

A short intro to quantum computing

Peter Love

Department of Physics

Department of Computer Science

Quantum bits and Bloch Sphere. Quantum Circuit Model. No Cloning. Universality.



UNIVERSITY OF
TORONTO

Quantum Bits

Two states, zero and one

Qubit state: $\begin{pmatrix} \langle 0 | \psi \rangle \\ \langle 1 | \psi \rangle \end{pmatrix}$ Born's rule: $P(0) = |\langle 0 | \psi \rangle|^2$
 $P(1) = |\langle 1 | \psi \rangle|^2$

“Partly a thing,
and partly our knowledge of a thing”



UNIVERSITY OF
TORONTO

Qubit zoology

Wild qubits:

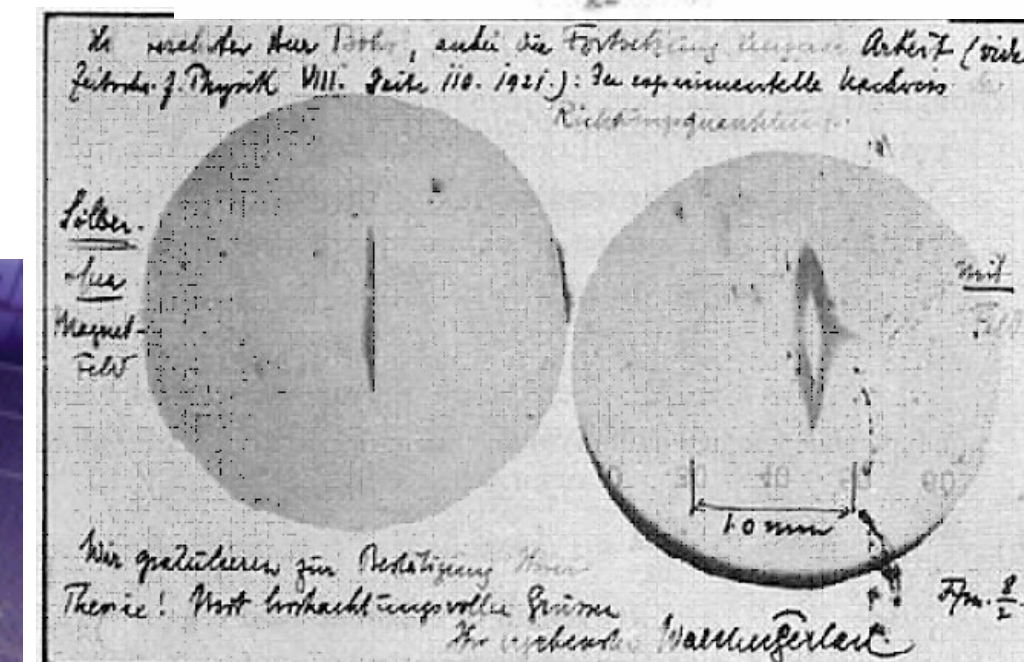
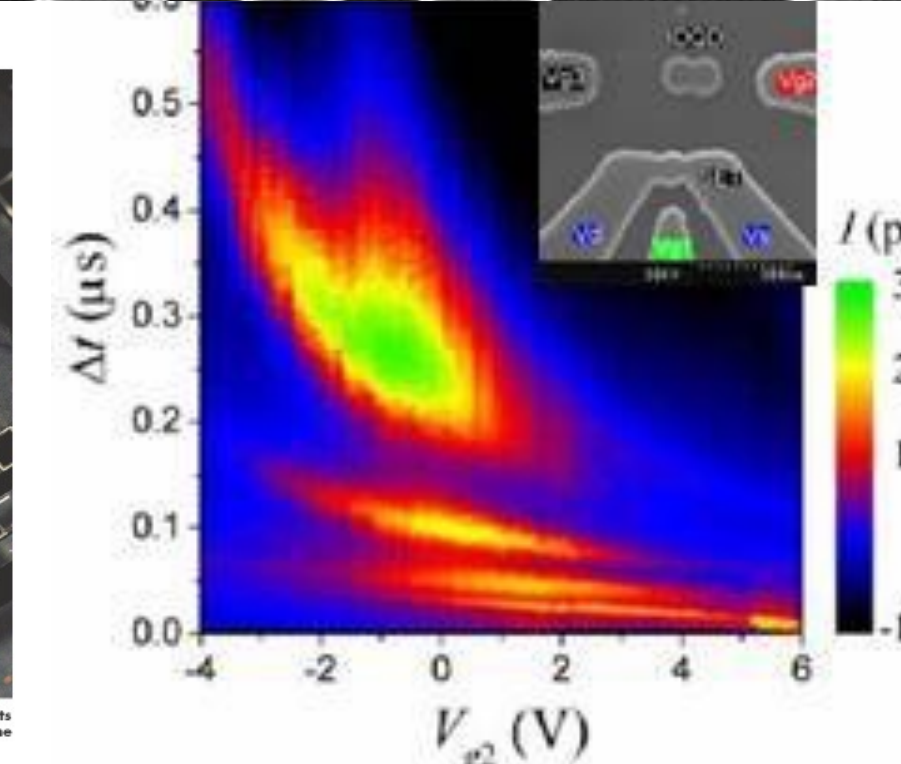
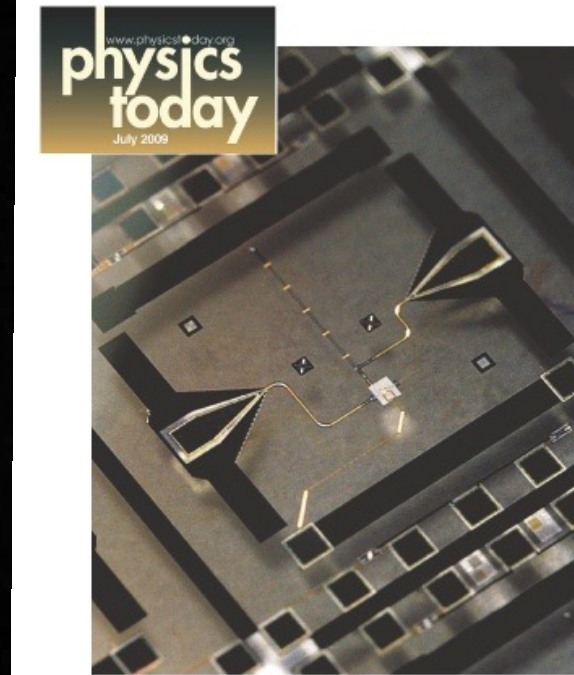
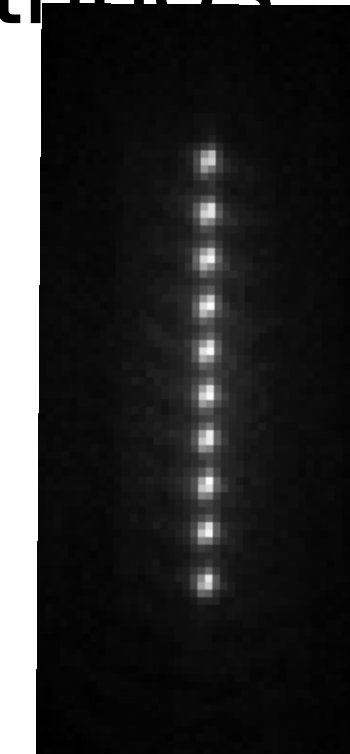
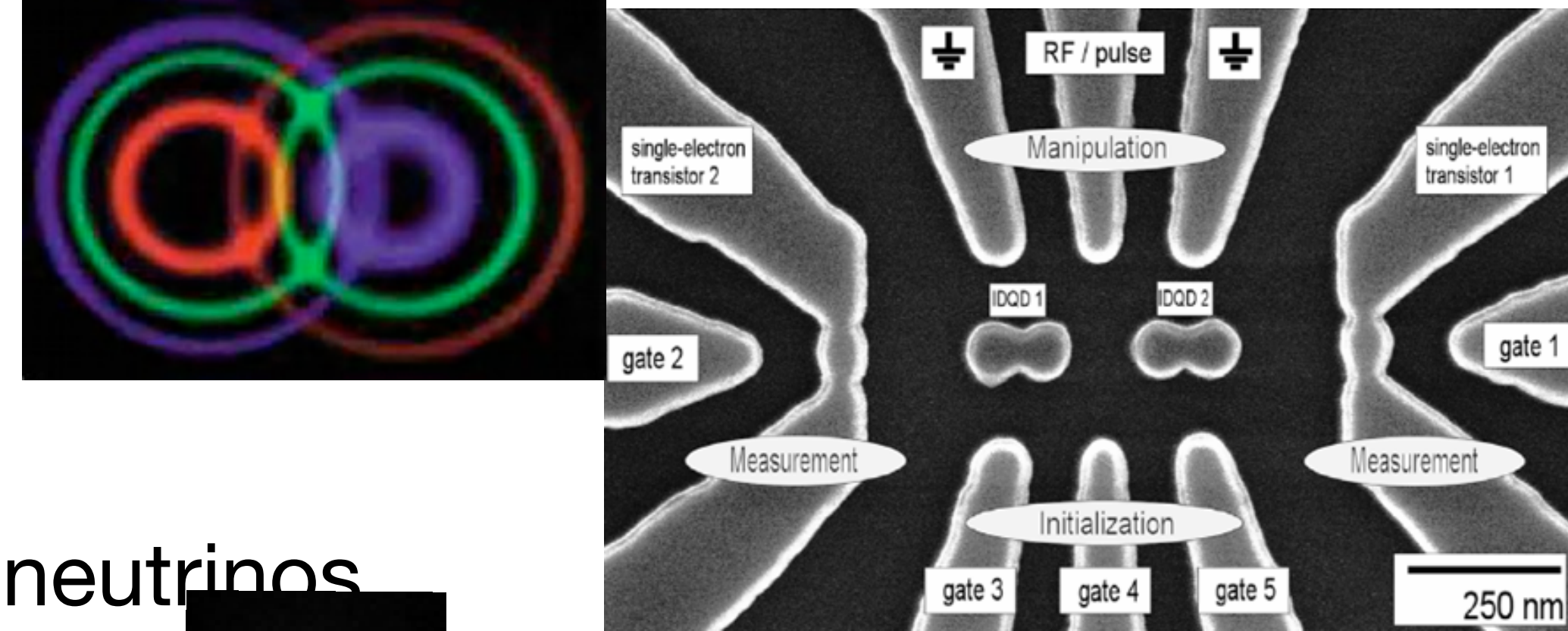
- NMR nuclear spins, Beryllium ions, photons, neutrinos
- Perfectly identical, naturally!
- WYGiWYG - No properties engineering

