Breve introducción a la computación cuántica

Joaquín KELLER

27 de marzo de 2025

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

arXiv > quant-ph > arXiv:2007.14044

Quantum Physics

[Submitted on 28 Jul 2020]

Polyadic Quantum Classifier

William Cappelletti, Rebecca Erbanni, Joaquín Keller

We introduce here a supervised quantum machine learning
to output a specific bit string corresponding to the class of
shows good accuracy --compared to a classical machine le
Furthermore, we evaluate with simulations how the algorith
dataset.

History

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:
Deutsch–Jozsa algorithm (theoretical result, no direct application)
Exponentially faster than any possible classical algorithm

1994:
Peter Shor’s algorithm for integer factorization (breaks RSA cryptography)
Exponentially faster than any known classical algorithm

How faster ?

breaking (factoring) a 2048-bit RSA key

Classical Computing

Best classical algorithm:

10^{34} steps

1 billion years

on El Capitan supercomputer
- 1.8 exaFLOPS
- 1M CPU - 10M GPU cores
- 10Mx faster than a gaming PC

Quantum Computing

Shor's quantum algorithm:

How faster ?

breaking (factoring) a 2048-bit RSA key

Classical Computing

Best classical algorithm:

10^{34} steps

1 billion years

on El Capitan supercomputer
- 1.8 exaFLOPS
- 1M CPU - 10M GPU cores
- 10Mx faster than a gaming PC

Quantum Computing

Shor's quantum algorithm:

10^{7} steps

8 hours

on a quantum computer
- 20M physical qubits
- 1M Qops/s per qubit
- (superconducting qubits)

Work in progress… doable in 2030?

Hardware now

(physical qubits)

1998: First quantum computer: 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`

Physical vs logical qubits

- Physical, real qubits are noisy

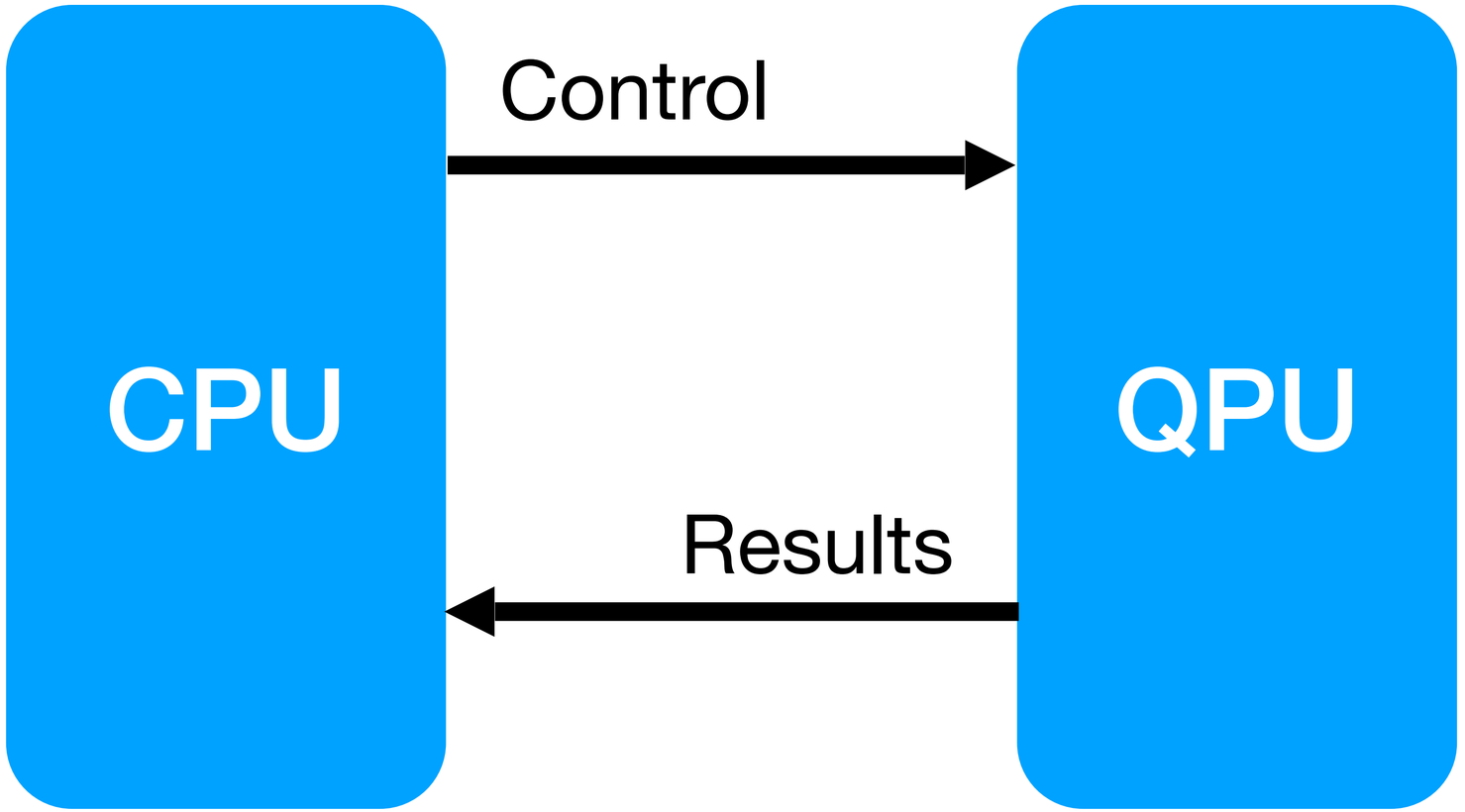
- With error correction 1000 physical qubits
  => 1 logical qubit

- QPU power is determined by:
  - number qubits
  - error rate
  - qubit connectivity

Quantum computers are not faster classical computers

- They compute in a different way, the algorithms are different
- They can solve some problems exponentially faster — O(n) vs $O(2^n)$
- We don’t know which problems
- We don’t now how

Hybrid Architecture



Cryptography and quantum computing

- «Quantum cryptography»
    - Quantum key distribution
- Post-quantum cryptography
    - Quantum-safe cryptography
- Quantum computers will break RSA

It’s hard

- Software

  - Quantum computers are alien
  - Hard to make them compute something at all
  - Even harder to make them compute something useful
  - But useful is not enough….
  - It needs to be useful, and faster than classical computers
  - We don’t have quantum computers to try stuff, to debug, to learn

- Hardware engineering

  - Qubits need to be isolated to exist
  - Qubits need to be manipulated to compute
  - Qubits are inherently unstable

Hardware roadmap (2020)

Google: a thousand error-corrected qubits “within the decade”

IBM: 4158+ physical qubits in 2025

IonQ: 1028 logical (error-corrected) qubits in 2028

PsiQuantum: 1 million of physical qubits by 2030

~1000 “physical” (noisy) qubits → one “logical” (corrected) qubit

Hardware paths

- Superconducting: Google, IBM, Rigetti, Alibaba
- Trapped ion: ionQ, Quantinuum (Honeywell), AQT, Universal Quantum, Huayi Boao
- Photonic: Xanadu, PsiQuantum, Jiuzhang
- Cold atoms: Pasqal, ColdQuanta, QuEra, Atom
- Cat qubits: Amazon, Alice&Bob
- Marjorana: Microsoft — Spin qubits: Silicon Quantum Computing — …

Potential applications (quantum advantage)

Cryptography: break RSA ok

Chemistry and material sciences: Quantum simulation maybe

Optimization: Logistics, finance maybe not

Quantum Machine Learning:

