El reto de la computación cuántica: calcular lo imposible.

Joaquín KELLER

24 de marzo de 2026

Academia Nacional de la Ingeniería y el Hábitat
Comisión de Ciencia, Tecnología e Innovación

INFORMÁTICA ingeniería

Universidad Monteávila

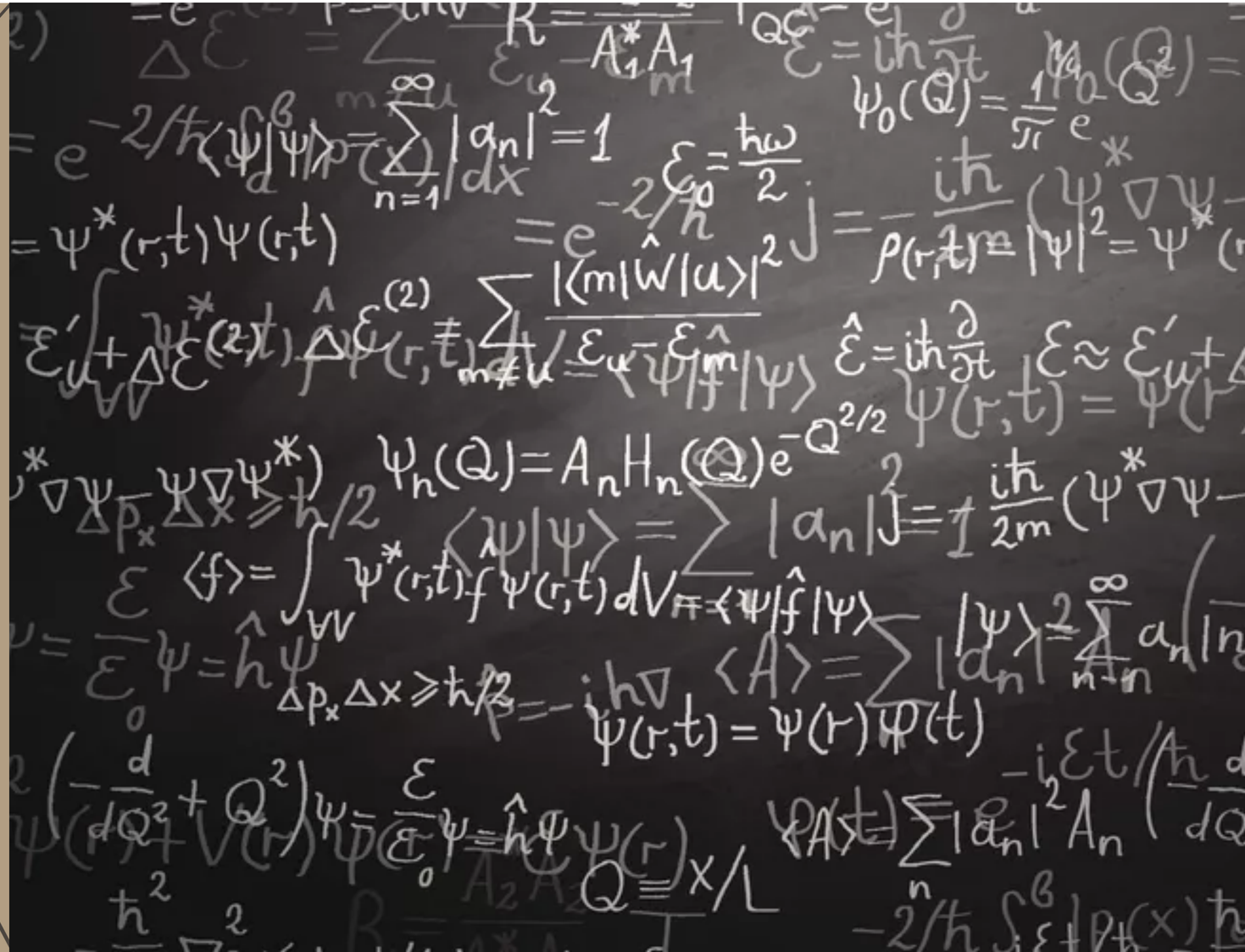
postgrado ucab

EL RETO DE LA COMPUTACIÓN CUÁNTICA: CALCULAR LO IMPOSIBLE

JOAQUÍN KELLER GONZÁLEZ

Investigador en quantum machine learning y algorítmica cuántica

Computación Cuántica ?!!



INVESTMENTS / NEWS / STARTUPS

TECHINASIA

Miguel Cordon · 11 May 2020 · 2 min read

Singapore quantum computing startup Entropica Labs bags $1.8m in seed funding

Founders of Entropica Labs (from left): Tommaso Demarie, Ewan Munro, and Joaquin Keller / Photo credit: Entropica Labs

IEEE COMPUTER SOCIETY IEEE

2020 IEEE International Conference on Quantum Computing and Engineering (QCE)

Polyadic Quantum Classifier

Year: 2020, Pages: 22-29
DOI Bookmark: 10.1109/QCE49297.2020.00013

Authors

William Cappelletti, Entropica Labs,Singapore
Rebecca Erbanni, Entropica Labs,Singapore
Joaquín Keller, Entropica Labs,Singapore

Abstract

We introduce here a supervised quantum machine learning algorithm for multi-class classification on NISQ architectures. A parametric quantum circuit is trained to output a specific bit string corresponding to the class of the input datapoint. We train and test it on an IBMq 5-qubit quantum computer and the algorithm shows good accuracy - compared to a classical machine learning model - for ternary classification of the Iris dataset and an

Un poco de historia...

1981:
Richard Feynman — *Simulating Physics with Computers, «Nature is quantum, dammit!»*

1985:
David Deutsch — *Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer*

1992:
Algoritmo de Deutsch–Jozsa (resultado teórico sin aplicación directa)
Un algoritmo cuántico exponencialmente más rápido que los algoritmos clásicos

1994:
El algoritmo de Peter Shor para factorizar números enteros (rompe la criptografía RSA)
Exponencialmente más rápido que cualquier algoritmo clásico

Cuán más rápido es eso ?

Romper una clave RSA de 2048 bits

Computación Clásica

El mejor algoritmo clásico:

10^{34} operaciones

1000 millones de años

En la supercomputadora El Capitán
- 1.8 exaFLOPS
- 1M CPU - 10M GPU
- 100M de veces mas rápido que un PC de gaming

Computación Cuántica

El algoritmo cuántico de Shor:

Cuán más rápido es eso ?

Romper una clave RSA de 2048 bits

Computación Clásica

El mejor algoritmo clásico:

10^{34} operaciones
1000 millones de años

En la supercomputadora El Capitán
- 1.8 exaFLOPS
- 1M CPU - 10M GPU
- 100M de veces mas rápido que un PC de gaming

Computación Cuántica

El algoritmo cuántico de Shor:

10^{7} operaciones
8 horas

En una computadora cuántica
- ~20M de qubits físicos, 8192 qubits lógicos
- 1M Qops/s por qubit
- (qubits superconductores o fotónicos)

Work in progress… posible en el 2030?

Hardware (qubits físicos)

1998: Primera computadora cuántica: 2-qubit

2000: 7-qubit

2006: 12-qubit

2017: IBM 17-qubit, Rigetti 19-qubit, Google 22-qubit

2018: IBM 50-qubit, Google 72-qubit, ionQ 79-qubit

2022: IBM 433-qubit, Pasqal 300-qubit

2023: IBM 1121-qubit

Qubits físicos vs qubits lógicos

- Los qubits lógicos son objetos teóricos, sin error
- Los qubits físicos, vienen con ruido, errores
- 1998: Surface code
  algoritmo de corrección de errores
- 1000 qubits físicos de 2023 —> 1 qubit lógico
- 1 qubit lógico: nivel de error no significativo

Qubits lógicos

- **Diciembre 2024**: Google anuncia Willow, una computadora cuántica de 105 qubits físicos, con fidelidad de 99.7% y por corrección de error logra 1-qubit lógico
- **Noviembre 2025**: Quantinuum anuncia Helios de 98 qubits físicos, con fidelidad de 99.921% y por corrección de error logra 50-qubit lógicos
- En 2024 entramos en la era de los qubits lógicos...
- Varios centenares de qubits lógicos para poder hacer algo útil... en 2027?

Evaluar la potencia de una computadora cuántica

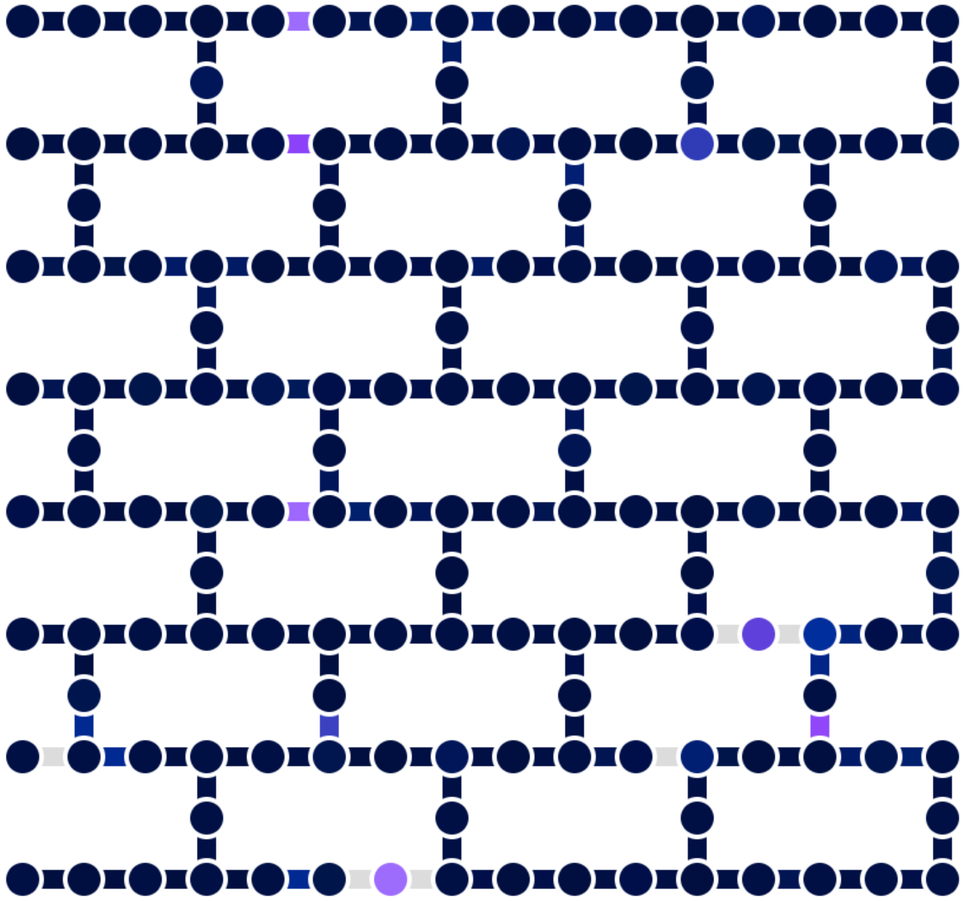
- Cuantos qubits lógicos
  (cuantos qubits físicos + tasa de error)