Tame qubits:

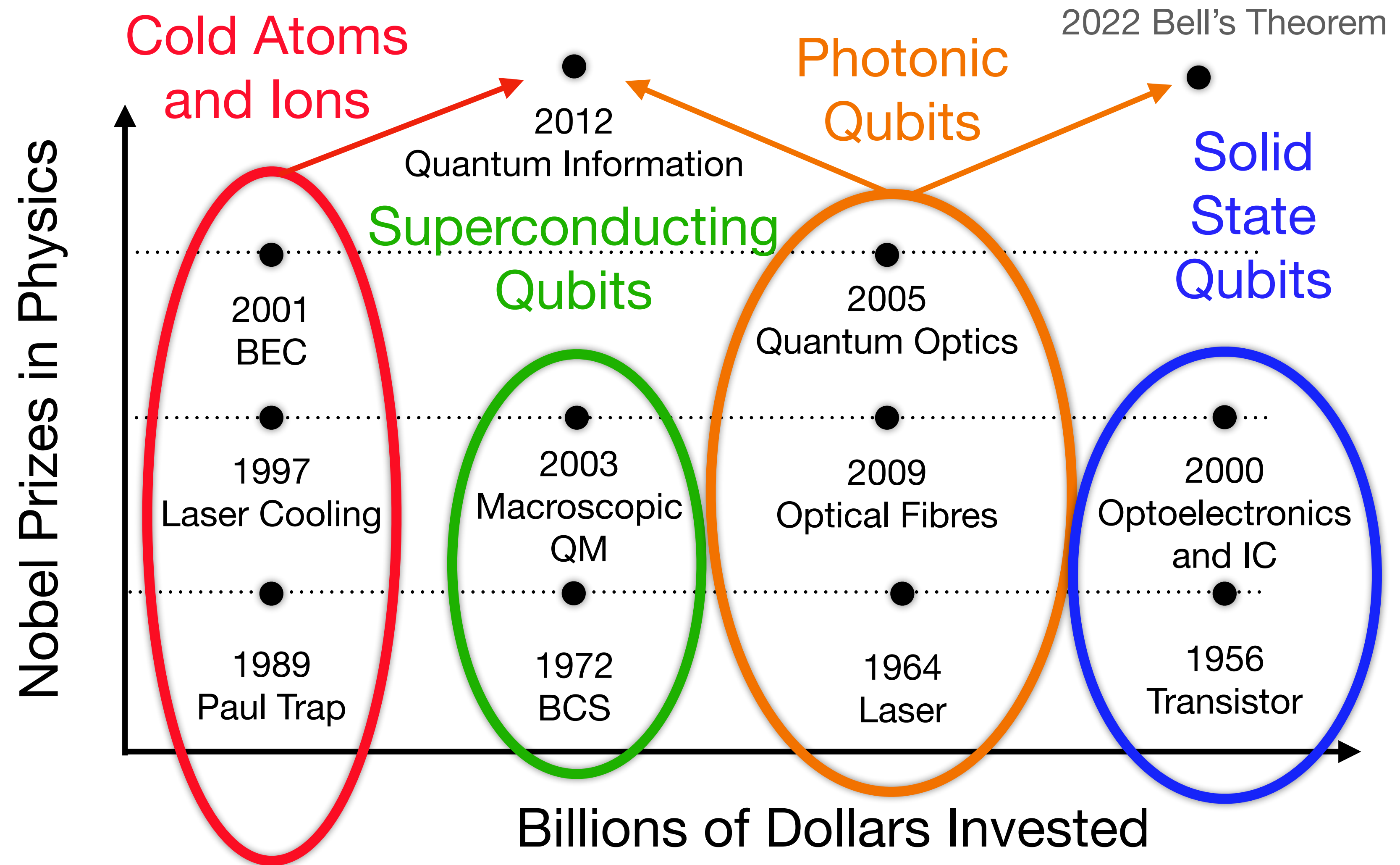
- SQUIDS, Quantum dots, NV diamond
- Home made - every one an original!
- Wide range of properties available (if you can control them)