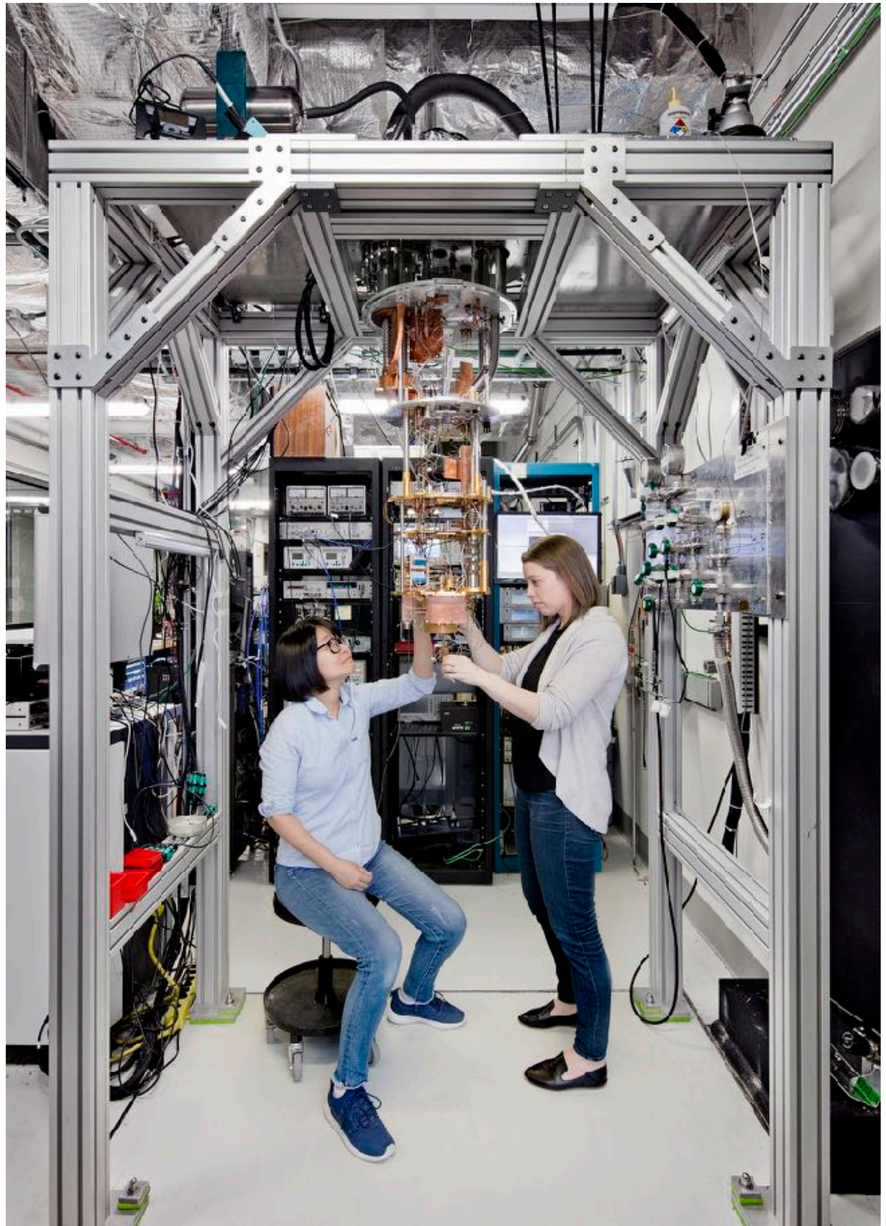
classical ML is already very good maybe

Skills for quantum computing

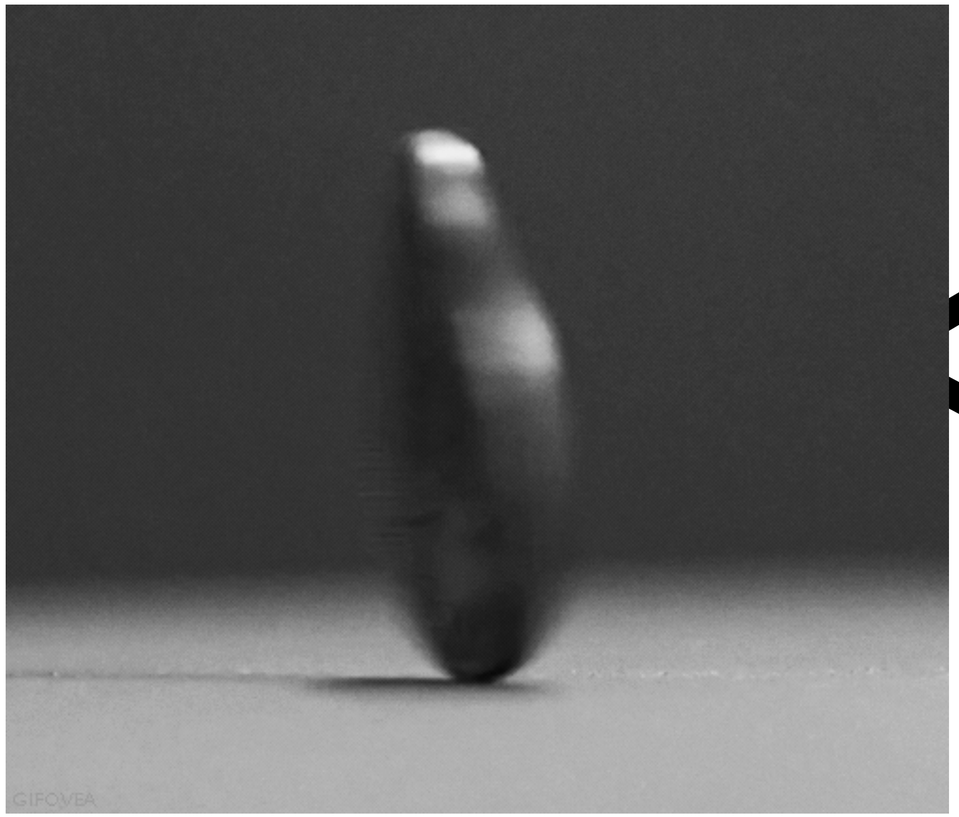
- Tensor algebra
- Statistics
- Theoretical Computer Science
- Programming
- Elements of quantum physics

1946

2016



Qubit

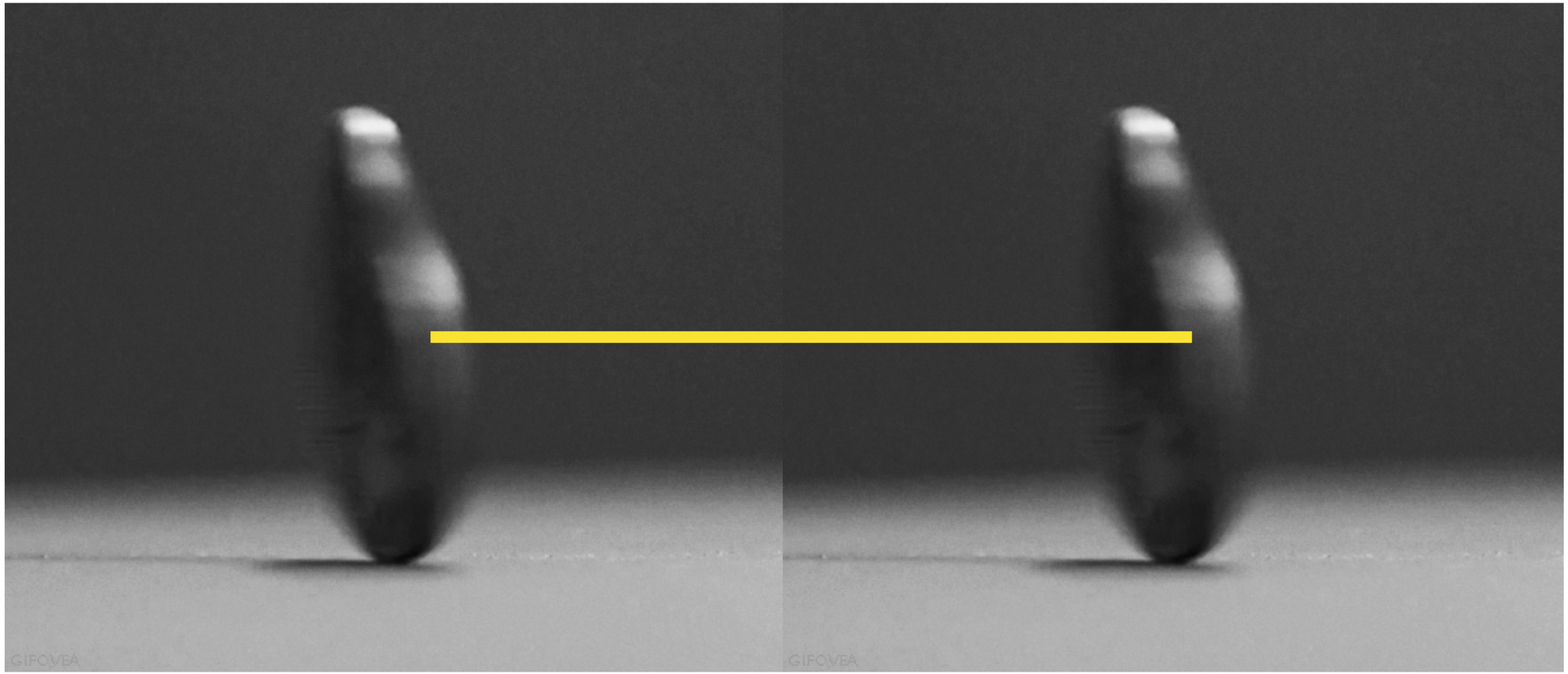


0

Measurement

1

Entangled Qubits



Entangled Qubits

Quantum state
1-qubit

a_0 0
a_1 1

a_0, a_1 are probability ‘amplitudes’

