

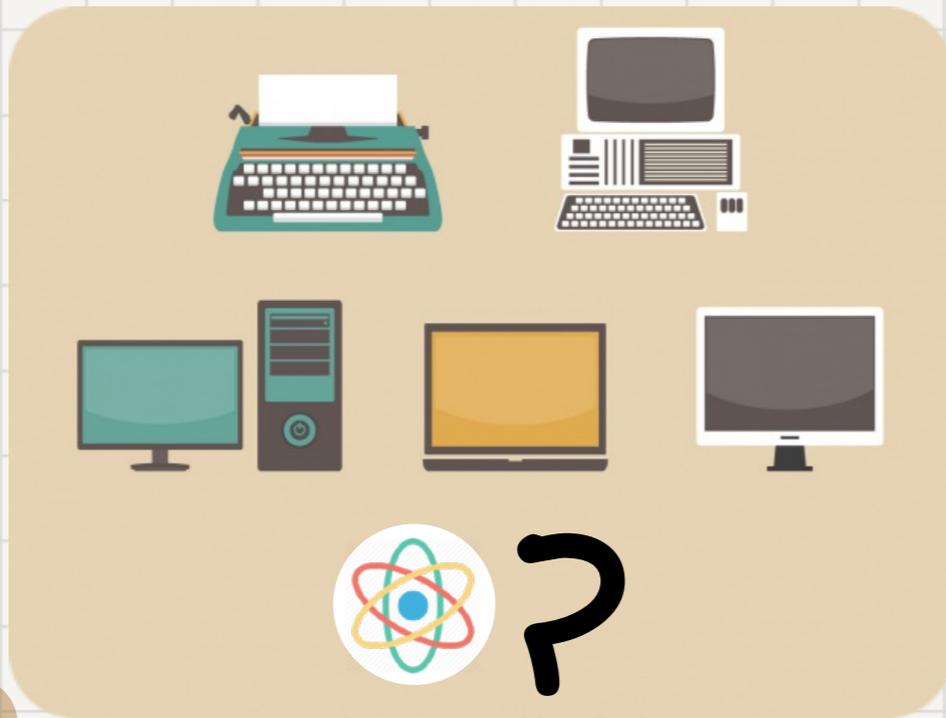
Complexity Theory



Lecture 12

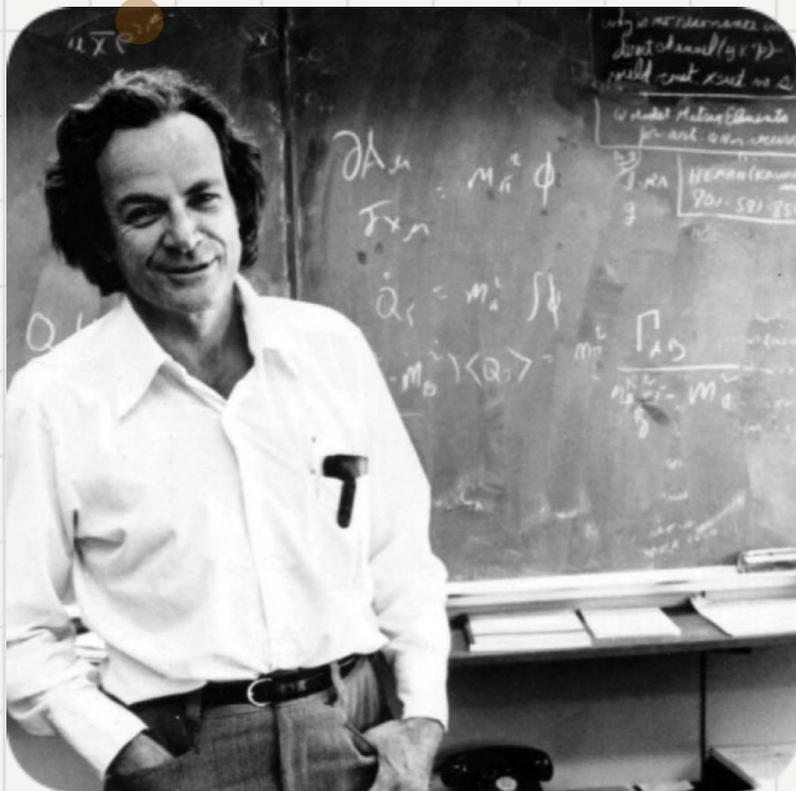
Quantum Complexity

What is quantum computing



The big idea:

Computers that rely on the
Powerful, but unintuitive,
principles of quantum mechanics



Quantum computing is... nothing less than a distinctively new way of harnessing nature... it will be the first technology that allows useful tasks to be performed in collaboration between parallel universes.