Care and feeding:

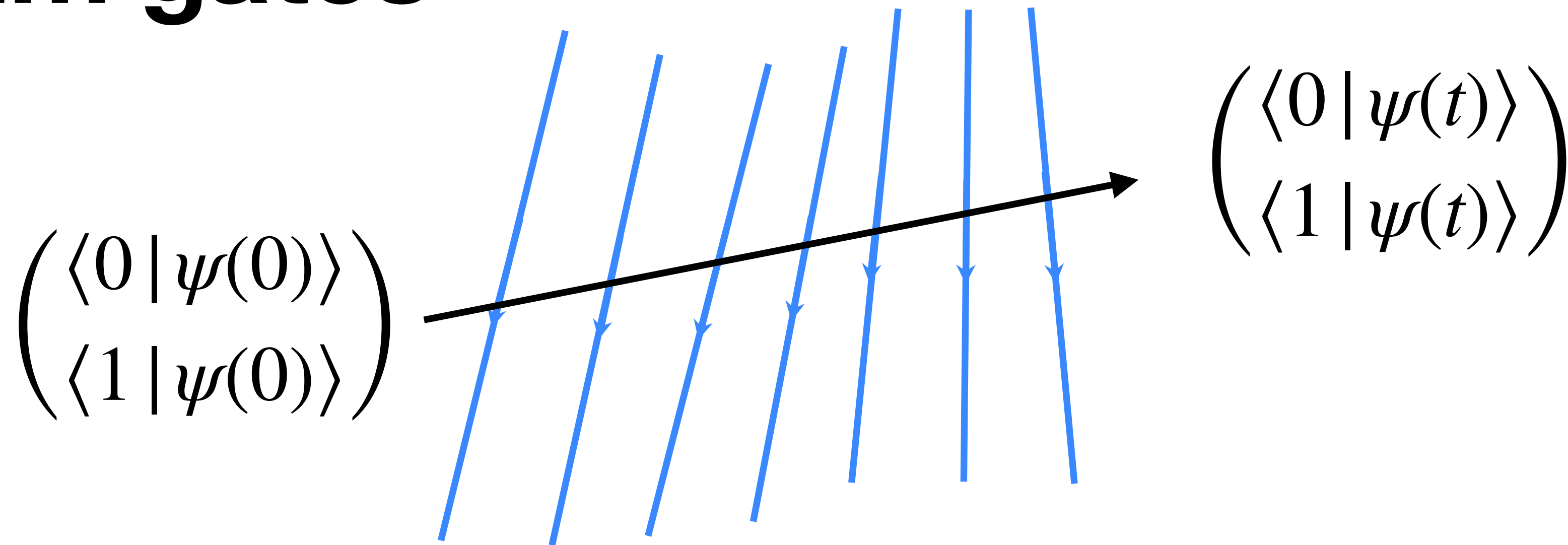
- Room temperature vs. mK
- NMR machine vs. Ion Trap vs. Dilution Fridge
- DC vs. Radio vs. Microwave vs. Laser control



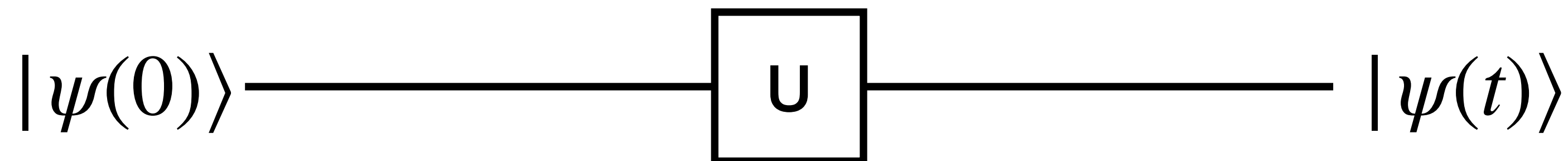
Qubits



Quantum gates



$$\begin{pmatrix} \langle 0 | \psi(t) \rangle \\ \langle 1 | \psi(t) \rangle \end{pmatrix} = \begin{pmatrix} U_{11}(t) & U_{12}(t) \\ U_{21}(t) & U_{22}(t) \end{pmatrix} \begin{pmatrix} \langle 0 | \psi(0) \rangle \\ \langle 1 | \psi(0) \rangle \end{pmatrix}$$

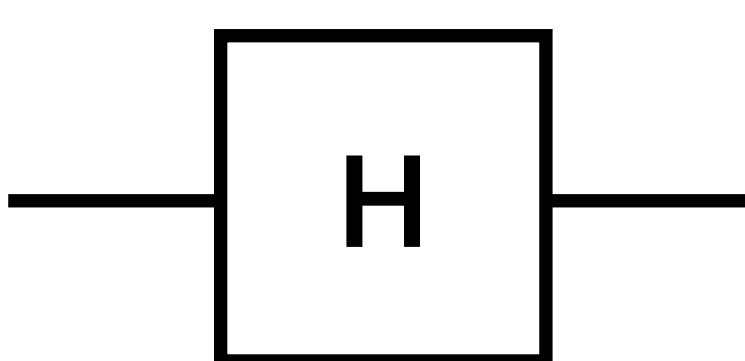


$$i\hbar \frac{\partial}{\partial t} |\psi\rangle = \hat{H} |\psi\rangle \quad |\psi(t)\rangle = \exp\left(-\frac{i\hat{H}t}{\hbar}\right) |\psi(0)\rangle$$

