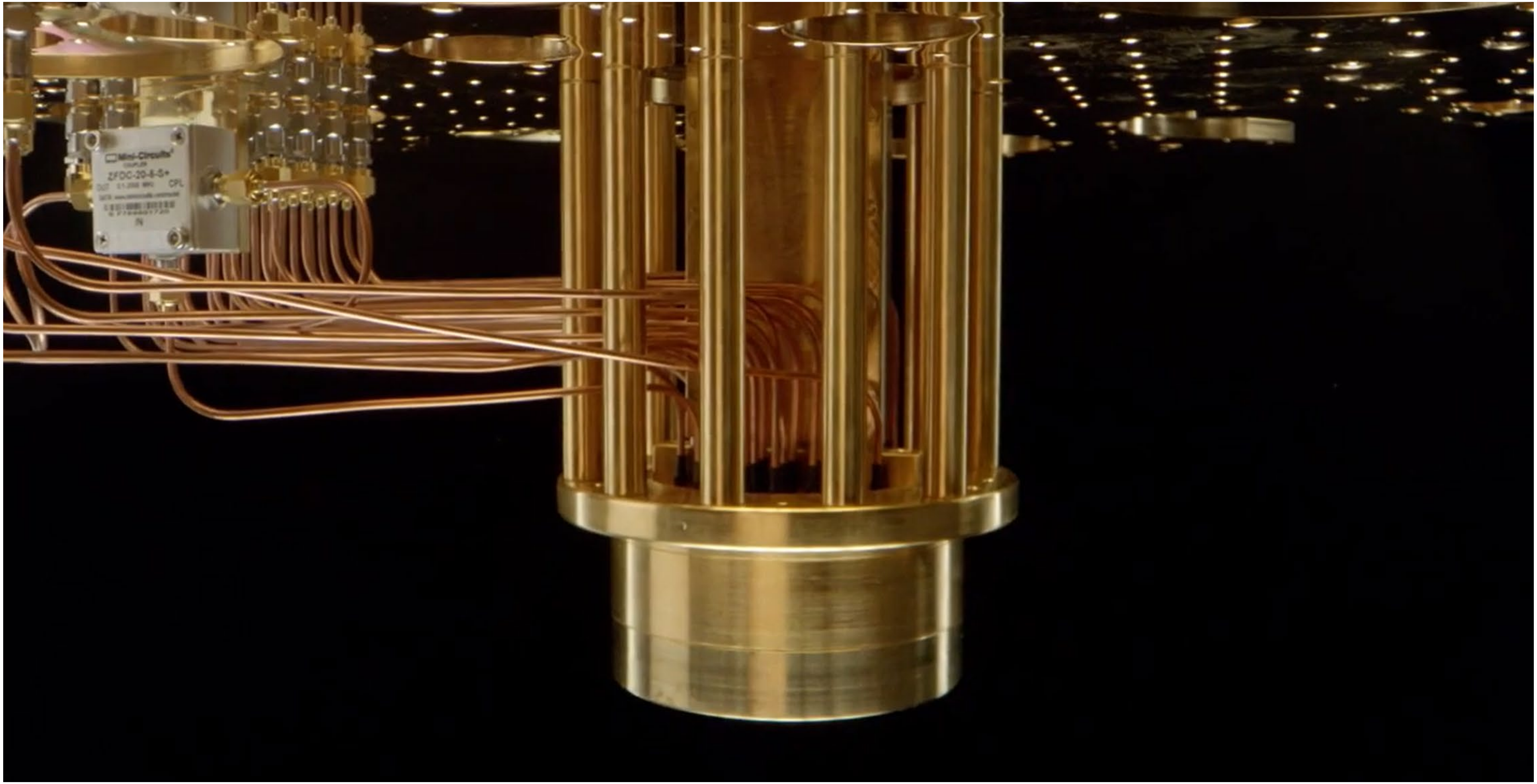
Mathematics of Quantum Computing: Ideas and Reality

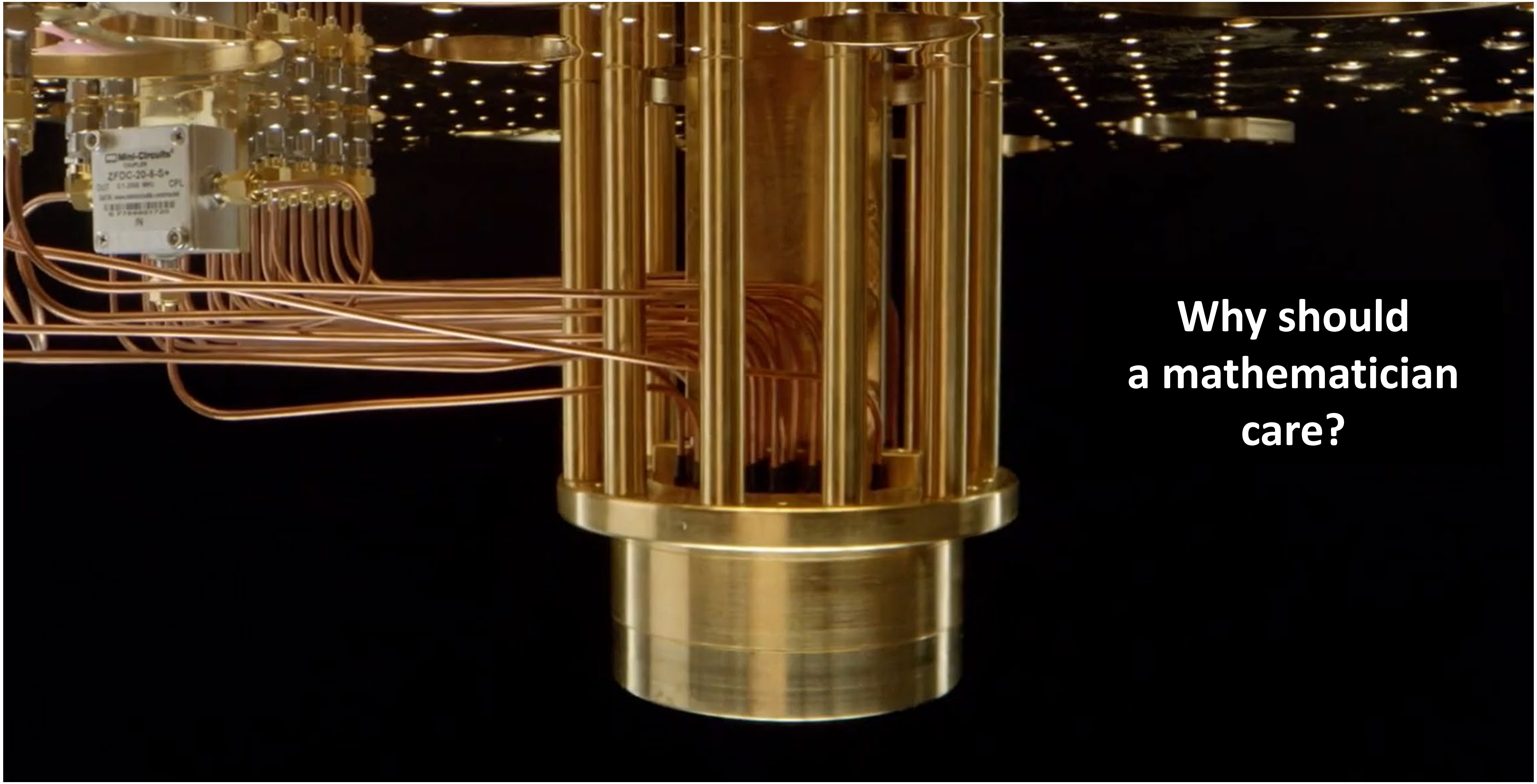
Alexei Bocharov

Microsoft (Quantum Systems)

Alexandre Vinogradov Memorial Conference, December 2021


Mini-Circuits
CPL
IN


Cryptography Apocalypse
Preparing for the Day When Quantum Computing Breaks Today's Crypto
Roger A. Grimes


Why should
a mathematician
care?

Abstract

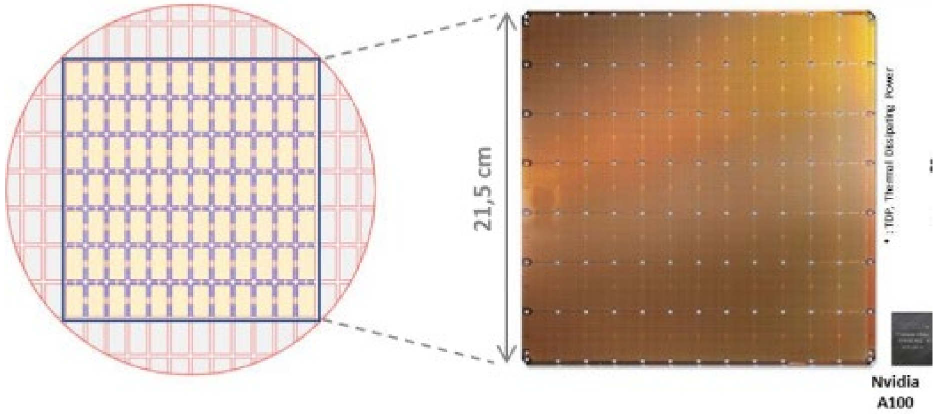
- This talk goes over the basics of quantum computing, gives a high-level view of Shor’s quantum-assisted integer factorization algorithm, introduces one of the key designs of Quantum error correction – the toric code - and emphasizes the need for native topological protection of quantum information.
- The talk is an introductory overview of quantum computing concepts meant for mathematicians. Basic familiarity with the principles of quantum mechanics is assumed.