—Fabric of reality



David Deutsch

THE FABRIC OF REALITY ▶ If space and time are not fundamental, then what is? Theoretical physicists are exploring several possible answers.

One clue
Quantum effects in the gravitational field of a black hole cause it to radiate energy as if it were hot, implying a deep connection between quantum theory, gravity and thermodynamics — the science of heat.

The black hole's mass is concentrated at a singularity of infinite curvature.

1. Gravity as thermodynamics
The equations of gravity can actually be derived from thermodynamics, without reference to space-time curvature.

This suggests that gravity on a macroscopic scale is just an average of the behaviour of some still-unknown 'atoms' of space-time.

2. Loop quantum gravity
The Universe is a network of intersecting quantum threads, each of which carries quantum information about the size and shape of nearby space.

Imagine drawing a closed surface anywhere in the network. Its volume is determined by the intersections it encloses; its area by the number of threads that pierce it.

3. Causal sets
The building blocks of space-time are point-like 'events' that form an ever-expanding network linked by causality.

An earlier event can affect a later one, but not vice versa.

4. Causal dynamical triangulations
Computer simulations approximate the fundamental quantum reality as tiny polygonal shapes, which obey quantum rules as they spontaneously self-assemble into larger patches of space-time.

Space at an instant

Space an instant later

5. Holograpy
A three-dimensional (3D) universe contains black holes and strings governed solely by gravity, whereas its 2D boundary contains ordinary particles governed solely by standard quantum-field theory.

Anything happening in the 3D interior can be described as a process on the 2D boundary, and vice versa.

"if you teach an introductory course on quantum mechanics, and the students don't have nightmares for weeks, tear their hair out, wander around with bloodshot eyes, etc., then you probably didn't get the point across."