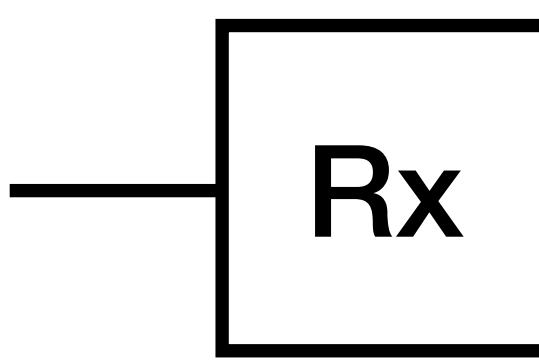


One Qubit Quantum Gates

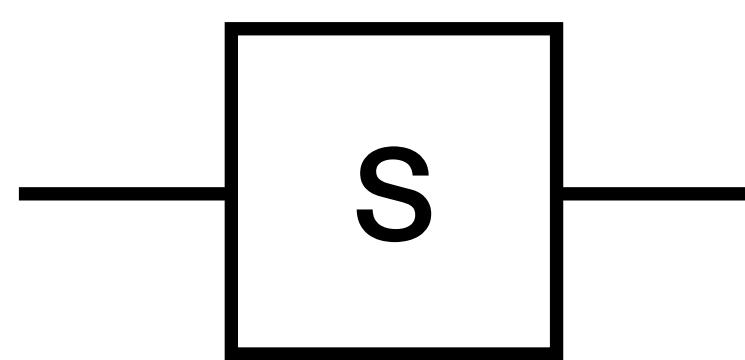
Hadamard

 $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

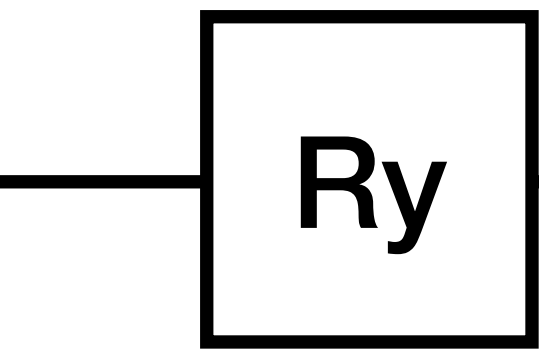
X rotation

 $\begin{pmatrix} \cos a/2 & i \sin a/2 \\ i \sin a/2 & \cos a/2 \end{pmatrix}$

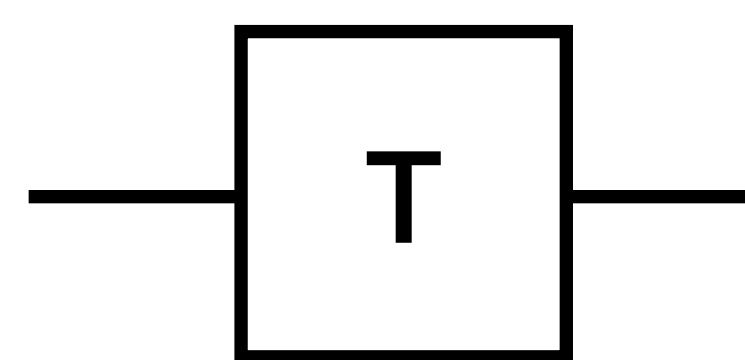
S gate

 $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

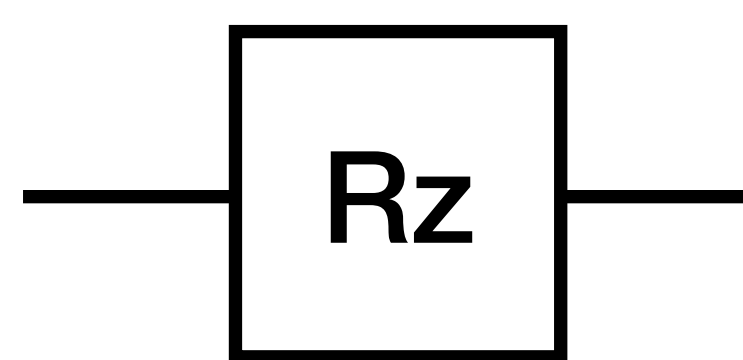
Y rotation

 $\begin{pmatrix} \cos a/2 & -\sin a/2 \\ \sin a/2 & \cos a/2 \end{pmatrix}$

T gate

 $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$

Z rotation

 $\begin{pmatrix} 1 & 0 \\ 0 & e^{ia/2} \end{pmatrix}$

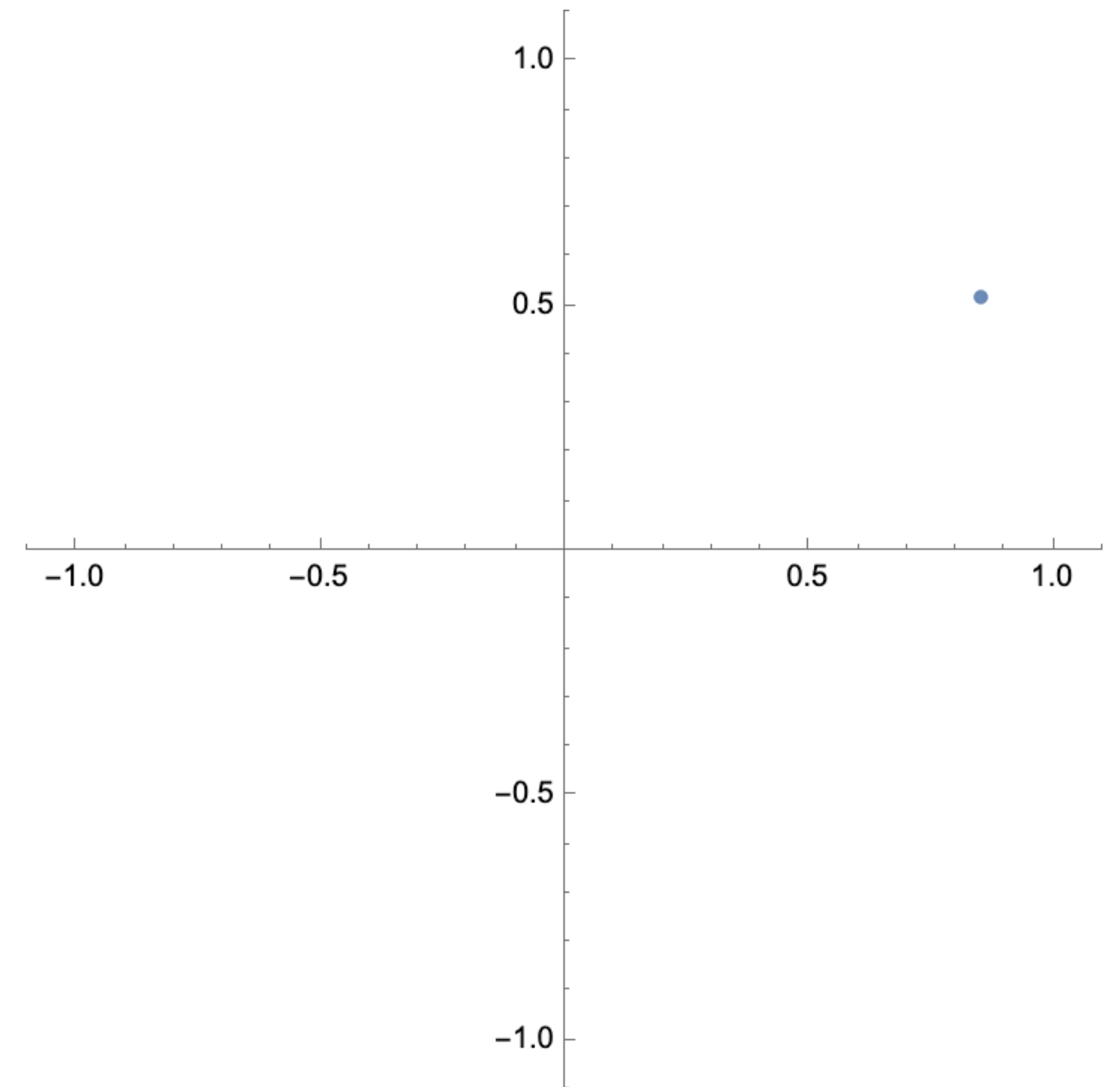
Single qubit gate synthesis

Hadamard

$$\text{---} \boxed{\text{H}} \text{---} \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

T gate

$$\text{---} \boxed{\text{T}} \text{---} \quad \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$



Fact: with combinations of T and H can make a rotation around an irrational multiple of π .

