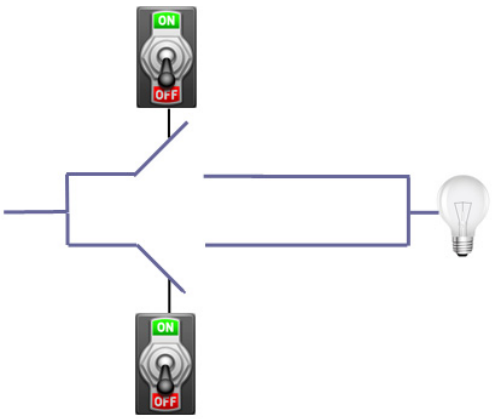
Computação quântica: Alguns (não tão) detalhes horríveis

PorMarianne Freiberger (/content/list-by-author/Marianne Freiberger)

Enviado por Marianne em 1 º de outubro de 2015

Este artigo faz parte do nosso projeto informações sobre informações, (/content/information-about-information)executado em colaboração com a FQXi (/content/information-about-information#fqxi). Clique aqui (/content/what-quantum-computing) para ler outros artigos sobre computação quântica.



Uma corrente que chega da esquerda atinge a lâmpada se um dos dois portões estiver fechado. Suponha que os dois portões estejam fechados quando os interruptores correspondentes estiverem ligados e escrevam 1 para um interruptor ligado, 0 para um interruptor desligado e 1 ou 0 para a lâmpada estar ligado ou desligado, respectivamente. Em seguida, uma entrada de dois bits (correspondente às posições do interruptor) gera uma saída de um bit (correspondente ao estado da lâmpada).

No artigo anterior, (/content/how-does-quantum-commuting-work) demos-lhe uma ideia áspera dos processos físicos que os computadores quânticos exploram para ser mais poderoso do que os comuns. Ou exploraria, se fosse possível construir computadores quânticos de grande escala poderosos o suficiente para executar tarefas úteis. Embora essa perspectiva ainda esteja a algumas décadas de distância, as pessoas entendem muita teoria da computação quântica. Usando a matemática da mecânica quântica e da lógica, você pode descobrir o que algoritmos quânticos podem fazer mesmo se você não tiver um computador real. Neste artigo olhamos para um desses algoritmos com mais detalhes: é uma versão mais simples do desenvolvido pela Deutsch e Jozsa que é discutido no artigo anterior. Você não precisa estar familiarizado com a matemática da mecânica quântica, pois vamos guiá-lo através do algoritmo dando-lhe tanta informação quanto você precisa.

Um portão muito importante

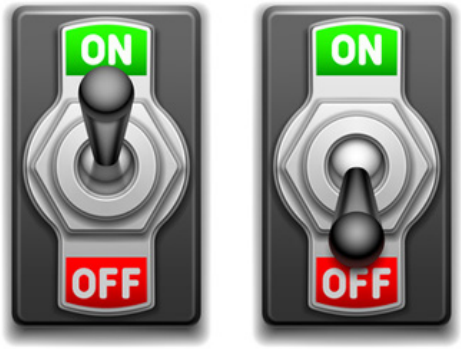
Um fato importante na ciência da computação comum é que qualquer algoritmo que você possa se importar em sonhar pode ser implementado usando uma combinação de uma pequena coleção de *portões lógicos*: como o nome sugere, estes são circuitos elétricos com portões neles, projetados para levar apenas um ou dois bits como entrada e produzir um novo pouco como saída. Um exemplo é o portão OR, mostrado à direita.

O mesmo vale para a computação quântica: uma combinação de um pequeno número de portões quânticos é suficiente para construir qualquer algoritmo quântico — que foi provado matematicamente. Um dos mais importantes é chamado de *portão Hadamard*, e pode realmente

ser construído na realidade (veja este artigo (/content/do-quantum-computers-exist) para um pouco mais de detalhes). Quando um portão Hadamard recebe um qubit no estado 0 como entrada, ele retorna um qubit como saída que está em uma superposição de 0 e 1 — são ambos simultaneamente.