amplitudes are complex numbers

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

Probability from amplitude: $p = |a|^2$

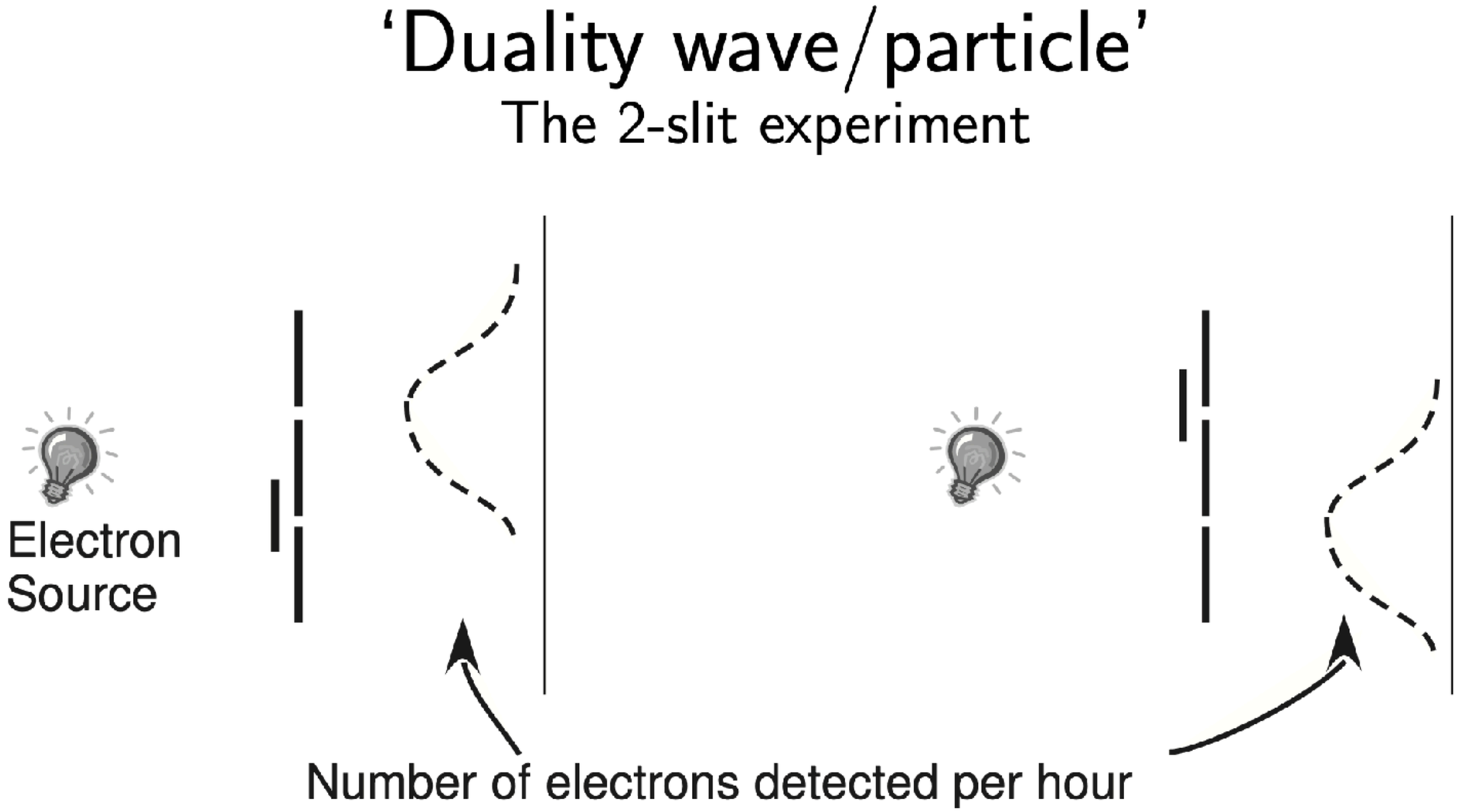


Figure 10.1 In the 2-slit experiment an electron source is placed between a wall with two slits and a detector array. When one slit is covered then, as expected, the number of electron detected is largest directly behind the open slit.

