Aula 22: Física Quântica

Bárbara Amaral
Instituto de Física da USP

Referências

- B. Amaral, A. Baraviera, M. Terra Cunha. Mecânica Quântica pra Matemáticos em Formação. Seção 2.14 e cap. 8.
- Nielsen e Chuang. Quantum Information and Quantum Computation. Subsec. 2.2.8.

Os postulados da Física Quântica

Dois Bits Quânticos

Um bit clássico

Variável que pode assumir dois valores: 0 e 1.

Um bit quântico

Um bit quântico

Temos dois estados extremais $|0\rangle$ e $|1\rangle$.

Um bit quântico

Temos dois estados extremais $|0\rangle$ e $|1\rangle$.

O sistema pode estar em superposição desses dois estados.

Um bit quântico

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

Dois bits clássicos

Variáveis que podem assumir quatro valores: 00, 01, 10 e 11.

Dois bits quânticos

Dois bits quânticos

Temos quatro estados extremais $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$.

Dois bits quânticos

Temos quatro estados extremais $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$.

O sistema pode estar em superposição desses quatro estados.

Dois bits quânticos

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle.$$

Postulado 4

Se o espaço de estados de um sistema é $\mathcal{H}_1$ e o espaço de estados de outro sistema é $\mathcal{H}_2$, o espaço de estados do sistema composto é $\mathcal{H}_1 \otimes \mathcal{H}_2$.

A Matemática

O Espaço $\mathbb{C}^2 \otimes \mathbb{C}^2 \simeq \mathbb{C}^4$

Sejam V e W espaços vetoriais complexos, $|v\rangle \in V$ e $|w\rangle \in W$. Criamos um novo elemento $|v\rangle \otimes |w\rangle$, chamado produto tensorial de $|v\rangle$ com $|w\rangle$.

O produto tensorial dos espaços vetoriais V e W, denotado $V \otimes W$, será o espaço vetorial gerado pelos vetores da forma $|v\rangle \otimes |w\rangle$.

1. $(\lambda|v\rangle) \otimes |w\rangle = \lambda|v\rangle \otimes |w\rangle = |v\rangle \otimes (\lambda|w\rangle)$;
2. $(|u\rangle + |v\rangle) \otimes |w\rangle = |u\rangle \otimes |w\rangle + |v\rangle \otimes |w\rangle$;
3. $|v\rangle \otimes (|w\rangle + |z\rangle) = |v\rangle \otimes |w\rangle + |v\rangle \otimes |z\rangle$.

Exercício

Sejam $\{|v_i\rangle\}_{i=1}^{m}$ e $\{|w_j\rangle\}_{j=1}^{n}$ bases para V e W, respectivamente.

1. Mostre que $\{|v_i\rangle \otimes |w_j\rangle\}$ é uma base para $V \otimes W$.

2. Determine a dimensão de $V \otimes W$.

Base para $\mathbb{C}^2 \otimes \mathbb{C}^2$:

$$|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$$

$$|v\rangle \otimes |w\rangle \equiv |v\rangle|w\rangle \equiv |vw\rangle.$$

Base para $\mathbb{C}^2 \otimes \mathbb{C}^2$:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

Produto Escalar

Para $|u\rangle, |v\rangle \in V$ e $|w\rangle, |z\rangle \in W$, define-se o produto escalar em $V \otimes W$ por

$$(\langle u| \otimes \langle z|)(|v\rangle \otimes |w\rangle) = \langle u|v\rangle\langle z|w\rangle.$$

Vetores decomponíveis e emaranhamento

Vetores da forma $|v\rangle \otimes |w\rangle$ são chamados decomponíveis.

$$|\phi\rangle = |v\rangle \otimes |w\rangle$$

- Pode ser preparado localmente;

$$|\phi\rangle = |v\rangle \otimes |w\rangle$$

- Pode ser preparado localmente;
- Testes locais dão resultados independentes;

$$|\phi\rangle = |v\rangle \otimes |w\rangle$$

- Pode ser preparado localmente;
- Testes locais dão resultados independentes;
- O estado posterior de um qbit não é afetado por testes no outro.

Exercício

Mostre que

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

não é decomponível.

Vetores não decomponíveis são chamados emaranhados.

