano, diz-se que ela está polarizada. Assim, para a direção de polarização vertical, atribui-se o valor lógico '0'; para a direção horizontal, o valor lógico '1'.

Através do uso de espelhos, divisores de feixes, detectores e outros aparatos ópticos, os *qubits* são manipulados para executarem operações lógicas.

NÚMEROS CRIPTOGRAFADOS

Computadores resolvem problemas matemáticos executando algoritmos. Um algoritmo é uma espécie de 'receita de bolo' matemática. Nos primeiros anos de escola, aprendemos algoritmos, por exemplo, para somar, subtrair,

A Lei de Moore

Em 1950, eram necessários 10^{19} átomos – ou seja, 10 bilhões de bilhões – para representar um único *bit* de informação.

Gordon Moore, fundador da empresa norte-americana de microprocessadores Intel, observou, na década de 1960 que esse número se reduzia à metade aproximadamente a cada ano e meio.

Essa relação é chamada de 'Lei de Moore'. Ela prevê que, em 2020, um *bit* será representado por um único átomo, como mostra o gráfico representado pela figura 2.

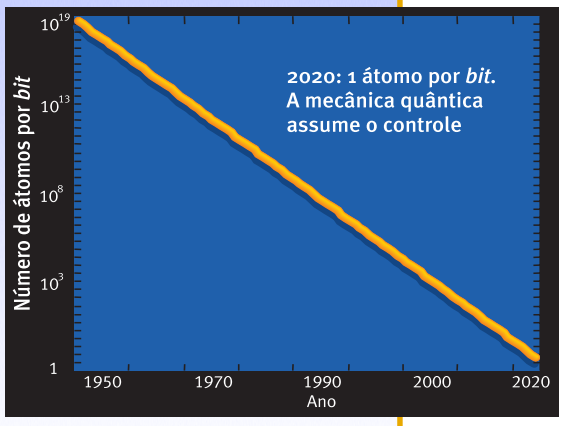


Figura 2. Previsão, segundo a Lei de Moore, para o número de átomos que representa um *bit*. Uma extrapolação dessa lei mostra que, em 2020, um *bit* será representado por um único átomo

FIGURAS CEDIDAS PELOS AUTORES

A Ressonância Magnética Nuclear

Certos núcleos atômicos possuem uma propriedade denominada momento angular – que se assemelha ao estado de rotação de um pião em torno do seu próprio eixo – e outra chamada momento magnético – que pode ser comparada ao comportamento da agulha de uma bússola.

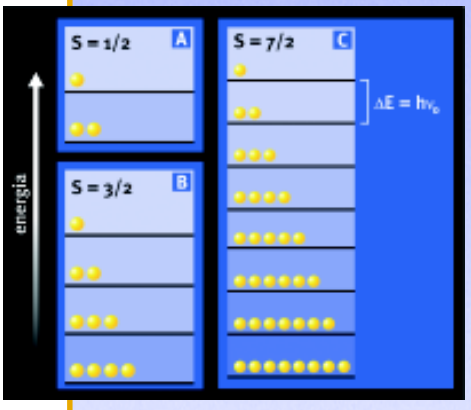


Figura 3. Níveis de energia e suas populações relativas. Em A, mostram-se os dois valores de energia possíveis para núcleos de hidrogênio (S= 1/2). Em B, os quatro níveis para os núcleos de sódio (S = 3/2). Em C, apresenta-se o esquema para o césio (S = 7/2). Ainda em C, $\Delta E = h\nu_0$ representa a quantidade de energia necessária para fazer a transição entre dois níveis contíguos. Os círculos representam esquematicamente o número de núcleos atômicos em cada nível de energia (população)

Tanto o momento angular quanto o momento magnético são proporcionais a outra grandeza denominada *spin* do núcleo (S), que só pode assumir valores inteiros ou semi-inteiros (1/2, 1, 3/2 etc.). Alguns exemplos de *spins* de núcleos atômicos: hidrogênio (S = 1/2), sódio (S = 3/2) e césio (S = 7/2).

