Quantum computers

The coming revolution?

J Avron

February 18, 2021

Overview

1. Revolution or hype?
2. What computers can't do
3. Quantum computers are different
4. What is a qubit
5. Quantum gates
6. Exponential storage capacity
7. Perspective

Four revolutions

1 KW

10^5 KW

Industrial Revolution	Technology	Century
First	Steam engines	18
Second	Electricity	19
Third	Digital	20
Fourth	Quantum	21

ABAQUS

1 b/s

10^9 b/s

Who is into quantum computing

Over 60 companies listed in Wikipedia

Microsoft

IBM

Google

intel

AT&T

amazon

NEC

TOSHIBA

Problems too difficult for ordinary computers

and easy for quantum computers–once they are built

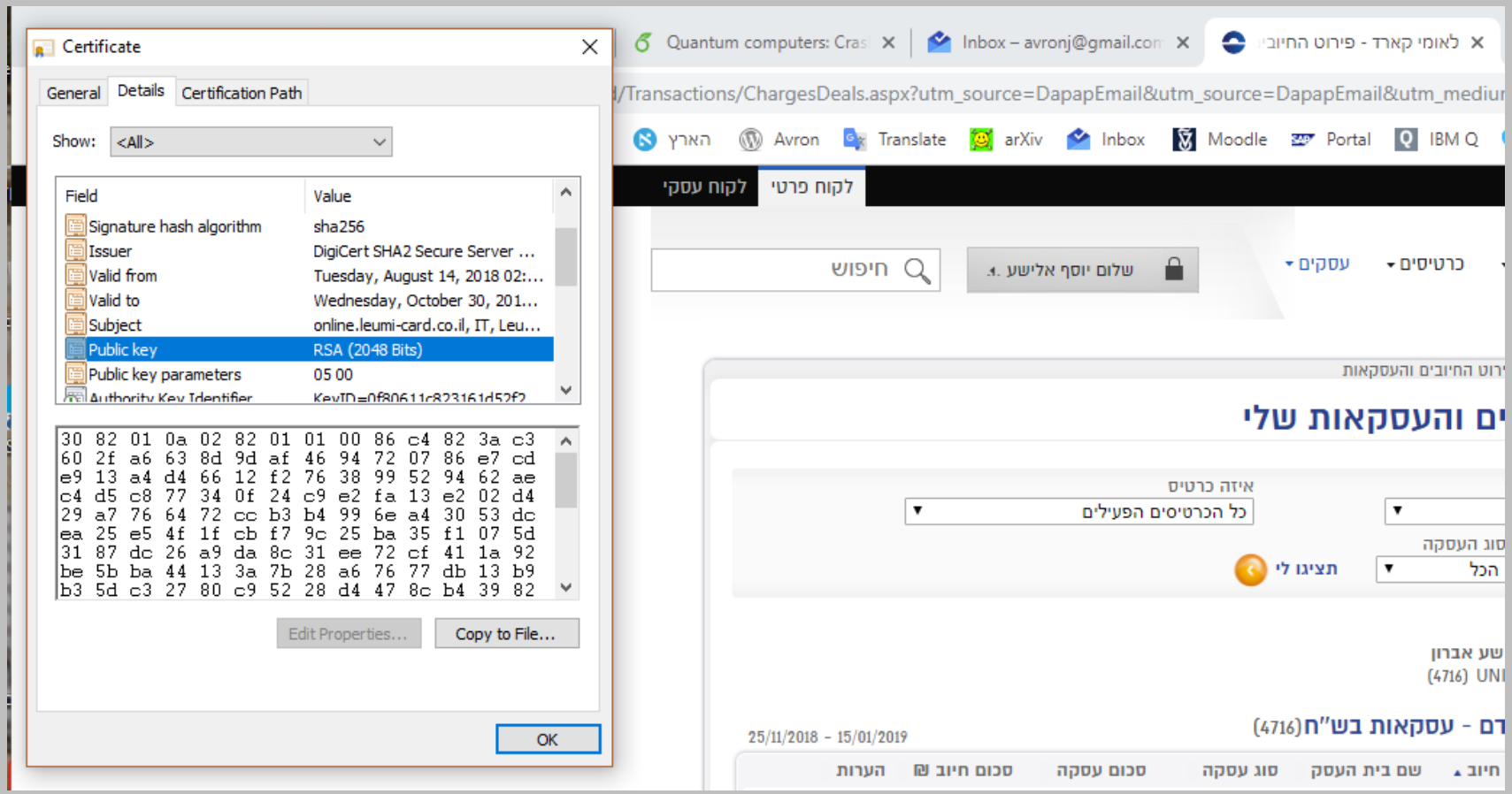
- Break RSA
- Factor large integers
- $19043 = 137 \times 139$
- $137, 139 \in \textit{Primes}$
- Optimiztion in huge dimensions
- Quantum mechanics