Mas não é uma superposição qualquer. Como mencionamos no artigo anterior, quando você mede um sistema em superposição, ele entra em colapso e observa apenas um dos possíveis resultados. Se medirmos a saída do portão hadamard depois que ele recebe um qubit que é um 0, há uma chance de 50:50 de ver um 0 ou um 1. Os físicos têm uma maneira especial de escrever esta superposição:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$



Um qubit na superposição é como um interruptor ligado e desligado ao mesmo tempo.

Os termos $|0\rangle$ $|1\rangle$ e a posição para o qubit $+$ ser um 0 ou um 1 e o símbolo indica que temos uma superposição de ambas as possibilidades. Mas por que cada $1/\sqrt{2}$ termo vem $1/2,$ com um e não um que corresponde à probabilidade de observá-lo?

A resposta nos levaria mais fundo nos mistérios da mecânica quântica, então vamos apenas dizer isso: na vida comum, lidamos com probabilidades, que são sempre números positivos. A soma das probabilidades de resultados alternativos (como ver um 0 ou ver um 1) é sempre 1. Na mecânica quântica há um conceito mais geral, chamado *de amplitude*de probabilidade , que é permitido ser um número negativo (na verdade, amplitudes são números complexos (/content/maths-minute-complex-numbers)). As amplitudes dos resultados alternativos não precisam somar 1, mas a soma de seus quadrados faz. Os coeficientes em nossa expressão acima são amplitudes, e satisfazem essa exigência:

$$(1/\sqrt{2})^2 + (1/\sqrt{2})^2 = 1/2 + 1/2 = 1.$$

As amplitudes estão relacionadas às probabilidades através do esquartejamento: a probabilidade de ver um determinado resultado quando você faz uma medição é o quadrado do valor absoluto de sua amplitude. Assim, em nosso exemplo $1/\sqrt{2}$ acima, a amplitude $1/2,$ corresponde à probabilidade de como necessário.

Lá se foi por alimentar um qubit no estado 0 em um portão hadamard. Quando um qubit que está no estado 1 passa por ele, ele também é colocado $|1\rangle$ em uma superposição de 0 e 1, mas desta vez a amplitude de é negativa:

$$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Como isso difere do estado que temos de colocar um 0? Os quadrados das amplitudes são os mesmos em cada caso, então medir dá 50:50 de chance de ver um 0 ou um 1 em ambos os casos. A diferença está na forma como os dois estados evoluem ao longo do tempo e interagem

com outros estados ou qubits. Amplitudes de probabilidade são números complexos, que contêm mais informações do que apenas um único número positivo. De certa forma, todo o mistério da mecânica quântica, os fenômenos estranhos como a superposição que não tome com nossa experiência do mundo, está escondido nessa informação extra.

Interferência

O portão de Hadamard também nos dá um bom exemplo de outro fenômeno que é importante na computação quântica, chamado *interferência.* Para ver como isso funciona, $|0\rangle$ vamos passar por um portão Hadamard para obter a superposição

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

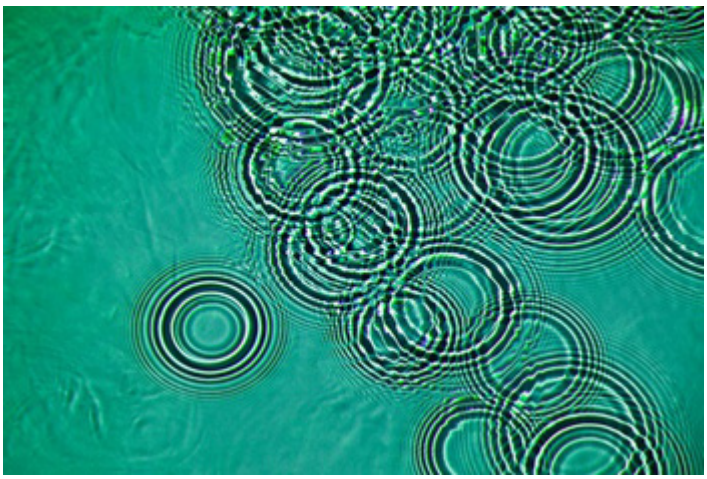
O que acontece com isso se passarmos por isso pelo portão de Hadamard de novo? Felizmente, a natureza tem sido gentil em tornar as matemáticas necessárias para resolver isso muito fácil. Podemos nos intrometer mesmo sem uma introdução formal: basta aplicar as fórmulas $|0\rangle$ de $|1\rangle,$ cima, que nos dizem o que o portão faz com um e a aos componentes individuais da superposição. Isso dá

$$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) + \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right).$$