What is in this talk

- Beyond Silicon, towards Quantum
- Mathematics of an Ideal Quantum Computer
- What is Exponential (Superpolynomial) Advantage
- Quantum Error Correction: Algebra and Topology
- Noisy Intermediate Scale Quantum
- Credits and further reading: Understanding Quantum Technologies 2021 [https://www.oezratty.net/wordpress/2021/understanding-quantum-technologies-2021/]

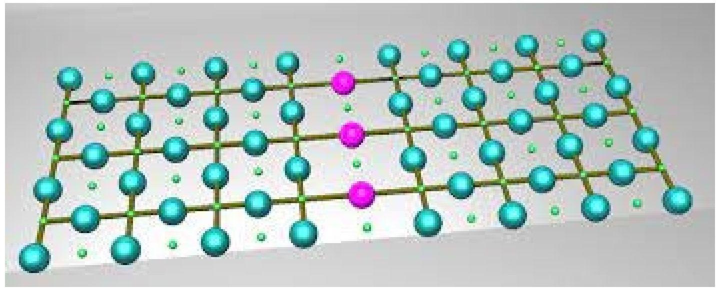
Beyond Silicon, towards Quantum

- Celebras' 2.6 trillion (7 nm) transistors, 15 kW consumption



10 x 

- How many qubits we need for similar compute?



[credit: New Journal of Physics, 2012]

$$2^{\mathbf{42}} > 2.6\ 10^{12}$$

Mathematics of an Ideal Quantum Computer, 1

- **Qubit. State space of a qubit.**

2-level quantum device with basis $|0\rangle, |1\rangle$ and state space $S^3 \subset \mathbb{C}^2$:

$$\alpha|0\rangle + \beta|1\rangle, \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

- **Z-measurement. Born rule.**

Observation procedure on a qubit. Forces the qubit into either $|0\rangle\ or\ |1\rangle$ state.

$$p_0 = |\alpha|^2; p_1 = |\beta|^2$$

- **Ideal RNG**: (1) prepare a qubit in state $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$; (2) measure; (3) repeat

- (699) Erwin Schrodinger Gets Pulled Over By Cops: Pirate Stu's Bootyful Joke of the Day #0036 - YouTube

Mathematics of an Ideal Quantum Computer, 1

- **Qubit. State space of a qubit.**

Labels for orthogonal contravariant vectors

2-level quantum device with basis $|0\rangle, |1\rangle$ and state space $S^3 \subset \mathbb{C}^2$

$$\alpha|0\rangle + \beta|1\rangle, \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

- **Z-measurement. Born rule.**

Observation procedure on a qubit. Forces the qubit into either $|0\rangle\ or\ |1\rangle$ state.

$$p_0 = |\alpha|^2; p_1 = |\beta|^2$$

- **Ideal RNG**: (1) prepare a qubit in state $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$; (2) measure; (3) repeat

- (699) Erwin Schrodinger Gets Pulled Over By Cops: Pirate Stu's Bootyful Joke of the Day #0036 - YouTube

Ideal Quantum Computer, 2 $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$

- **Multi-qubit ensemble. State-space of n–qubit register.**

State space of an ensemble of n ideal qubits is S^{2N-1},$N = 2^n$

In the basis $|0\rangle, \ldots |N-1\rangle$ an n–qubit state is

$$|\psi\rangle = \sum_{k=0}^{N-1} \alpha_k |k\rangle, \alpha_k \in \mathbb{C}, \sum_{k=0}^{N-1} |\alpha_k|^2 = 1$$

- **Observables and measurements.**

An observable for n–qubit states is a Hermitian operator on $\mathbb{C}^N$

Let $\mathcal{O}$ be an observable and $E_1 \oplus \cdots \oplus E_M = \mathbb{C}^N$ be its eigen-decomposition. Then measurement of $\mathcal{O}$ in quantum state $|\psi\rangle$ projects the quantum state onto one of the E_m with the probability

$$p_m = \left|Pr_{E_m}\psi\right|^2$$

- Thus a quantum state can be viewed as **probability distribution for observation outcomes.**

Mathematics of an Ideal Quantum Computer, 3

- **Full $\boldsymbol{n}$–qubit measurement**

If we measure out each of n qubits we get a bit string of length n

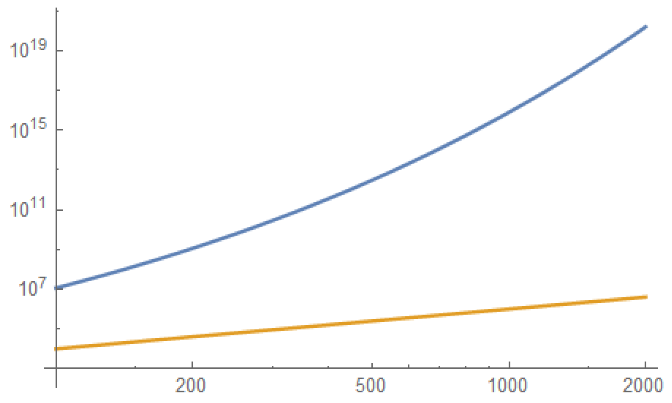
Suppose $\mathcal{H}$ is the Hilbert state space of the n qubits, $|\psi_0\rangle$ is some standard initial state, $U: \mathcal{H} \to \mathcal{H}$ is some constructive unitary operator.

Measurements of quantum state $U|\psi_0\rangle$ define a probability distribution on $\{0,1\}^n$:

$$\boldsymbol{x} \in \{0,1\}^n: P_U(\boldsymbol{x}) = |\langle \nu(\boldsymbol{x}) | U\psi_0 \rangle|^2$$

At the **core of a typical quantum algorithm** there is a specifically designed unitary U that implements a distribution over bit strings, where probabilities of the desired bit strings are higher than the probabilities of undesired ones.

Shor's Integer Factorization (1994): Concepts



- **Claims:**

Consider a product of two odd primes $N = P_1 P_2$

The best traditional (field sieve) method for finding these primes has "sub-exponential" time complexity of roughly $\tilde{O}\left(\exp(1.9\,(\log N)^{1/3})\right)$

Using ideal quantum computer this can be done in time $\tilde{O}\left((\log N)^2\right)$

- This is called **superpolynomial** speed-up (or, loosely, "exponential" speed up)

Practical takeaway: a 1024-bit RSA encryption key, for one, can be broken in **minutes** using ideal quantum computer instead of estimated **½ million core-years**.

Shor’s Integer Factorization: Concepts, 2

$N = P_1 P_2$

- **The core idea (number theory, reduction to period finding)**

Pick a random integer $a < \mathrm{N}$. W.l.o.g. $\gcd(a, N) = 1$

Then the function $\boldsymbol{f(k) = a^k \; mod \; N}$ has a period $r < N$

If r is even and $a^{r/2} \neq -1 \; mod \; N$ then $\gcd\left(a^{r/2} + 1, N\right)$ and $\gcd\left(a^{r/2} - 1, N\right)$ are non-trivial factors of N

- **The core quantum idea**

Let r be the desired period of the $f(k) = a^k mod \; N$

Can we manufacture a quantum state

$$|\psi\rangle = \sum_{x=0}^{M} \alpha_x |x\rangle,$$

in a way that we can infer r from the most probable outcome $|y\rangle$ of measuring out $|\psi\rangle$ **?**

- In Shor’s algorithm: the outcome y is such that $\frac{y\,r}{M}$ is very close to an integer

Shor's Integer Factorization: Concepts, 3

Quantum Ingredients

- 1) **Quantum Fourier Transform** $(N \sim 2^n)$

$$QFT_N = \frac{1}{\sqrt{N}} \left[\left[\, \dots \omega_N^{jk} \dots \right]\right], \omega_N = e^{2\pi i/N}, j, k \in [0, N-1]$$

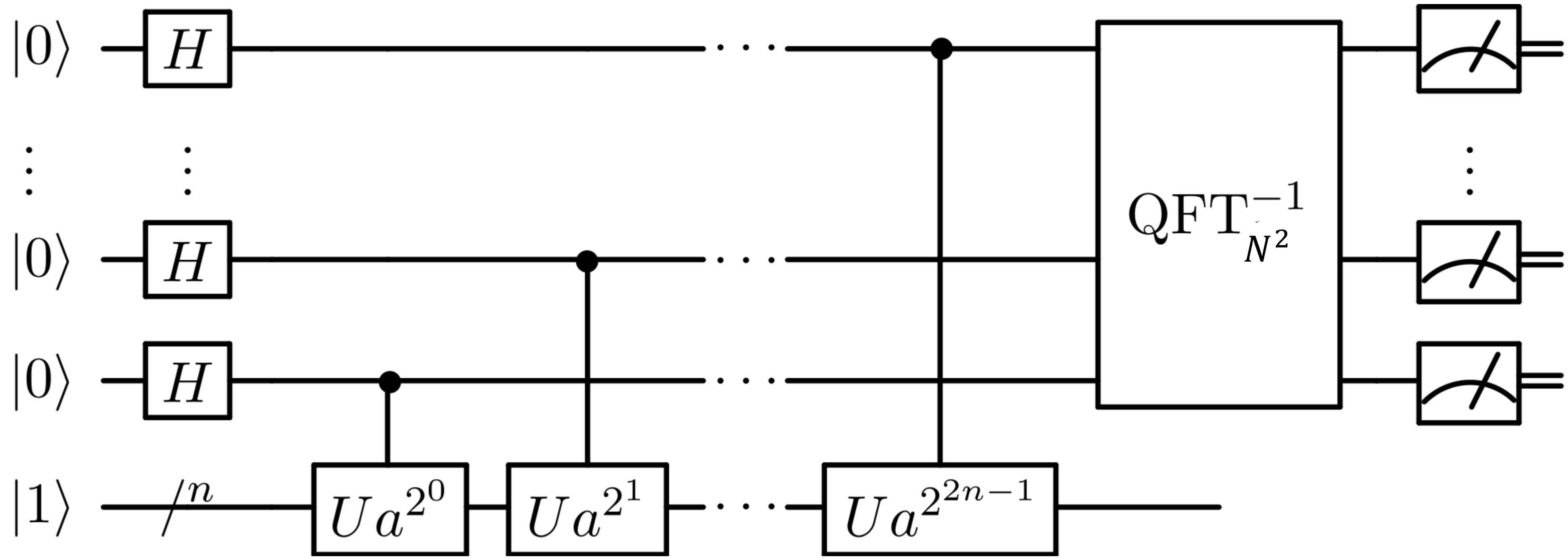
Time complexity $O(n^2) = O((\log N)^2)$ [vs. classical $O(N \log N)$]