Hard problems can be useful

RSA relies on the fact that computers can factor large integers

RSA

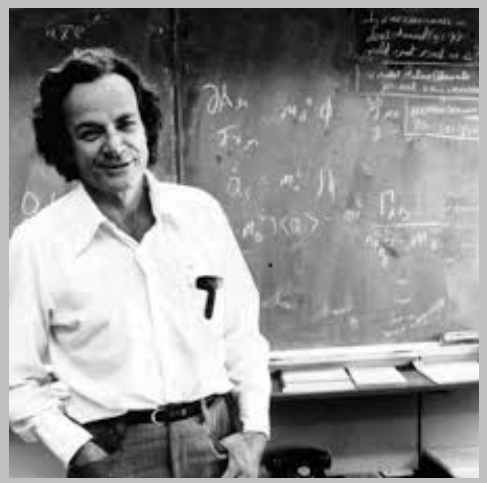
To encrypt you need 137×139 to decript you need the factors



Simulating quantum mechanics is impractical

Suggests: Q-Computers may be more powerful

36 simple atoms need terabyte memory



R. Feynman
1918-1988

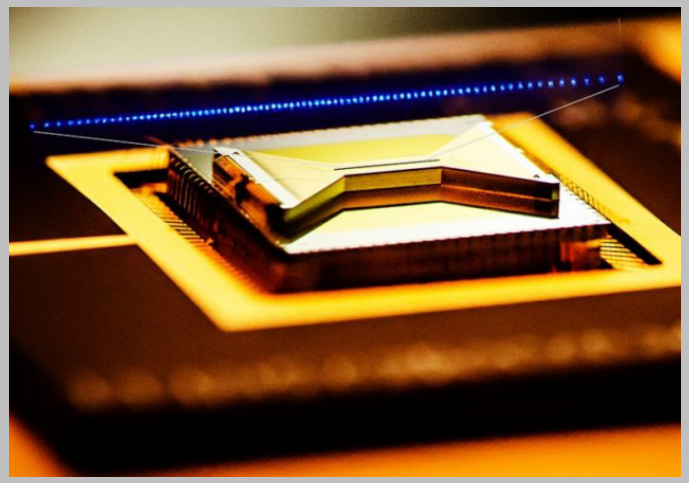
Experiments are expensive

Programming is cheap

Current status: NISQ era

Noisy Intermediate scale quantum

- 50-160 noisy qubits
- Quantum simulations
- Pharma
- Deep learning
- Games
- Education



Killer application: Nobody knows!

Shor algorithm 1994

Breaking RSA

- A Quantum computer will break RSA
- Exponential speedup
- An algorithm
- Need: $O(10^4)$ clean qubits
- Exists: $O(10^2)$ dirty qubits
- Not an imminent threat

Grover search algorithm-1996

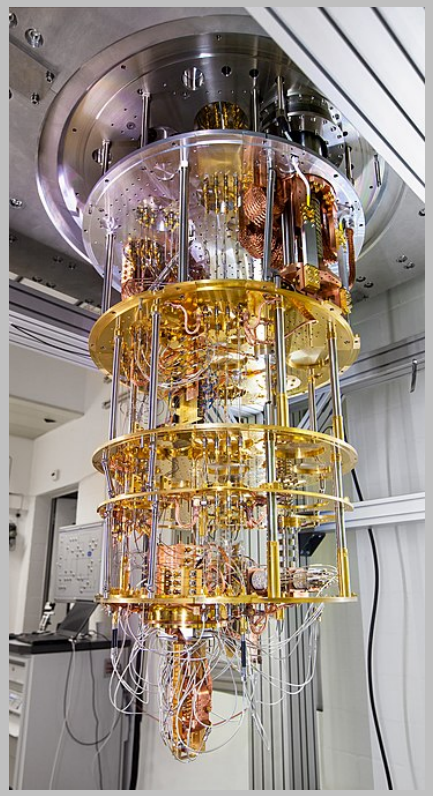
Searching an unstructured data base

- Phone book: $N = 10^6$ entries
- Sorted for Name: $O(\log_2 N) \approx 18$
- Unsorted for Number: $O(N) \approx 10^6$
- Grover: $O(\sqrt{N}) \approx 10^3$

Needs: Phone-book in a Quantum computer

How does a Q-Computer look like?