Quando esses núcleos estão sujeitos a campos magnéticos, eles adquirem energias magnéticas cujos valores dependem basicamente de seus *spins*. Uma característica que só pode ser explicada através da mecânica quântica é que a energia dos núcleos só pode assumir certos valores específicos, discretamente distribuídos (figura 3). O número de níveis de energia é dado por uma fórmula simples: 2S + 1.

No caso dos prótons (núcleos dos átomos de hidrogênio), cujo *spin* vale 1/2, existem apenas dois valores possíveis de energia (2 x 1/2 + 1 = 2), com a maior parte dos núcleos no nível de energia mais baixa (figura 3a). No caso de núcleos com *spin* 3/2 ou 7/2, a situação é diferente, pois eles podem adquirir, respectivamente, quatro e oito valores de energia magnética (figuras 3b e 3c).

Para fazer a energia do núcleo 'saltar' para um nível imediatamente superior de energia, é preciso fornecer a ele uma energia extra, que denominaremos aqui ΔE. Isso se faz aplicando radiação eletromagnética de determinada freqüência (ν_0), cuja energia transportada é dada por $E = h\nu_0$, sendo h uma constante (figura 3c). Sabe-se que essa freqüência (ν_0) pode variar de dezenas até centenas de megahertz (MHz) – ou seja, da ordem de vários milhões de oscilações por segundo. Essa faixa de radiação eletromagnética é denominada radiofreqüência (RF) e é a mesma usada pelas emissoras de rádio para transmitir suas programações.

Assim, se aplicarmos radiação eletromagnética ao sistema de *spins* nucleares com uma freqüência próxima a ν_0, induziremos transições (ou 'saltos') entre os dois níveis, alterando as populações dos mesmos (figura 4). Desse modo, podemos manipular a quantidade de núcleos em cada nível, controlando a duração e a intensidade da radiação. Por exemplo, se desligarmos a radiação exatamente quando as populações dos dois níveis forem iguais, teremos promovido a equalização das populações entre os níveis. Nessa situação, dizemos que foi aplicado um pulso de 90° (ou $\pi/2$) – como mostra a figura 4a –, pois equivale à rotação dos momentos magnéticos com esse ângulo relativamente à direção do campo magnético, mais ou menos como se 'forçássemos', com a ajuda de um ímã, a agulha de uma bússola a se deslocar 90° no sentido anti-horário em relação à direção Norte-Sul.

No entanto, se deixarmos a radiofreqüência ligada por um tempo ainda maior, poderemos atingir uma situação em que as populações dos níveis são invertidas e, nesse caso, teremos o que denominamos pulso de 180° (ou π), visto

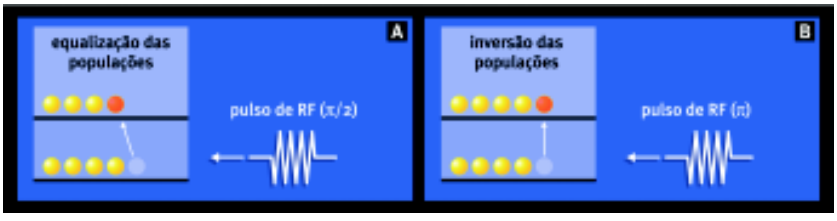


Figura 4. Modificação nas populações de núcleos atômicos induzidas pela aplicação de radiofreqüência. Em A, o número de núcleos nos dois níveis é igual. Em B, o número de núcleos é invertido