$|\phi\rangle \neq |v\rangle \otimes |w\rangle$

- Não pode ser preparado localmente;

$|\phi\rangle \neq |v\rangle \otimes |w\rangle$

- Não pode ser preparado localmente;
- Testes locais (em geral) exibem correlações;

$$|\phi\rangle \neq |v\rangle \otimes |w\rangle$$

- Não pode ser preparado localmente;
- Testes locais (em geral) exibem correlações;
- Correlação entre os estados finais dos qubits.

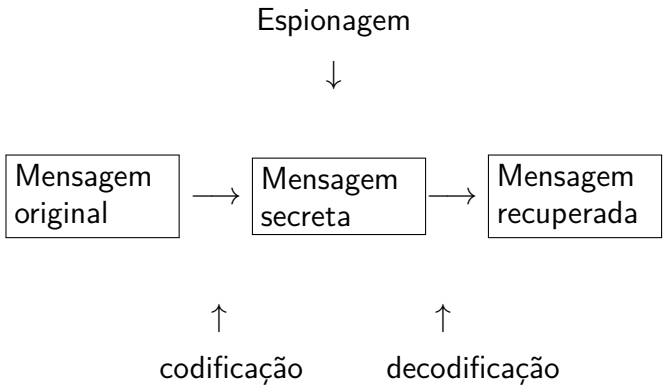
O estado de cada um dos qubits individuais não pode ser associado a um vetor em seu espaço de estados!

Estados de Bell

$$
\begin{aligned}
|\Phi_{\pm}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \\
|\Psi_{\pm}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).
\end{aligned}
$$

Distribuição de chave quântica

Criptografia de chave privada



Informação codificada em bits

Para mandar uma mensagem com n bits, precisamos de uma chave também com n bits.

$$
\begin{array}{rll}
 & 011011101001 & \text{msg original} \\
+ & 101100011010 & \text{chave} \\
\hline
 & 110111110011 & \text{msg criptografada}
\end{array}
$$

Para que a comunicação seja segura, devemos trocar a chave a cada uso.

Distribuição de chave quântica

A criptografia quântica permite o estabelecimento de chaves para a criptografia de chave privada.

Estado Emaranhado

$$|\Phi_+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Estado Emaranhado

$$|\Phi_+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

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

Teste ZZ

As respostas de Alice e Bob são sempre iguais!

Teste XX

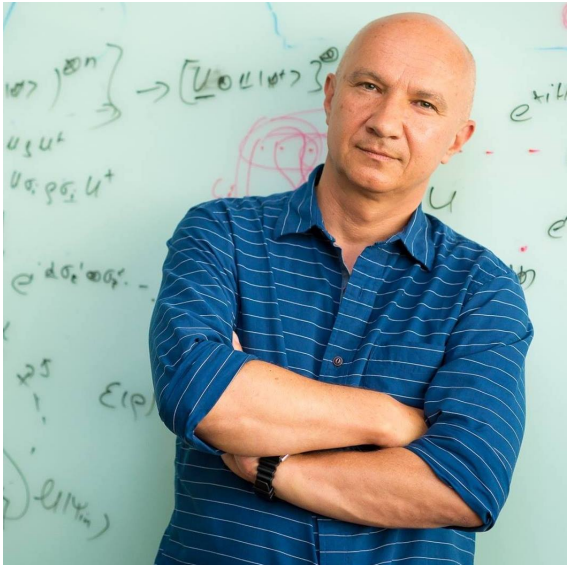
As respostas de Alice e Bob são sempre iguais!

Teste XZ ou ZX

Não existe correlação entre as respostas de Alice e Bob.

Essa propriedade do estado $|\Phi_+\rangle$ é a base de um protocolo de distribuição de chave quântica chamado Ekert91.

Protocolo Ekert 1991



Primeiro Passo

Para estabelecer uma chave com n bits, as duas partes envolvidas no protocolo, Alice e Bob, recebem n pares de qubits no estado $|\Phi_+\rangle$.

Segundo Passo

Para cada par, Alice e Bob escolhem um teste X ou Z aleatoriamente e independentemente e medem seu qubit usando o teste escolhido.

Ao final desse processo, Alice e Bob possuem uma sequência de bits.