- 2) **Coherent modular arithmetic** (in superposition)

For integer a and some large $M \geq N^2$ prepare quantum state of the form

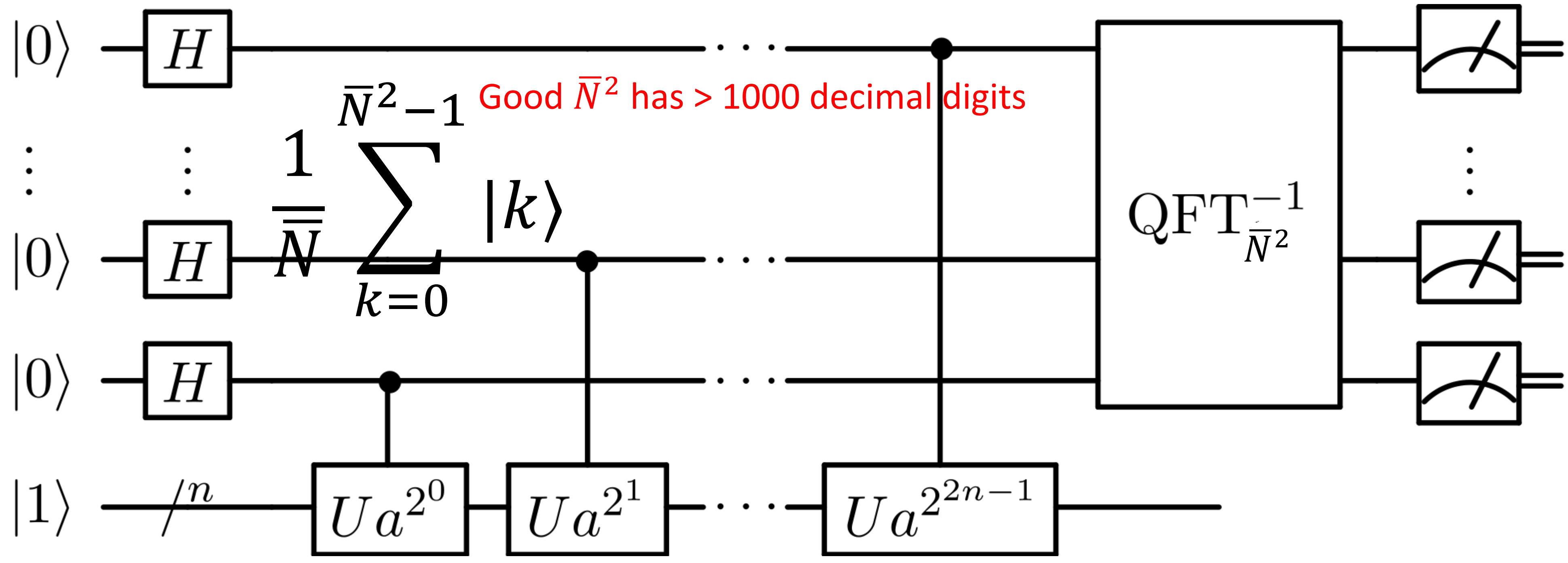
$$\frac{1}{\sqrt{M}} \sum_{k=0}^{M} |k\rangle \otimes |a^k \, mod \, N\rangle$$

Integer Factorization: putting it all together



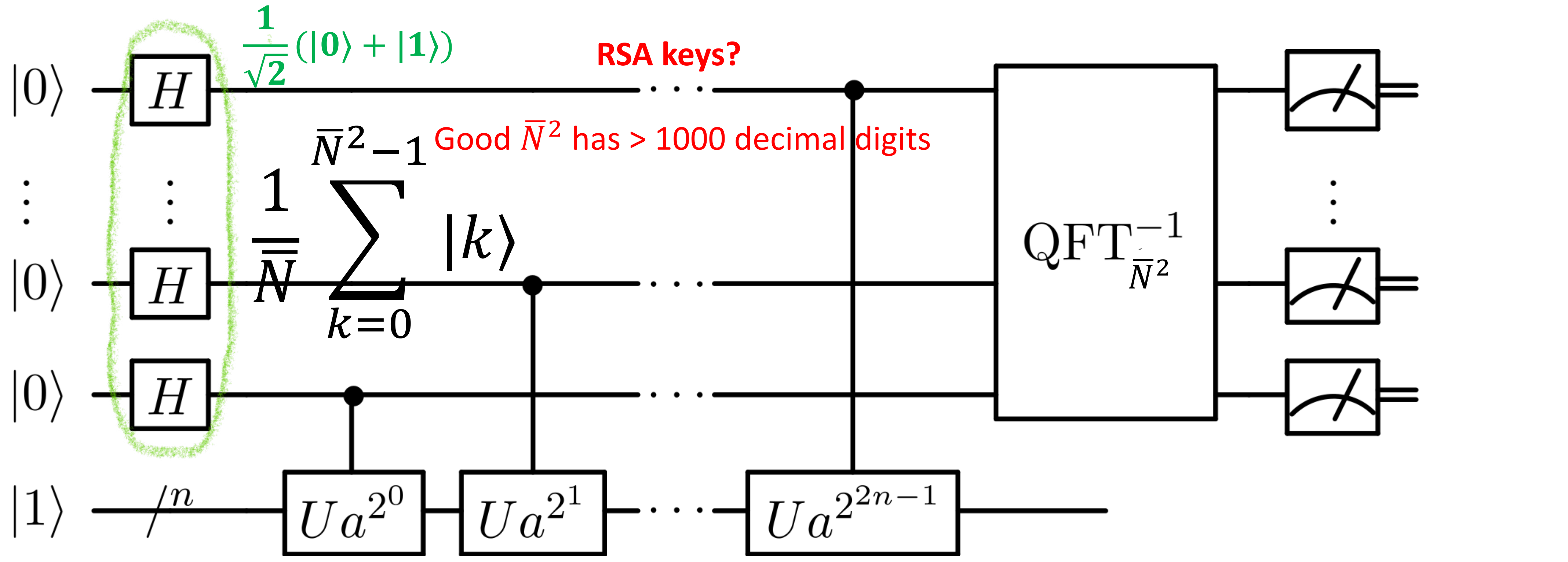
- [credit: Wikipedia.org]

Integer Factorization: $N = N_1 N_2, n = \text{ceil}[\log_2 N], \bar{N} = 2^n$



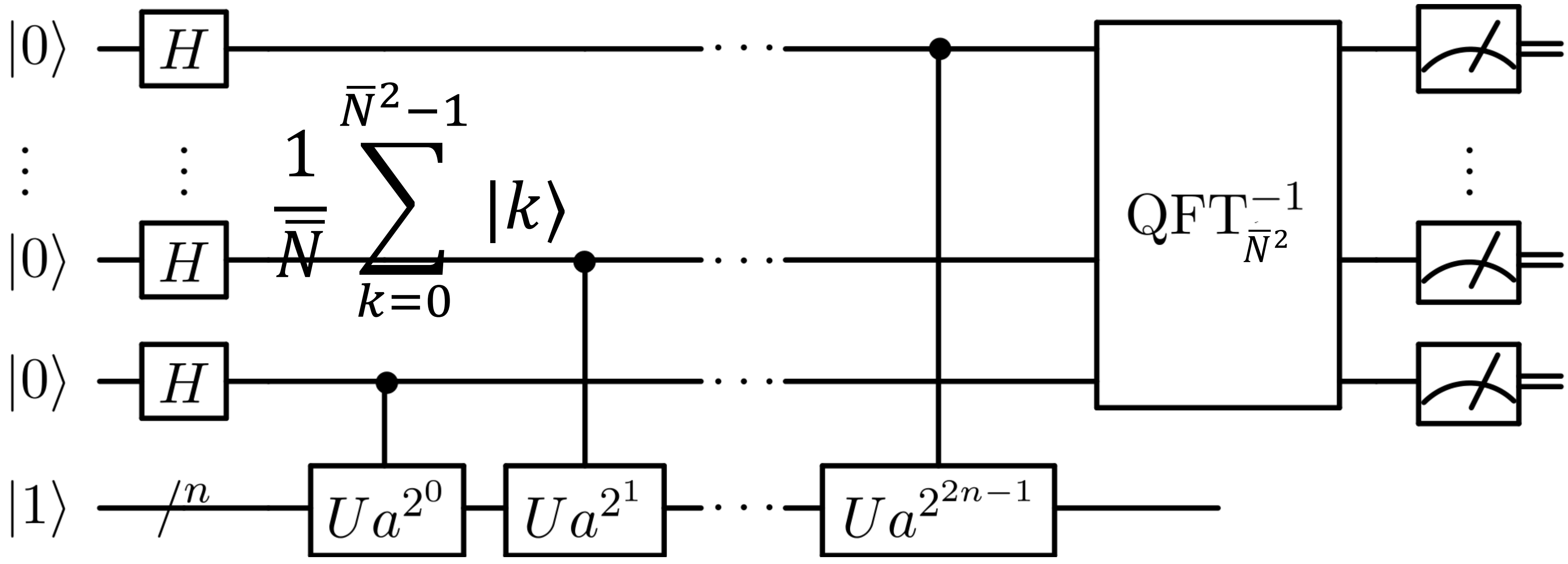
- [credit: Wikipedia.org]

Integer Factorization: $N = N_1 N_2, n = \text{ceil}[\log_2 N], \bar{N} = 2^n$



- [credit: Wikipedia.org]

