Quantum computers The coming revolution?

J Avron

February 18, 2021

JA (Technion)

Quantum computers

February 18, 2021 1/24

Overview

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



イロト イヨト イヨト イヨト

Four revolutions







1	ndustrial Revolution	Technology	Century	
F	First	Steam engines	18	
9	Second	Electricity	19	
٦	Third	Digital	20	
F	Fourth	Quantum	21	
QUS QUAL CONTRACTOR CONTRACTOR TANAN TA		10 ⁹ b/s		

ABA

◆□→ ◆□→ ◆国→ ◆国→ 三国

Who is into quantum computing

Over 60 companies listed in Wikipedia



Problems too difficult for ordinary computers

and easy for quantum computers-once they are built

- Break RSA
- Factor large integers
- 19043 = 137 × 139
- 137, 139 ∈ *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 \times 139 to decript you need the factors

Certificate	💰 Quantum computers: Cras x 🔺 🟫 Inbox – avronj@gmail.com x
General Details Certification Path	//Transactions/ChargesDeals.aspx?utm_source=DapapEmail&utm_source=DapapEmail&utm_mediur
Show: <all></all>	🔇 הארץ 🕅 Avron 隆 Translate 🧱 arXiv 🔮 Inbox 📓 Moodle 📨 Portal 💽 IBM Q
Field Value A Signature hash algorithm sha256 hash Islower Dig/Cert SHA2 Secure Server livel of form Valid from Tug/Sect SHA2 Secure Server livel of form Valid from Wednesday, October 30, 201 livel of form Subject Online.leumi-action, JT, Leu livel of the secure Secu	לקוח פרטי לקוח עסקי קוח פרטי לקוח עסקים - 🗎 שלום יופף אלישע א עסקים - עסקים - 🗎 שלום יופף אלישע א
RAAk tey RAA (289 Bit) PARA tey parametes 000 Wathorthy Kay Identifier Kai(T)=0160611+6331614577 V 30 82 01 0e 02 82 01 01 00 08 c4 82 3a c3 a c407=0160611+6331614577 V 40 82 01 0e 02 82 01 01 00 08 c4 82 3a c3 a c407=0160611+6331614577 V 50 24 a6 c3 80 94 af c4 64 94 72 07 76 6e 7 cd c40 c2 c8 7 7 34 07 24 c4 c9 c2 c4 12 c2 02 44 c2 c8 c2 c3 c4 c2 c8 c2 c3 c4 c2 c8 c3 c3 c4 c3 c5 c4 c5 c5 c3 c4 c3 c5 c4 c5 c5 c3 c4 c3 c5 c4 c4 c5 c5 c3 c4 c3 c5 c4 c4 c3 c5 c5 c4 c5 c5 c3 c4 c4 7 c5 c4 c4 c3 c8 c5 c4 c4 c5 c5 c5 c4 c4 c4 c8 c4 c4 c5 c4 c4 c5 c4 c4 c4 c5 c4 c4 c5 c4 c4 c4 c5 c4 c4 c4 c5 c4 c4 c4 c5 c4 c4 c5 c4 c4 c4 c4 c4 c5 c4 c4 c4 c5 c4 c4 c4 c4 c4 c4 c4 c5 c4	יזם ההיבים העסקאות ים והעסקאות שלי איזה כרטים שג העסקה הכל יד תציגו לי יי
Edt Properties Copy to File	שע אברון ועו (אנז-) דם - עסקאות בש"ח(אורא) דים - עסקאות בש"ח (אורא) חיוב - שם בית העסק סוג עסקה סכום עסקה סכום חיוב ₪ הערות

February 18, 2021

6/24

Quantum computers

JA (Technion)

Simulating quantum mechanics is impractical

Suggests: Q-Computers may be more powerful

36 simple atoms need terabyte memory



Experiments are expensive Programming is cheap



R. Feynman 1918-1988

・ロ・・ 日本・ ・ 日本・

Current status: NISQ era

Noisy Intermediate scale quantum

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



Killer application: Nobody knows!

<ロト < 同ト < 回ト < 回ト = 三日

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



<ロト < 同ト < 回ト < 回ト = 三日

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

February 18, 2021 10/24

<ロト < 同ト < 回ト < 回ト = 三日 - 三日 -

Quantum computers are differen

How does a Q-Computer look like?

IBM: Super-conducting qubits



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

JA (Technion)

Quantum computers

February 18, 2021 11/24

Cloud quantum computing

IBM 5 qubits quantum computer

≡	IB	A Quantum Experience 😂 Untitled Experim 😂 * Untitled Experim 😂 bell
ඛ		File Edit Inspect OpenQASM Help
—		bell
≔		
앜	1	Circuit composer
ζ).	۲	Gates
		H S S' 🕻 🕻 🖨 X Y Z ID U1 U2 U
œ	lafi	
_	J	q[0] 0>
(?)		
		q[2] 0) - H
		q[3] 0)
		q[4] 0>
		+ c5
		2 1

Measure the qubits at the end of the program

JA (Technion)

Quantum computers

February 18, 2021 12/24

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

February 18, 2021 13/24

Data processed by qubits

Qubit: The basic unit of quantum information

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

Ο . . .

Quantum states • Measure $|0\rangle$ or $|1\rangle$ Just like a bit





<ロト < 同ト < 回ト < 回ト = 三日 - 三日 -

|1>

 $|0\rangle$

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 $|1\rangle$



Quantum gates rotate $|0\rangle$ to *superposition* $\cos(\theta/2) |0\rangle + \sin(\theta/2) |1\rangle$ The information in θ is hidden

February 18, 2021 15/24

・ロット (四) ・ (日) ・ (日) ・ (日)

Quantum gates rotate the qubit

Bit can flip, qubit can rotate arbitrarily

$NOT = 180^{\circ}$ rotation around x axis



Any rotation around any axis is allowed

JA (Technion)

Quantum computers

February 18, 2021 16/24

<ロト < 同ト < 回ト < 回ト = 三日

Superposition gate-Hadamard

Making avocado form quantum guacamole



Э

<ロト < 四ト < 回ト < 回ト

Hadamard: Superposition gate

Rotation by π



JA (Technion)

February 18, 2021 18/24

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



<ロト < 同ト < 回ト < 回ト = 三日

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



▲□▶ ▲□▶ ▲□▶ ▲□▶ □ ののの

The belly of the beast

Q-Computers compactly store huge vectors as superpositions

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



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

・ロット (四) ・ (日) ・ (日) ・ (日)

No free lunch

You don't measure c_j



$Prob(|010\rangle) = |c_{010}|^2$ Q-Computers are useful if most $c_j \approx 0$

JA (Technion)

Quantum computers

February 18, 2021 21/24

Э

The art of quantum programming

Superposition with few terms



Э

<ロト < 四ト < 回ト < 回ト

Quantum computers are good a period finding

Long sequence of unknown period



Perspective

Q-Computers

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



וּמֵעֵּץ הַדַּעַת טוב וָרָע לָא תאכל מִמֶּנוּ כִּי בְּיוֹם אֲכָלְךָ מִמֶּנוּ מָוֹת תָּמְוּת

February 18, 2021 24/24