Multiplicando os suportes é fácil ver $|1\rangle$ que os termos cancelam, deixando-nos com

$$\frac{1}{2}|0\rangle + \frac{1}{2}|0\rangle = |0\rangle.$$

A amplitude $|0\rangle$ desta expressão $1,$ é o que significa que se medirmos 0o qubit agora, definitivamente veremos um .



As ondas podem interferir construtivamente, re-serendo umas às outras, ou destrutivamente, cancelando umas às outras.

Interferência é exatamente esse cancelamento ou somamento de termos. Há *interferênciadestrutiva,* onde os coeficientes $|1\rangle$ de um termo — em nosso exemplo — cancelam, para que o termo desapareça. E há também interferência *construtiva,* com coeficientes somando. Foi o que aconteceu $|0\rangle$ com o termo, em nosso exemplo. As pessoas muitas vezes pensam nisso em termos de ondas, que também podem interferir construtivaou ou destrutivamente (veja aqui (https://en.wikipedia.org/wiki/Interference_(wave_propagation)) uma explicação).

Interferência significa que $|0\rangle$ começar com e aplicar o portão Hadamard duas vezes dá-lhe de volta a inicial $|0\rangle$:

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \rightarrow |0\rangle.$$

Você pode convencer a si mesmo que a coisa análoga acontece quando você começa com um $|1\rangle$:

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \rightarrow |1\rangle.$$

Um exemplo

Agora vamos voltar ao algoritmo desenvolvido por Deutsch e Jozsa, que usamos como exemplo no artigo anterior. A tarefa a desempenhar era verificar se uma função que toma bit-strings de 0s e 1s como entrada é *constante* ou *equilibrada*. Constante significa que a função aloca o mesmo valor, 0 ou 1, para todas as cordas de bit. Equilibrado significa que ele aloca um 1 a exatamente metade das cordas bit e um 0 para a outra metade.

A situação mais simples possível é quando as cordas bit-strings que formam a entrada da função têm apenas um pouco de comprimento. Uma função f constante seria:

$$f(0) = 0 \text{ and } f(1) = 0,$$

Ou

$$f(0) = 1 \text{ and } f(1) = 1.$$

E uma função equilibrada seria ou

$$f(0) = 1 \text{ and } f(1) = 0,$$

Ou

$$f(0) = 0 \text{ and } f(1) = 1.$$

Se você está trabalhando com um computador clássico, então um programa que descobre se a função é constante ou 0 equilibrada precisa procurar $1.$ os valores da função duas vezes: uma vez para verificar seu valor e uma vez para verificar se não há uma maneira mais rápida de encontrar a resposta para sua pergunta. O que Deutsch e Jozsa mostraram em 1992 é que há um algoritmo $0\ 1$ quântico que pode procurar o valor da função tanto para e simultaneamente e depois dizer se a função é constante ou equilibrada.

A ideia geral

O algoritmo usa dois fatos básicos. O primeiro fato envolve o estado de superposição

$$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Você pode alterar este estado em 1 seu negativo simplesmente adicionando a $1 + 1$ cada componente, 2usando *adição binária*, o que significa que é igual, não a , mas a 0. Isso dá

$$\frac{|0+1\rangle - |1+1\rangle}{\sqrt{2}} = \frac{|1\rangle - |0\rangle}{\sqrt{2}} = -\frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Vamos ter isso em mente como um método potencial para mudar de sinal.

O segundo fato é o que já vimos acima. Que um portão Hadamard muda os estados de superposição

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \text{and} \quad \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

em $|0\rangle$ $|1\rangle$ e, respectivamente.