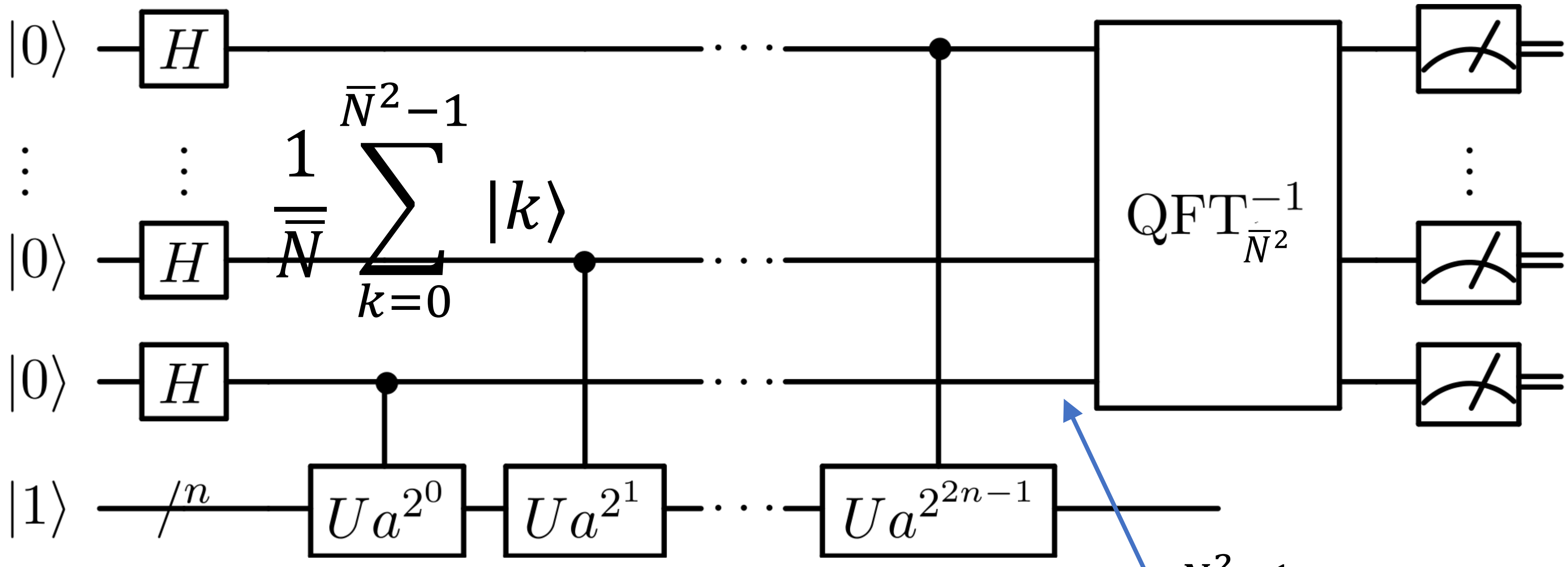
Integer Factorization: $N = N_1 N_2, n = \text{ceil}[\log_2 N], \bar{N} = 2^n$



$U_a \colon |x\rangle \mapsto |a\, x \bmod N\rangle$

- [Wikipedia.org]

Integer Factorization: $N = N_1 N_2, n = \text{ceil}[\log_2 N], \bar{N} = 2^n$



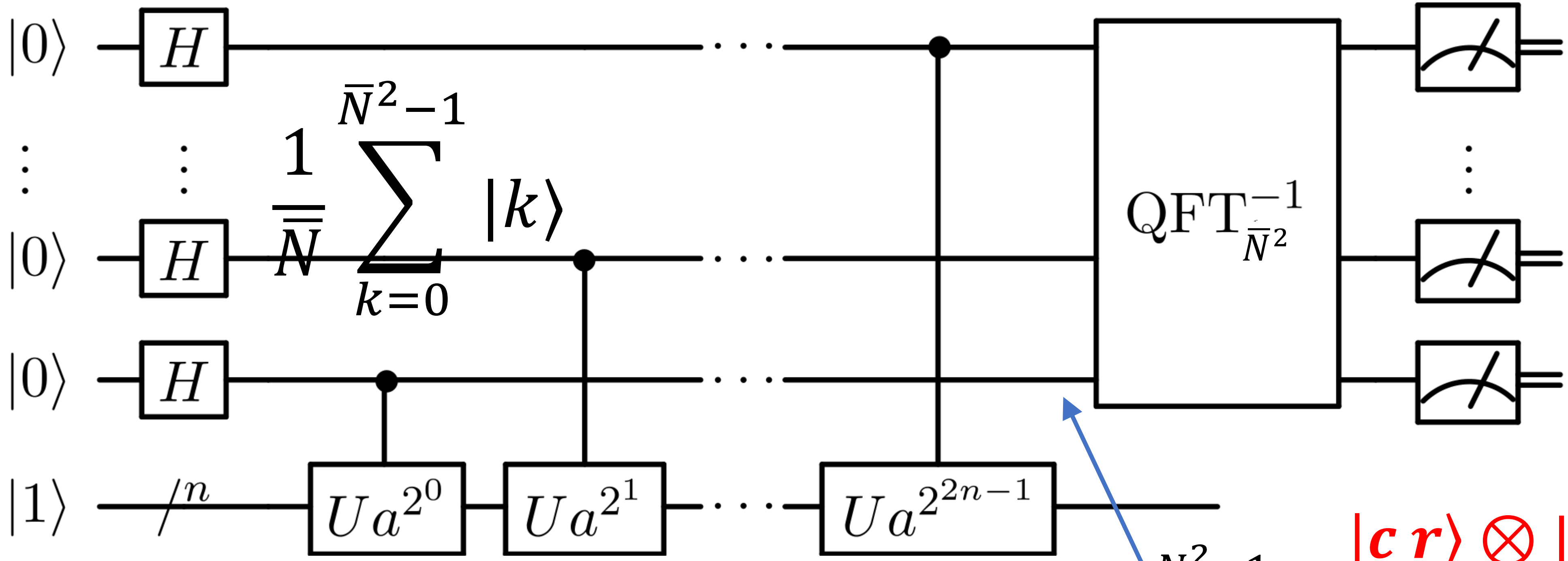
$$\frac{1}{\bar{N}} \sum_{k=0}^{\bar{N}^2-1} |k\rangle$$

$$U_a : |x\rangle \mapsto |a\, x\; mod\; N\rangle$$

$$\frac{1}{N} \sum_{k=0}^{N^2-1} |k\rangle \otimes |a^k\; mod\; N\rangle$$

- [Wikipedia.org]

Integer Factorization: $N = N_1 N_2, n = \text{ceil}[\log_2 N], \bar{N} = 2^n$



$$U_a : |x\rangle \mapsto |a\, x \bmod N\rangle$$

$$\frac{1}{N} \sum_{k=0}^{N^2-1} |k\rangle \otimes |a^k \bmod N\rangle$$

$$|\boldsymbol{c\, r}\rangle \otimes |\mathbf{1}\rangle$$

- [Wikipedia.org]

Shor Algorithm in Q# Library

- [Applications in the Q# standard libraries - Azure Quantum | Microsoft Docs]

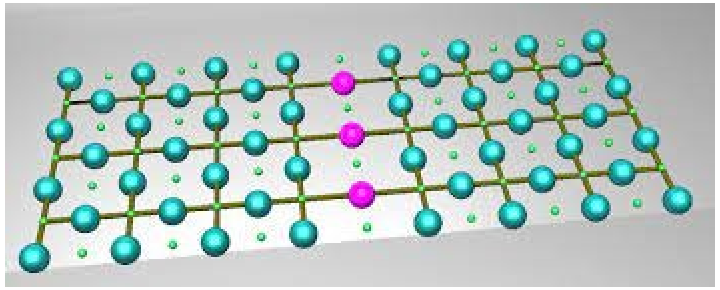
[https://docs.microsoft.com/en-us/azure/quantum/user-guide/libraries/standard/applications#shors-algorithm]

- [Programming Quantum Period Finding (Shor's Algorithm) – tsmatz (wordpress.com)]

[https://tsmatz.wordpress.com/2019/06/04/quantum-integer-factorization-by-shor-period-finding-algorithm/]

$\nexists$ Ideal Quantum Computer

Noisy qubits



- In traditional silicon device an encoded bit can occasionally flip:

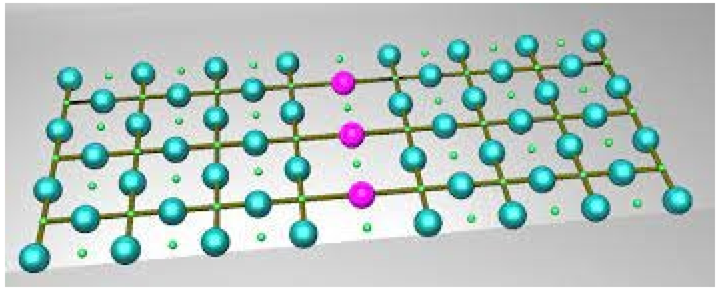
100101010111010101010100001011111

- A qubit

$$\alpha|0\rangle + \beta|1\rangle, \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

Can be flipped in more than one way:

Noisy qubits



- In traditional silicon device an encoded bit can occasionally flip:

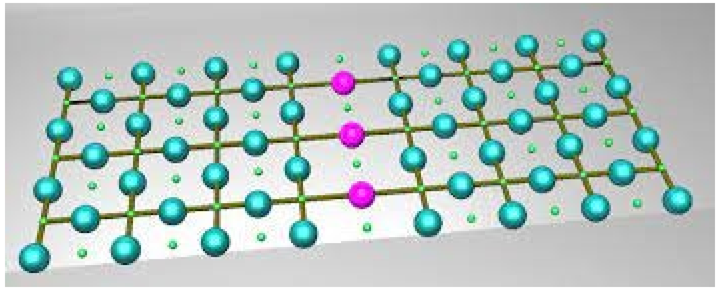
10010101011101010101010010101111

- A qubit

$$\alpha|0\rangle + \beta|1\rangle, \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