- Velocidad de las operaciones sobre los qubits

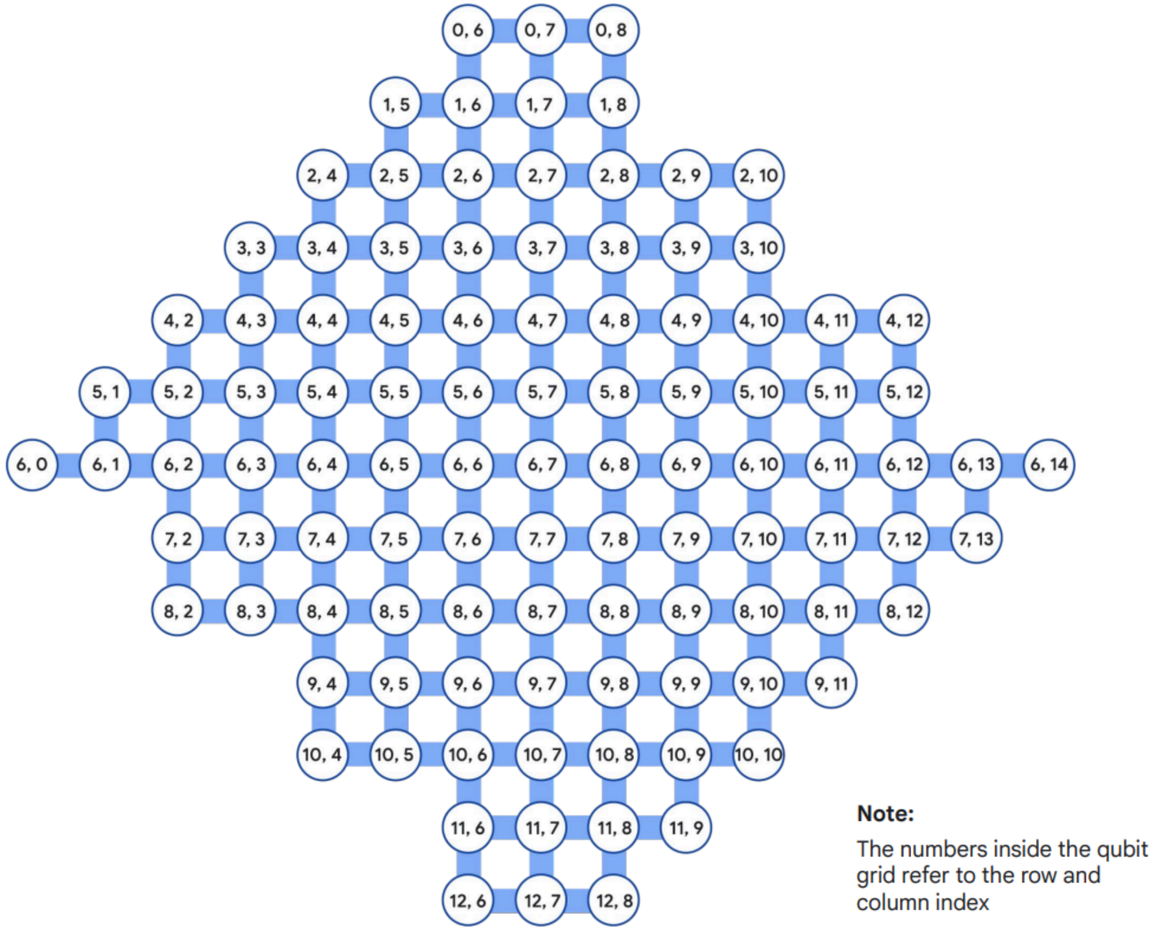
- Longitud máxima de los «programas» cuánticos

- Conectividad de los qubits

Conectividad de los qubits



IBM Q Heron r2 157-qubit



Google Willow 105-qubit

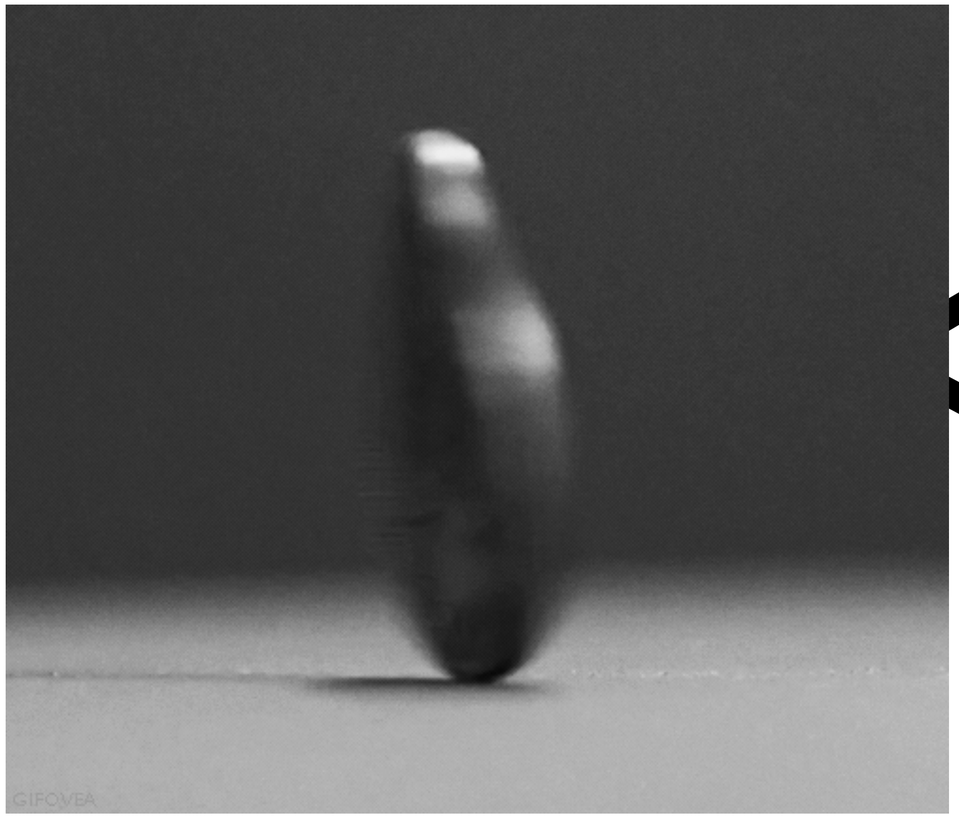
Tecnologías de Hardware

- Superconductores: Google, IBM, Rigetti, Alibaba
- iones atrapados: ionQ, Quantinuum (Honeywell), AQT, Universal Quantum, Huayi Boao
- Fotónico: Xanadu, PsiQuantum, Jiuzhang
- Átomos fríos: Pasqal, ColdQuanta, QuEra, Atom
- Qubits de gato: Amazon, Alice&Bob
- Marjorana: Microsoft — Spin qubits: Silicon Quantum Computing — …

El hardware cuántico es difícil

- Los qubits necesitan estar aislados para existir
- Los qubits se tienen que poder manipular
- Los qubits son inestables, de corta duración

Qubit

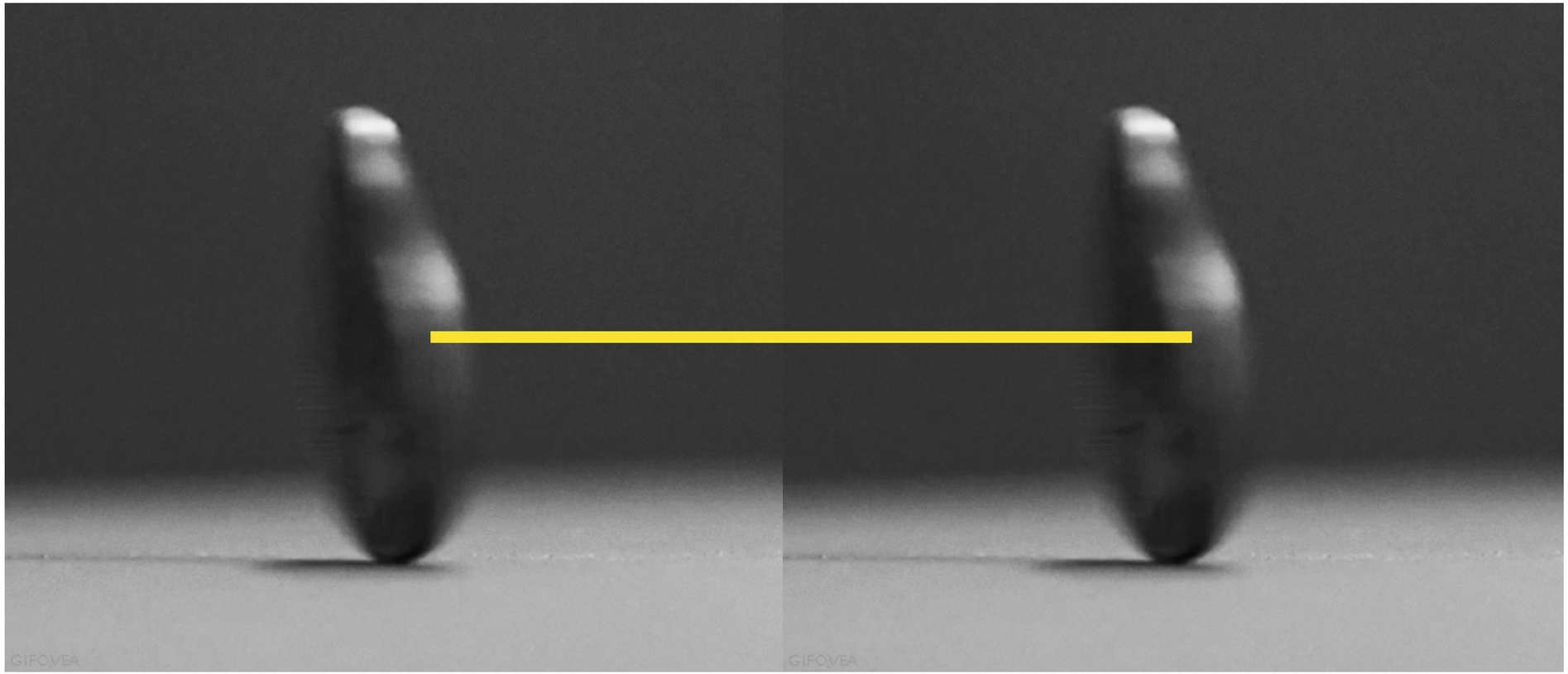


0

Medición

1

Qubits entrelazados



Qubits entrelazados

Estado cuántico de 1-qubit

a_0 0
a_1 1

a_0, a_1 ‘amplitudes’ de probabilidad

las amplitudes son números complejos

$a_0, a_1 \in \mathbb{C}$

La amplitud permite calcula la probabilidad: $p = |a|^2$

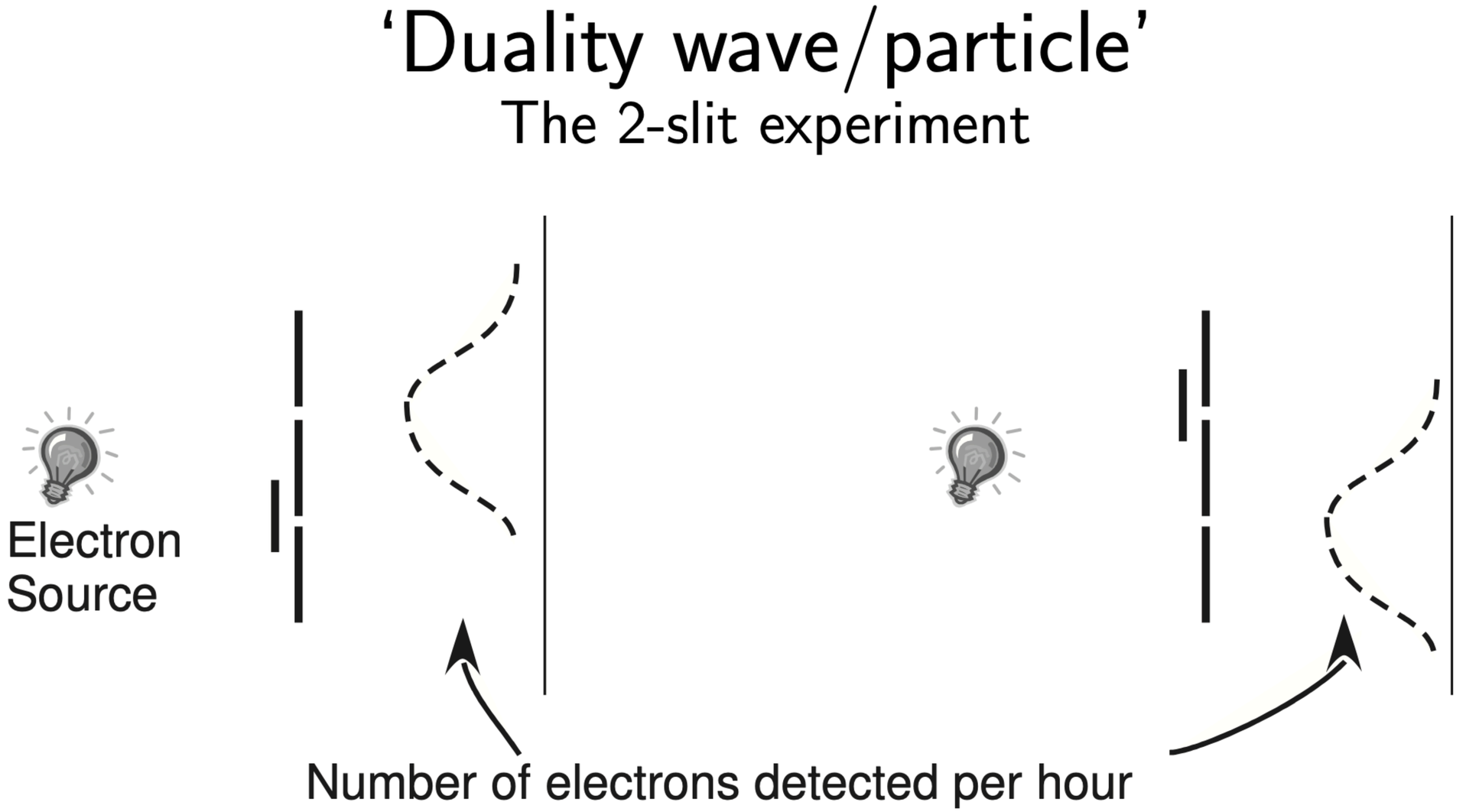


Figure 10.1 In the 2-slit experiment an electron source is placed between a wall with two slits and a detector array. When one slit is covered then, as expected, the number of electron detected is largest directly behind the open slit.