Then can make any rotation



UNIVERSITY OF
TORONTO

More than one qubit: the Tensor Product

Tensor product in a basis take: $\begin{pmatrix} \langle 0 | \psi_1 \rangle \\ \langle 1 | \psi_1 \rangle \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$ and $\begin{pmatrix} \langle 0 | \psi_2 \rangle \\ \langle 1 | \psi_2 \rangle \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix}$

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a \begin{pmatrix} c \\ d \end{pmatrix} \\ b \begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$

A state that can be written as the tensor product of the state of system 1 with the state of system 2 is called *separable*.

Are all states separable?

Entanglement

Are all quantum states separable?

NO!!

Example: Bell states

Bell States

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

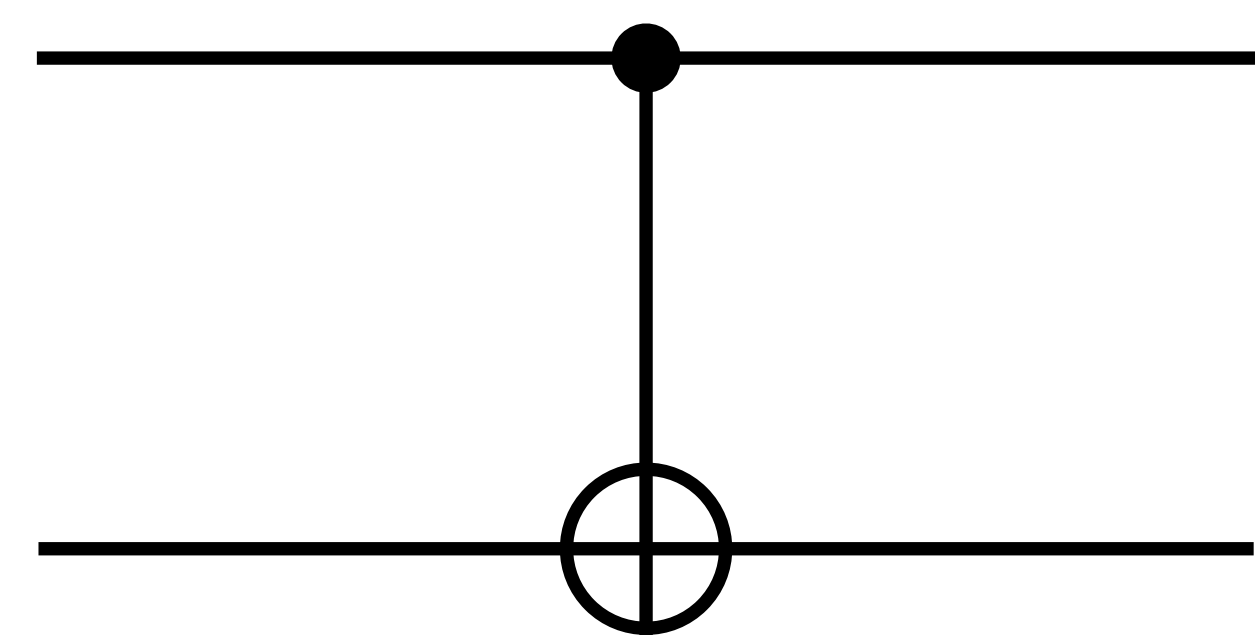
$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$$