Can be flipped in more than one way:

Noisy qubits



- In traditional silicon device an encoded bit can occasionally flip:

1001010101110101010101001**1**0101111

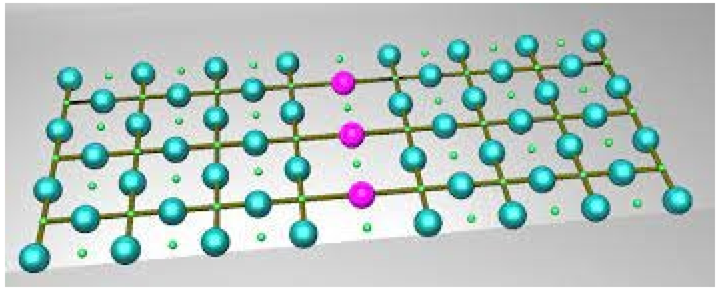
- A qubit

$$\alpha|0\rangle + \beta|1\rangle, \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

Can be flipped in more than one way:

phase-flip: $\alpha|0\rangle + e^{i\gamma}\beta|1\rangle$

Qubit and Gate Fidelity



- In traditional silicon device an encoded bit can occasionally flip:

10010101011101010101010010101111

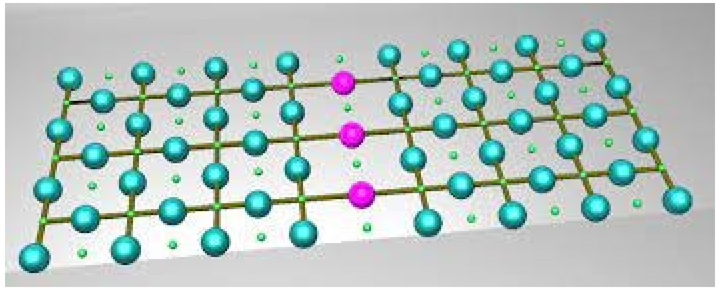
- A qubit

$$\alpha|0\rangle + \beta|1\rangle, \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

can be flipped in more than one way:

phase-flip: $\alpha|0\rangle \boldsymbol{+ e^{i\gamma}}\beta|1\rangle$, X-flip: $\alpha|\mathbf{1}\rangle + \beta|\mathbf{0}\rangle$

Noisy qubits



- In traditional silicon device an encoded bit can occasionally flip:

10010101011101010101010010101111

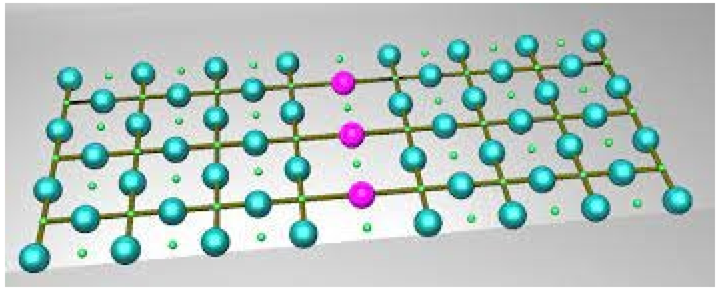
- A qubit

$$\alpha|0\rangle + \beta|1\rangle, \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

can be flipped in more than one way:

p-flip: $\alpha|0\rangle + e^{i\gamma}\beta|1\rangle$, X-flip: $\alpha|1\rangle + \beta|0\rangle$, Y-flip: $\alpha|1\rangle + e^{i\gamma}\beta|0\rangle$

Noisy qubits



- In traditional silicon device an encoded bit can occasionally flip:

1001010101110101010101001**1**0101111

- A qubit

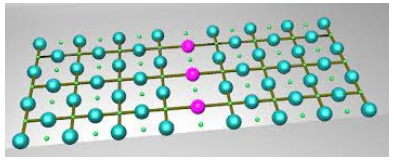
$$\alpha|0\rangle + \beta|1\rangle, \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

can be flipped in more than one way:

p-flip: $\alpha|0\rangle + \boldsymbol{e^{i\gamma}}\beta|1\rangle$, X-flip: $\alpha|\mathbf{1}\rangle + \beta|\mathbf{0}\rangle$, Y-flip: $\alpha|\mathbf{1}\rangle + \boldsymbol{e^{i\gamma}}\beta|\mathbf{0}\rangle$

A qubit can also **decohere**: e.g. $\alpha|0\rangle + \beta|1\rangle \mapsto |\mathbf{1}\rangle$

(In)Fidelity of state preparation



- It is not easy to prepare a qubit in a coherent state $\alpha|0\rangle + \beta|1\rangle$

In the best case, states s.a. $|0\rangle, |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$ are easy to prepare. Others must be **approximated**.

For instance the all-essential QFT is approximate beyond $n > 2$ qubits. E.g. preparing qubits of the form

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{\pi i/2^k}|1\rangle)$$

that are critical for QFT circuits requires expensive “quantum magic states” for $k > 1$

- Furthermore:

Primitive quantum operations (“gates”) themselves used in state manipulation are not error-tolerant. As a result, on current experimental devices, you are lucky if you get a 1-qubit state such as $\frac{1}{\sqrt{2}}(|0\rangle + e^{\pi i/2^k}|1\rangle)$ with 99% precision 99% of the time.

Fidelity of 2-qubit operations, used to “entangle” qubits is even worse (90% with luck)

⇒ Need for **Error Correction** methods

Quantum Error Correction, 1

- How do we protect classical information from random errors?

1	1	0	1	0	0	1	1	0	0	0	1	0	1	0	1
1	1	0	1	0	0	1	1	0	1	0	1	0	1	0	1
1	1	0	1	0	0	1	1	0	0	0	1	0	1	0	1

- Quantum "no-cloning" rule: *can not create an identical copy of unknown quantum state.*
- Quantum "observer effect" : *observation may change the state of quantum system.*

⇒ **How can we even detect quantum errors** (if we cannot observe the system) **?**

Quantum Error Correction, 2

- Key ingredient: (non-destructive) **stabilizer codes**
- Algebra:

1) Let $\mathcal{H}$ be n-qubit state space, $\mathcal{S} \subset Aut(\mathcal{H})$ – an Abelian subgroup of Hermitian operators.

2) *Require*: n-qubit state $|\psi\rangle$ to be stabilized by $\mathcal{S}$,i.e.$\forall \mathcal{O} \in \mathcal{S}, \mathcal{O}|\psi\rangle = |\psi\rangle$

3) $\Rightarrow$ measuring any or all $\mathcal{O} \in \mathcal{S}$ in such state $|\psi\rangle$ does not affect the state

4) Now, let us design $\mathcal{S} \subset Aut(H)$ such that one quantum error (or, small number of uncorrelated errors) pushes $|\psi\rangle$ out of the +1 eigenspace of $\mathcal{S}$.

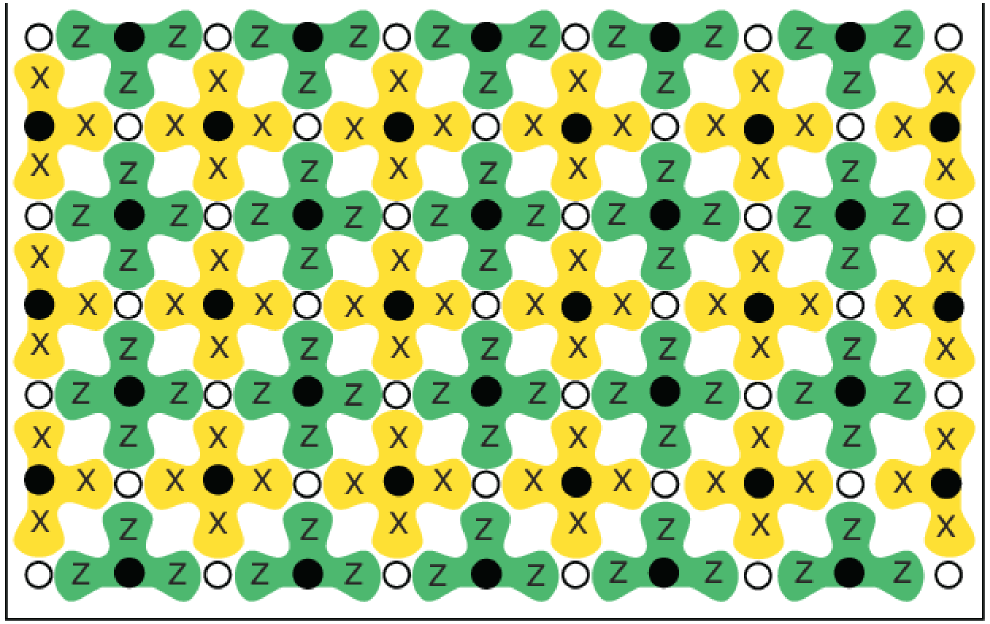
5) Then measuring observables $\{\mathcal{O} \in \mathcal{S}\}$ will signal the presence of quantum errors.

6) With some sophistication, these errors can be *coherenty corrected*.