Feynman: *"negative probabilities"*

Interference

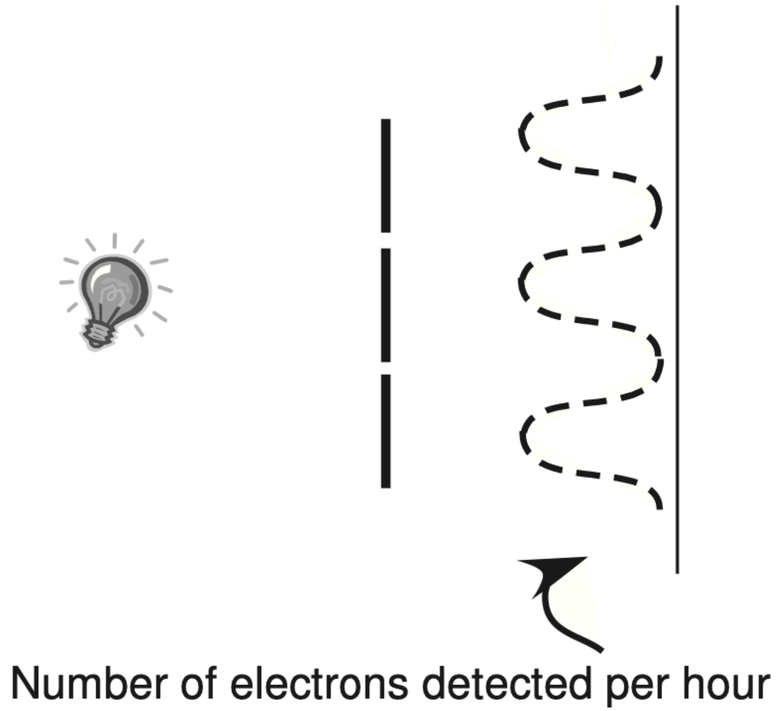
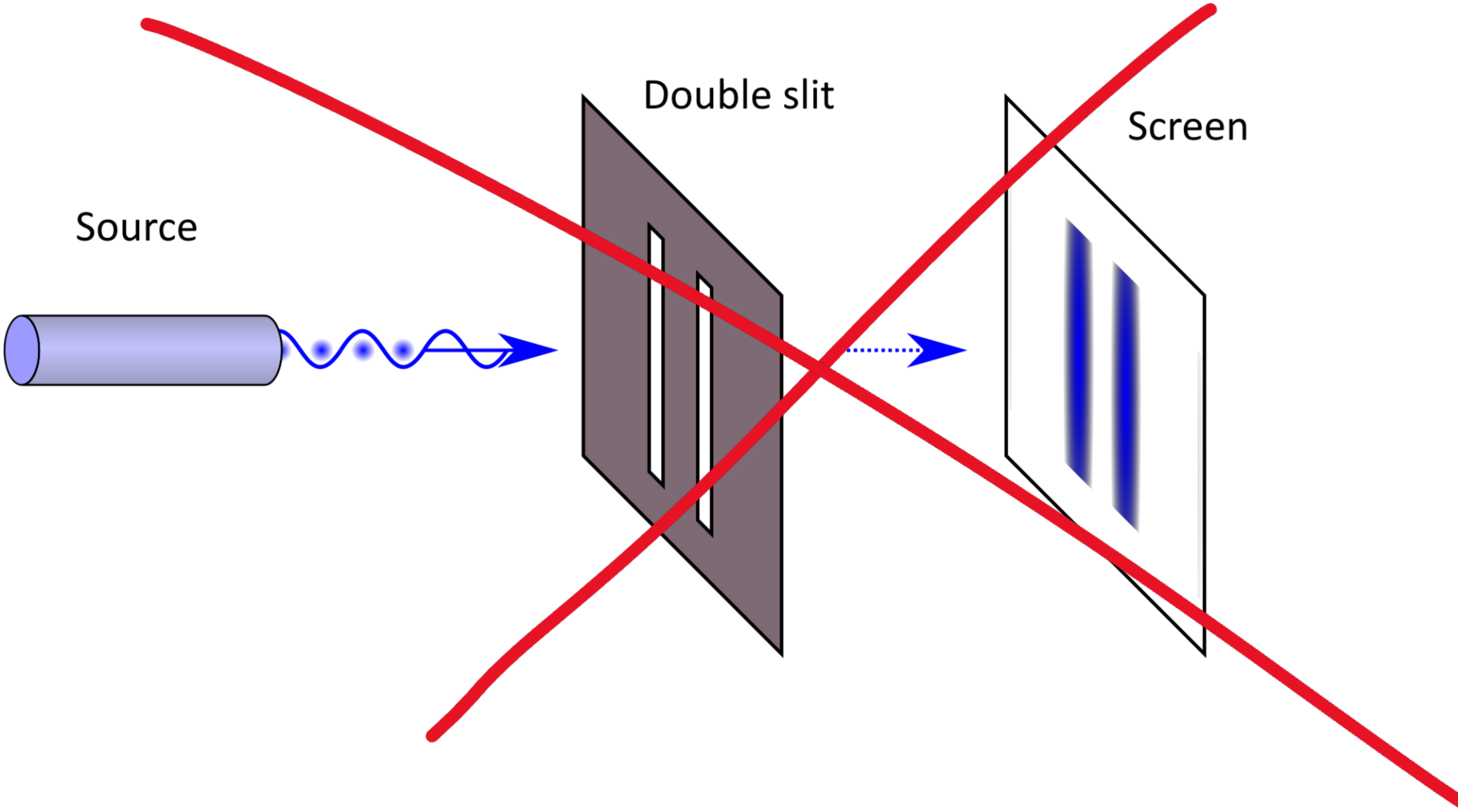
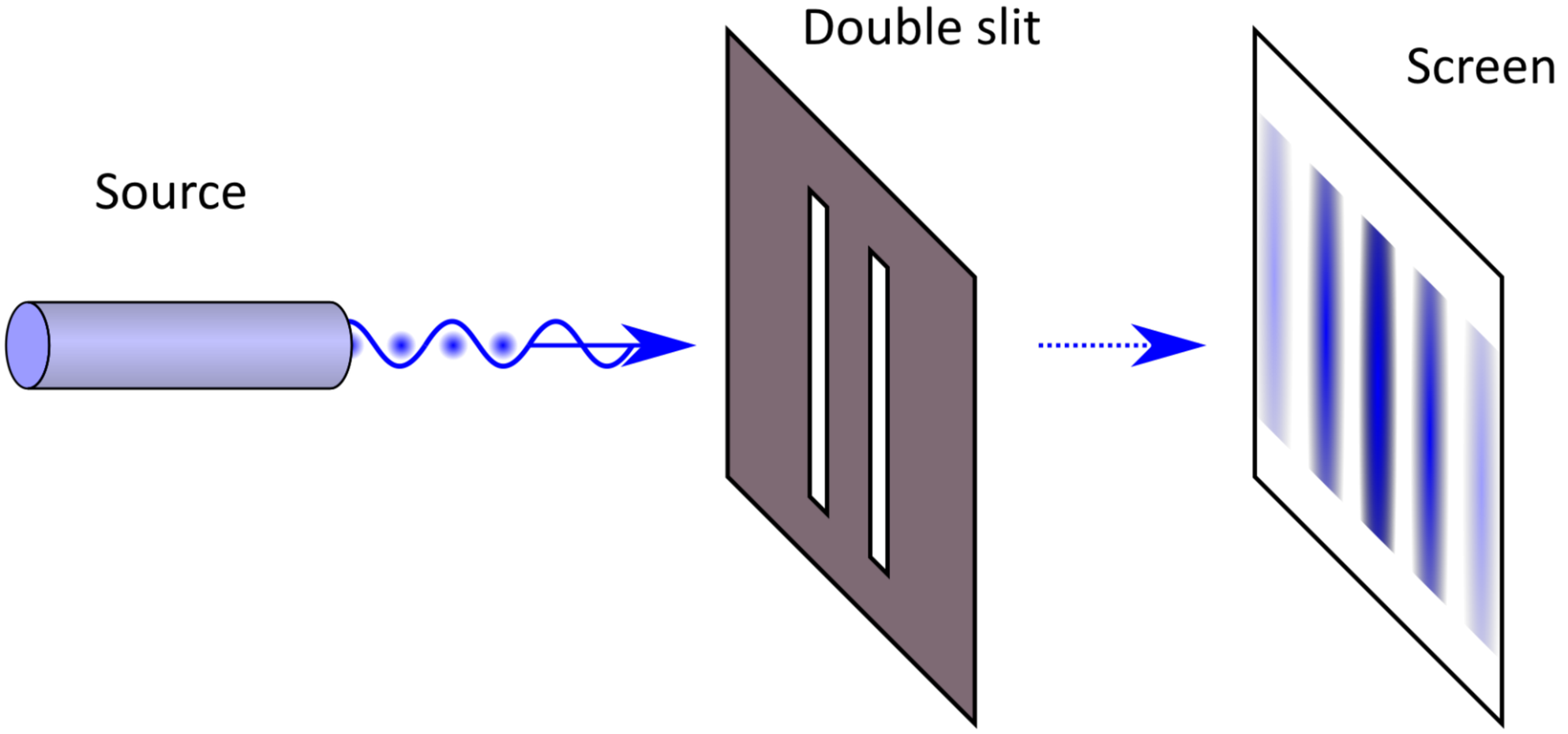
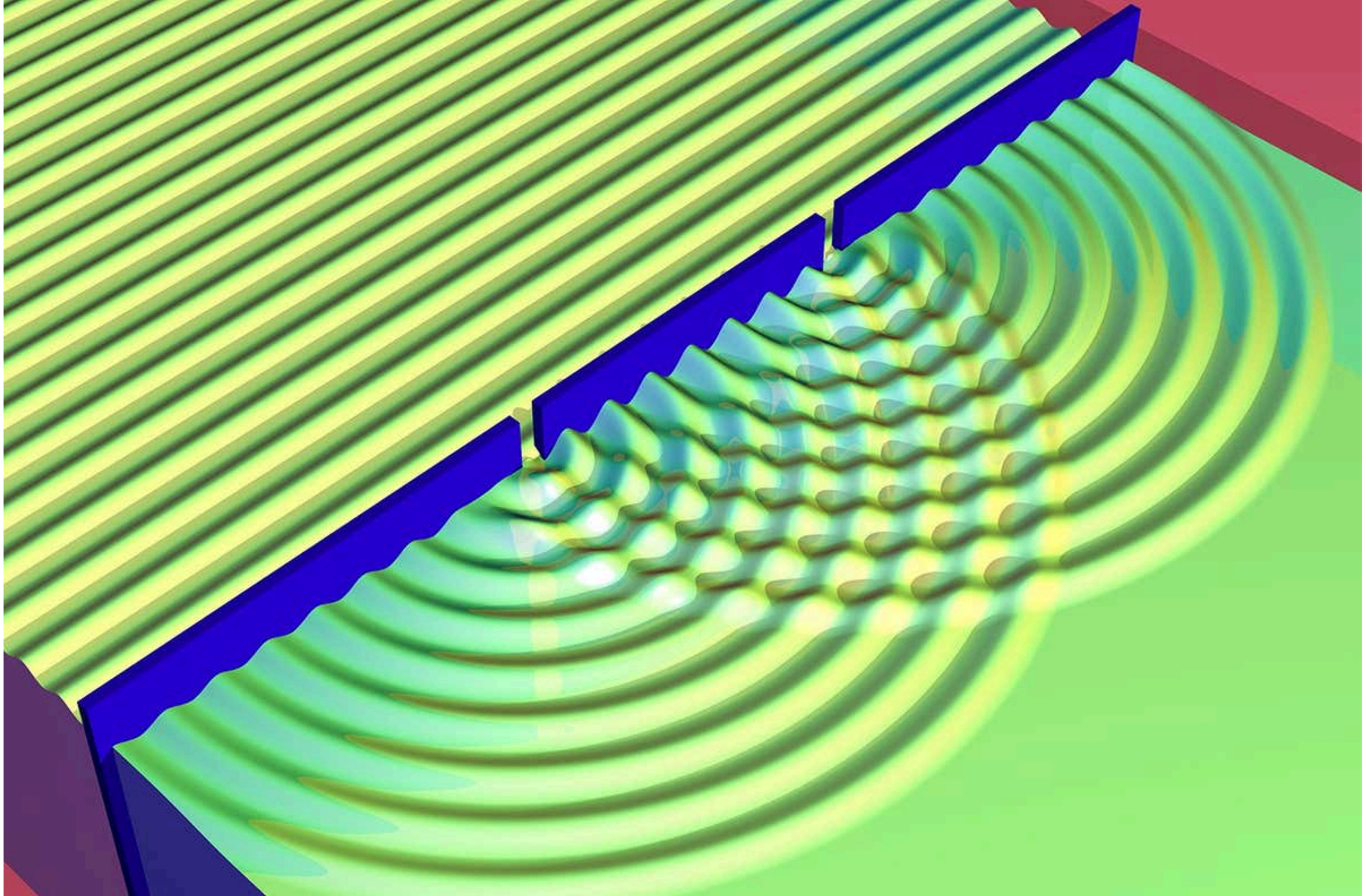


Figure 10.2 When both slits are open in the 2-slit experiment, the number of electrons detected at each position is *not* the sum of numbers when either slit is opened. There are even positions that are hit when each slit is open on its own, but are *not* hit when both slits are open.