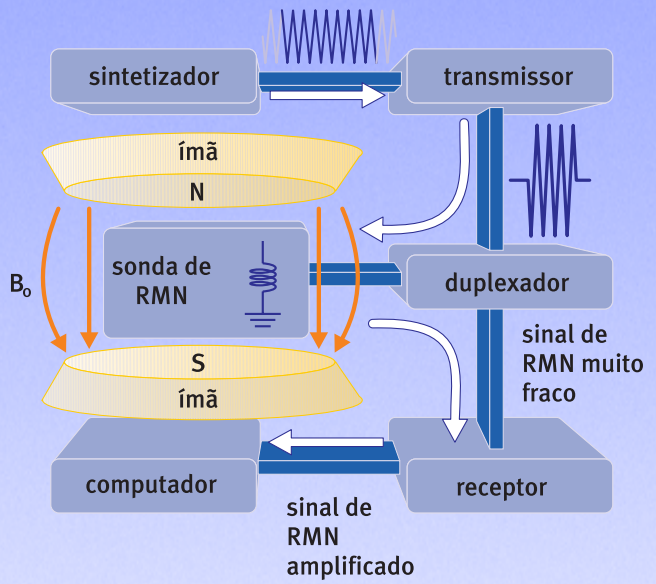


Figura 5. Esquema de equipamento usado na Ressonância Magnética Nuclear. O campo magnético é representado por B_o e a bobina pode ser vista – com a forma de uma pequena 'mola' – dentro da sonda

na figura 4b – esse caso equivaleria a fazer a agulha da bússola apontar para o Sul, forçando-a a dar uma meia-volta.

Para a realização dos experimentos de RMN, utiliza-se um equipamento como o esquematizado na figura 5. Um sintetizador produz, de forma contínua no tempo, uma corrente alternada com freqüência de oscilação ν_o, que é transformada em uma forma pulsada e amplificada através de um transmissor. Esse pulso intenso de corrente alternada alimenta uma bobina que, por sua vez, gera a radiofreqüência (RF) necessária para excitar os núcleos atômicos que se encontram no interior da mesma.

Como a sonda que contém a bobina está localizada no interior do ímã e os núcleos atômicos são excitados de modo a executarem o movimento de precessão com a mesma freqüência (ou em ressonância), após a aplicação dos pulsos de radiofreqüência surge um sinal de RMN muito fraco, que é amplificado pelo receptor e processado por um computador.

dividir, multiplicar e fatorar. Dado um número inteiro, como escrevê-lo na forma de um produto de fatores primos? Esse procedimento de fatoração sempre envolve uma etapa de 'tentativa e erro': tentamos dividir o número pelo menor dos números primos (2); se não for divisível, passamos ao primo seguinte (3) e assim sucessivamente. Dessa forma, podemos mostrar que, por exemplo, 20 = 2 x 2 x 5; 156 = 2 x 2 x 3 x 13.

Mas o que aconteceria se o número a ser fatorado fosse muito grande? Mesmo utilizando um supercomputador atual, um número com, digamos, 300 algarismos levaria milhares de anos para ser fatorado!

Longe de ser um problema, essa propriedade da fatoração possui uma tremenda utilidade prática: a criptografia. Criptografar é escrever em códigos. Suponha que você queira enviar o número de um cartão de crédito através da Internet para comprar um livro. Ao digitar o número do cartão, um programa realiza várias operações numéricas, de modo a gerar, a partir do original, um novo número, dessa vez criptografado. Esse novo número é o que viaja pela rede e, mesmo que interceptado por um *hacker*, não poderá ser utilizado, a menos que ele saiba como decompor números grandes em fatores primos. Somente quem conhecer a operação que gerou o número poderá obter o número do cartão.

SISTEMAS DE SEGURANÇA

A criptografia está na raiz dos sistemas de segurança em redes de computadores atuais. Em 1993, a crença nessa segurança foi violentamente abalada por um artigo publicado por Peter Shor, da empresa norte-americana AT&T. Ele propôs um algoritmo quântico que permite fatorar números grandes em tempos muito menores do que os gastos por algoritmos clássicos.

A figura 6 mostra algumas comparações entre esses tempos estimados para fatoração de números de comprimentos diferentes. No caso do algoritmo clássico (coluna do meio), o tempo é estimado com base na velocidade dos processadores atuais. No entanto, acredita-se que esses números não seriam muito diferentes, mesmo projetando-se a atual tecnologia para o ano de 2020.

A perplexidade diante desses números levou o físico Artur Ekert, da Universidade de Oxford (Inglaterra), e seus colegas que trabalham com criptografia quântica à seguinte observação:

Manipulando *qubits* via RMN

Operações quânticas podem ser realizadas através da técnica de RMN pulsada (ver 'A Ressonância Magnética Nuclear'). Os estados lógicos são rotulados de acordo com a orientação que o *spin* nuclear adquire no campo magnético, ou seja, 'o' se estiver paralelo ao campo e '1' no caso contrário (figura 7).