Quantum Error Correction, 3

- **Engineering, toric code**

$\boldsymbol{M^2}$ **data qubits (black dots)**
$\boldsymbol{M^2}$ **syndrome qubits (white dots)**

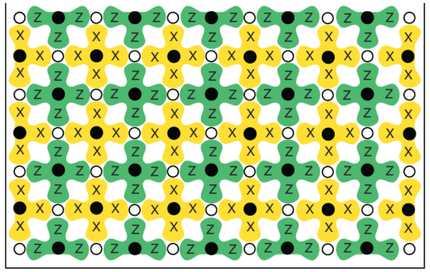


[credit: https://en.wikipedia.org/wiki/Toric_code]

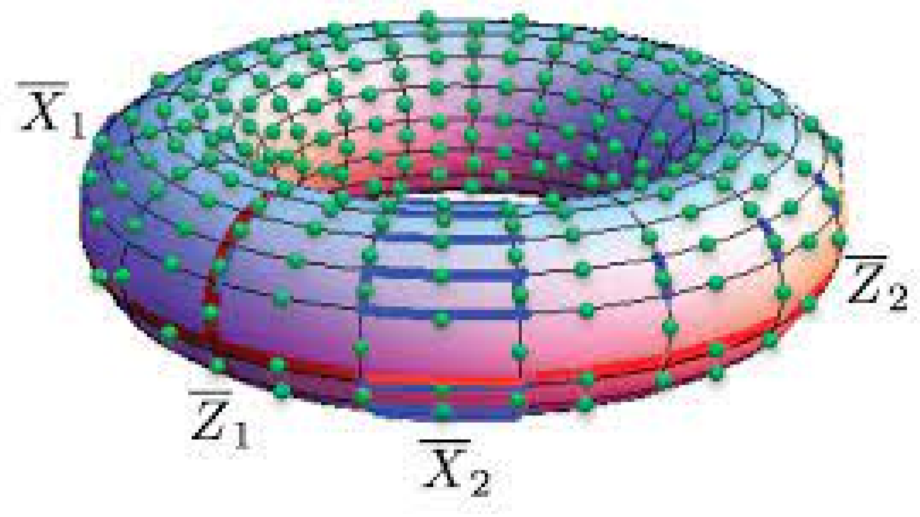
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- $\mathcal{S} = \{\ldots\ \boldsymbol{X_a X_b X_c X_d}, \boldsymbol{Z_a Z_b Z_c Z_d}, \ldots\}$

Quantum Error Correction, 4



- Topological interpretation:



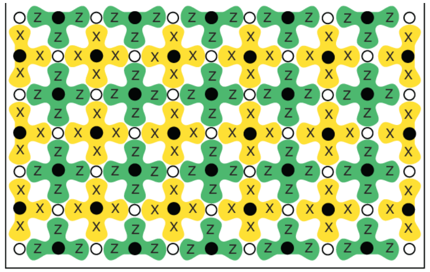
$\mathcal{S} = \{\ldots\ \boldsymbol{X_a X_b X_c X_d}, \boldsymbol{Z_a Z_b Z_c Z_d}, \ldots\}$

$|\mathcal{S}| = 2M^2 - 2$, for $2M^2$ qubits

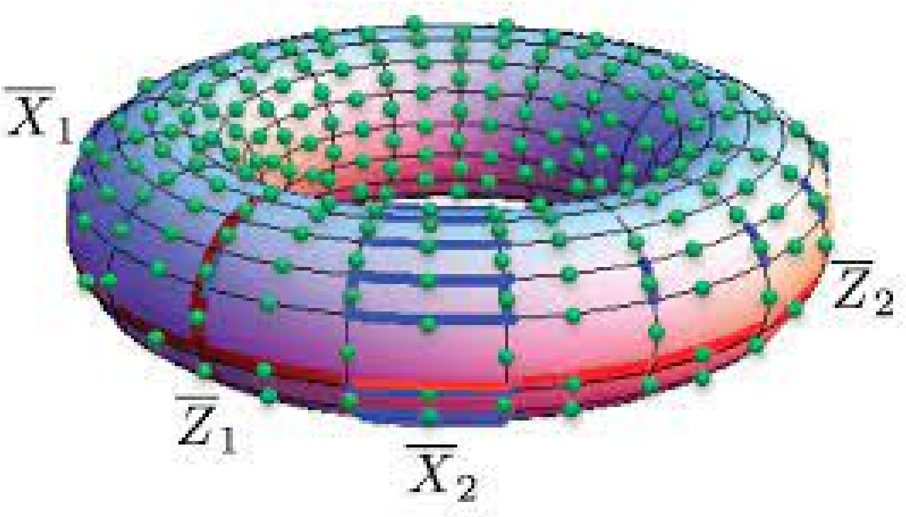
$\dim E_{+1} = 4$

- [credit: Lecture2.pdf (fu-berlin.de)]

Quantum Error Correction, 4



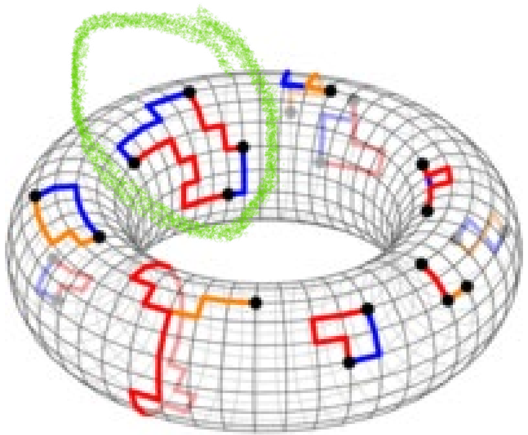
- Topological interpretation:



$S = \{\dots\ \boldsymbol{X_a X_b X_c X_d}, \boldsymbol{Z_a Z_b Z_c Z_d}, \dots\}$

$|S| = 2M^2 - 2$, for $2M^2$ qubits

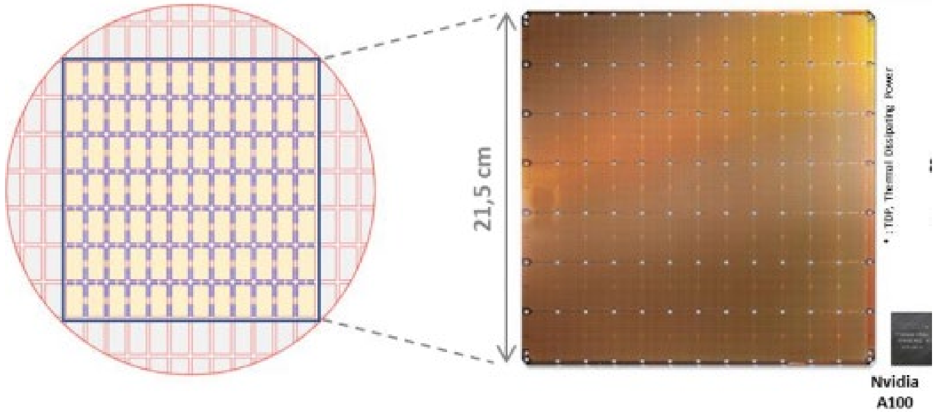
$\dim E_{+1} = 4$



- [credit: Lecture2.pdf (fu-berlin.de)]

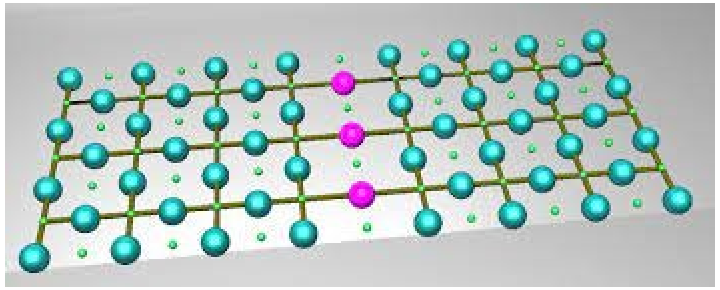
Beyond Silicon, towards Quantum

- Celebras’ 2.6 trillion (7 nm) transistors, 15 kW consumption



10 x 

- How many qubits we need for similar compute?

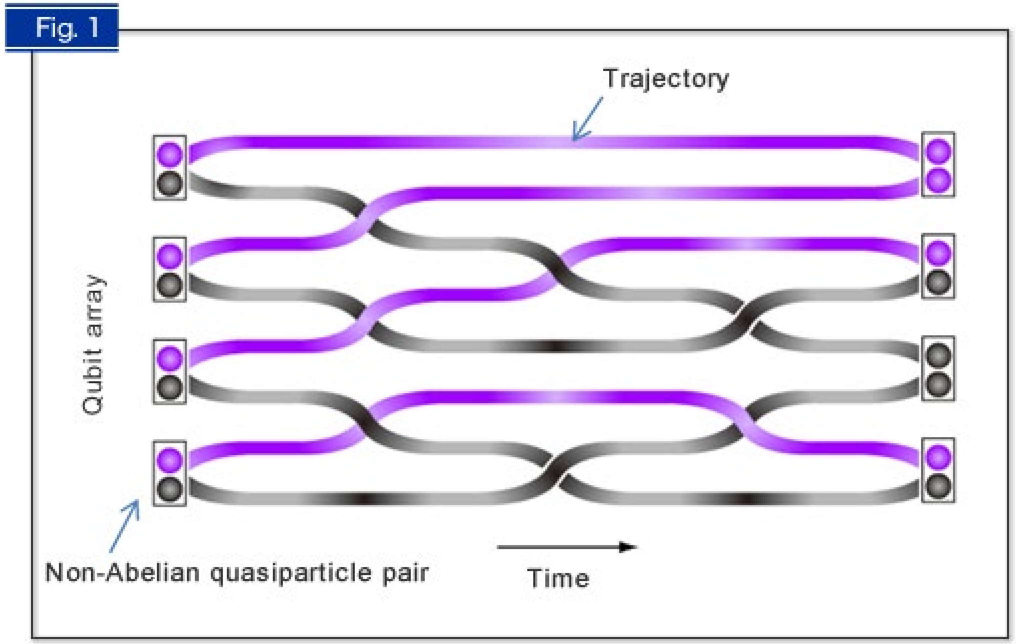


[credit: New Journal of Physics, 2012]

$$2^{\mathbf{42}} > 2.6\ 10^{12}$$

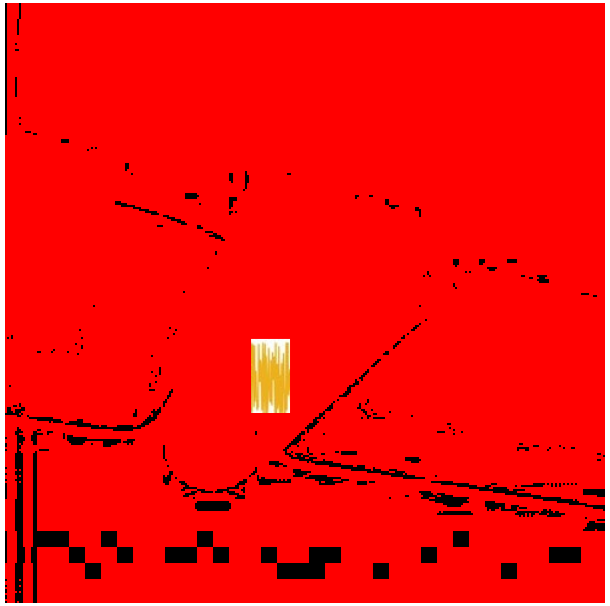
$$\mathbf{42 \rightarrow 42 \times 10000 = 420\ 000}$$