Source
Double slit
Screen


Source
Double slit
Screen



Estado cuántico de 1-qubit

a_0 0
a_1 1

a_0, a_1 ‘amplitudes’ de probabilidad

las amplitudes son números complejos

$a_0, a_1 \in \mathbb{C}$

La amplitud permite calcula la probabilidad: $p = |a|^2$

Estado cuántico 2-qubit

a_0 00
a_1 01
a_2 10
a_3 11

Estado cuántico 3-qubit

a_0 000
a_1 001
a_2 010
a_3 011
a_4 100
a_5 101
a_6 110
a_7 111

Estado cuántico 4-qubit

a_{00} 0000
a_{01} 0001
a_{02} 0010
a_{03} 0011
a_{04} 0100
a_{05} 0101
a_{06} 0110
a_{07} 0111
a_{08} 1000
a_{09} 1001
a_{10} 1010
a_{11} 1011
a_{12} 1100
a_{13} 1101
a_{14} 1110
a_{15} 1111

Estado cuántico 5-qubit

a_{00} 00000
a_{01} 00001
a_{02} 00010
a_{03} 00011
a_{04} 00100
a_{05} 00101
a_{06} 00110
a_{07} 00111
a_{08} 01000
a_{09} 01001
a_{10} 01010
a_{11} 01011
a_{12} 01100
a_{13} 01101
a_{14} 01110
a_{15} 01111
a_{16} 10000
a_{17} 10001
a_{18} 10010
a_{19} 10011
a_{20} 10100
a_{21} 10101
a_{22} 10110
a_{23} 10111
a_{24} 11000
a_{25} 11001
a_{26} 11010
a_{27} 11011
a_{28} 11100
a_{29} 11101
a_{30} 11110
a_{31} 11111

Estado cuántico 6-qubit

a_{00} 000000
a_{01} 000001
a_{02} 000010
a_{03} 000011
a_{04} 000100
a_{05} 000101
a_{06} 000110
a_{07} 000111
a_{08} 001000
a_{09} 001001
a_{10} 001010
a_{11} 001011
a_{12} 001100
a_{13} 001101
a_{14} 001110
a_{15} 001111
a_{16} 010000
a_{17} 010001
a_{18} 010010
a_{19} 010011
a_{20} 010100
a_{21} 010101
a_{22} 010110
a_{23} 010111
a_{24} 011000
a_{25} 011001
a_{26} 011010
a_{27} 011011
a_{28} 011100
a_{29} 011101
a_{30} 011110
a_{31} 011111
a_{00} 100000
a_{01} 100001
a_{02} 100010
a_{03} 100011
a_{04} 100100
a_{05} 100101
a_{06} 100110
a_{07} 100111
a_{08} 101000
a_{09} 101001
a_{10} 101010
a_{11} 101011
a_{12} 101100
a_{13} 101101
a_{14} 101110
a_{15} 101111
a_{16} 110000
a_{17} 110001
a_{18} 110010
a_{19} 110011
a_{20} 110100
a_{21} 110101
a_{22} 110110
a_{23} 110111
a_{24} 111000
a_{25} 111001
a_{26} 111010
a_{27} 111011
a_{28} 111100
a_{29} 111101
a_{30} 111110
a_{31} 111111

Estado cuántico 300-qubit

Estado cuántico de longitud: $2^n = 2^{300} = 10^{90}$

Número de átomos en el universo: 10^{80}

10^{90} : número de átomos en 10 mil millones de universos

Feynman: No se puede simular un sistema cuántico con una computadora clásica

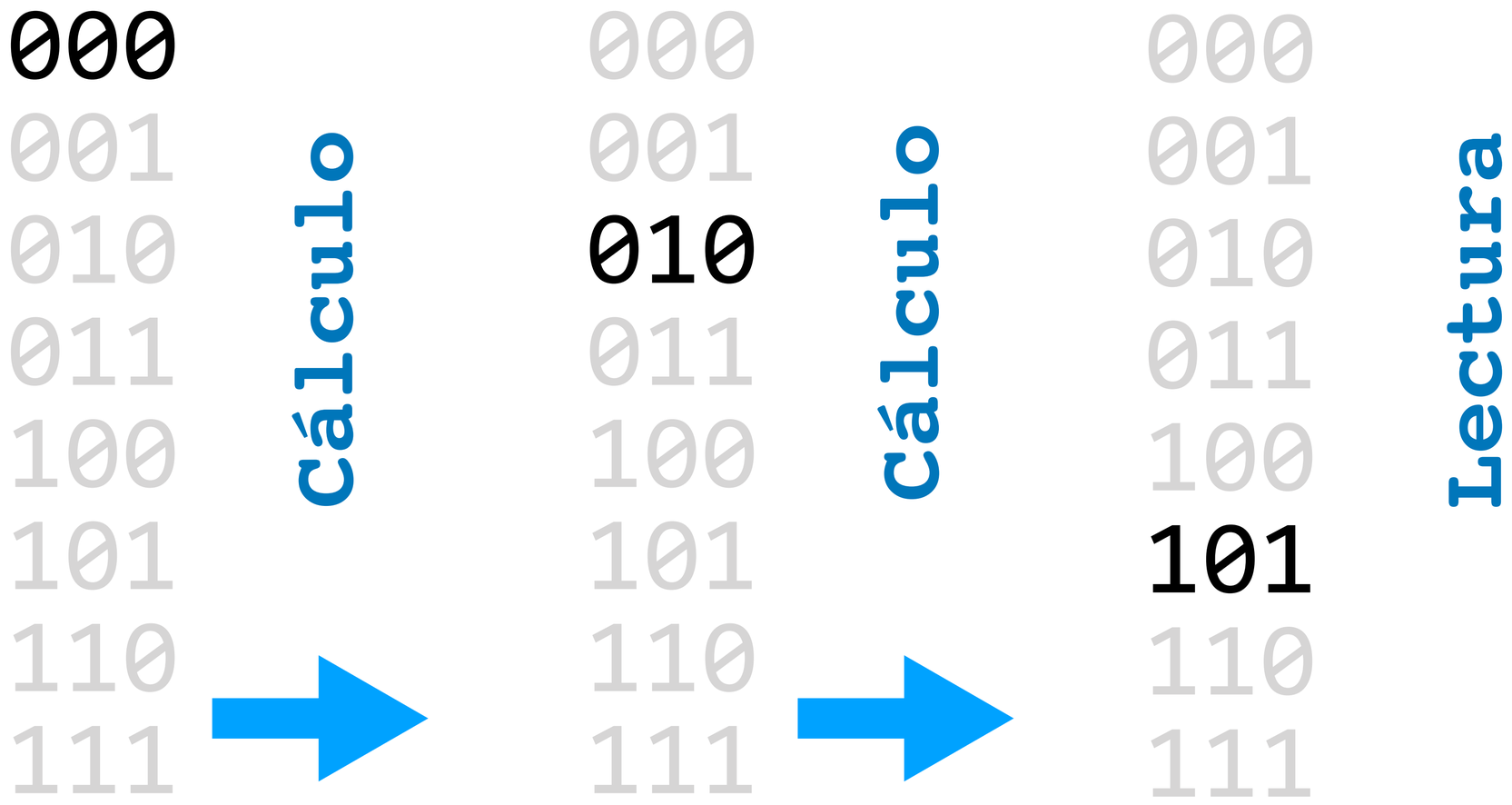
Estado cuántico 3-qubit

a_0 000
a_1 001
a_2 010
a_3 011
a_4 100
a_5 101
a_6 110
a_7 111

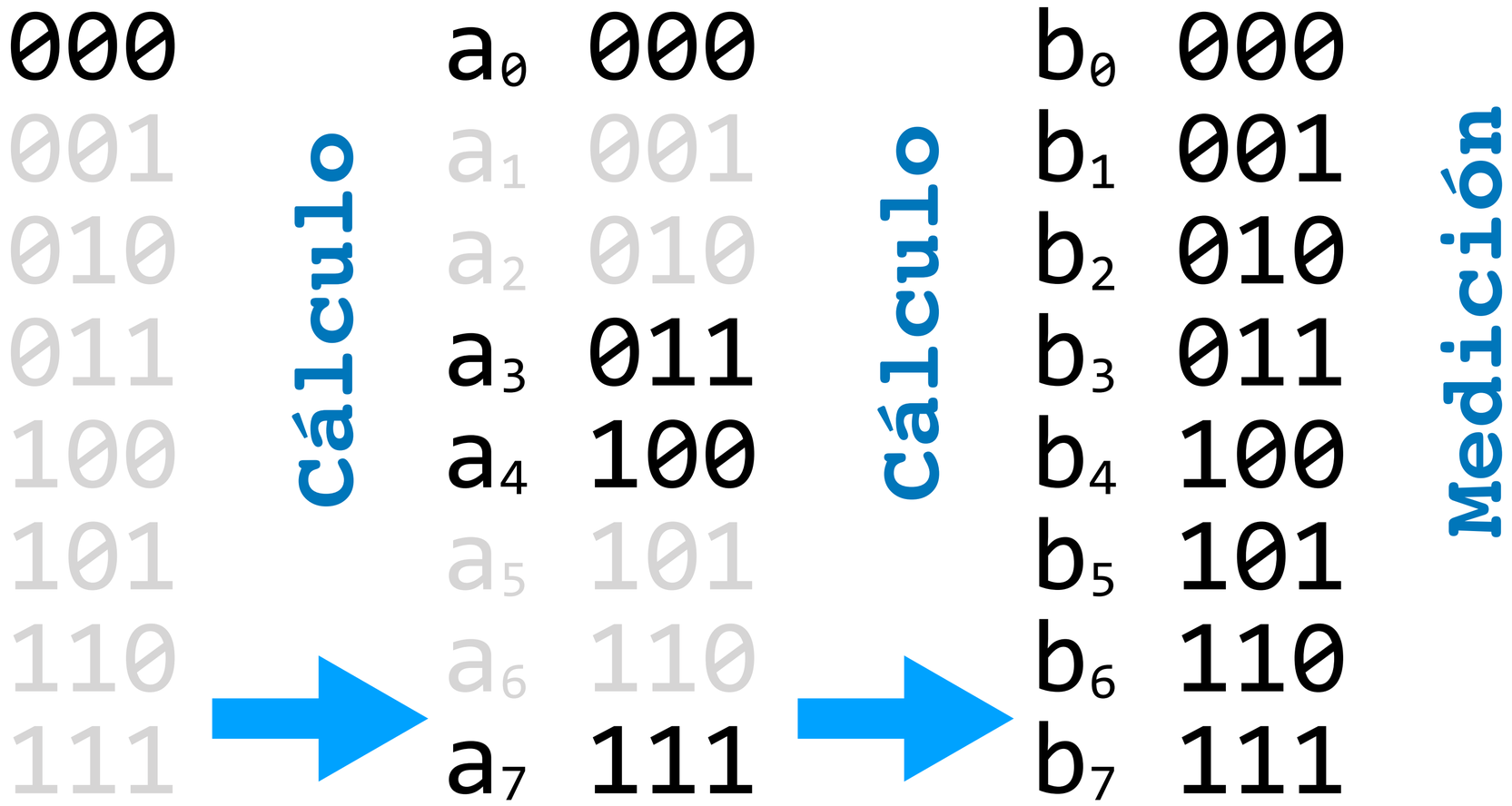
Estado clásico
3-bit

000
001
010
011
100
101
110
111

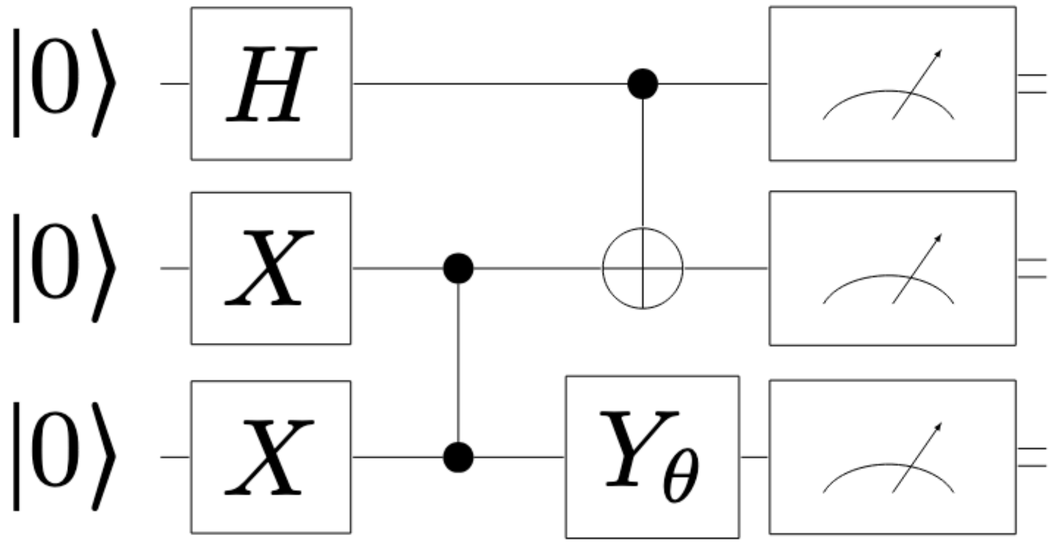
Cálculo clásico
3-bit



Cálculo cuántico 3-qubit



Cálculo Cuántico (1)