Feynman: *"negative probabilities"*

Interference

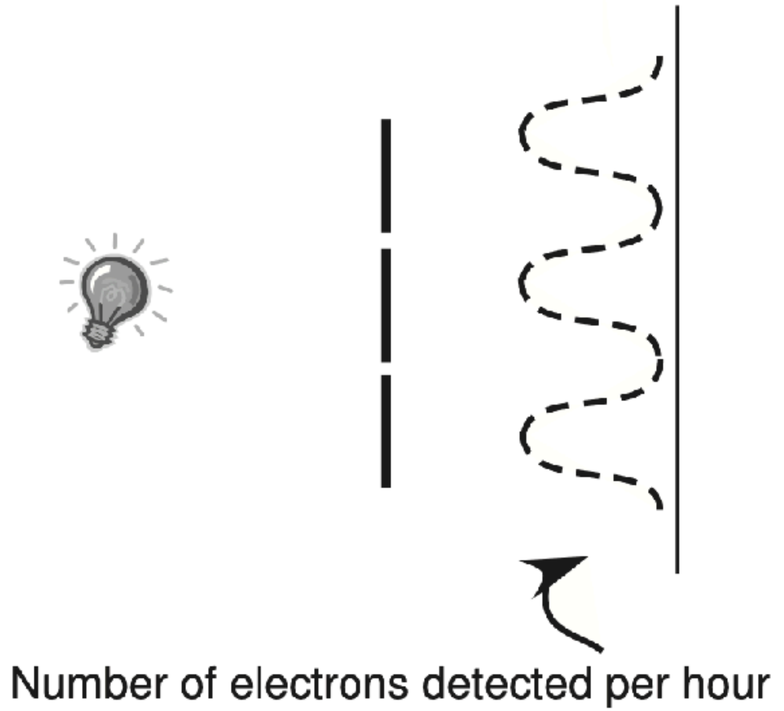
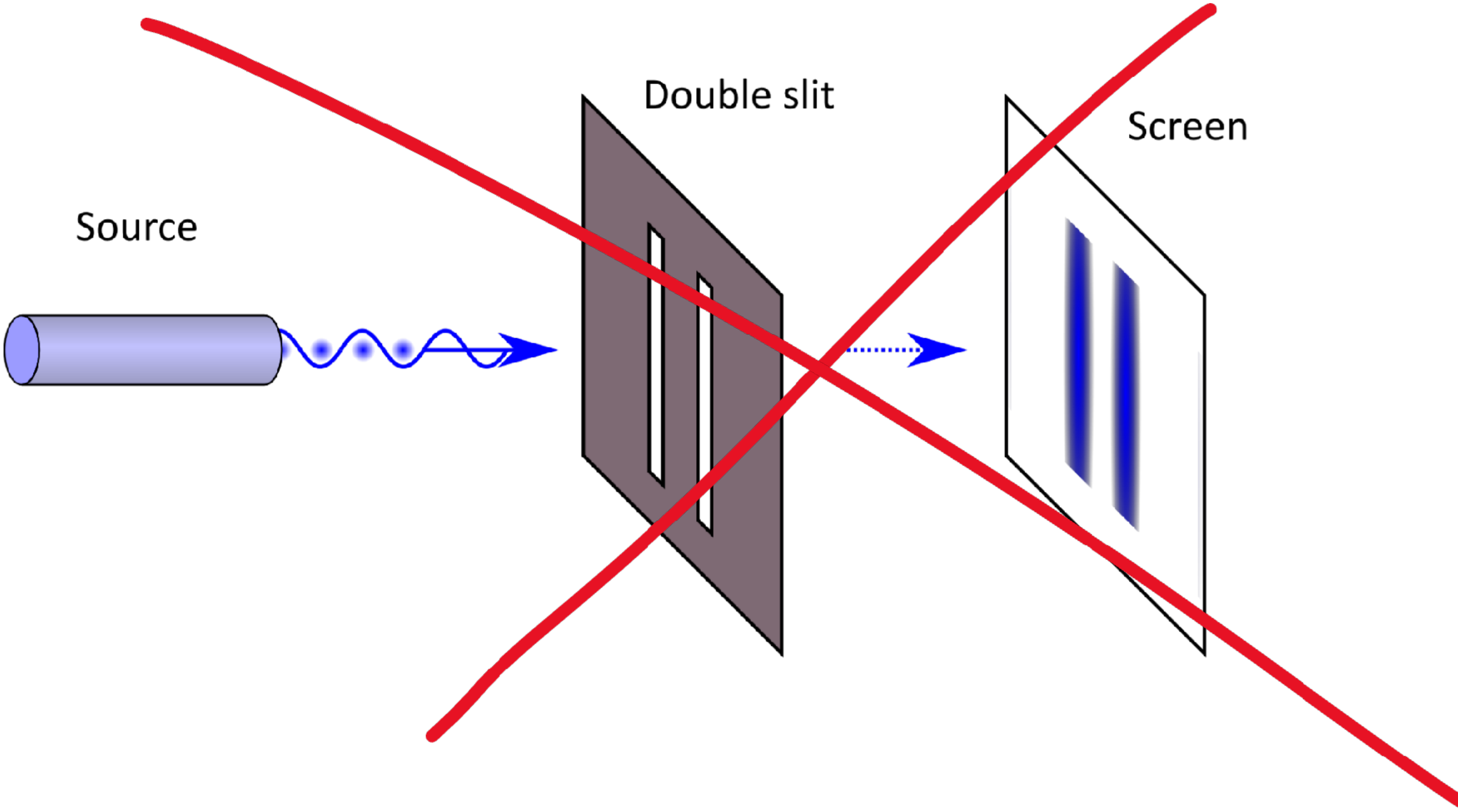
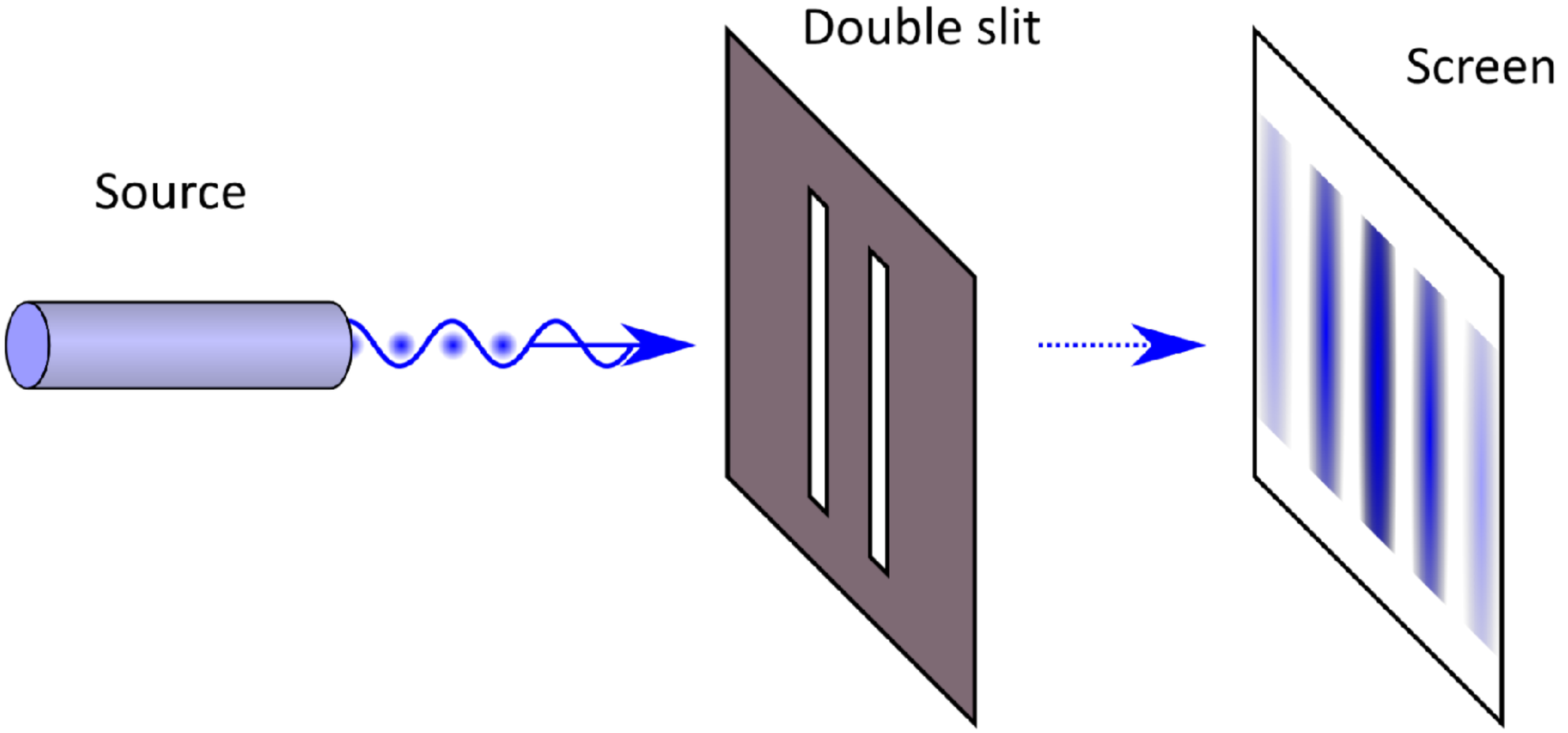
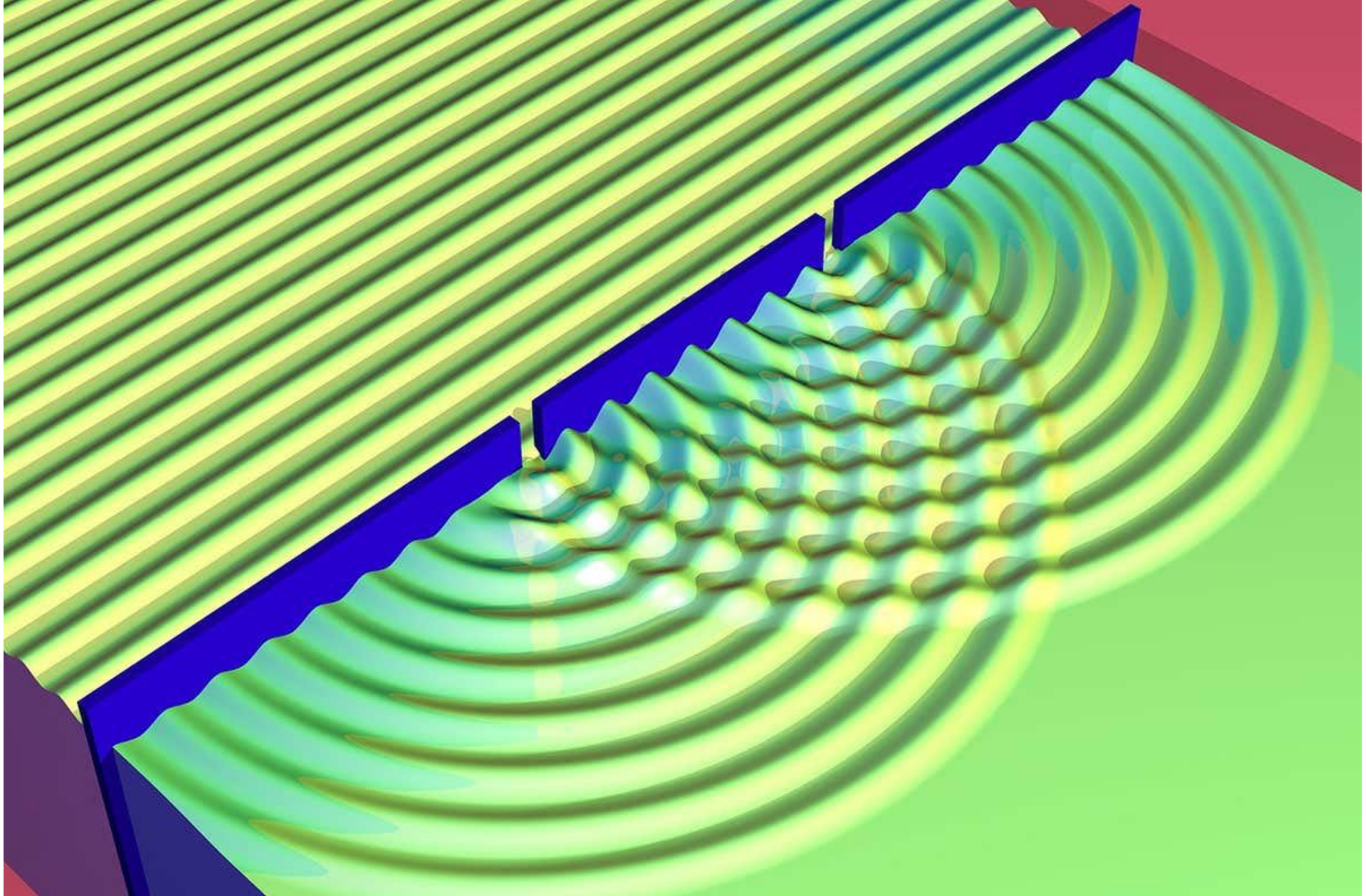


Figure 10.2 When both slits are open in the 2-slit experiment, the number of electrons detected at each position is *not* the sum of numbers when either slit is opened. There are even positions that are hit when each slit is open on its own, but are *not* hit when both slits are open.