Quando Alice e Bob têm certeza de que seus bits são iguais?

Quando realizam os mesmos testes!

Terceiro Passo

Alice e Bob anunciam que testes realizaram. Eles descartam os bits em que os testes foram diferentes e guardam os bits em que os testes foram iguais.

Alice e Bob possuem agora uma sequência perfeitamente correlacionada de bits, ou seja, uma chave criptográfica.

Por que esse protocolo é seguro?

A presença de uma espiã altera as correlações entre as respostas de Alice e Bob.

Verificação de erros

Quarto Passo

Bob envia a Alice uma fração dos bits correlacionados obtidos nesse processo.

Qualquer erro pode ser detectado por Alice se ela comparar seus bits com os bits enviados por Bob!

Se temos uma espiã tentando obter a informação sobre o bit enviado por Alice, os bits de Bob não estarão mais perfeitamente correlacionados os bits de Alice!

Referências

- Quantum Computer Science, David Mermin.
- Nielsen e Chuang, cap. 4.
- Quantum supremacy using a programmable superconducting processor, Nature (2019).

Descrição matemática

Bit clássico: álgebra booleana.

Bit quântico: álgebra linear.

Portas lógicas

Porta lógica clássica

Função que leva uma sequência de bits em outra.

Porta lógica clássica

Função que leva uma sequência de bits em outra.

$$0 \mapsto 0 \qquad 1 \mapsto 1$$

$$0 \mapsto 1 \qquad 1 \mapsto 0$$

$$00 \mapsto 00 \qquad 01 \mapsto 10 \qquad 10 \mapsto 01 \qquad 11 \mapsto 11$$

Porta lógica quântica

Função que leva um vetor em outro.

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

Medições

Medição clássica

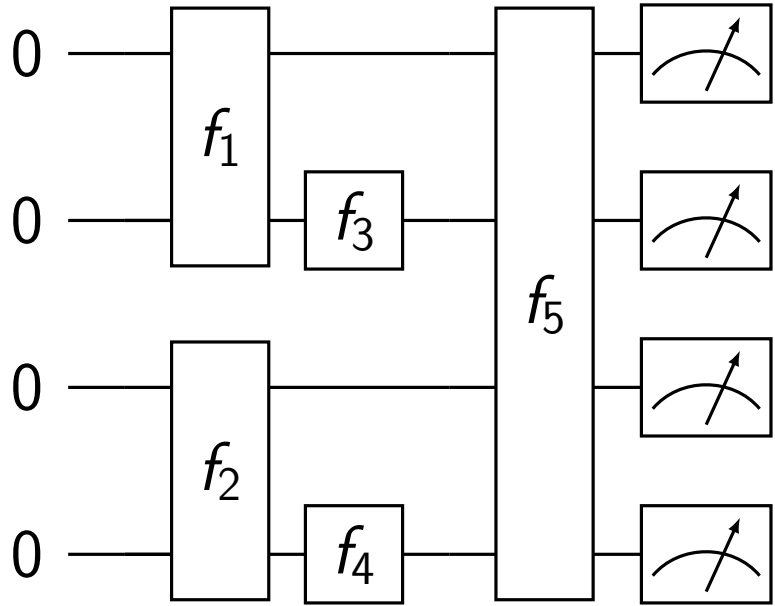
Ler os bits.