1000 'shots' →

'000': 240
'001': 174
'010': 228
'011': 5
'100': 84
'101': 107
'110': 138
'111': 24

Cálculo Cuántico (2)

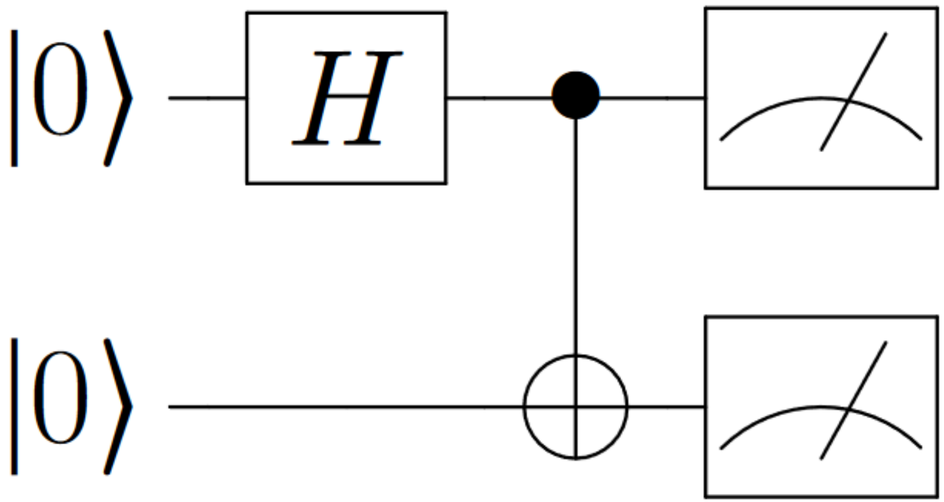
Estocástico: el resultado es un muestreo de la distribución de probabilidades subyacente

1 'shot': correr el circuito cuántico, medición

Resultado del cálculo: características de la distribución

Ejemplo: Cuáles son las series de bits con frecuencia > 10%
correr 100 shots —> se obtiene la lista

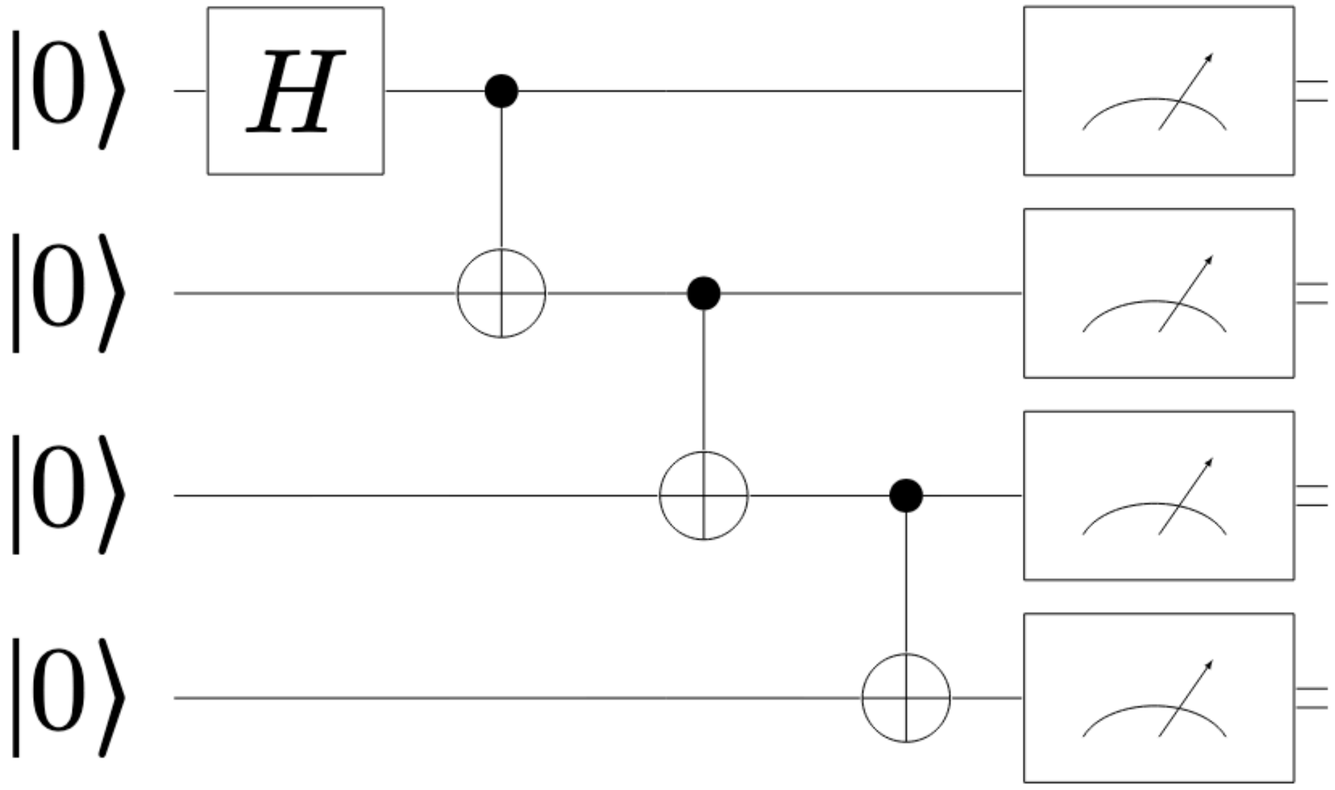
Circuitos



50% 00
0% 01
0% 10
50% 11

Estado de Bell

Circuitos

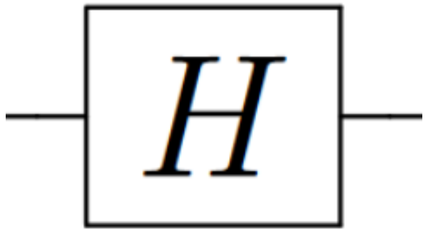



```
50% 0000
0%  0001
0%  0010
0%  0011
0%  0100
0%  0101
0%  0110
0%  0111
0%  1000
0%  1001
0%  1010
0%  1011
0%  1100
0%  1101
0%  1110
50% 1111
```

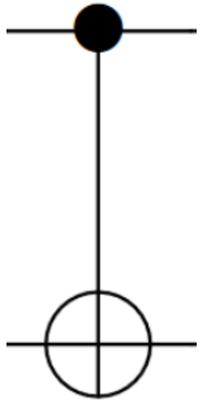
Estado GHZ (Greenberger–Horne–Zeilinger)

Los circuitos son tensores

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$



$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



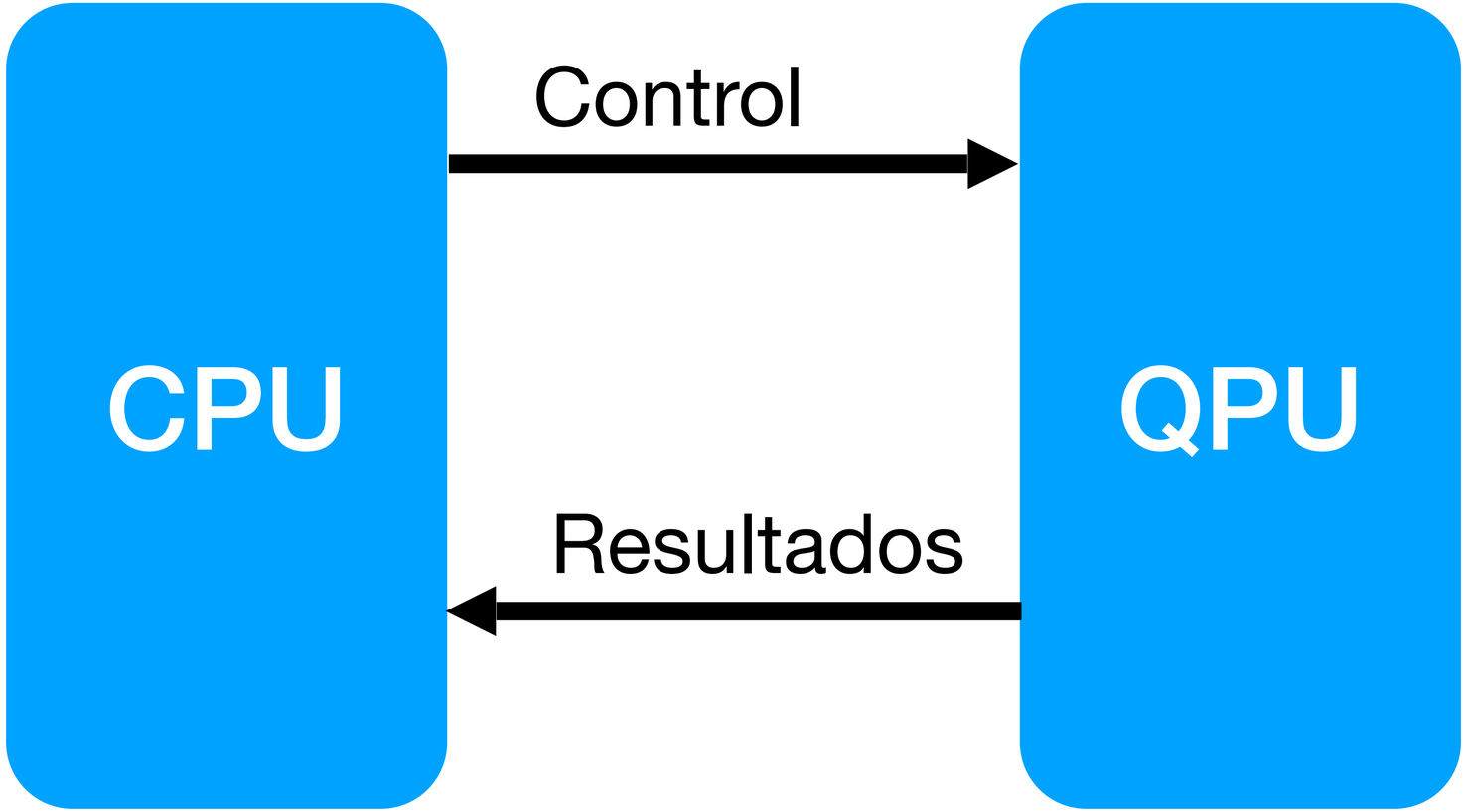
$$H^0 |0\rangle = (H \otimes \mathbb{I}) |00\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}$$

Estado de Bell

$$CNOT^{0,1}\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\\frac{1}{\sqrt{2}}\\0\end{pmatrix}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\\frac{1}{\sqrt{2}}\\0\end{pmatrix}=\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{pmatrix}$$

~~Laptop~~ procesador cuántico



Criptografía y Cuántica

- «Criptografía cuántica»
    - Red cuántica de distribución de claves de criptografía
- Criptografía post-cuántica
    - Criptografía clásica, inmune a la computación cuántica
- Criptoanálisis cuántico: RSA y curvas elípticas no son seguras con la computación cuántica
- Bitcoin: el hash no está impactado por la cuántica
  hay necesidad de migrar la autenticación

Las computadoras cuánticas no son computadoras clásicas más rápidas

- Calculan de manera diferente —> algoritmos **cuánticos**

- Pueden resolver algunos problemas exponencialmente más rápido — O(n) vs $O(2^n)$
  Con tal de tener un algoritmo cuántico para eso
  Un algoritmo cuántico con exponencialmente menos operaciones

- Cuales son esos problemas? No se sabe...
  Hay que inventar los algoritmos cuánticos uno por uno

Ventaja cuántica exponencial

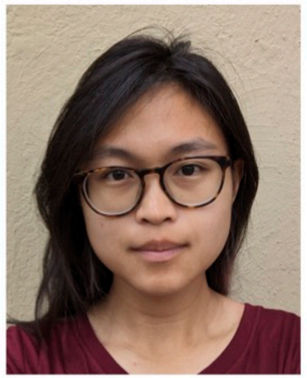
Requisitos para la ventaja cuántica exponencial:

Un problema imposible de calcular clásicamente:
En el algoritmo clásico el número de operaciones crece exponencialmente con el tamaño de problema

Un algoritmo cuántico en que el número de operaciones crece polinomialmente

Algoritmo de Kerenidis–Prakash

2016: Kerenidis y Prakash diseñan un algoritmo cuántico para un problema de machine learning que es exponencialmente más rápido que el mejor algoritmo clásico *conocido*



2018: Ewing Tang, 17 años, diseña un algoritmo clásico que es igual de rápido. El algoritmo de Kerenidis–Prakash pierde su ventaja cuántica...