Source
Double slit
Screen


Source
Double slit
Screen



Quantum state
1-qubit

a_0 0
a_1 1

a_0, a_1 are probability ‘amplitudes’

amplitudes are complex numbers

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

Probability from amplitude: $p = |a|^2$

Quantum state
2-qubit

a_0 00
a_1 01
a_2 10
a_3 11

Quantum state
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

Quantum state
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

Quantum state
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

Quantum state
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

Quantum state
300-qubit

Length of the quantum state vector: $2^n = 2^{300} = 10^{90}$

Number of atoms in the universe: 10^{80}

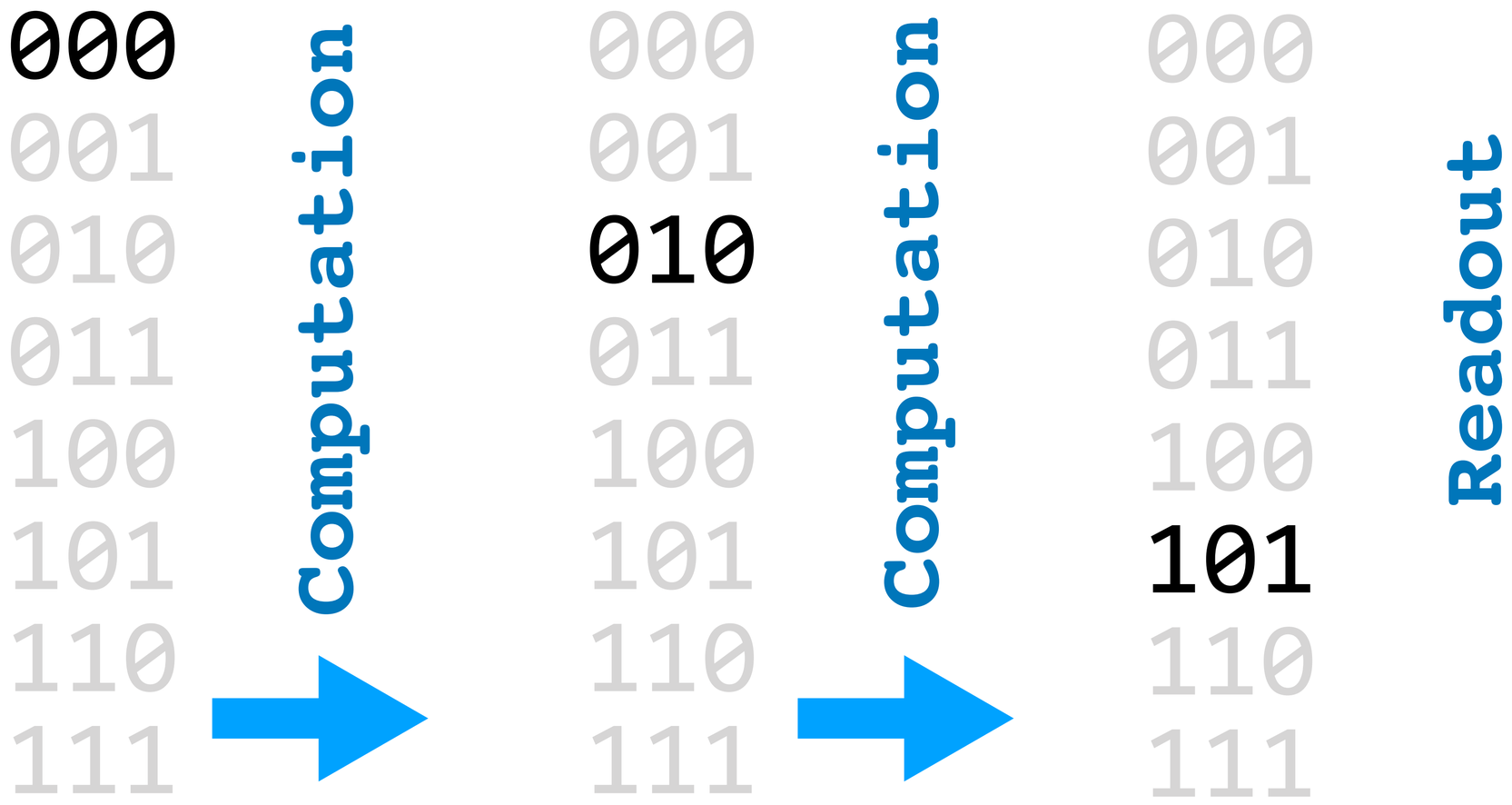
Quantum state
3-qubit

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

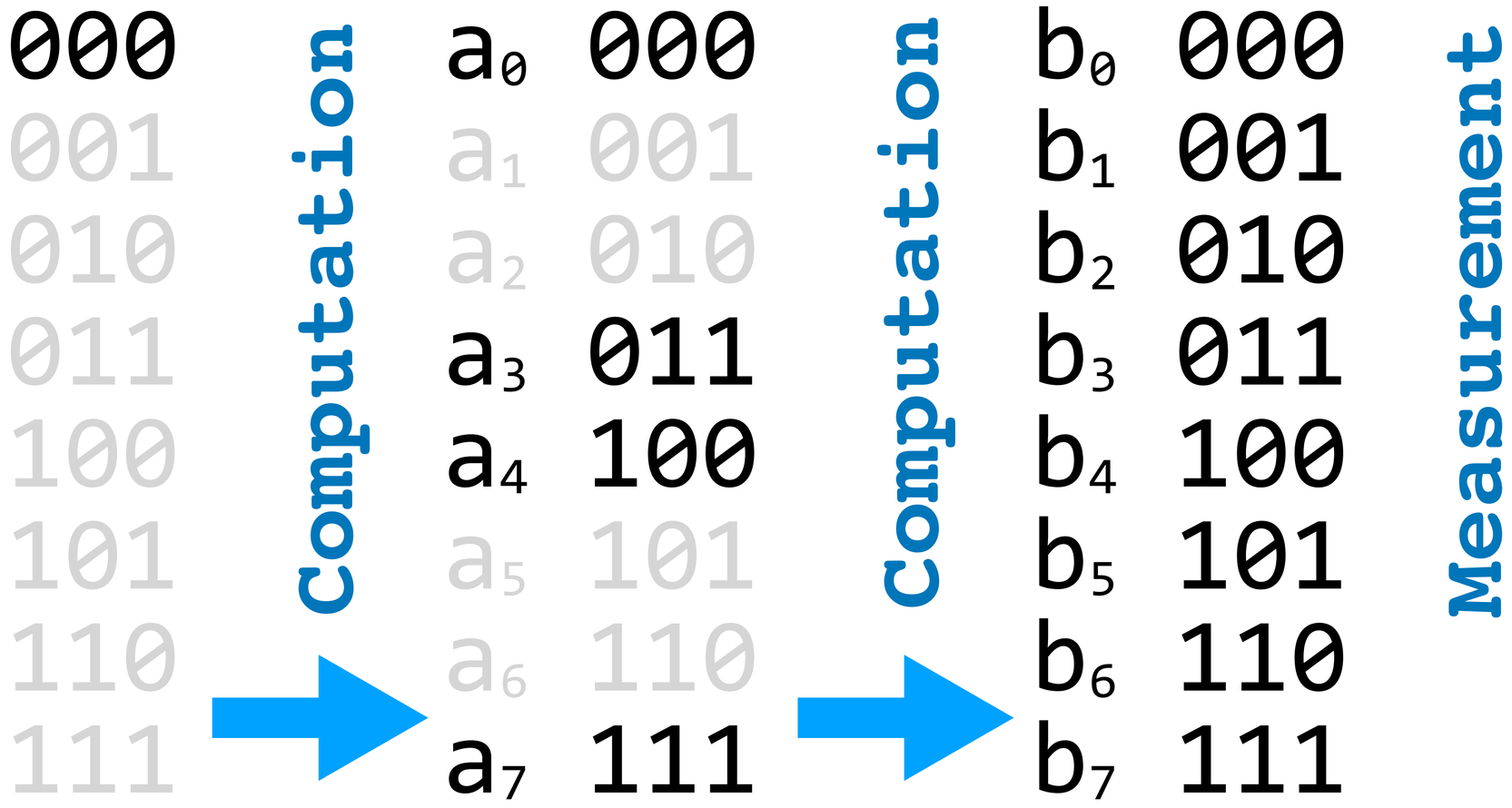
Classical state
3-bit

000
001
010
011
100
101
110
111

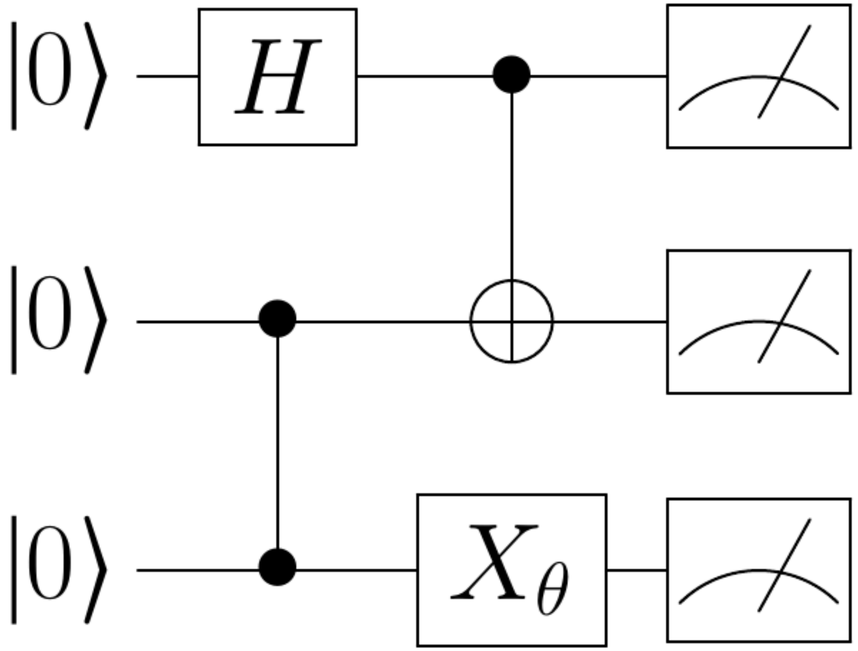
Classical Computation
3-bit



Quantum Computation
3-qubit



Quantum calculation (1)



1000 ‘shots’

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

Quantum calculation (2)

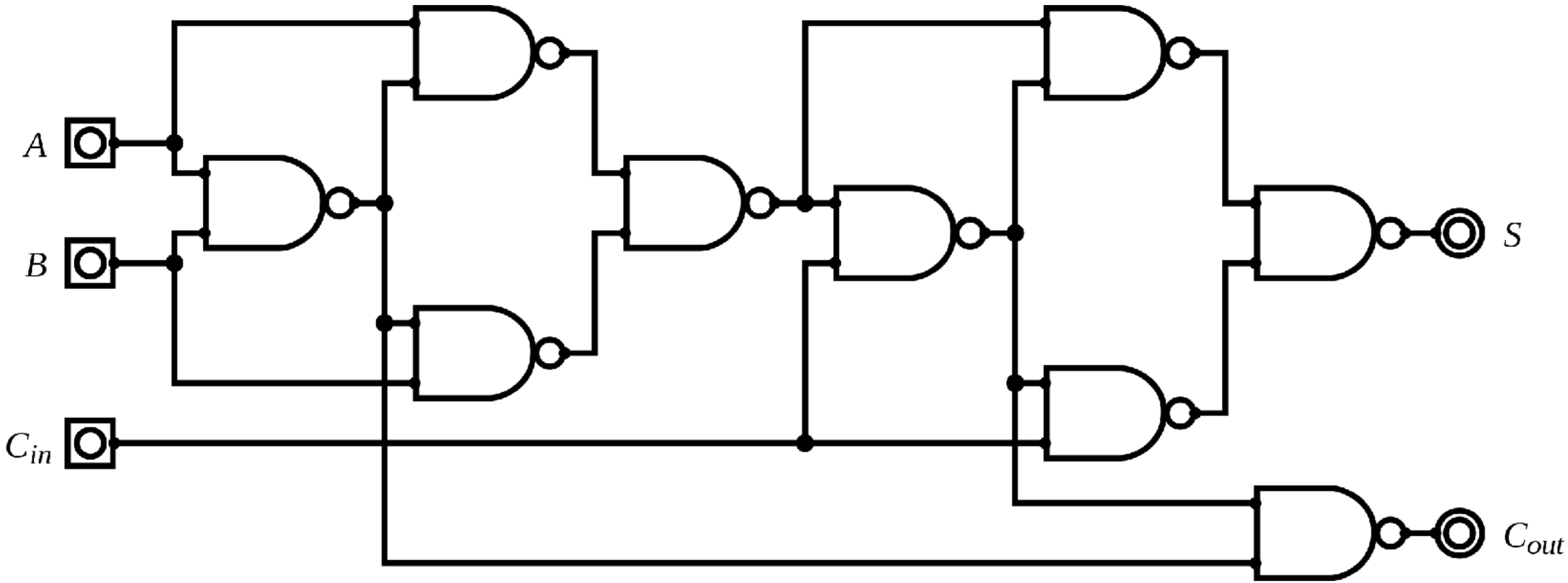
Stochastic: the result is a probability distribution