É ainda necessário que se controle a direção em que os pulsos são aplicados. Adota-se a direção do campo magnético como sendo vertical. Os pulsos são sempre aplicados ao longo do plano horizontal, em ambas direções ('x' e 'y'). Um pulso, de 90°, aplicado perpendicularmente em relação ao campo magnético, ao longo da direção 'x', por exemplo, é representado por $X(\pi/2)$, como mostra a figura 8. Esse pulso faz os momentos magnéticos dos núcleos girarem 90°. Essa situação representa uma superposição dos estados 'o' e '1'. Se a rotação for de 180° – $X(\pi)$ –, o momento magnético é girado do estado 'o' para o estado '1' , o que representa a operação lógica NÃO (figura 8).

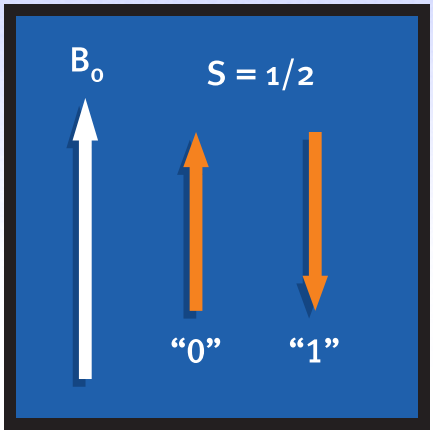


Figura 7. Dois estados possíveis para o *spin* nuclear (S = 1/2) de um próton (núcleo de hidrogênio). Os estados lógicos são rotulados segundo a orientação que o *spin* nuclear adquire no campo magnético (B_0)

Outras operações lógicas são construídas por seqüências mais complexas de pulsos, como no caso da porta *XOR* (OU-exclusivo). Para um sistema simples de dois *qubits* (A e B) e que esteja utilizando núcleos de *spin* S = 1/2, essa porta é construída com dois pulsos de radiofreqüência de 90° – $Y_A(\pi/2)$ e $X_A(\pi/2)$ –, aplicados sobre o *qubit* A, com um intervalo de tempo específico τ entre os pulsos – de modo mais técnico, essa seqüência pode ser simbolizada por $Y_A(\pi/2) \cdot \tau \cdot X_A(\pi/2)$. Mas o que vale enfatizar é o fato de essa operação inverter o

COMPRIMENTO DO NÚMERO A SER FATORADO (EM *BITS*)	TEMPO DE FATORAÇÃO POR ALGORITMO CLÁSSICO	TEMPO DE FATORAÇÃO COM O ALGORITMO DE SHOR
512	4 dias	34 segundos
1024	100 mil anos	4,5 minutos
2048	100 mil bilhões de anos	36 minutos
4096	100 bilhões de quatrilhões de anos	4,8 horas

Figura 6. Comparações entre os tempos estimados para fatoração de números de comprimentos diferentes com um algoritmo clássico e com o de Shor

"De certo modo, sistemas criptográficos contemporâneos já são inseguros. Qualquer mensagem criptografada atualmente deixará de ser secreta momentos após o primeiro computador quântico ser ligado, e os sistemas criptográficos atuais terão de ser abandonados nesse dia feliz. Confiança na morosidade do progresso tecnológico é a única base da segurança do sistema atual."