Time travel

Parallel universes

Teleportation

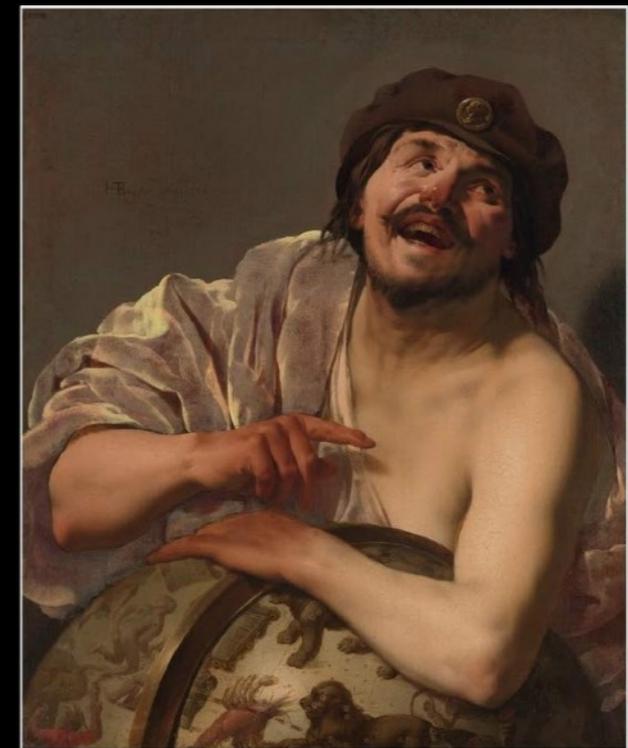
Cloning

Faster-than-light
communication

Determinism

Chaos

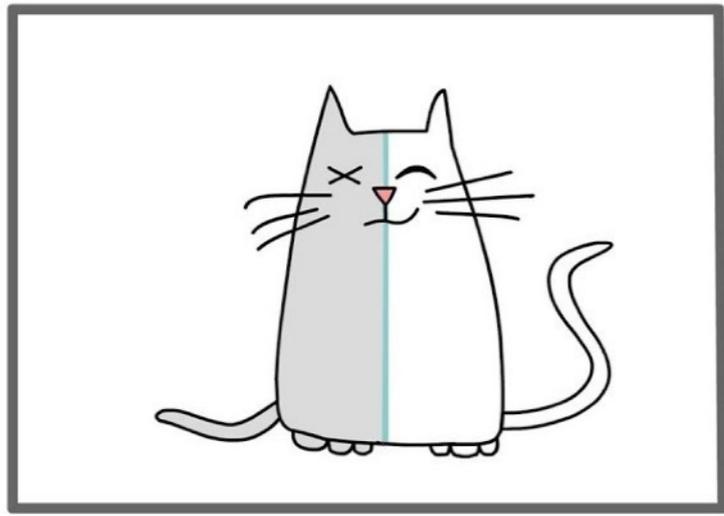
QUANTUM COMPUTING SINCE DEMOCRITUS



SCOTT AARONSON

Superposition, parallel worlds, and cats

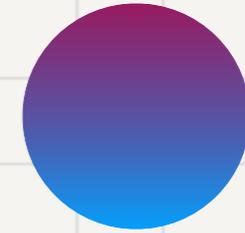
Schrödinger's Cat



Bit

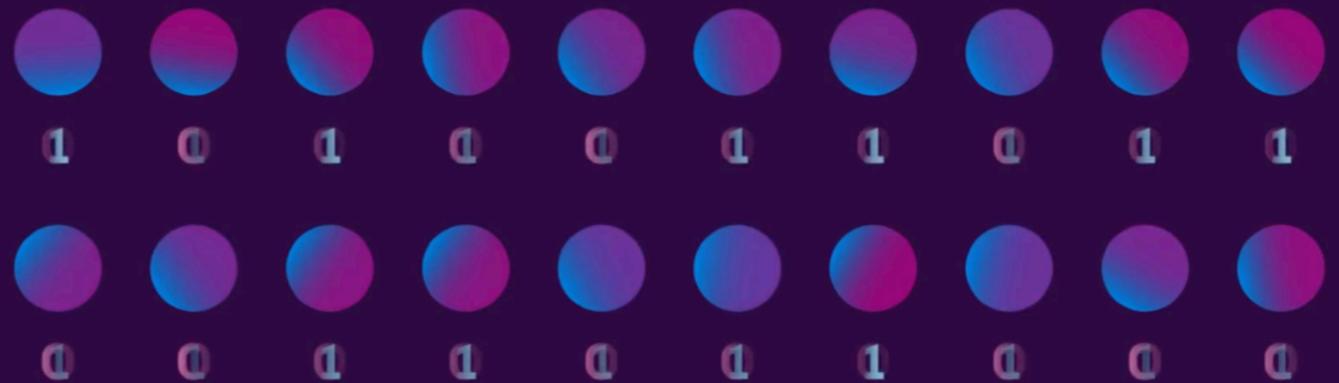


Qubit



$$\alpha|0\rangle + \beta|1\rangle$$

$$\frac{1}{\sqrt{2}}|\text{cat}\rangle + \frac{1}{\sqrt{2}}|\text{no cat}\rangle$$



$2^{20} = 1,048,576$
configurations at once

A crash course on quantum computing

Quantum mechanics is a \mathbb{C} probability theory

Fully captured by 4 postulates:

① Superposition

A quantum state

is a vector $v \in \mathbb{C}^n$

s.t. $\|v\|_2^2 = 1$.