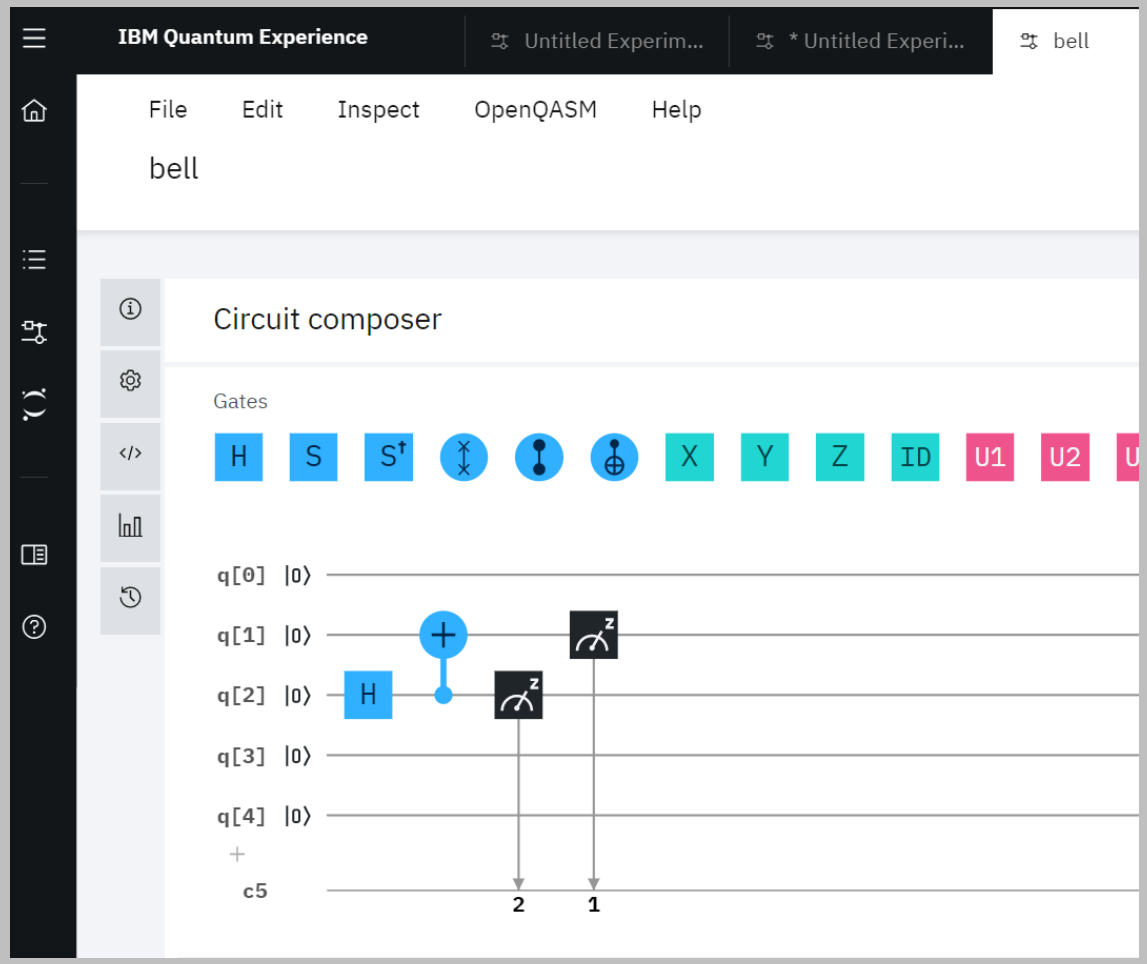
IBM: Super-conducting qubits



Low temperatures: $O(10^{-2} Klevin)$

Cloud quantum computing

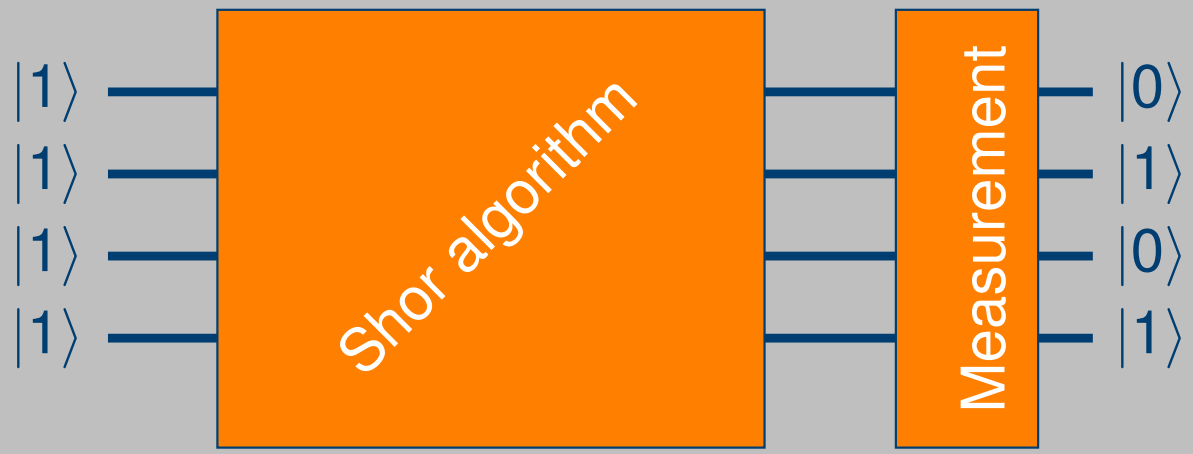
IBM 5 qubits quantum computer

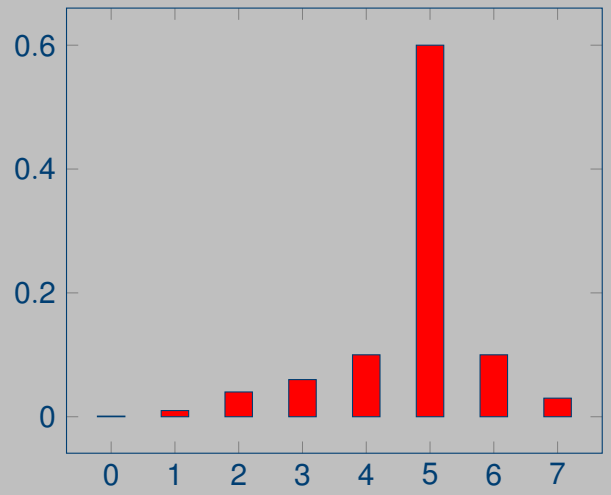


Measure the qubits at the end of the program

Q-Computers are probabilistic

Can be used as oracles





- Feed $15 = 5 \times 3$ into factoring algorithm
- Output: 5 with probability (e.g. $> 1/2$)
- Test if output divides 15 (easy)
- If fail, try again

Data processed by qubits

Qubit: The basic unit of quantum information

- Single photon
- Single atom
- Nuclear spins (MRI)
- Artificial systems
- . . .

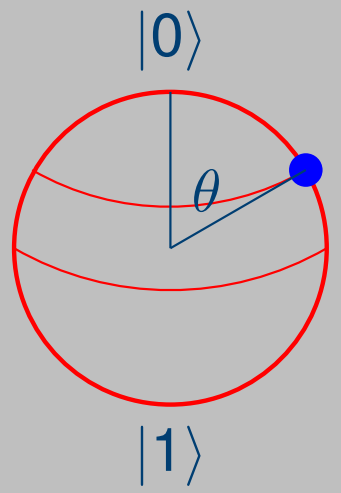
Quantum states

- Measure $|0\rangle$ or $|1\rangle$
- Just like a bit

What is a qubit?

Sphere replacing the coin

- Bit: The two sides of a coin
- Qubit: The unit sphere
- Any superposition is legit
- Measured only: $|0\rangle$ or $|1\rangle$