One 'shot': run a quantum circuit, measure

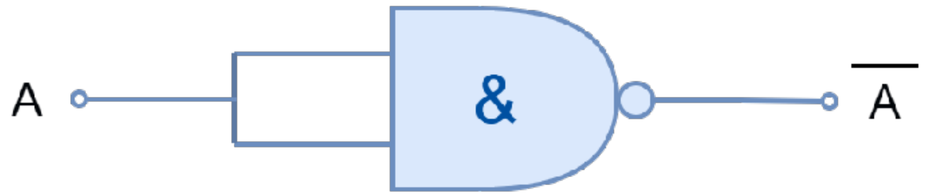
Many shots: sampling the distribution

Result: the vector of probabilities for each qubit string

Classical circuit 1940s

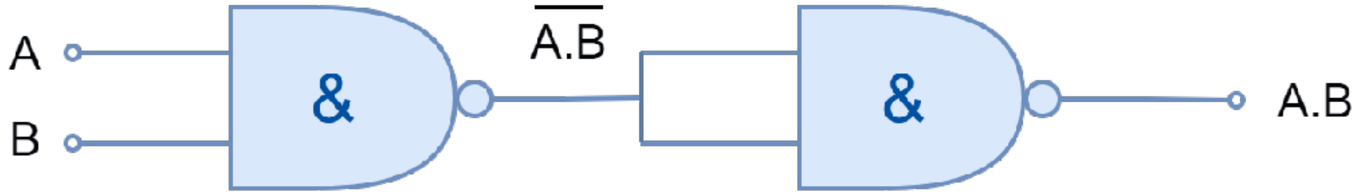


NOT Logic



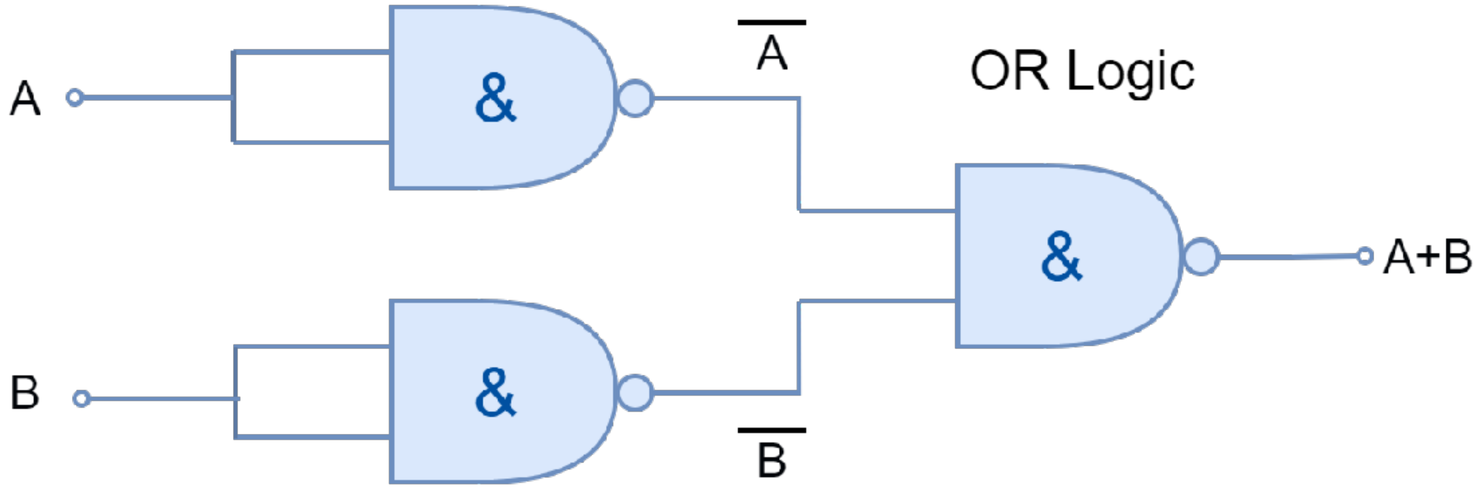
A	Q
0	1
1	0

AND Logic

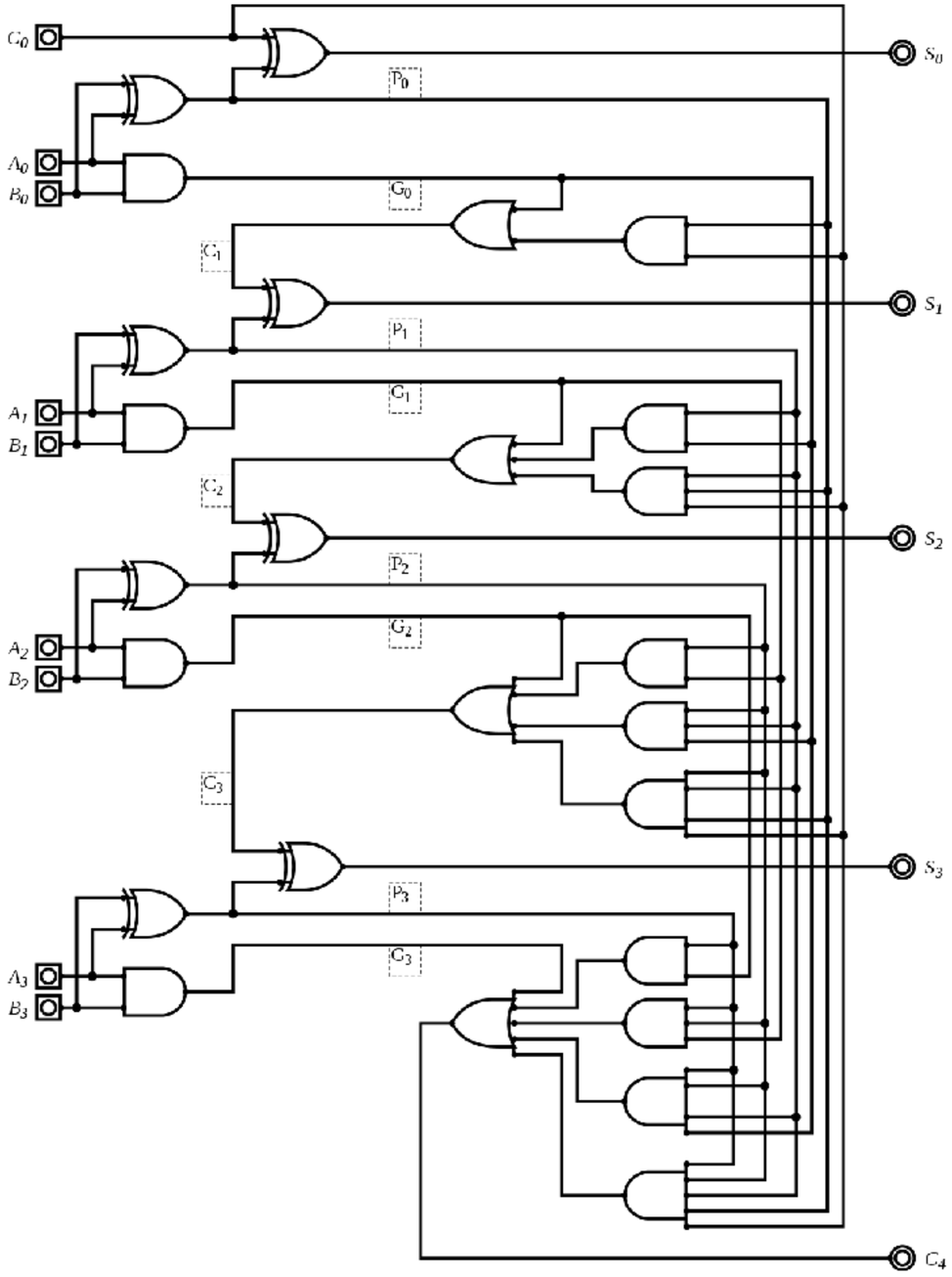


A	B	$\overline{A.B}$	Q
0	0	1	0
0	1	1	0
1	0	1	0
1	1	0	1

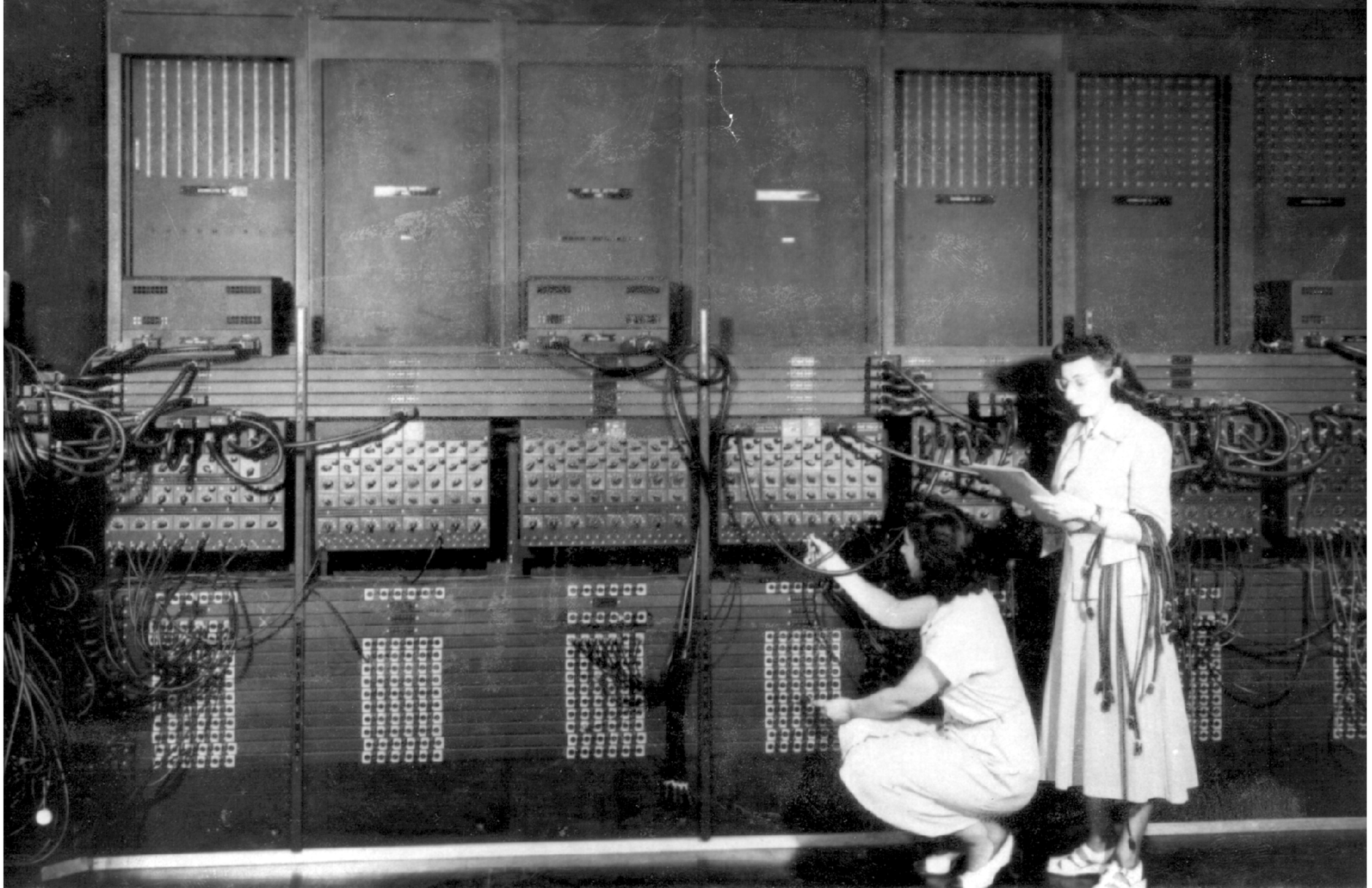
OR Logic



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

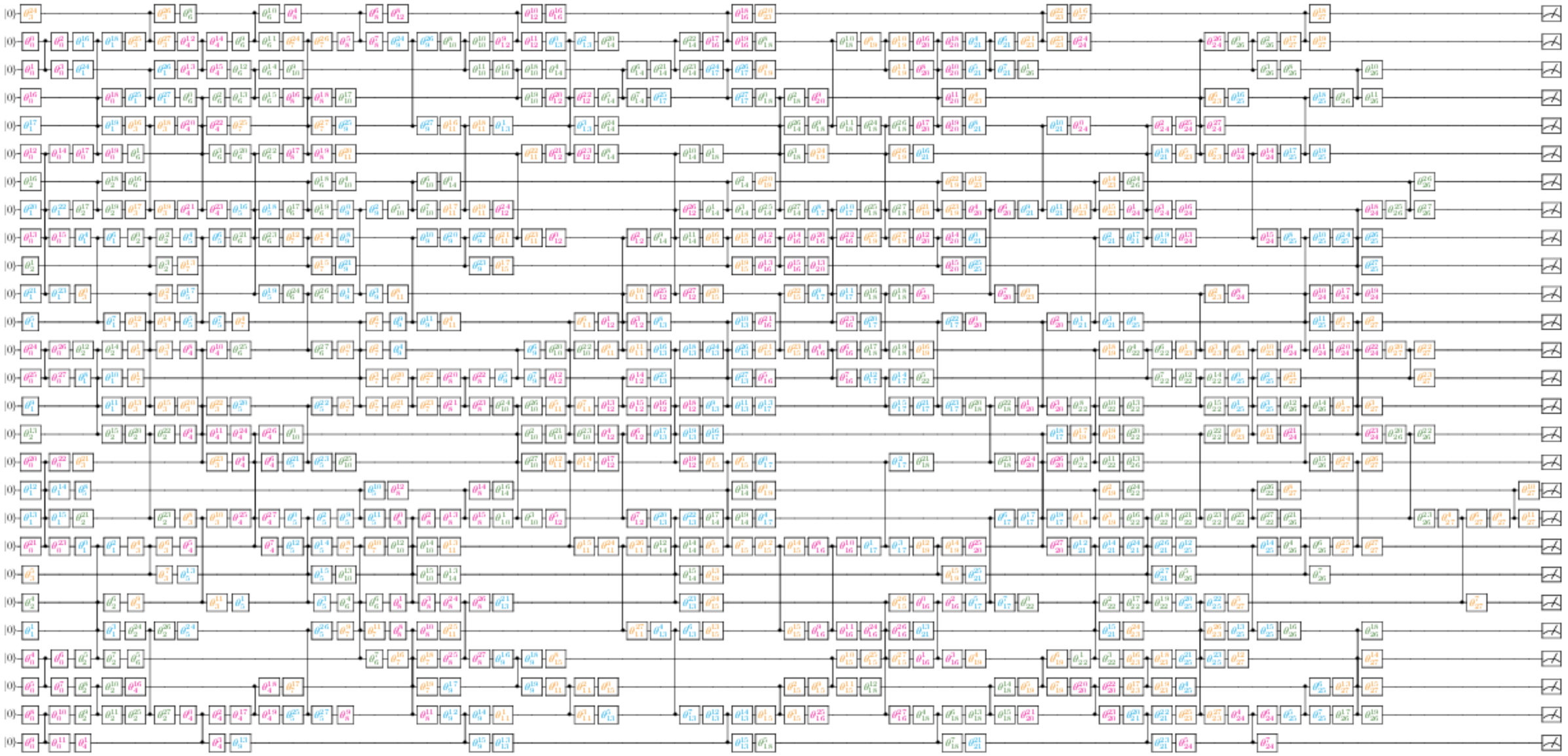


4-bit addition




HOURS
ACCUMULATOR
NO. 8
HEATERS
OFF
ON

27 Qubits



The future of quantum computing

Computers in the future may weigh no more than 1.5 tons

Popular Mechanics, 1949

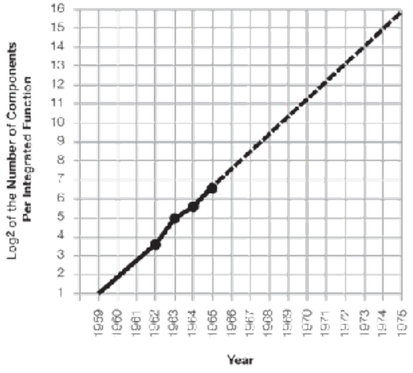
a two-mil square can also contain several kilohms of resistance or a few diodes. This allows at least 500 components per linear inch or a quarter million per square inch. Thus, 65,000 components need occupy only about one-fourth a square inch.