Ex: a qubit $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, $|\alpha|^2 + |\beta|^2 = 1$

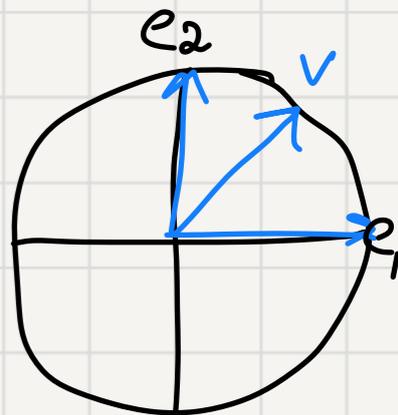
② Measurement

Measuring state (x_1, \dots, x_n) in

the computational basis

collapses it to e_i

w.p. $|\alpha_i|^2$



Mathematical abstraction of quantum computing

III Evolution

A quantum state $v \in \mathbb{C}^n$

evolves to $v' \in \mathbb{C}^n$

via a unitary map

$$\begin{pmatrix} | \\ | \\ v' \\ | \end{pmatrix} = U \cdot \begin{pmatrix} | \\ | \\ v \\ | \end{pmatrix}$$

IV Entanglement

States $u, v \in \mathbb{C}^n$ are

composed via the tensor

product $u \otimes v$.

Ex: $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} =$

Entangled states

are not of that

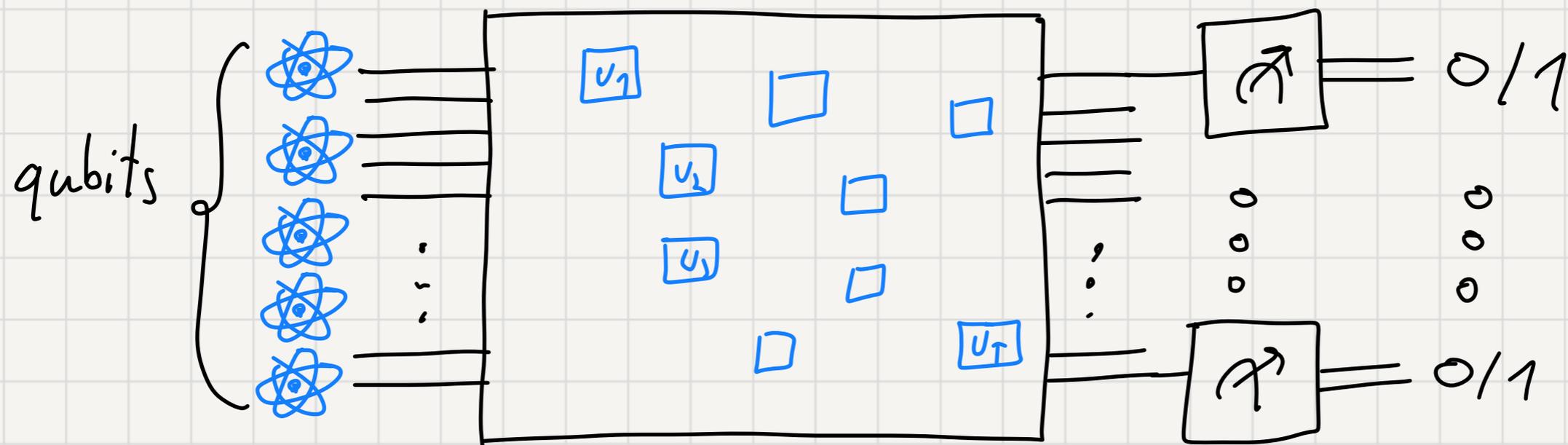
form!

$$\begin{pmatrix} 1 & 000 \\ 0 & 001 \\ 0 & 010 \\ 0 & 011 \\ 0 & 100 \\ 0 & 101 \\ 0 & 110 \\ 0 & 111 \end{pmatrix}$$

Quantum algorithms

Quantum Turing machines ...are not very nice to work with...

Instead, we typically work with quantum circuits.