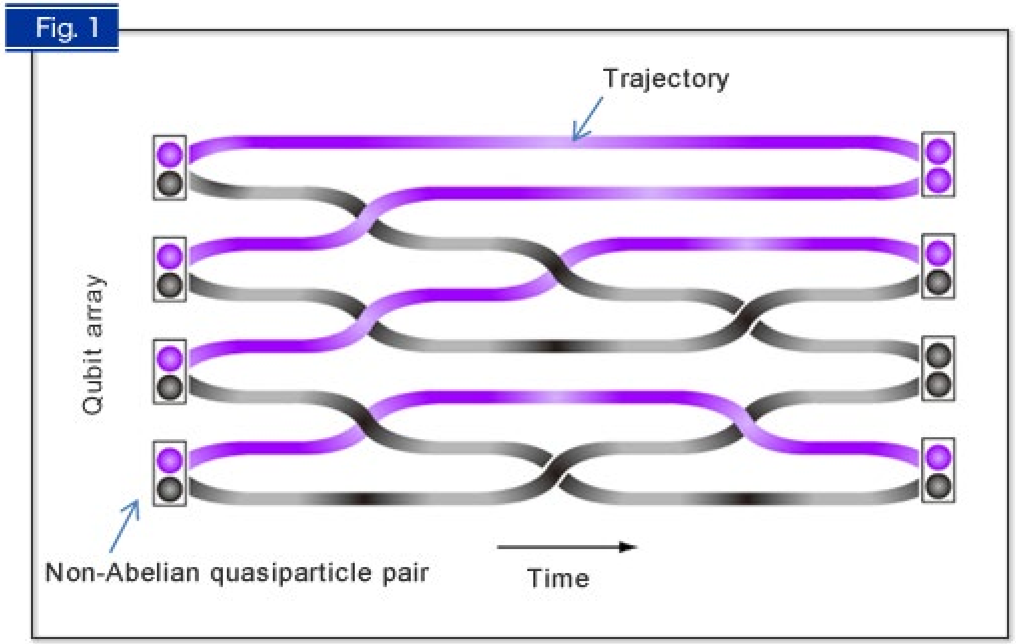
Towards native topological protection: non-Abelian anyons



- Credit: Topological Quantum Computing Market to See Major Growth by 2026 (openpr.com) [https://www.openpr.com/news/2293601/topological-quantum-computing-market-to-see-major-growth-by-2026]

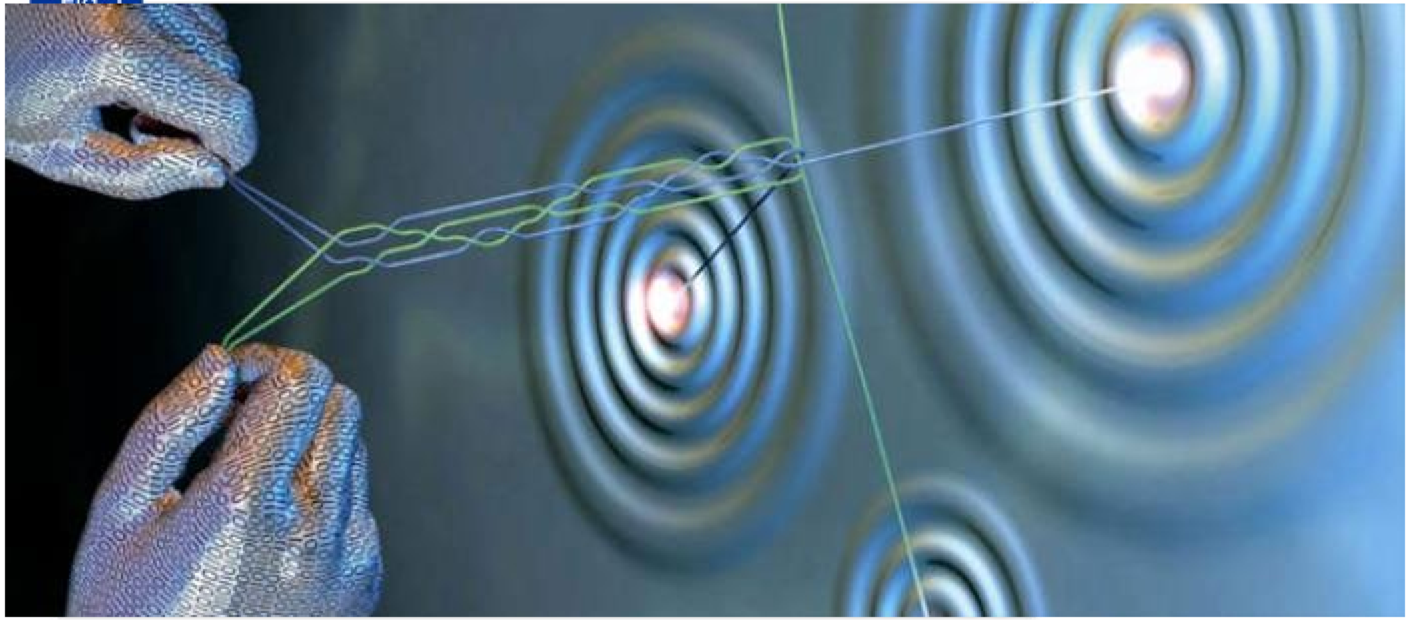
Towards native topological protection: non-Abelian anyons





- Credit: Topological Quantum Computing Market to See Major Growth by 2026 (openpr.com) [https://www.openpr.com/news/2293601/topological-quantum-computing-market-to-see-major-growth-by-2026]

Towards native topological protection: non-Abelian anyons



- Credit: [Topological Quantum Computing Market to See Major Growth by 2026 (openpr.com)] [https://www.openpr.com/news/2293601/topological-quantum-computing-market-to-see-major-growth-by-2026]

Topological qubit – a high-stakes prize

- New physics discovery from the Microsoft Quantum team: topology with a twist
- A Topological Quantum Computer — Experts Suggest Rethinking The Idea | by Anna Ned | Cantor’s Paradise (cantorsparadise.com)

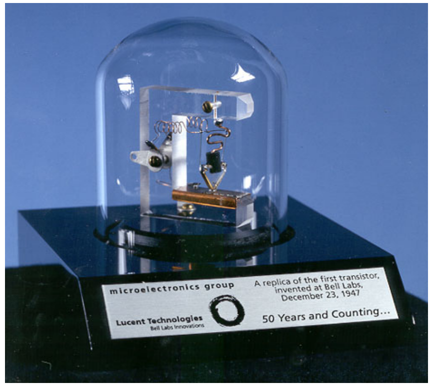
What are Microsoft resources for all the good Quantum stuff?

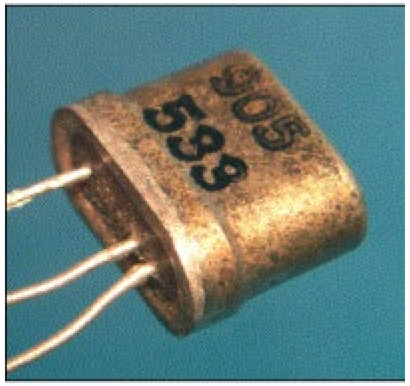
Azure Quantum Platform

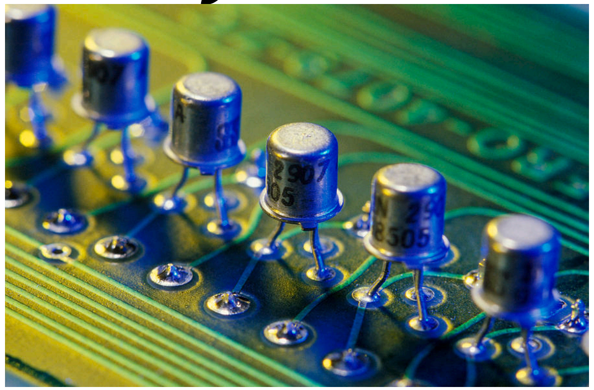
- Algorithms, quantum tools, languages, simulators, resource estimators and tutorials developed at Microsoft are available for public preview within the Azure Quantum Platform: Azure Quantum - Quantum Service | Microsoft Azure [https://azure.microsoft.com/en-us/services/quantum/#product-overview]
- The Service, moreover provides access to quantum hardware from IonQ or Honeywell via "quantum credits" program Azure Quantum Credits application (qualtrics.com) [https://microsoft.qualtrics.com/jfe/form/SV_3fl9dfFrkC3g0aG]

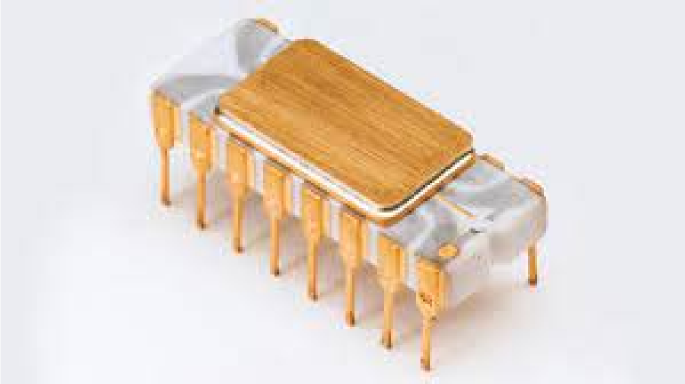
Historic Allusions, 74 years of Transistor