La algorítmica cuántica es difícil

- Las computadoras cuánticas son extraterrestres,
  los humanos son computadoras clásicas
- Un problema clásico exponencial, imposible...
  pero un algoritmo cuántico polinomial
- No tenemos computadoras cuánticas para experimentar

Aplicaciones y valor económico

- Criptoanálisis

  Ventaja cuántica: Sí Valor: casi cero

Aplicaciones y valor económico

- Criptoanálisis

  Ventaja cuántica: Sí Valor: casi cero

- Simulación de física cuántica

  Ventaja cuántica: incierto Valor: incierto

Aplicaciones y valor económico

- Criptoanálisis

  Ventaja cuántica: Sí Valor: casi cero

- Simulación de física cuántica

  Ventaja cuántica: incierto Valor: incierto

- Optimización

  Ventaja cuántica: por el momento no

Aplicaciones y valor económico

- Criptoanálisis

  Ventaja cuántica: Sí Valor: casi cero

- Simulación de física cuántica

  Ventaja cuántica: incierto Valor: incierto

- Optimización

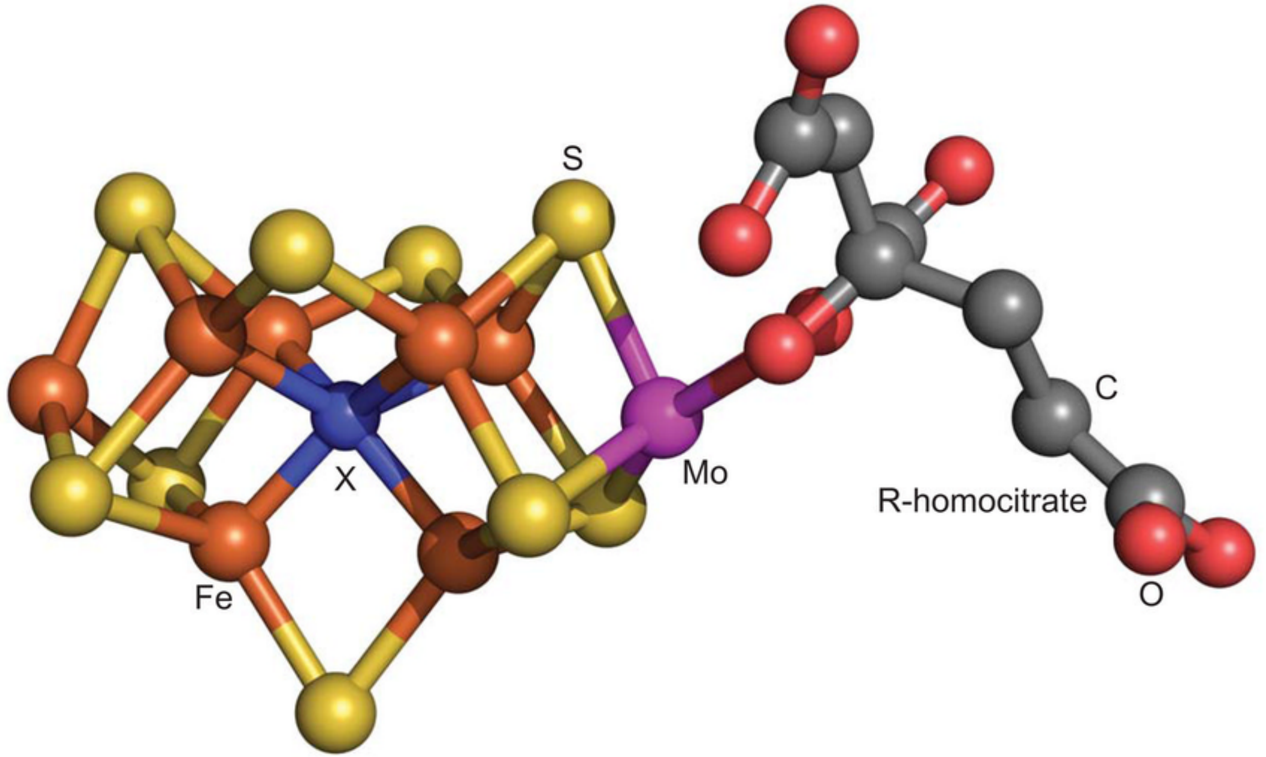
  Ventaja cuántica: por el momento no

- Inteligencia artificial cuántica

  Ventaja cuántica: por el momento no

Cofactor hierro molibdeno (FeMoco)

Parte del complejo catalítico utilizado por las bacterias para la síntesis de amoníaco, base de los fertilizantes agrícolas



Se piensa que la computación cuántica podría ayudar a entender los mecanismos de acción de ese complejo catalítico

Eso ayudaría al diseño de un proceso industrial que necesitase menos energía que el actual proceso de Haber-Bosch

Esto es hipotético, los investigadores trabajando sobre FeMoco, seguro intentarán utilizar la computación cuántica

The Grand Challenge of Quantum Applications

Ryan Babbush,* Robbie King,† Sergio Boixo, William Huggins, Tanuj Khattar, Guang Hao Low, Jarrod R. McClean, Thomas O'Brien, and Nicholas C. Rubin
Google Quantum AI, Santa Barbara, CA 93111, United States
(Dated: December 5, 2025)

This perspective outlines promising pathways and critical obstacles on the road to developing useful quantum computing applications, drawing on insights from the Google Quantum AI team. We propose a five-stage framework for this process, spanning from theoretical explorations of quantum advantage to the practicalities of compilation and resource estimation. For each stage, we discuss key trends, milestones, and inherent scientific and sociological impediments. We argue that two central stages—identifying concrete problem instances expected to exhibit quantum advantage, and connecting such problems to real-world use cases—represent essential and currently under-resourced challenges. Throughout, we touch upon related topics, including the promise of generative artificial intelligence for aspects of this research, criteria for compelling demonstrations of quantum advantage, and the future of compilation as we enter the era of early fault-tolerant quantum computing.

Ryan Babbush · 2nd

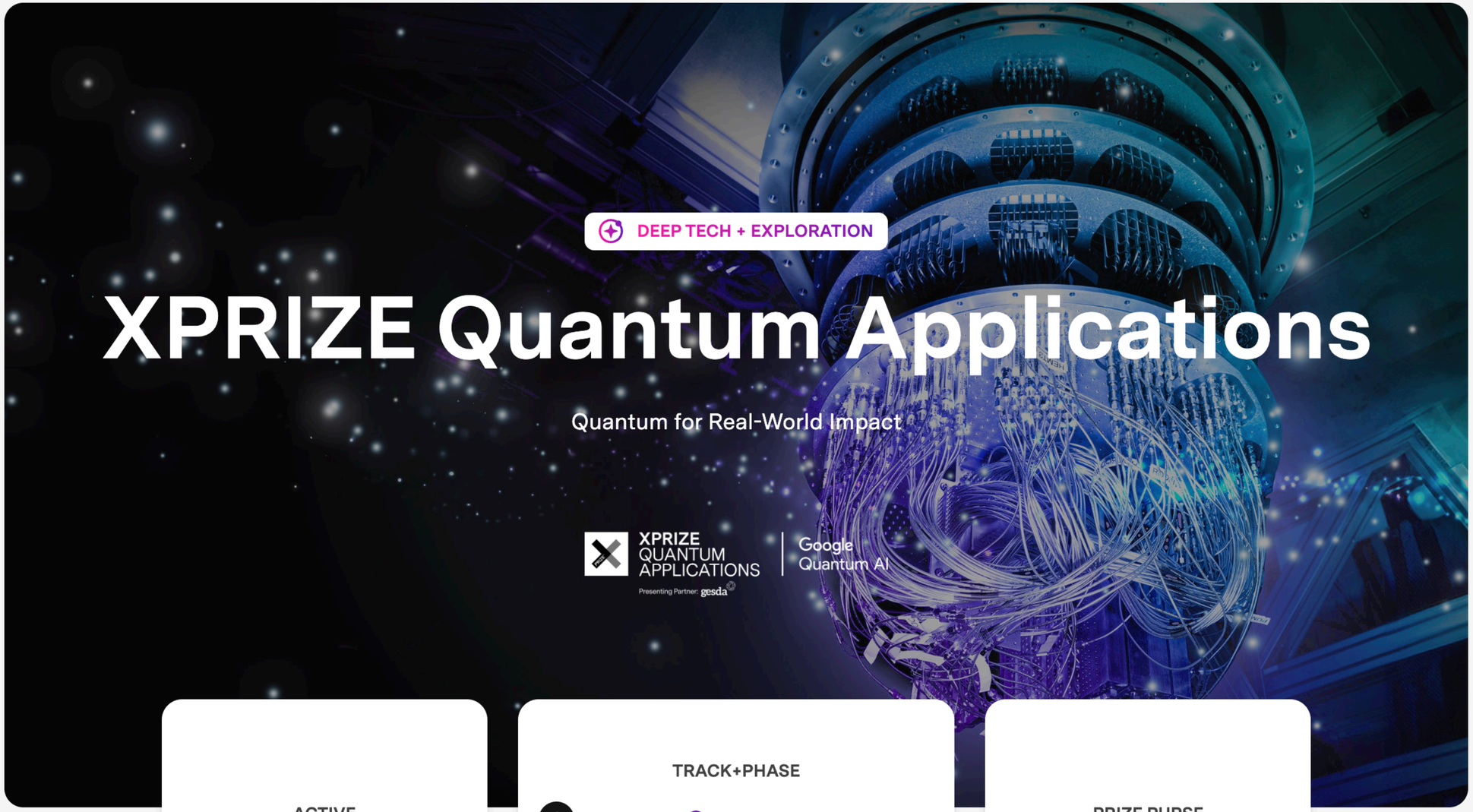
Director of Quantum Algorithms & Applications Research at Google