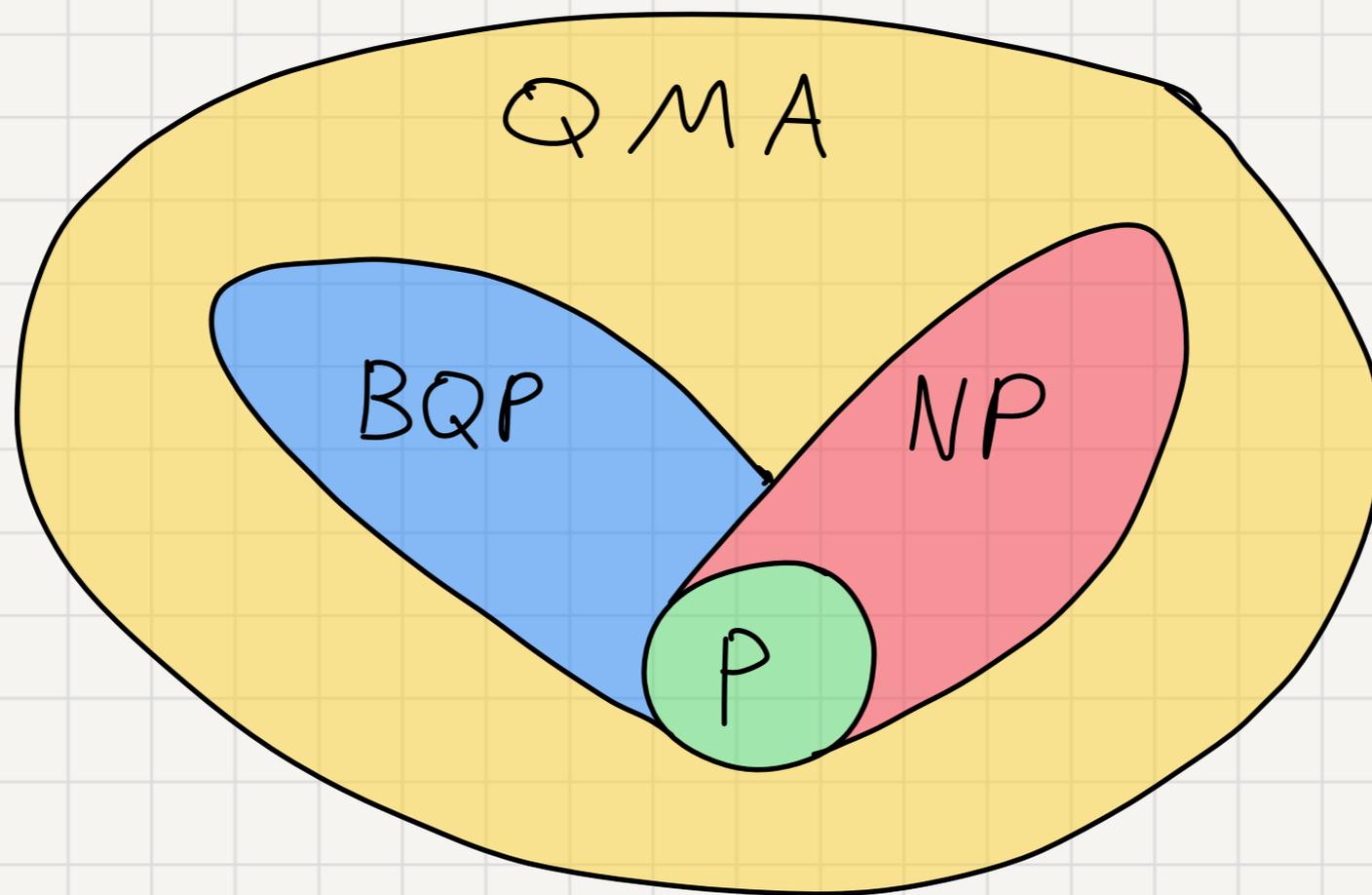
We apply quantum gates (unitary maps) to qubits.

Measure at the end to get classical bits.

Quantum complexity classes

BQP = "quantum P"

QMA = "quantum NP"



BQP

The set of all problems solvable by a poly-time uniform quantum circuits

$(C_n)_{n \in \mathbb{N}}$ of polynomial size, w.p. $\geq 2/3$

(i.e., $\forall x \in \{0,1\}^n \Pr[C_n(x) = \mathbb{1}_L(x)] \geq 2/3$)

$T(n)$ -uniformity: C_n can be generated

in $T(n)$ time

Circuit size: # gates \rightarrow time complexity

Error reduction

Let A be a q -algo for computing f such that $\Pr[A(x) = f(x)] \geq \frac{2}{3} \quad \forall x$.