Agora suponha que você está lidando com um estado de superposição semelhante, $f$mas com os sinais das duas amplitudes determinadas pelos valores da função . Vamos chamar este $|\psi\rangle$ estado:

$$|\psi\rangle = \frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}.$$

Isso significa que $|0\rangle$ a amplitude de $f(0) = 1$ tem um $f(0) = 0.$ sinal negativo se e $|1\rangle.$ um positivo do mesmo vale para a amplitude de Uma função constante, portanto, lhe daria

$$|\psi\rangle = \pm\frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

e uma função equilibrada

$$|\psi\rangle = \pm\frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Quando aplicamos o portão hadamard ao estado $|\psi\rangle,$ as placas simplesmente passam pelo processo. Uma função constante resulta em um $|0\rangle$ ou a $-|0\rangle.$ qualquer o que for, quando fizermos uma medição, definitivamente veremos um $0.$

Uma função equilibrada resulta $|1\rangle$ em $-|1\rangle.$ um ou a seja o que for, quando fizermos uma medição, definitivamente veremos um $1.$

Portanto, se pudermos produzir $|\psi\rangle$ o Estado de alguma forma, o portão hadamard nos dará a resposta à nossa pergunta, seja f constante ou equilibrada, com certeza.

O algoritmo

Agora vamos juntar tudo isso e ver como o algoritmo funciona. Uma vez que é baseado em dois fatos, você pode não se surpreender que ele usa dois qubits. Primeiro note que para responder f à questão de se é constante ou equilibrado, se fazemos isso de forma clássica ou usando computação quântica, obviamente $f$precisamos 0 assumir 1 que o computador tem algum $f(0)$ $f(1)$ método para "olhar para cima", ou computação, valores de : dado um ou um que ele precisa ser capaz de descobrir o que ou é. Isso é algo que tomamos como um dado, e é por isso que chamamos esse método de *caixa preta*: sabemos o que ele faz, mas não nos importamos como ele faz.

We can equally-well assume that we have a black box that works with two pieces of information, an *input register* and an *output register*. In the case of classical bits, given an input register set to i (which is a 0 or a 1) and an output register set to j, (also a 0 or a 1) the black box finds $f(i)$ and adds it to j, giving $i, j + f(i)$ as the result. The addition here is again binary (and hints towards our first fact above). Our box is just another way of telling us what $f(i)$ is, and in terms of answering our question, this doesn't make a difference: we would still need to use the box twice to decide if the function is constant or balanced.

In the quantum context the registers are qubits and the black box is a quantum gate which transforms the two-bit system made up of $|i\rangle$ and $|j\rangle$ (where i and j are 0 or 1) into $|i\rangle$ and $|j + f(i)\rangle$.

And here comes the trick. To produce the state ψ we apply the box with input register

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

and with output register

$$\frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

O registro de entrada $\psi.$ será transformado em A transformação envolve $f$nada mais do que potenciais interruptores de sinais (dependendo) e estes serão realizados com a ajuda do registro de saída, que, como se diz acima, é capaz de realizar essa tarefa.

Uma $|\psi\rangle$ vez produzido desta forma (com um uso de sua caixa preta) simplesmente f usamos o portão Hadamard para descobrir se é constante ou equilibrado.

O cálculo

Para mostrar que nossa caixa realmente faz a coisa certa, fazemos uso do fato muito conveniente de que nosso sistema de dois bits pode ser matematicamente representado como um produto:

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right),$$

que pode ser reescrito como

$$\frac{1}{\sqrt{2}}\left(|0\rangle\frac{(|0\rangle - |1\rangle)}{\sqrt{2}} + |1\rangle\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}\right). \quad (1)$$

Para ver o que a caixa preta faz com o termo

$$|0\rangle\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

simplesmente vemos o que ele faz com $|0\rangle - |1\rangle.$ cada componente da superposição Isso dá:

$$|0\rangle\frac{(|0 + f(0)\rangle - |1 + f(0)\rangle)}{\sqrt{2}}.$$

Quando $f(0) = 0$, isso é justo

$$|0\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}.$$

Mas $f(0) = 1$, quando um acima nos diz que temos

$$|0\rangle \frac{-(|0\rangle - |1\rangle)}{\sqrt{2}}.$$

Juntando isso (passando a potencial mudança de sinal através da expressão) temos

$$(-1)^{f(0)}|0\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}. \quad (2)$$