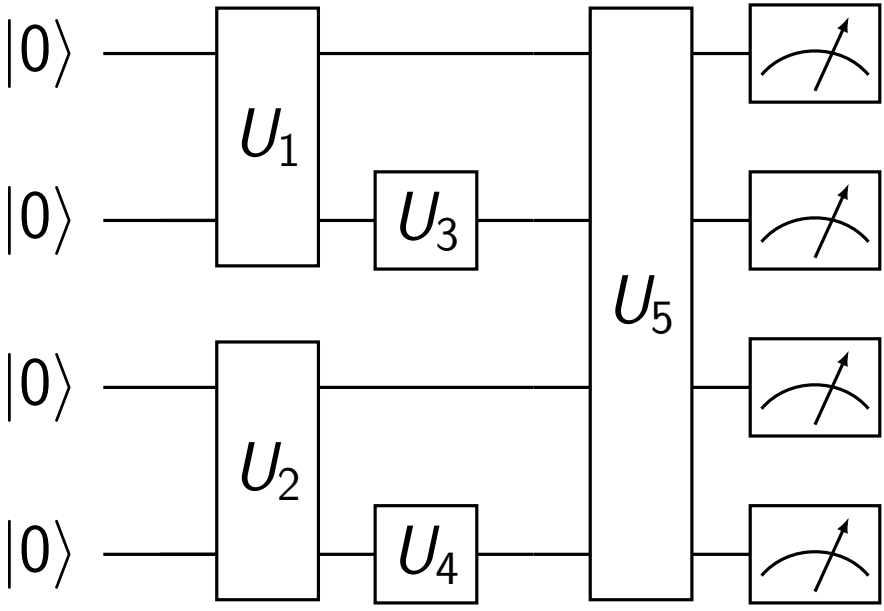
Medição quântica

Em um teste podemos apenas distinguir entre os estados $|0\rangle$ e $|1\rangle$.

$$p(0) = |a_0|^2$$
$$p(1) = |a_1|^2$$

Algoritmos


0
0
0
0
f_1
f_2
f_3
f_4
f_5


$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
U_1
U_2
U_3
U_4
U_5

O que é vantagem computacional quântica?

O limiar em que os computadores quânticos passam a fazer coisas que nenhum computador clássico pode fazer é chamado de vantagem computacional quântica.

Para alcançar a vantagem quântica, um computador quântico teria que realizar qualquer cálculo que, para todos os efeitos práticos, um computador clássico não consiga realizar.

Para alcançar a vantagem quântica, um computador quântico teria que realizar qualquer cálculo que, para todos os efeitos práticos, um computador clássico não consiga realizar.

Não necessariamente um cálculo útil...

Pode não ser útil agora, mas...

Construir um computador quântico que supera computadores clássicos - mesmo na solução de um único problema inútil - pode nos ensinar coisas que ajudarão a construir computadores quânticos úteis no futuro.

Não importa se é inútil. É uma marca importante de qualquer forma.

Tese estendida de Church-Turing: um computador clássico pode executar com eficiência qualquer cálculo que qualquer outro tipo de computador pode executar com eficiência.

Tese estendida de Church-Turing: um computador clássico pode executar com eficiência qualquer cálculo que qualquer outro tipo de computador pode executar com eficiência.

A vantagem computacional quântica seria a primeira violação experimental desse princípio.

Como demonstrar vantagem quântica?

Resolvendo eficientemente em um computador quântico um problema que não pode ser resolvido em um computador clássico.

Um sistema quântico pode ser projetado para executar um cálculo complexo o suficiente e com erros baixos o suficiente para fornecer uma aceleração quântica em relação aos algoritmos clássicos?

Um sistema quântico pode ser projetado para executar um cálculo complexo o suficiente e com erros baixos o suficiente para fornecer uma aceleração quântica em relação aos algoritmos clássicos?

Podemos formular um problema difícil para um computador clássico, mas fácil para computador quântico?

Candidatos à vantagem quântica

Fornecem evidências teóricas muito fortes da intratabilidade clássica, enquanto esperam ser fisicamente realizados a longo prazo...

Candidatos à vantagem quântica

Fornecem evidências teóricas muito fortes da intratabilidade clássica, enquanto esperam ser fisicamente realizados a longo prazo...

...ou...

Candidatos à vantagem quântica

Fornecem evidências teóricas muito fortes da intratabilidade clássica, enquanto esperam ser fisicamente realizados a longo prazo...

...ou...

...excelentes perspectivas de realização física no curto prazo, fornecendo evidências mais fracas de intratabilidade clássica.

Este artigo mostra que essas categorias se interceptam fornecendo fortes evidências teóricas da intratabilidade clássica para o candidato principal da última categoria: amostragem de circuitos aleatórios.

A. Bouland, B. Fefferman, C. Nirkhe, U. Vazirani, **Quantum Supremacy and the Complexity of Random Circuit Sampling** (2018).

Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5

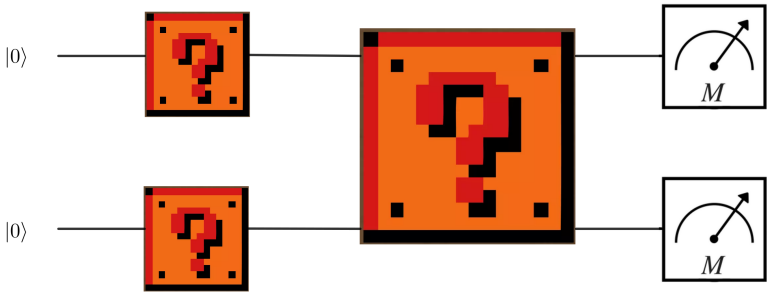
Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], Dave Bacon[1], Joseph C. Bardin[1,2], Rami Barends[1], Rupak Biswas[3], Sergio Boixo[1], Fernando G. S. L. Brandao[1,4], David A. Buell[1], Brian Burkett[1], Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Roberto Collins[1], William Courtney[1], Andrew Dunsworth[1], Edward Farhi[1], Brooks Foxen[1,5], Austin Fowler[1], Craig Gidney[1], Marissa Giustina[1], Rob Graff[1], Keith Guerin[1], Steve Habegger[1], Matthew P. Harrigan[1], Michael J. Hartmann[1,6], Alan Ho[1], Markus Hoffmann[1], Trent Huang[1], Travis S. Humble[7], Sergei V. Isakov[1], Evan Jeffrey[1], Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Kechedzhi[1], Julian Kelly[1], Paul V. Klimov[1], Sergey Knysh[1], Alexander Korotkov[1,8], Fedor Kostritsa[1], David Landhuis[1], Mike Lindmark[1], Erik Lucero[1], Dmitry Lyakh[9], Salvatore Mandrà[3,10], Jarrod R. McClean[1], Matthew McEwen[5], Anthony Megrant[1], Xiao Mi[1], Kristel Michielsen[11,12], Masoud Mohseni[1], Josh Mutus[1], Ofer Naaman[1], Matthew Neeley[1], Charles Neill[1], Murphy Yuezhen Niu[1], Eric Ostby[1], Andre Petukhov[1], John C. Platt[1], Chris Quintana[1], Eleanor G. Rieffel[3], Pedram Roushan[1], Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. Satzinger[1], Vadim Smelyanskiy[1], Kevin J. Sung[1,13], Matthew D. Trevithick[1], Amit Vainsencher[1], Benjamin Villalonga[1,14], Theodore White[1], Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], Hartmut Neven[1] & John M. Martinis[1,5]*

Amostragem de Circuito Aleatório


|0⟩
|0⟩
M
M

$$a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

Distribuição de probabilidade

$$p(00) = |a_{00}|^2$$
$$p(01) = |a_{01}|^2$$
$$p(10) = |a_{10}|^2$$
$$p(11) = |a_{11}|^2$$

Pedimos ao computador que produza sequências de bits seguindo corretamente essa distribuição de probabilidade.

Considere um circuito que atue em 50 qubits.

Considere um circuito que atue em 50 qubits.

No final do circuito, os 50 qubits estão em uma superposição de 2^{50} estados possíveis.

Se você medir os qubits, obteremos como resposta uma única sequência de 50 bits.

Se você medir os qubits, obteremos como resposta uma única sequência de 50 bits.

É como jogar um dado, exceto que, em vez de seis possibilidades, você tem 2^{50} ou 1 quadrilhão de possibilidades e nem todas têm a mesma probabilidade de ocorrer.

Os computadores quânticos devem ser capazes de produzir com eficiência uma série de amostras desse circuito aleatório que seguem a distribuição de probabilidade correta.

Os computadores quânticos devem ser capazes de produzir com eficiência uma série de amostras desse circuito aleatório que seguem a distribuição de probabilidade correta.

Para computadores clássicos, no entanto, não conhecemos nenhum algoritmo eficiente para gerar essas amostras.

Quais são os desafios?

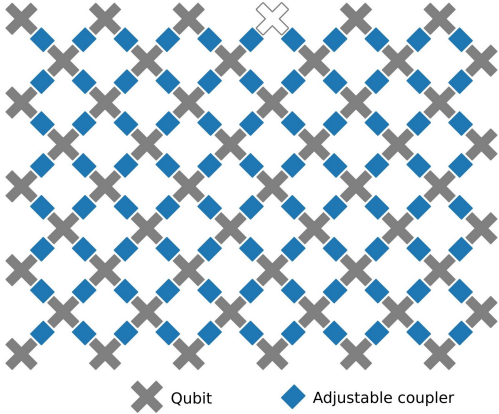
Enquanto os circuitos quânticos permanecerem pequenos, os computadores clássicos podem simulá-los com eficiência.