Santa Barbara, California, United States · **Contact info**

Google

Harvard University

Google



ACTIVE

2024 - 2027

TRACK+PHASE

1 FINALS

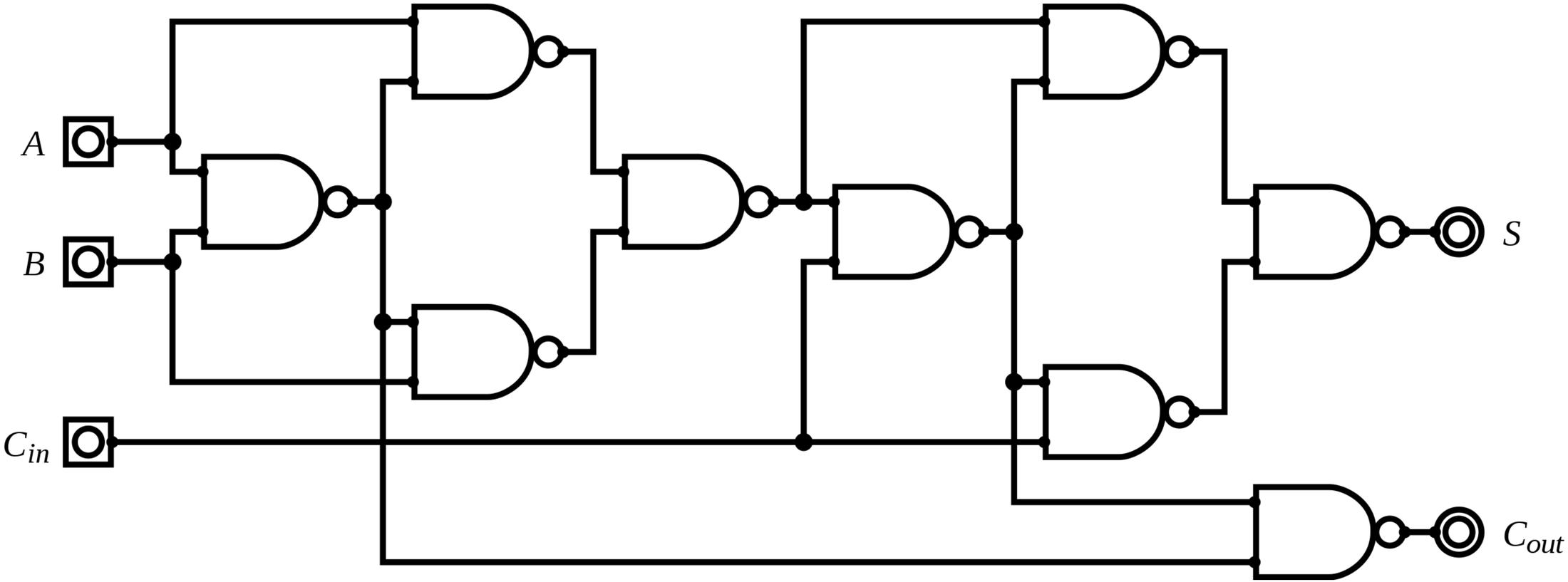
2 REGISTRATION

3 REGISTRATION

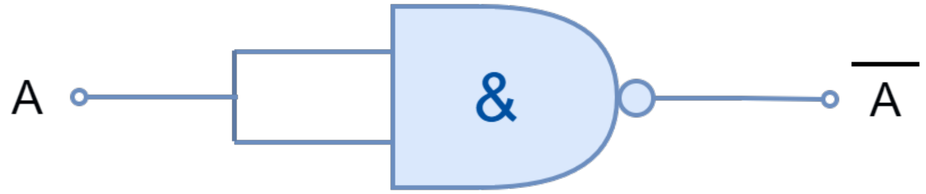
PRIZE PURSE

$5 Million

Circuito lógico 1940s

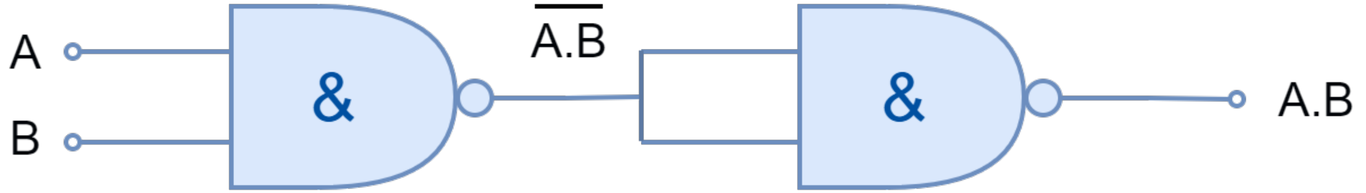


NOT Logic



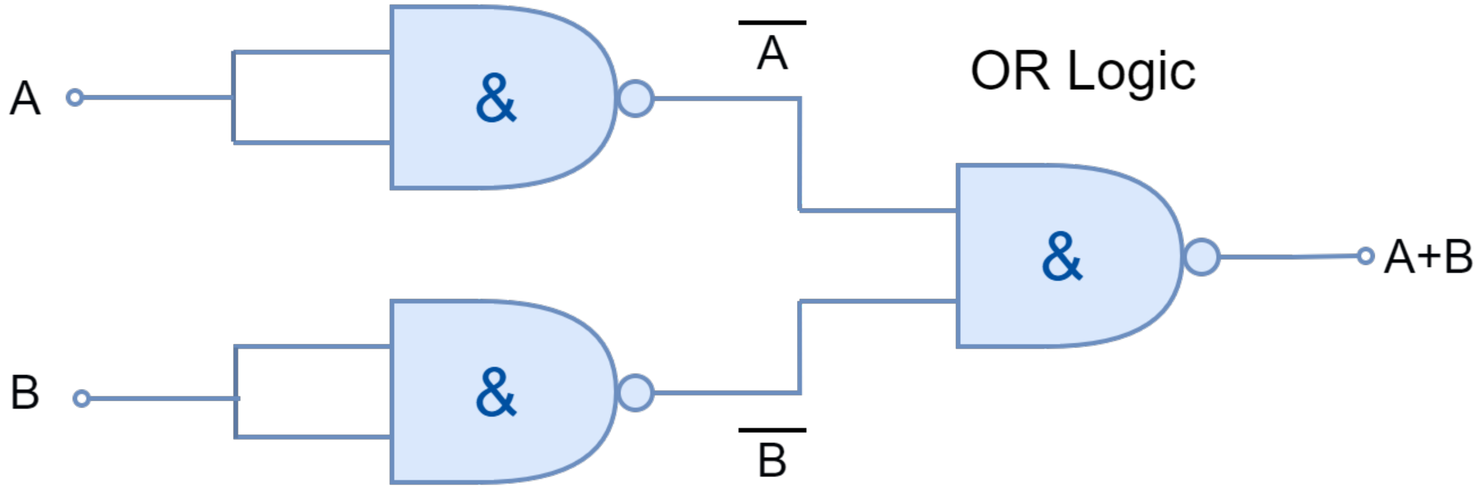
A	Q
0	1
1	0

AND Logic

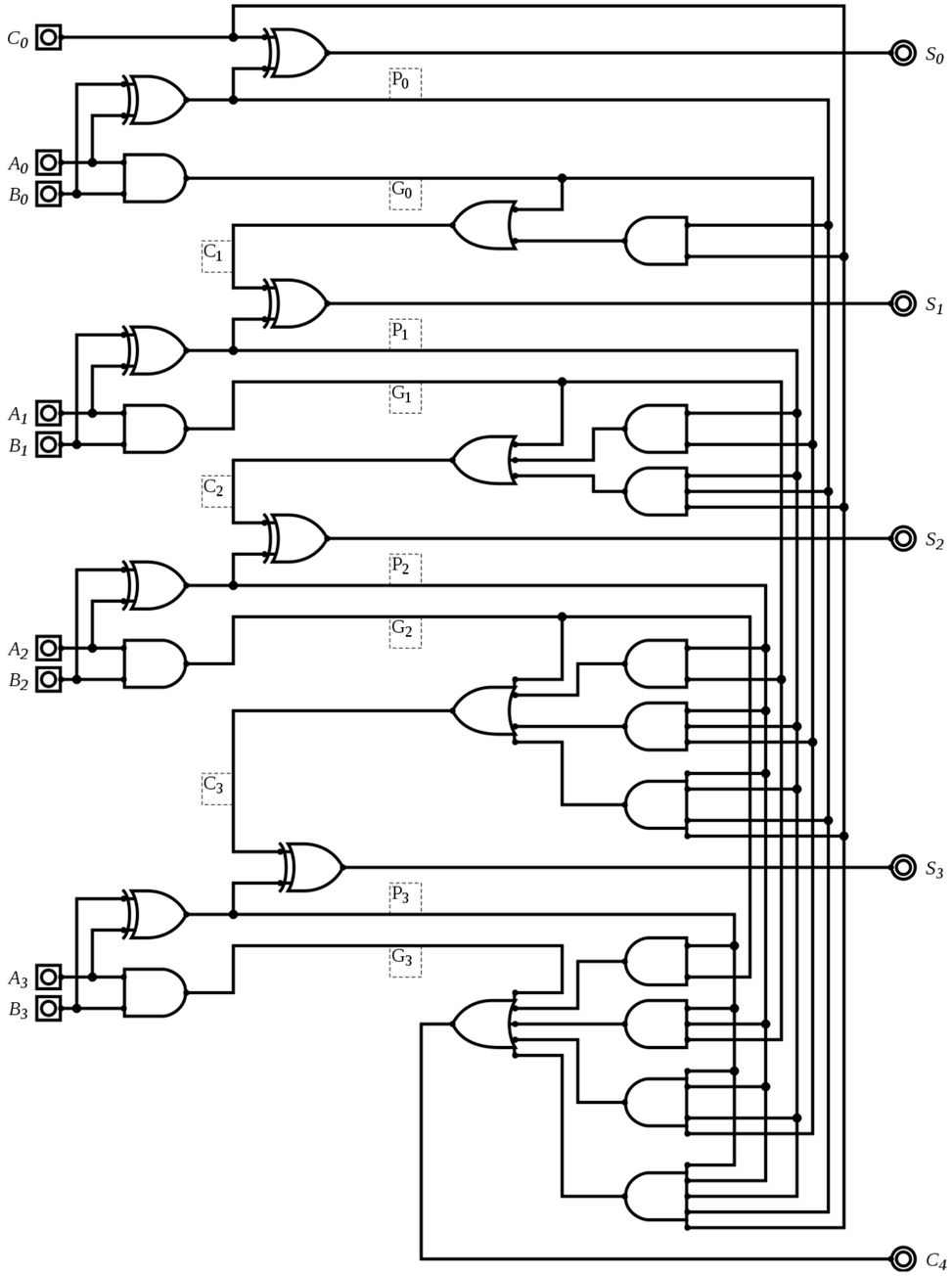


A	B	$\overline{A.B}$	Q
0	0	1	0
0	1	1	0
1	0	1	0
1	1	0	1

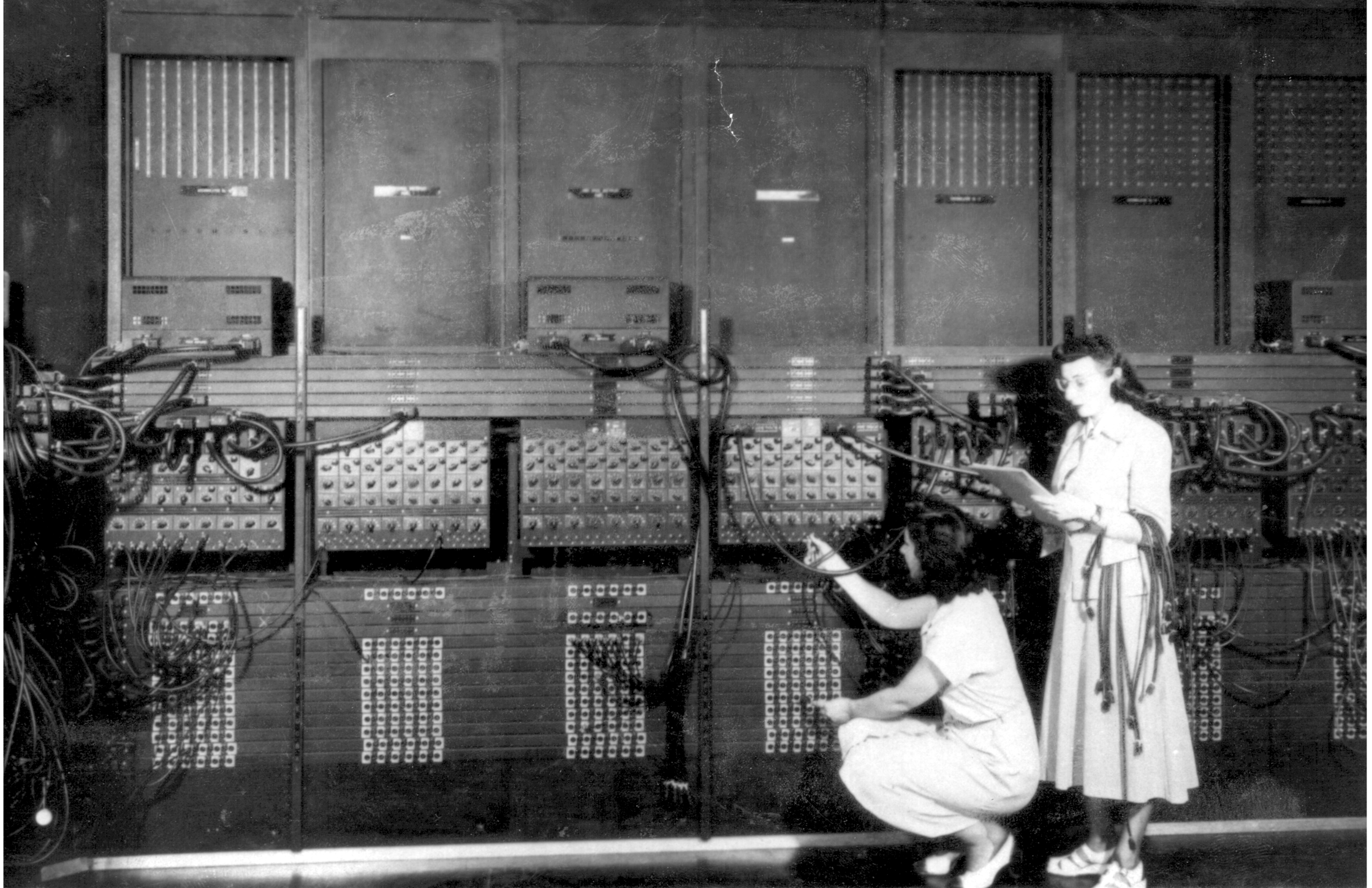
OR Logic



A	B	$\overline{A}$	$\overline{B}$	Q
0	0	1	1	0
0	1	1	0	1
1	0	0	1	1
1	1	0	0	1

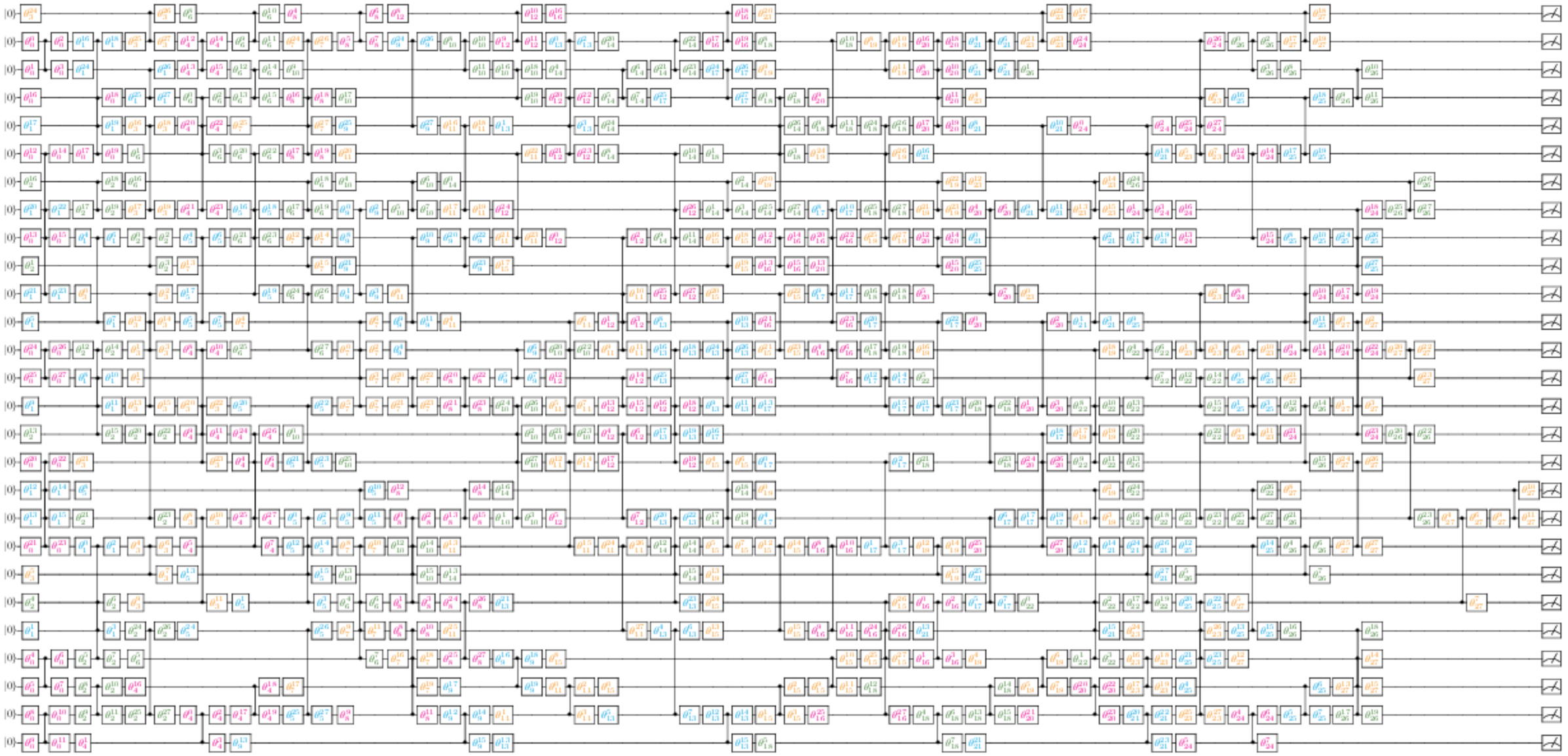


4-bit addition



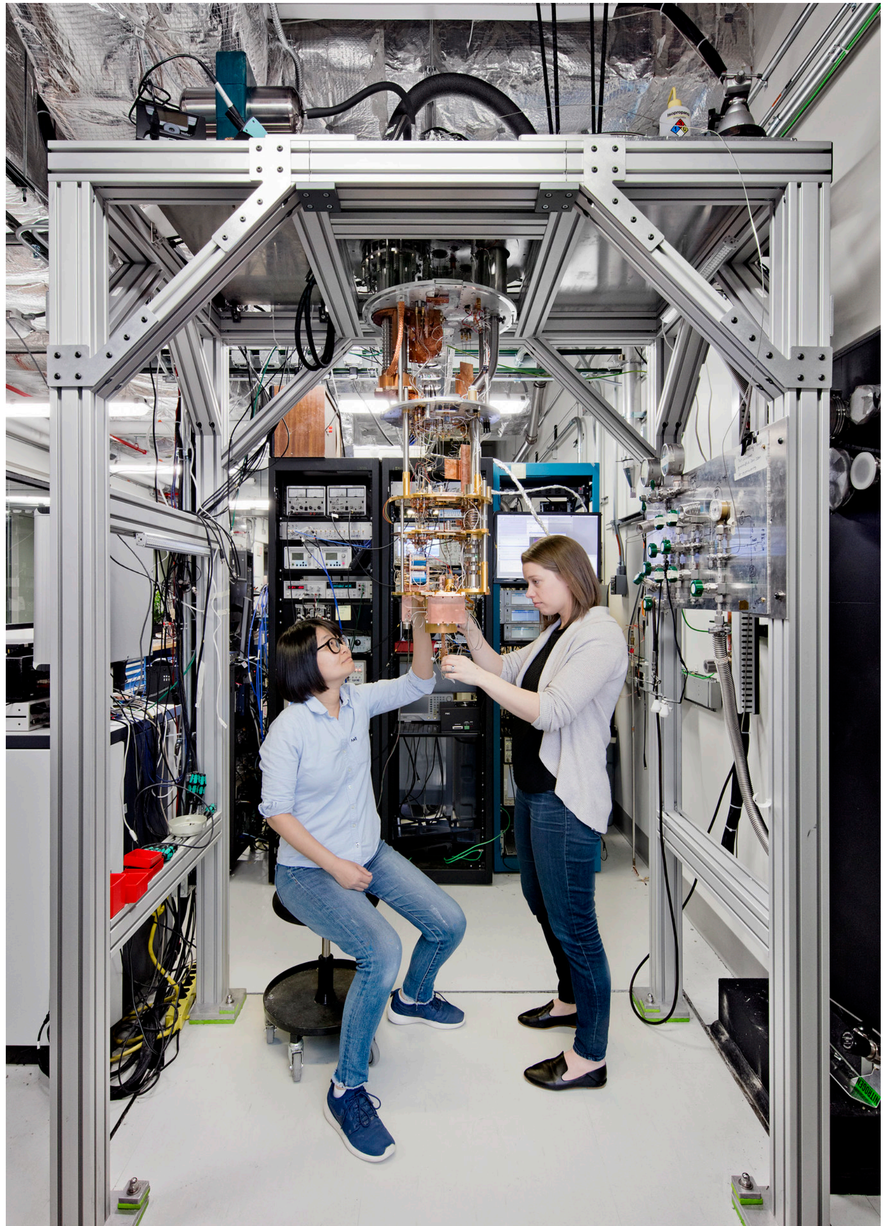

7709
HOURS
ACCUMULATOR
NO. 8
HEATERS
ON

27 Qubits



1946

2016



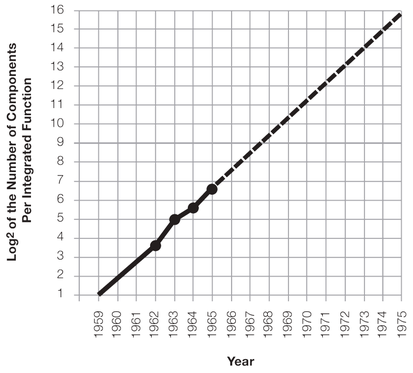
a two-mil square can also contain several kilohms of resistance or a few diodes. This allows at least 500 components per linear inch or a quarter million per square inch. Thus, 65,000 components need occupy only about one-fourth a square inch.

On the silicon wafer currently used, usually an inch or more in diameter, there is ample room for such a structure if the components can be closely packed with no space wasted for interconnection patterns. This is realistic, since efforts to achieve a level of complexity above the presently available integrated circuits are already underway using multilayer metalization patterns separated by dielectric films. Such a density of components can be achieved by present optical techniques and does not require the more exotic techniques, such as electron beam operations, which are being studied to make even smaller structures.

Increasing the yield

There is no fundamental obstacle to achieving device yields of 100%. At present, packaging costs so far exceed the cost of the semiconductor structure itself that there is no incentive to improve yields, but they can be raised as high as is economically justified. No barrier exists comparable to the thermodynamic equilibrium considerations that often limit yields in chemical reactions; it is not even necessary to do any fundamental research or to replace present processes. Only the engineering effort is needed.

In the early days of integrated circuitry, when yields were extremely low, there was such incentive. Today ordinary integrated circuits are made with yields comparable with those obtained for individual semiconductor devices. The same pattern will make larger arrays economical, if other considerations make such arrays desirable.