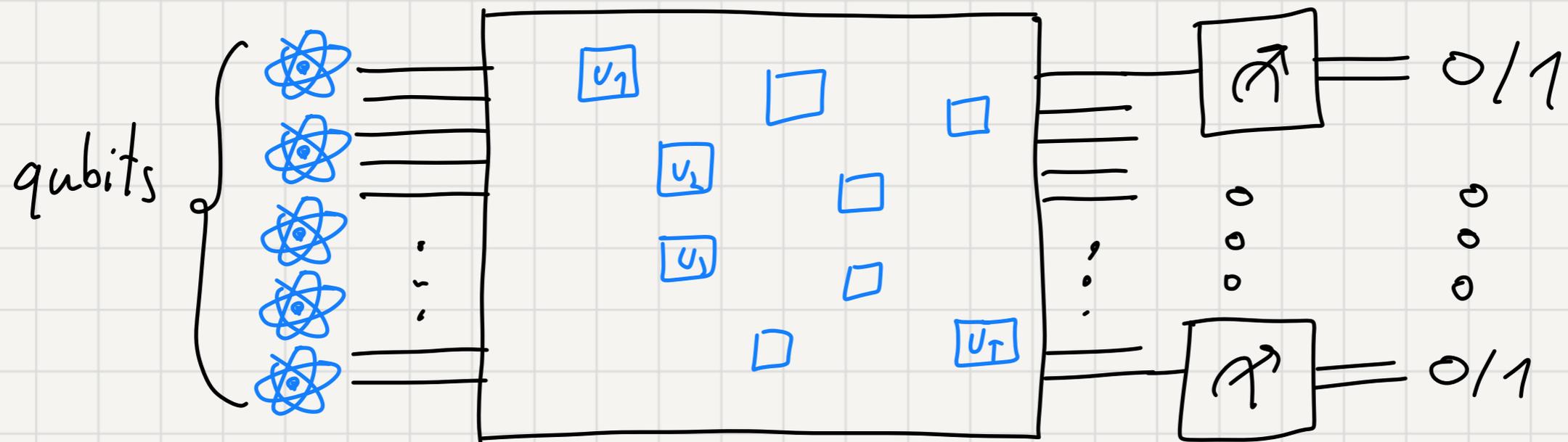
$\frac{1}{3}$ error prob. can be reduced to ϵ !

Repeat A : $A_1, A_2, \dots, A_{\underbrace{\log(\frac{1}{\epsilon})}_+}$, rule by Maj.

Chernoff bound:

$$\Pr\left[\frac{\sum_{i \in [t]} A_i}{t} - \mathbb{E}[X_i] \leq \frac{1}{\delta}\right] \leq \exp(-t)$$

Quantum algorithms



3 examples where quantum algorithms excel:

- (I) Finding sub-group structure (Shor's factoring)
- (II) Rapid mixing of Markov chains (Grover's search)
- (III) Computing Fourier Transforms (QFT)

Factoring

Given $n \in \mathbb{N}$, output primes p_1, \dots, p_n s.t.

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_n$$

Decision problem

Factor $(n, k) = 1$

iff n has a prime factor $\leq k$

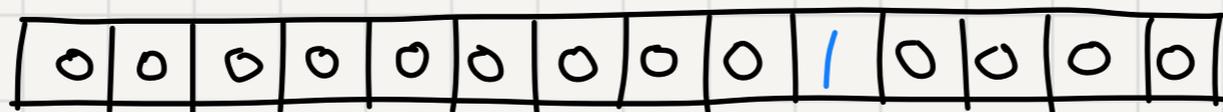
Shor's algorithm

Factor $\in \text{BQP}$

We know Factor $\in \text{NP} \cap \text{coNP}$.

Grover's search

Given a string $x \in \{0,1\}^n$, output $i \in [n]$ such that $x_i = 1$



Classical complexity? $\Omega(n)$

Quantum complexity $\Omega(\sqrt{n})$

Quantum Fourier Transform

Given $(f_1, f_2, \dots, f_N) \in \mathbb{C}^N$, output the DFT $(\hat{f}_1, \hat{f}_2, \dots, \hat{f}_N)$

Classical complexity? $O(N \log N)$

Quantum complexity $\tilde{O}(\log N)$

Ask Me Anything