superposition

Quantum gates rotate $|0\rangle$ to *superposition*

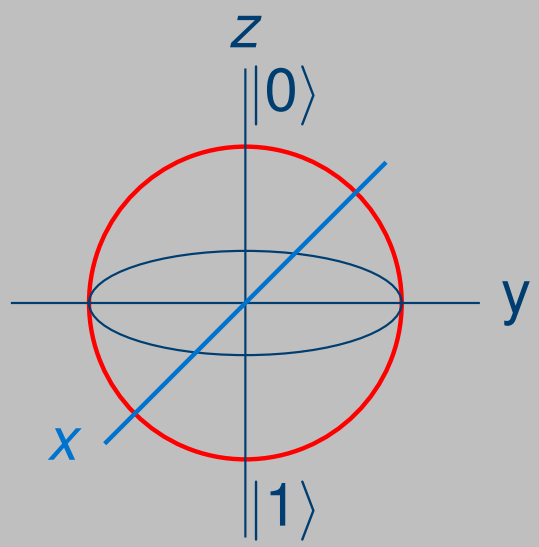
$$\cos(\theta/2)\,|0\rangle + \sin(\theta/2)\,|1\rangle$$

The information in θ is hidden

Quantum gates rotate the qubit

Bit can flip, qubit can rotate arbitrarily

$NOT = 180^0$ rotation around x axis

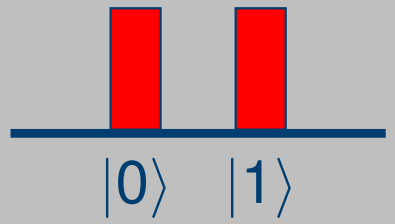


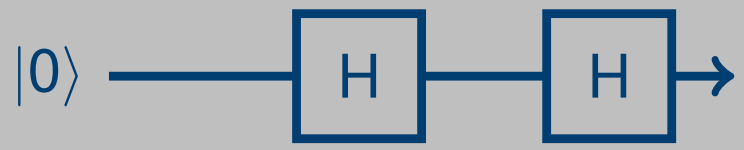
Any rotation

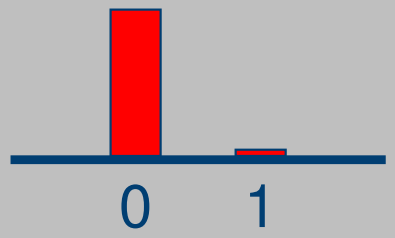
around any axis is allowed

Superposition gate–Hadamard

Making avocado form quantum guacamole





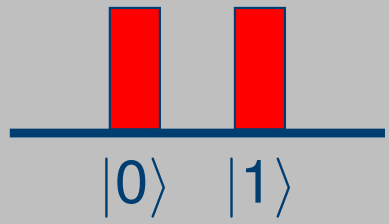


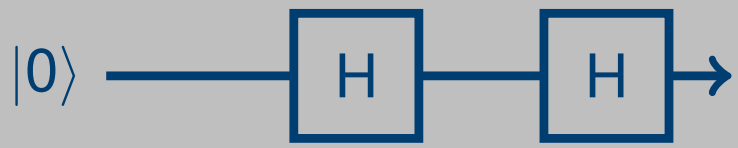
H

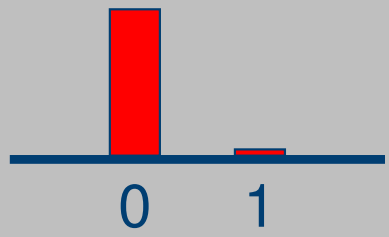
H

Hadamard: Superposition gate

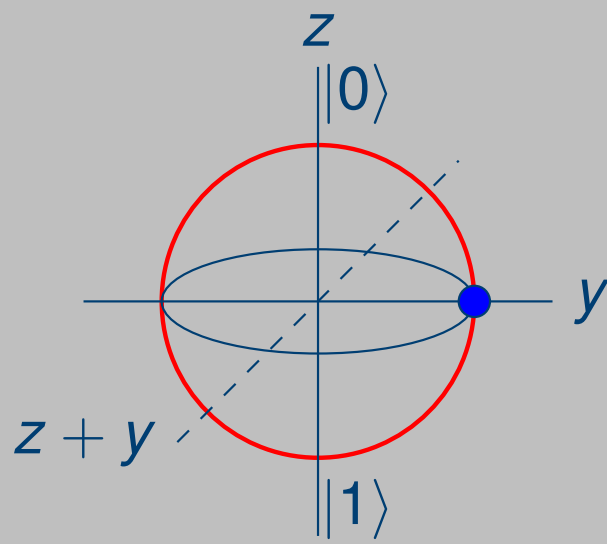
Rotation by π







$H = 180^0$ rotation about the $x + y$ axis



El Khawarizmi, 800 AD

The importance of zero

- 3 decimal digits, label 0-999 numbers
- 3 binary digit, label $2^3 = 0 - 7$ numbers
- Exponential growth
- Age of the universe in seconds: 60 binary digits