Heat problem

Will it be possible to remove the heat generated by tens of thousands of components in a single silicon chip?

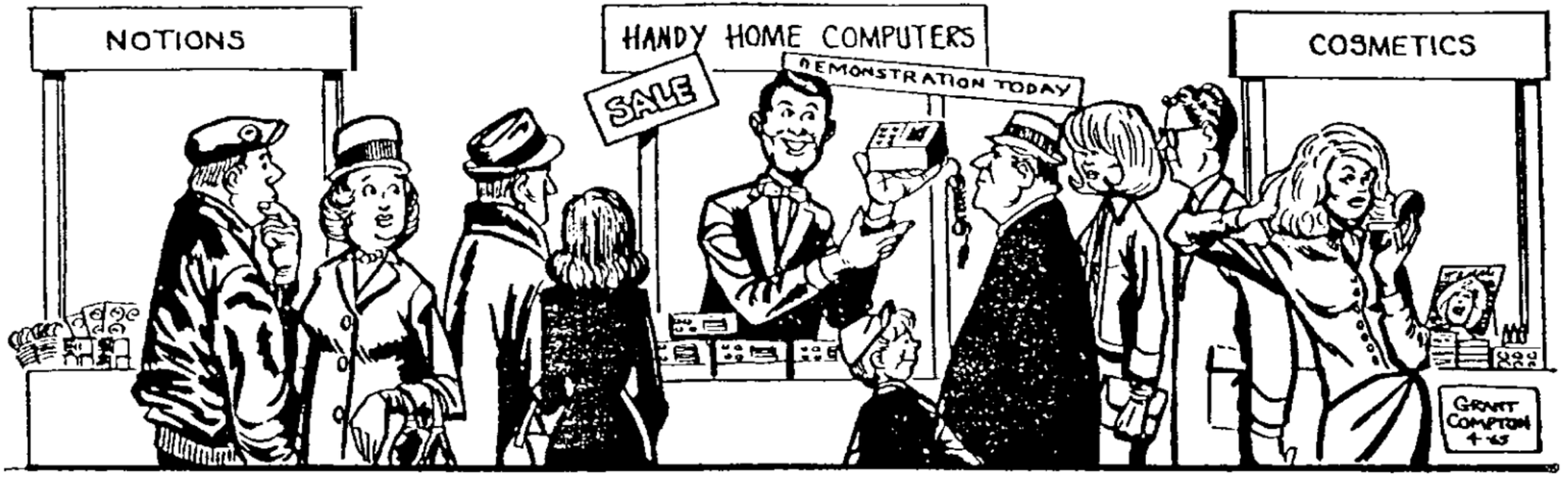
If we could shrink the volume of a standard high-speed digital computer to that required for the components themselves, we would expect it to glow brightly with present power dissipation. But it won't happen with integrated circuits. Since integrated electronic structures are two-dimensional, they have a surface available for cooling close to each center of heat generation. In addition, power is needed primarily to drive the various lines and capacitances associated with the system. As long as a function is confined to a small area on a wafer, the amount of capacitance which must be driven is distinctly limited. In fact, shrinking dimensions on an integrated structure makes it possible to operate the structure at higher speed for the same power per unit area.

Day of reckoning

Clearly, we will be able to build such component-crammed equipment. Next, we ask under what circumstances we should do it. The total cost of making a particular system function must be minimized. To do so, we could amortize the engineering over several identical items, or evolve flexible techniques for the engineering of large functions so that no disproportionate expense need be borne by a particular array. Perhaps newly devised design automation procedures could translate from logic diagram to technological realization without any special engineering.

It may prove to be more economical to build large

Gordon E. Moore
1965


NOTIONS
HANDY HOME COMPUTERS
SALE
DEMONSTRATION TODAY
COSMETICS
GRANT COMPTON '43

- 1958, H. A. Simon and Allen Newell: «within 10 years a digital computer will be the world's chess champion» and «within 10 years a digital computer will discover and prove an important new mathematical theorem»
- 1970, Marvin Minsky: «In from 3 to 8 years we will have a machine with the general intelligence of an average human being»
- 1974–1980: primer invierno de la IA

Habilidades par ser dev cuántico

- Álgebra lineal, tensores
- Probabilidades, estadística
- Computación teórica
- Programming
- (elementos de física cuántica)

Puntos importantes

- Las computadoras cuánticas al fin están llegando
  (primeros qubits lógicos)
- No tenemos software/algoritmos para esas computadoras
- La investigación en algorítmica cuántica se va a intensificar