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?

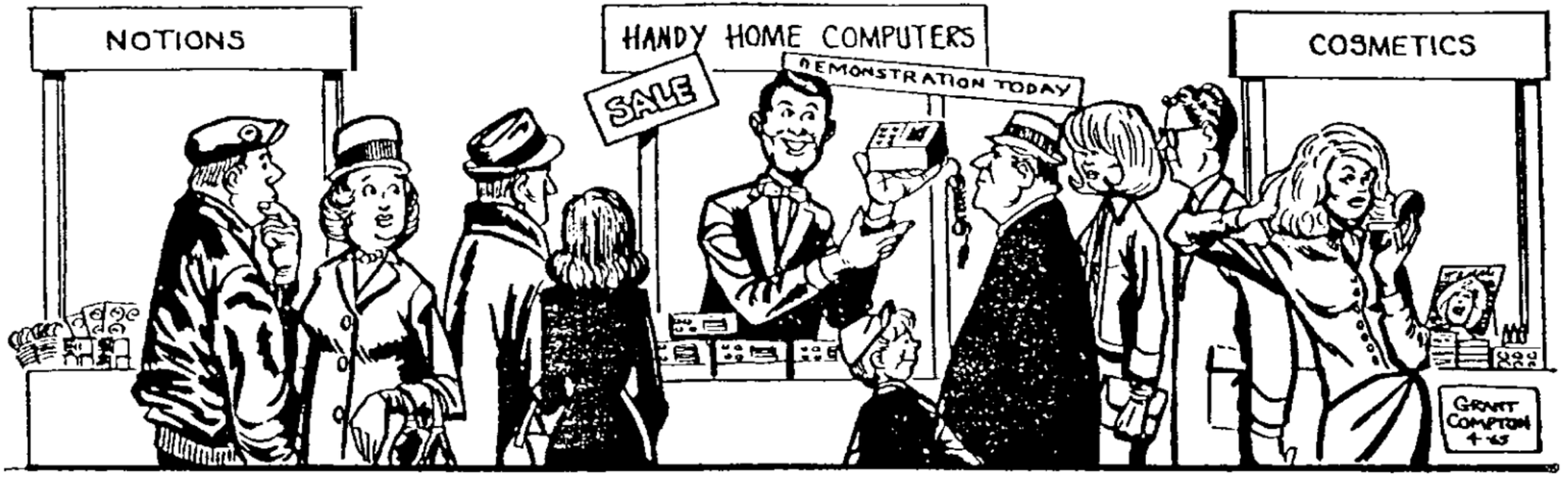
If we could shrink the volume of a standard high-speed digital computer to that required for the components themselves, we would expect it to glow brightly with present power dissipation. But it won't happen with integrated circuits. Since integrated electronic structures are two-dimensional, they have 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.

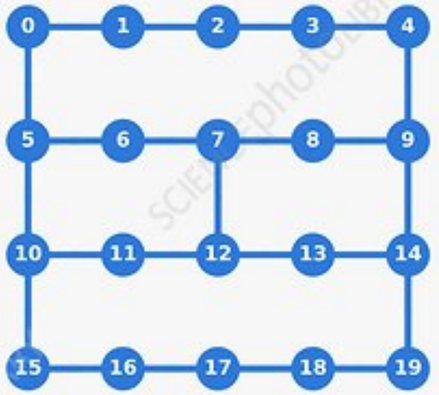
It may prove to be more economical to build large

Gordon E. Moore
1965


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

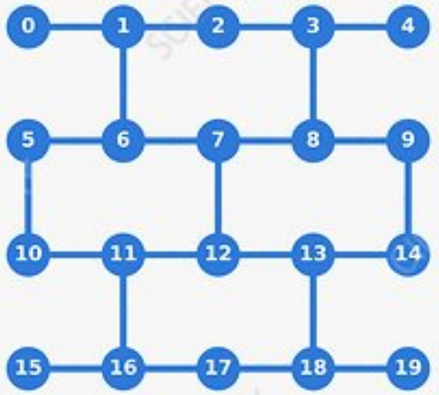
Takeaway message

- Useful quantum computers will arrive in ~2030
- Today there is no quantum software
- Few quantum computer scientists



Johannesburg

Poughkeepsie



Almaden

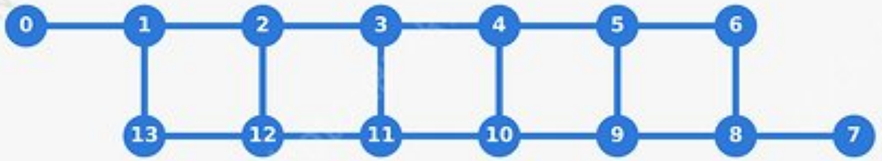
Boeblingen

Singapore

Ourense

Valencia

Vigo



Melbourne

Yorktown