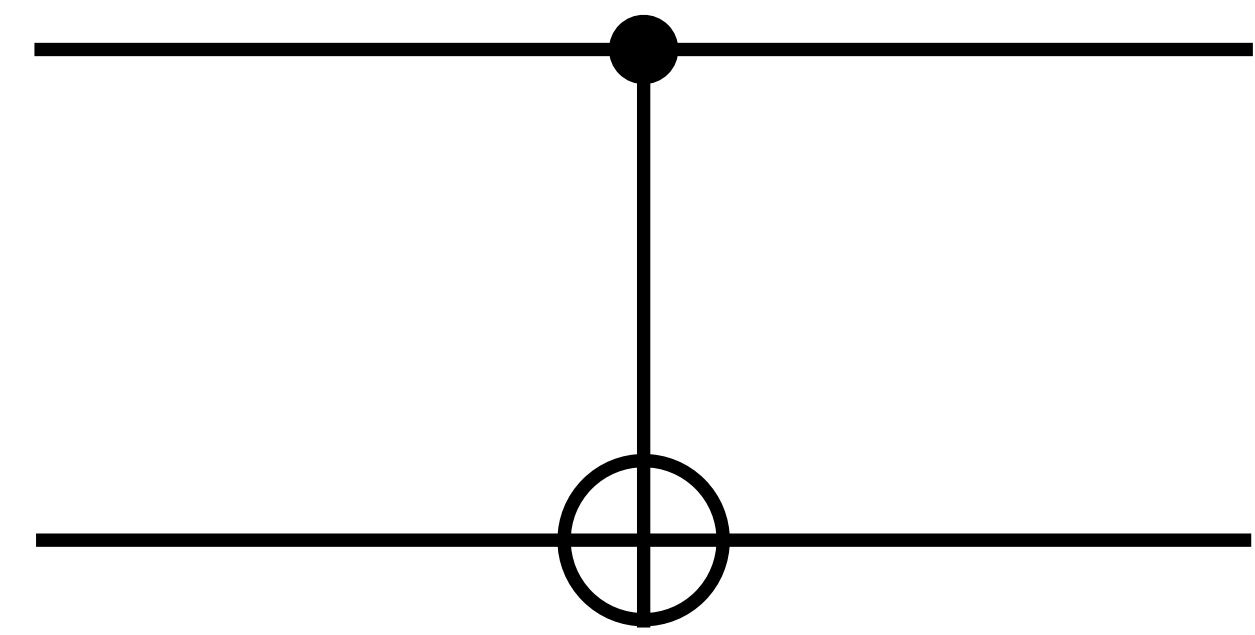
Two qubit Quantum Gates: Examples

CNOT

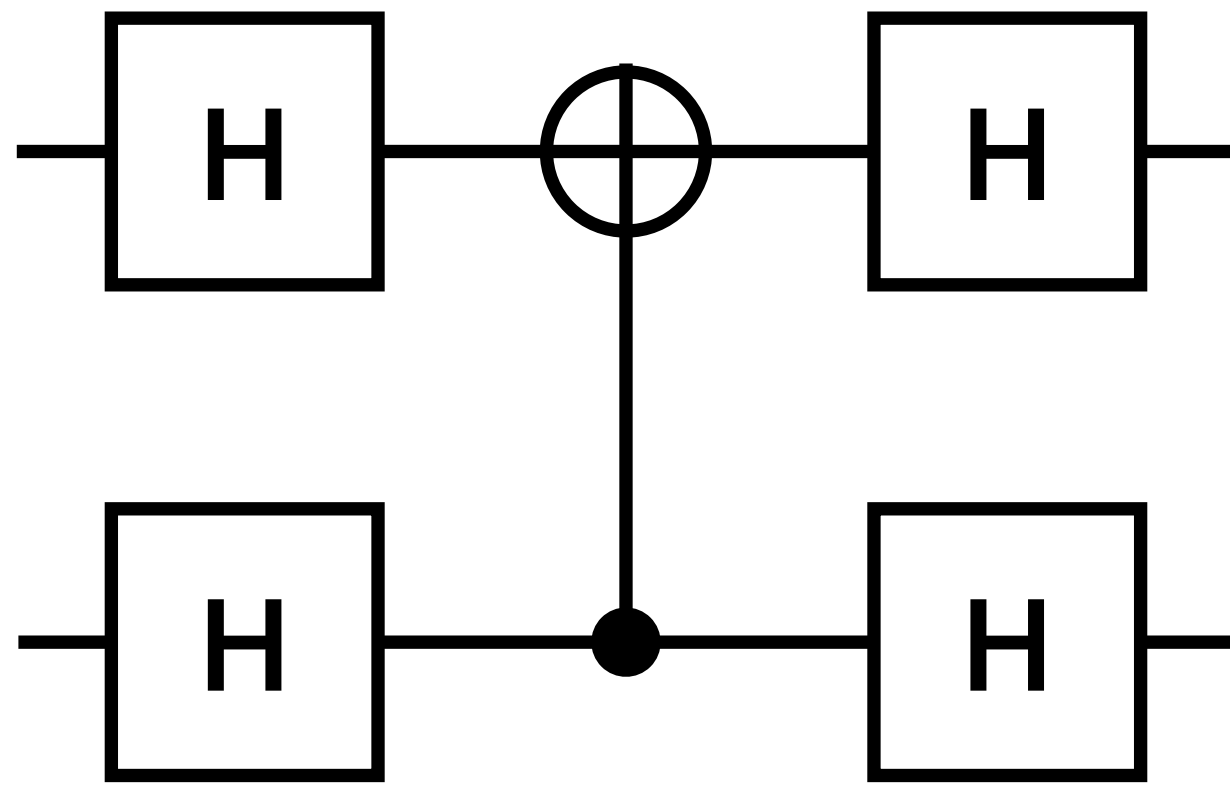


$$\begin{pmatrix} \langle 00 | \psi(t) \rangle \\ \langle 01 | \psi(t) \rangle \\ \langle 10 | \psi(t) \rangle \\ \langle 11 | \psi(t) \rangle \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \langle 00 | \psi(0) \rangle \\ \langle 01 | \psi(0) \rangle \\ \langle 10 | \psi(0) \rangle \\ \langle 11 | \psi(0) \rangle \end{pmatrix}$$

Control and target can be changed by one-qubit gates



=

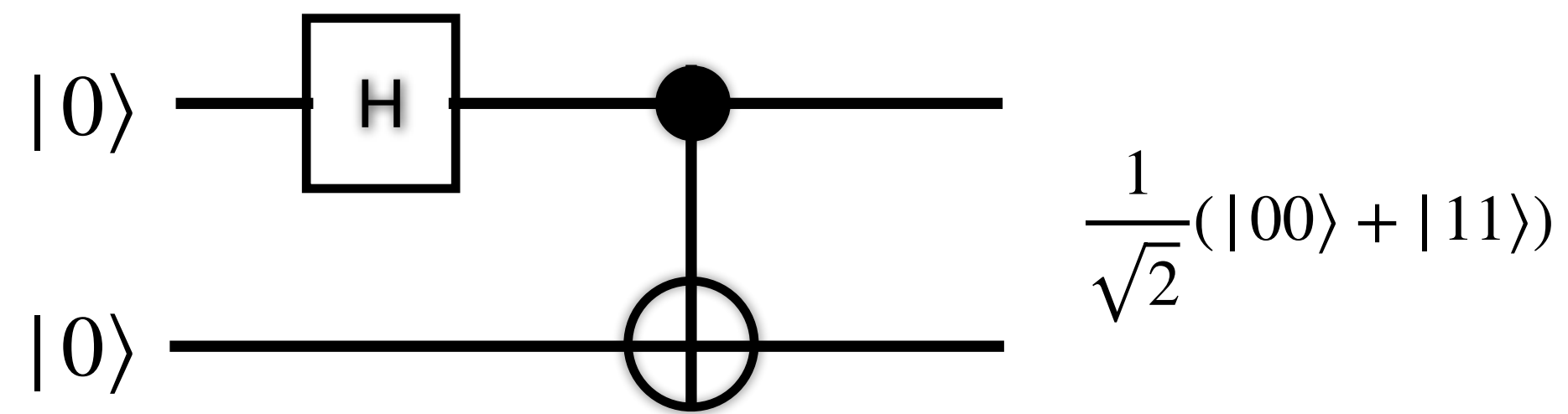


Quantum Circuit Model

Quantum Circuit: a single qubit is denoted by a line



Complex circuits - many lines, many gates



Can denote a register with n qubits



Linearity

Quantum gates and circuits act on superposition states

Simple example: $X|0\rangle = |1\rangle, X|1\rangle = |0\rangle$

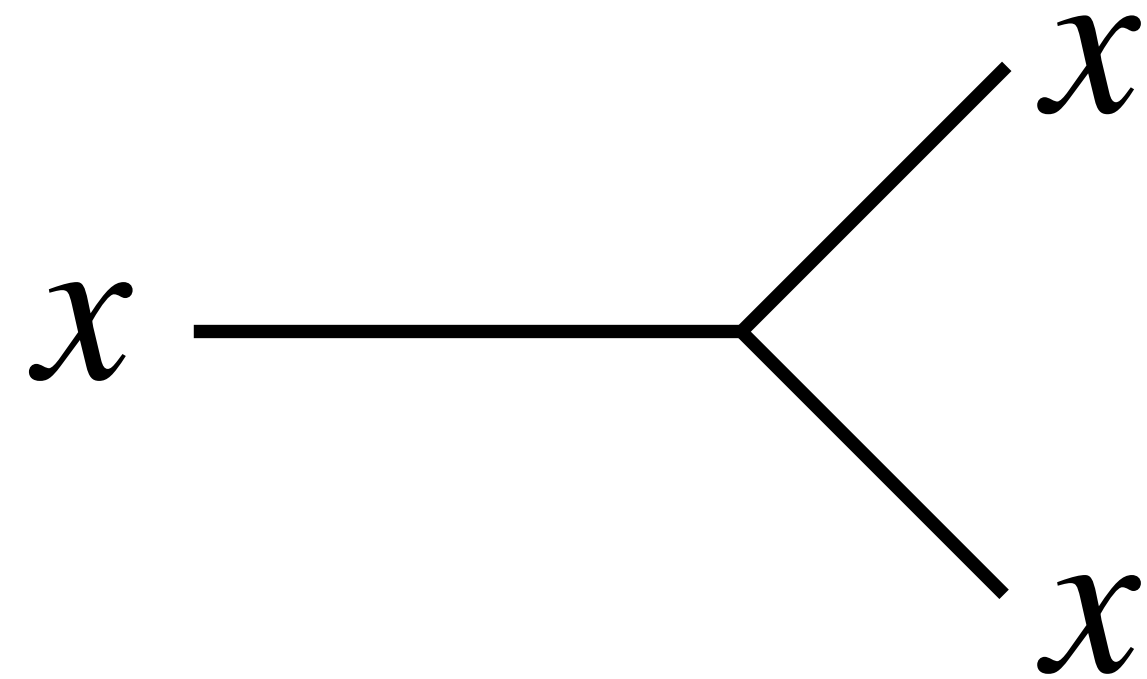
$$X(a|0\rangle + b|1\rangle) = (a|1\rangle + b|0\rangle)$$