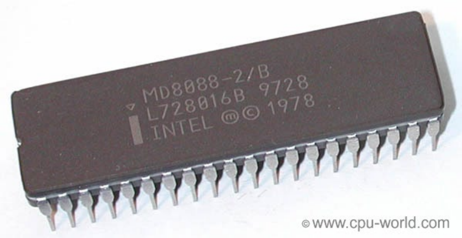
$$\leftarrow \sim 25\ years \rightarrow$$

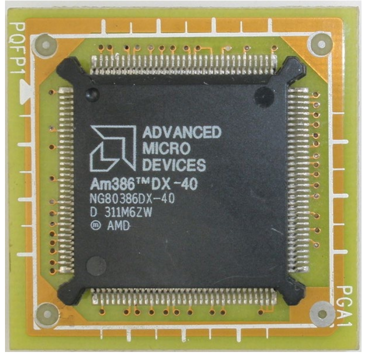


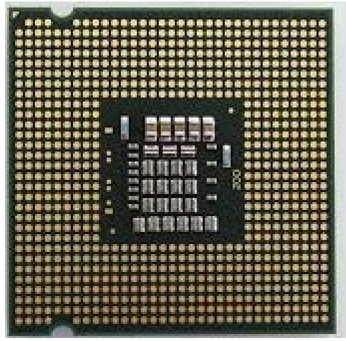


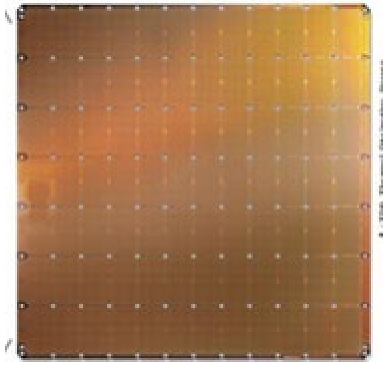




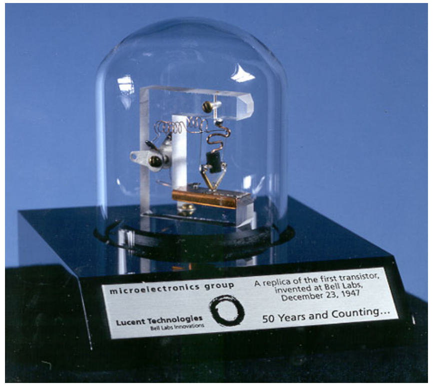


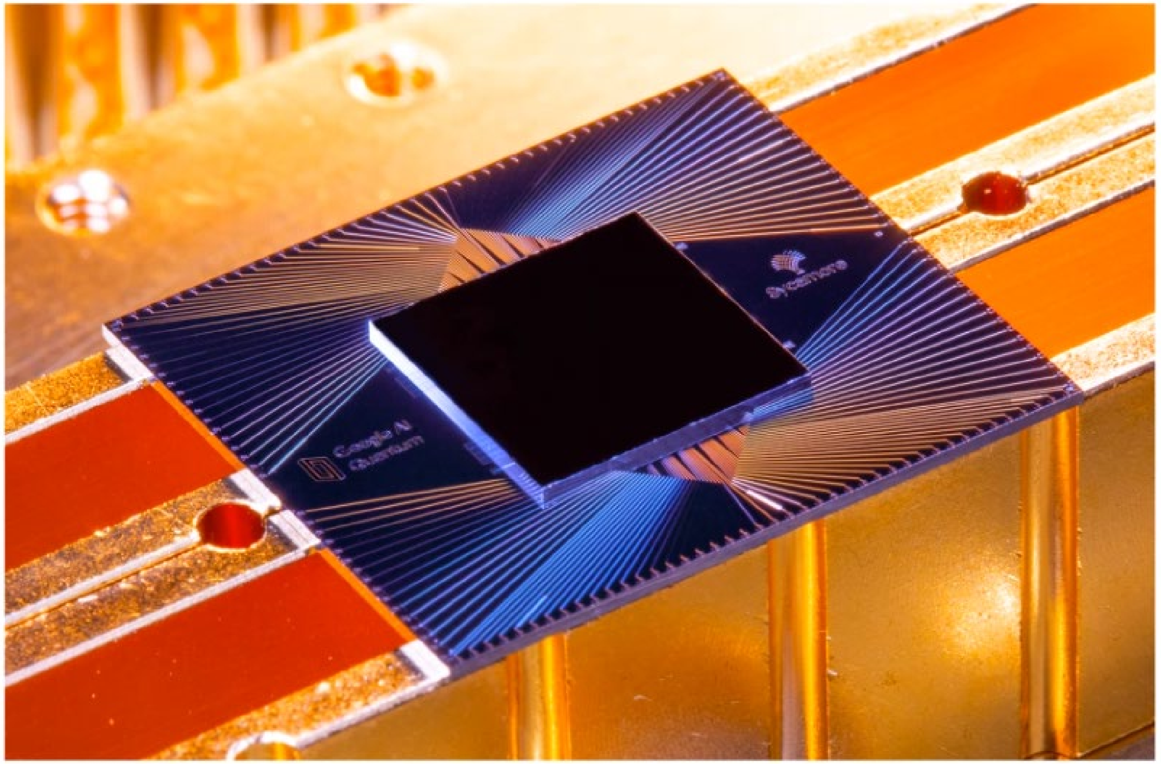


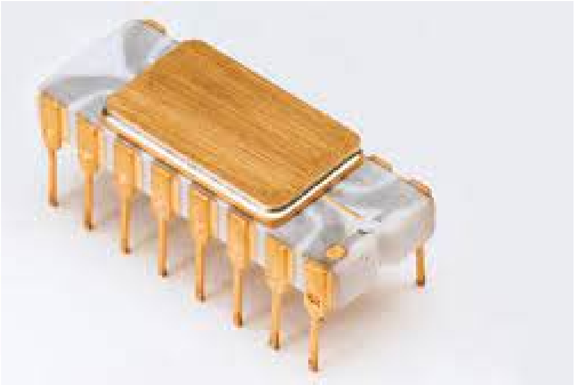


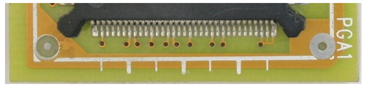


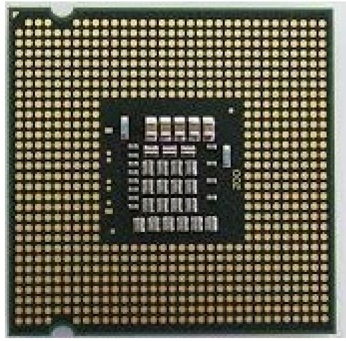
Historic Allusions and NISQ Quantum Chips,2019











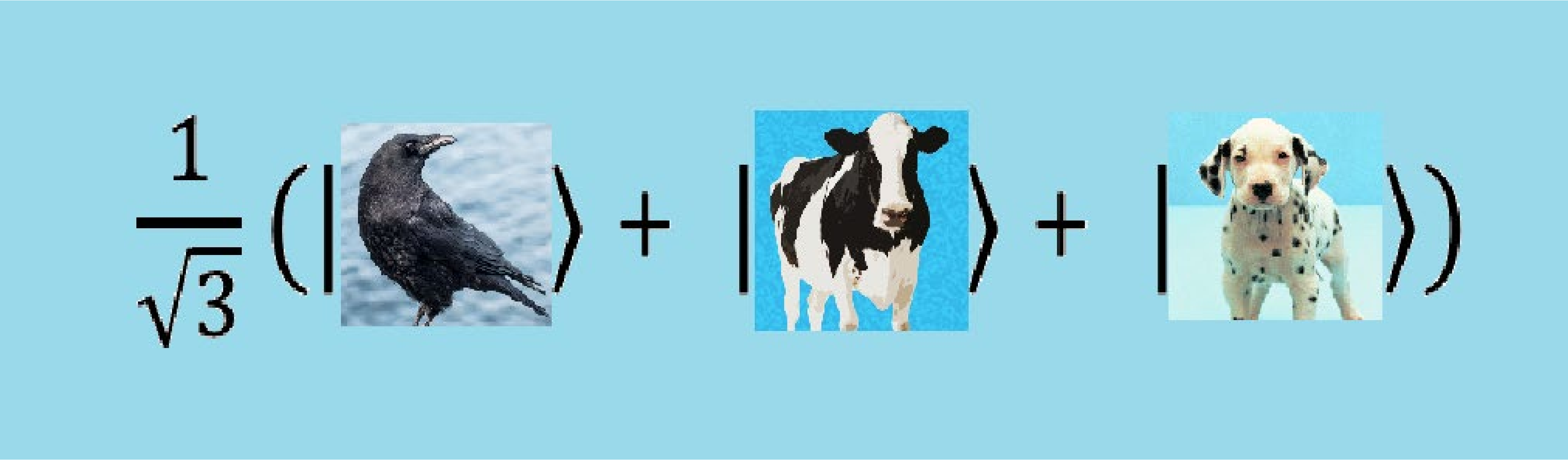
Historic Allusions and NISQ Quantum Chips,2019

← ~ 25 years →

Conclusion

- Quantum computing is at the stage of rapid (explosive) growth.
- Having scored major achievements and breakthroughs in recent years, presently QC science and engineering are facing two major challenges: (1) challenge of scale and (2) challenge of fidelity.
- Installations with millions of fully controllable qubits are needed for practical quantum advantage.
- From 50 – 100 qubits with fidelity less than 0.99 we need to scale out to 10s of thousands of qubits with fidelities 0.99999 and better.
- Error correction codes and/or native topological protection of quantum information will get us there.

Thanks!



- Credit: [https://www.culture.ru/poems/48738/plastilinovaya-vorona]