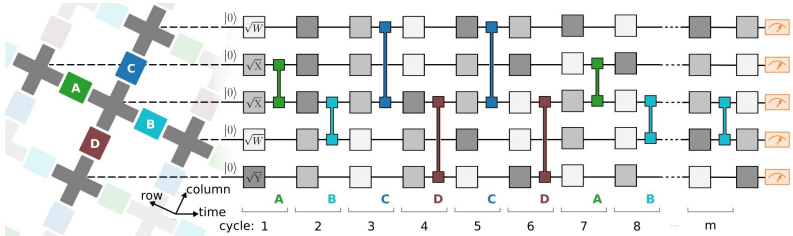
Enquanto os circuitos quânticos permanecerem pequenos, os computadores clássicos podem simulá-los com eficiência.

Para demonstrar a superioridade quântica através do problema de amostragem de circuitos aleatórios, precisamos ser capazes de construir circuitos quânticos de um tamanho mínimo.

À medida que o número de qubits e portas aumenta, o mesmo ocorre com a taxa de erros. E se a taxa de erro for muito alta, os computadores quânticos perdem sua vantagem sobre os clássicos.

Precisamos de um circuito relativamente grande e com baixa taxa de erros.


Qubit
Adjustable coupler


C
A
B
D
row
column
time
|0⟩
√W
√X
√Y
A
B
C
D
C
D
A
B
cycle: 1
2
3
4
5
6
7
8
m

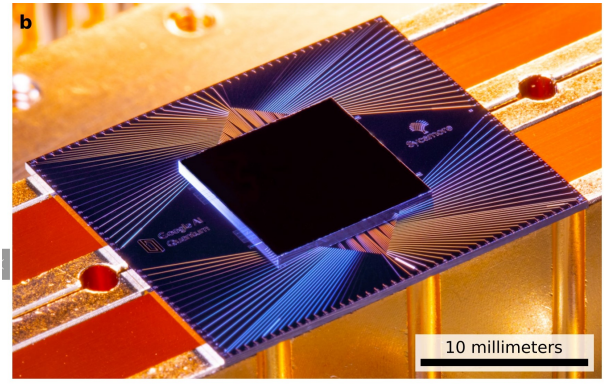


FIG. 1. **The Sycamore processor. a,** Layout of processor showing a rectangular array of 54 qubits (gray), each connected to its four nearest neighbors with couplers (blue). Inoperable qubit is outlined. **b,** Optical image of the Sycamore chip.

We are only one creative algorithm away from valuable near-term applications.

CERTIFIED RANDOMNESS FROM QUANTUM SUPREMACY

I'll describe a novel application for near-term quantum computers with 50-70 qubits: namely, generating cryptographic random bits, whose randomness can be certified even if the quantum computer is untrusted (e.g., has been backdoored by an adversary). Unlike schemes based on Bell inequality violation, ours requires only a single device able to solve classically hard sampling problems. Our protocol harvests the outputs of the sampling process and feeds them into a randomness extractor, while occasionally verifying the outputs using exponential classical time. I'll also compare to the beautiful independent work of Brakerski et al., who proposed a scheme for the same problem that has much more efficient verification, but that probably can't be implemented on near-term devices. Paper still in preparation.

SHARE

RESEARCH ARTICLE

Hartree-Fock on a superconducting qubit quantum computer

Google AI Quantum and Collaborators*,†, Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Bare…
+ See all authors and affiliations

Science 28 Aug 2020:
Vol. 369, Issue 6507, pp. 1084-1089
DOI: 10.1126/science.abb9811

Twelve-qubit quantum computing for chemistry

NEWS · 14 OCTOBER 2020

First room-temperature superconductor excites — and baffles — scientists

A compound of hydrogen, carbon and sulfur has broken a symbolic barrier — but its high pressure conditions make it difficult to analyse.

Davide Castelvecchi