In general if $|\psi\rangle = \sum_{x=0}^{2^n-1} c_x |x\rangle$

Then U acts LINEARLY: $U|\psi\rangle = \sum_{x=0}^{2^n-1} c_x U|x\rangle$

No Cloning

A simple classical gate is fanout:



$$x \in \{0,1\}$$

This copies classical bits.

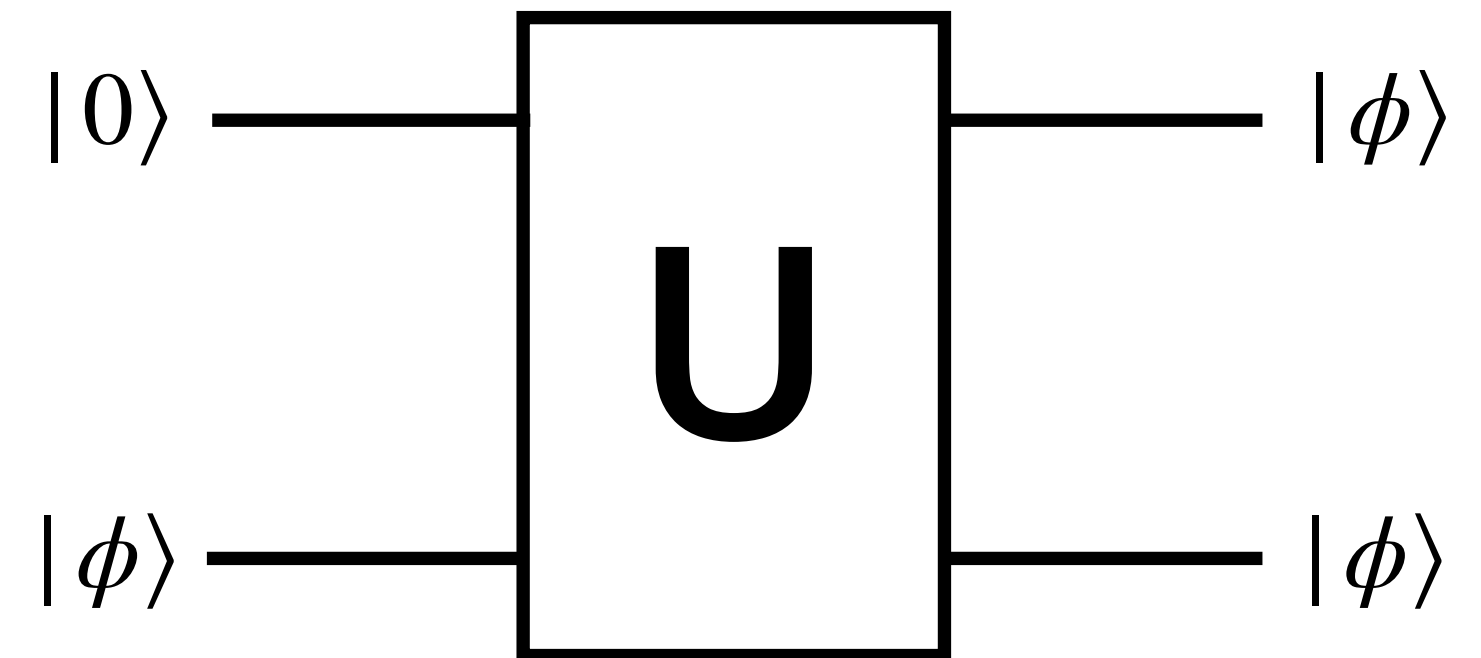
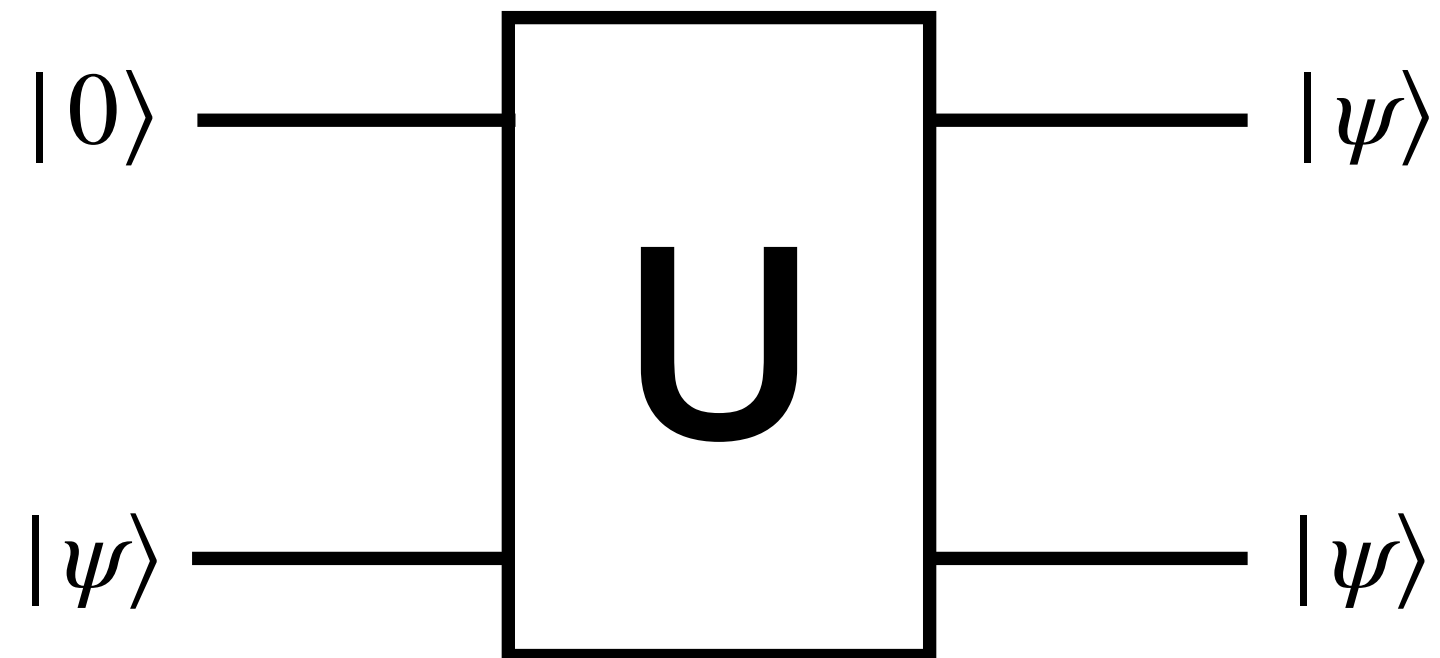
Can we copy quantum information?