3 qubits

- read/write 8 numbers: $|000\rangle, \ldots, |111\rangle$
- Hold any superposition $c_0 |000\rangle + \cdots + c_7 |111\rangle$
- Hold 8 strings $(c_0, \ldots, c_7)$ of complex numbers

El Khawarizmi, 800 AD

The importance of zero

- 3 decimal digits, label 0-999 numbers
- 3 binary digit, label $2^3 = 0 - 7$ numbers
- Exponential growth
- Age of the universe in seconds: 60 binary digits

3 qubits

- read/write 8 numbers: $|000\rangle, \ldots, |111\rangle$
- Hold any superposition $c_0 |000\rangle + \cdots + c_7 |111\rangle$
- Hold 8 strings $(c_0, \ldots, c_7)$ of complex numbers

The belly of the beast

Q-Computers compactly store huge vectors as superpositions

- Classical computer: 8 (32 bits) registers store c_j
- Q-Computer: 3 qubits hold c_j in superposition

30 qubits can store $2^{30} \approx 10^9$ complex numbers c_j

No free lunch

You don't measure c_j

Measurement

Random integer e.g. $|010\rangle$

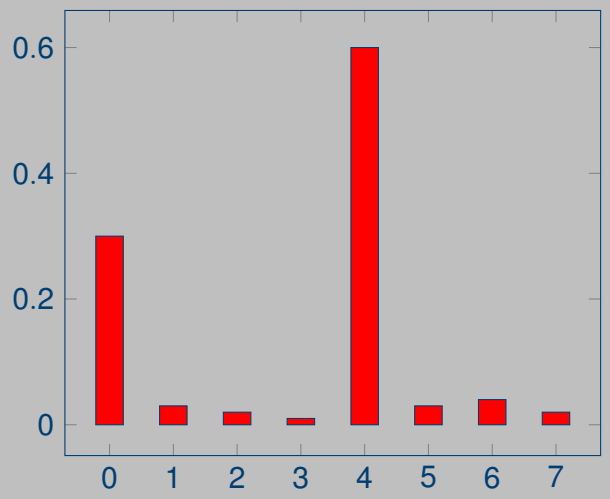
$$c_{000}|000\rangle + c_{001}|001\rangle + \cdots + c_{111}|111\rangle$$

$$Prob(|010\rangle) = |c_{010}|^2$$

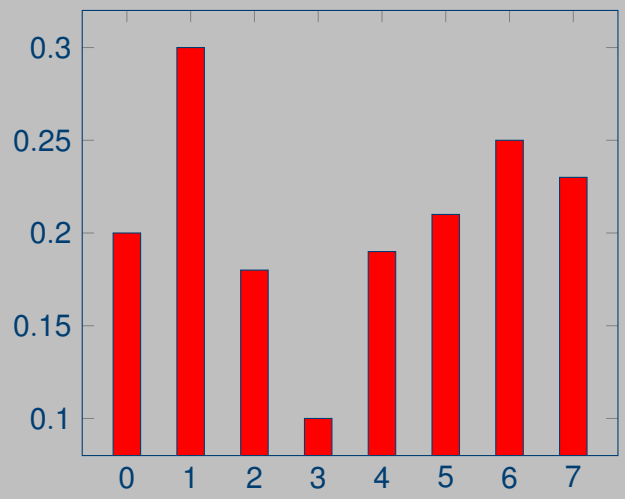
Q-Computers are useful if most $c_j \approx 0$