BOAS E MÁS NOTÍCIAS

Nesse aspecto, há boas e más notícias. Primeiro as boas: todos os algoritmos e as operações quânticas descobertos teoricamente foram

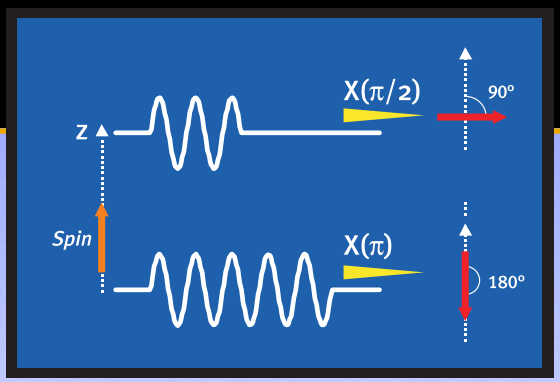
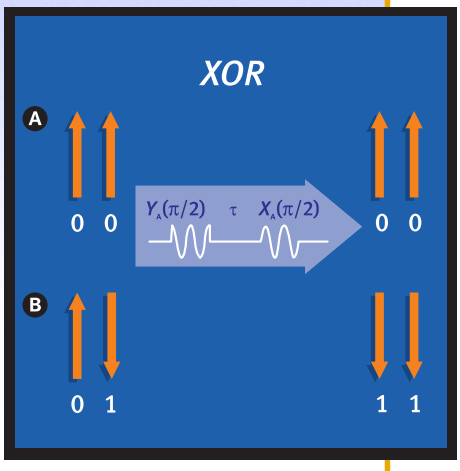


Figura 8. Um pulso de radiofreqüência aplicado perpendicularmente à direção do campo magnético – representado por X(π/2) – faz os momentos magnéticos dos núcleos girarem 90 graus, situação que representa uma superposição dos estados 'o' e '1'. Se a rotação for de 180 graus – sendo o pulso, no caso, X(π) –, o momento magnético é girado do estado 'o' para o estado '1', o que representa a operação lógica NÃO

estado lógico de um dos *qubits*, condicionado ao estado do outro. Por exemplo: 01 muda para 11 e este para 01, enquanto 00 e 10 não mudam (figura 9).

A combinação de várias operações lógicas através de seqüências de pulsos de radiofreqüência executam algoritmos quânticos através da RMN.

Figura 9. Em A, depois dos pulsos de radiofreqüência, o *qubit* permanece inalterado. Em B, o *qubit* altera seu estado. Essas mudanças representam a operação lógica conhecida por XOR



demonstrados na prática em laboratórios de física por vários grpos de pesquisa espalhados pelo mundo, inclusive no Brasil. Várias técnicas têm sido utilizadas para manipular a informação quântica, mas somente a RMN foi capaz de demonstrar todos os algoritmos e as operações lógicas quânticas propostos até agora (ver 'Manipulando *qubits* via RMN').

As más notícias: todas as demonstrações experimentais feitas até o presente utilizaram sistemas com um número muito pequeno de *qubits* para terem qualquer utilidade prática – o maior foi na demonstração do algoritmo de Shor, na qual se operou com sete *qubits* para decompor o número 15 em seus fatores primos (15 = 3 x 5). O aumento do número de *qubits* na RMN depende do desenvolvimento de novos materiais, sintetizados artificialmente. Estima-se em 1 mil o número de *qubits* necessários para que computadores quânticos superem as capacidades dos seus 'ancestrais' clássicos, mesmo projetando-se a tecnologia atual para daqui a 20 anos.

A melhor notícia, no entanto, foi dada pelo norte-americano Richard Feynman (1918-1988), um dos grandes físicos do século 20, que, no início da década de 1980, esteve envolvido nas primeiras discussões sobre computação quântica: "Parece que as leis da física não se opõem à diminuição do tamanho dos *bits* de computadores até que eles alcancem dimensões atômicas, região governada pelas leis da mecânica quântica." ■

Sugestões para leitura

GERSHENFELD, NEIL e CHUANG, ISAAC L. 'Quantum Computing with Molecules', *Scientific American*, junho de 1998.

SARTHOUR, R. S., BULNES, J. D., BELMONTE, S. B., GUIMARÃES, A. P. e OLIVEIRA, I. S. *Computação Quântica via Ressonância Magnética Nuclear*, Monografia do Centro Brasileiro de Pesquisas Físicas, janeiro de 2002. Disponível em http://www.biblioteca.cbpf.br/.

NIELSEN, M. A. e CHUANG, I. L. *Quantum Computation and Quantum Information*, Cambridge University Press, 2002.