Da mesma forma, a caixa preta vira o termo

$$|1\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

Em

$$(-1)^{f(1)}|1\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}. \quad (3)$$

Substituindo (2) e (3) de volta para (1) dá

$$\begin{aligned}
&\frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} + (-1)^{f(1)}|1\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}\right) \\
=&\left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\
=&|\psi\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}.
\end{aligned}$$

Aqui está $|\psi\rangle$ o estado que estávamos atrás!

O algoritmo de Deutsch e Jozsa foi um avanço porque foi o primeiro algoritmo quântico que foi comprovadamente melhor do que um clássico: ele precisava de apenas uma chance de olhar para os valores da função (simultaneamente para 0 e 1) em vez de dois. Mais tarde, eles generalizaram o algoritmo para trabalhar para funções que não tomam apenas 0s e 1s como entrada, mas strings deles (ver o artigo anterior (/content/how-does-quantum-commuting-work)). Eles provaram que, neste caso, o algoritmo quântico é exponencialmente mais rápido do que sua contraparte clássica.

Isso é tudo muito excitante, mas é útil? O problema que o algoritmo Deutsch-Jozsa resolve não é particularmente útil no mundo real. Que outras tarefas quânticas podem ter um desempenho melhor do que as clássicas? E quão longe estamos de ter computadores quânticos totalmente funcionais? Para descobrir, leia os seguintes artigos:

- O que os computadores quânticos podem fazer? (/content/what-can-quantum-computers-do)
- Os computadores quânticos existem? (/content/do-quantum-computers-exist)

Sobre este artigo

Marianne Freiberger (/content/people/index.html#marianne) é Editora da *Plus*. Ela gostaria de agradecer a Richard Jozsa (http://www.damtp.cam.ac.uk/people/r.jozsa/), Leigh Trapnell Professor de Física Quântica na Universidade de Cambridge, por suas explicações extremamente úteis, muito pacientes e geralmente inestimáveis.

Richard Jozsa

Adicione novo comentário (/content/comment/reply/6395#comment-form)

Comentários

O Artigo (/content/comment/8637#comment-8637)

Permalink (/content/comment/8637#comment-8637) Apresentado por Mike Channon em 25 de janeiro de 2018

O diagrama no início deste artigo é enganoso. Dado que o circuito está aberto a menos que ambos os interruptores sejam fechados, a declaração inicial parece estar incorreta.

Resposta (/content/comment/reply/6395/8637)

Eu pensei que isso no início (/content/comment/8757#comment-8757)

Permalink (/content/comment/8757#comment-8757) Enviado por Jim Howe em 4 de abril de 2018

Eu pensei que isso à primeira vista também, mas deve-se supor que ambos os lados do circuito mostrado se conectam fora da porção mostrada. Como os dois interruptores estão em paralelo, se ambos forem fechados, o circuito será concluído.

Resposta (/content/comment/reply/6395/8757)

Usar um monte de fótons em vez de qubits individuais parece melhor (/content/comment/8718#comment-8718)

Permalink (/content/comment/8718#comment-8718) Apresentado por Hal em 7 de março de 2018

Então, pelo que entendi isso, um grupo de qubits únicos nunca dará tantos detalhes quanto precisamos, melhor fazer uma grande série de fótons de pares individualmente emaranhados, então você pode ler muito mais pontos de dados de uma equação, usando apenas um emaranhado para cada medição.

Resposta (/content/comment/reply/6395/8718)

Adição Binária (/content/comment/10050#comment-10050)

Permalink (/content/comment/10050#comment-10050) Apresentado por Jeremy L. em 23 de outubro de 2019

De que forma o resultado da adição binária de 1+1 =0? Estamos nos referindo ao valor do dígito e as informações restantes são retiradas ou algo assim? Muito ligado a isso.

Resposta (/content/comment/reply/6395/10050)