The art of quantum programming

Superposition with few terms



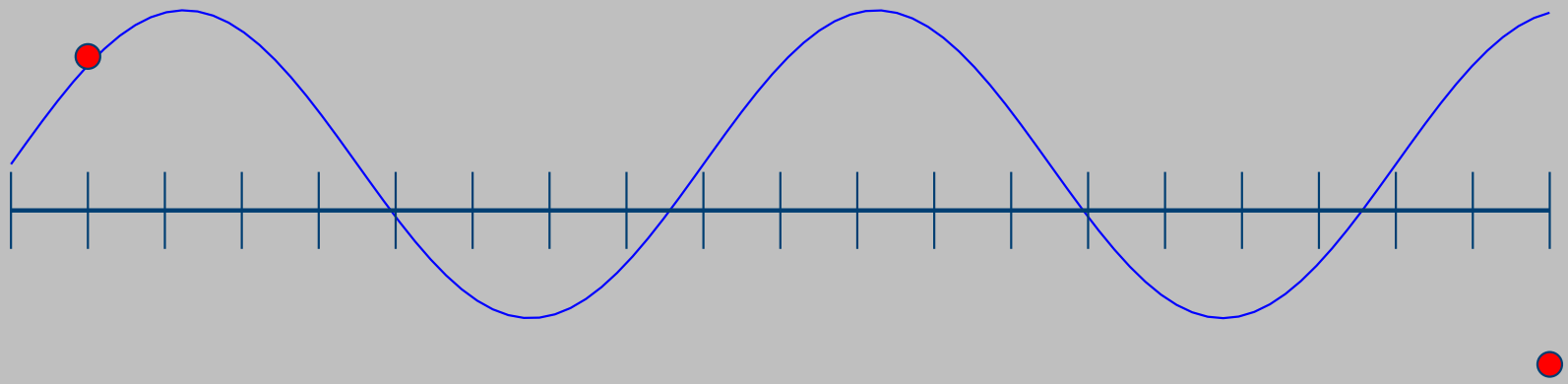
A great algorithm



Bad algorithm

Quantum computers are good a period finding

Long sequence of unknown period

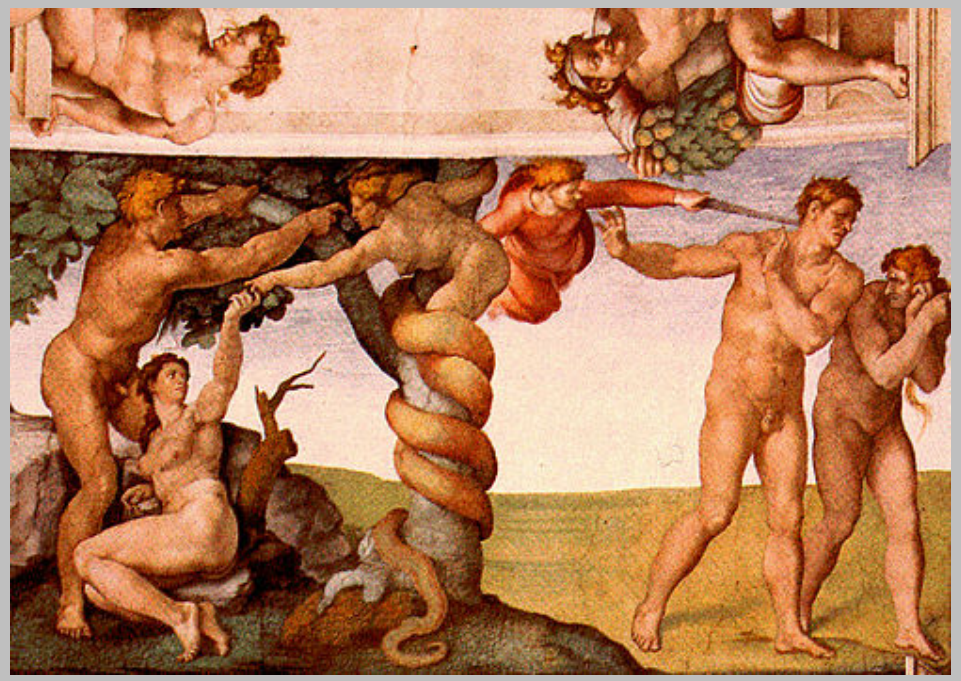


A periodic sequence c has length 2^{10}

- Task: Find the period
- Store c as superposition of 10 qubits
- Computes Fourier transform $\tilde{c}$ (quantumly)
- $\tilde{c}$ is a small superposition
- e.g. $\tilde{c}_0 |0 \dots 0\rangle + \tilde{c}_{2^5} |0 \dots 010 \dots 0\rangle$
- Measurement discloses the period

Q-Computers

- A new computing age
- Superior at some tasks
- Not a panacea
- No threat to RSA yet
- Technological challenge
- Clean qubits



וּמֵעֵ֣ץ הַדַּ֗עַת טֹ֚וב וָרָ֔ע לֹ֥א תֹאכַ֖ל מִמֶּ֑נּוּ כִּ֗י בְּיֹ֛ום אֲכָלְךָ֥ מִמֶּ֖נּוּ מֹ֥ות תָּמֻֽות׃