No Cloning

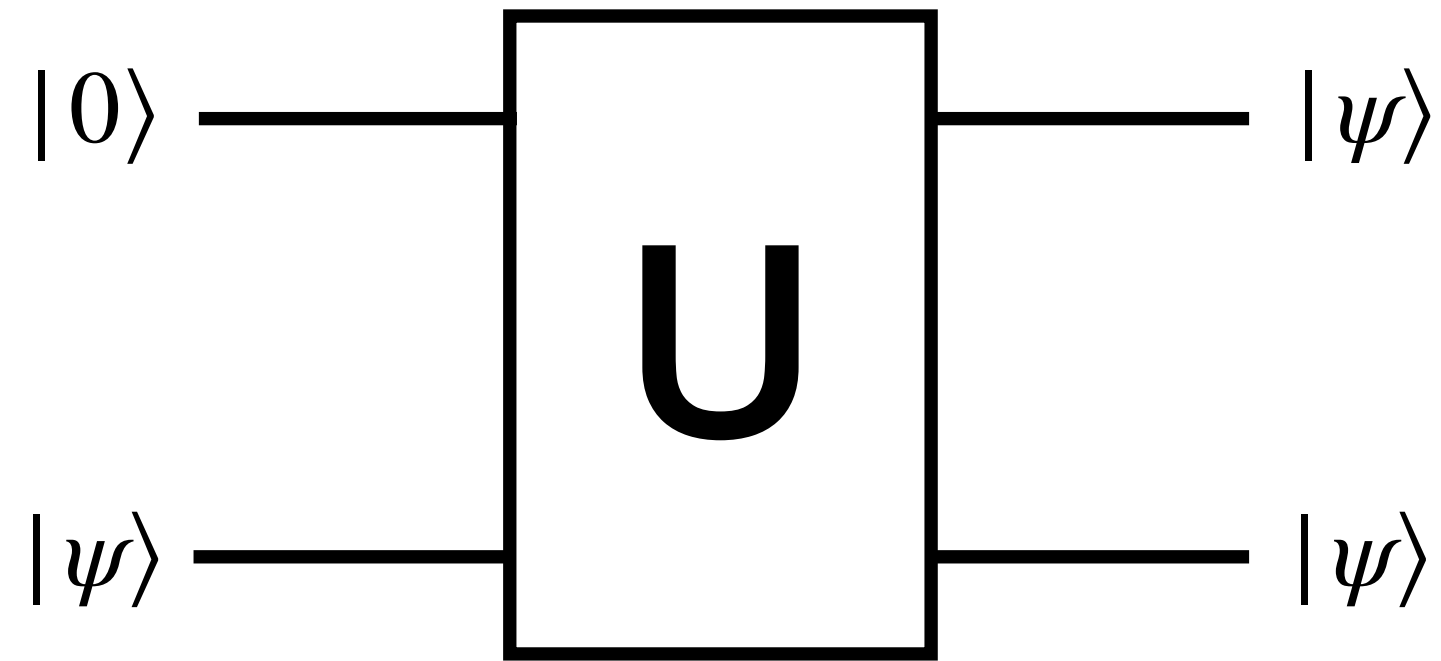
Suppose I might have $|\psi\rangle$ or $|\phi\rangle$ but I don't know which.

Can I copy my unknown quantum state?

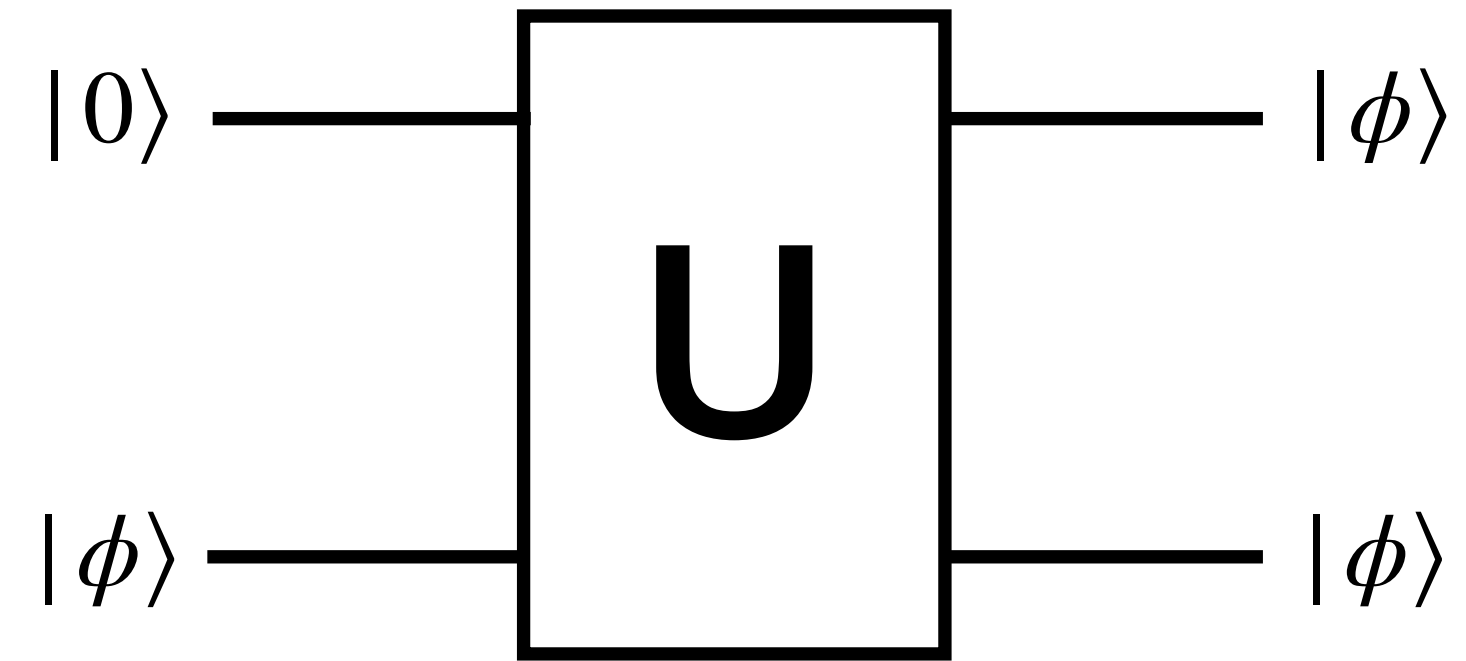
Is there a U such that:



No Cloning Theorem



$$U|0\rangle \otimes |\psi\rangle = |\psi\rangle \otimes |\psi\rangle$$



$$U|0\rangle \otimes |\phi\rangle = |\phi\rangle \otimes |\phi\rangle$$

Take the inner products of both sides:

$$\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2$$

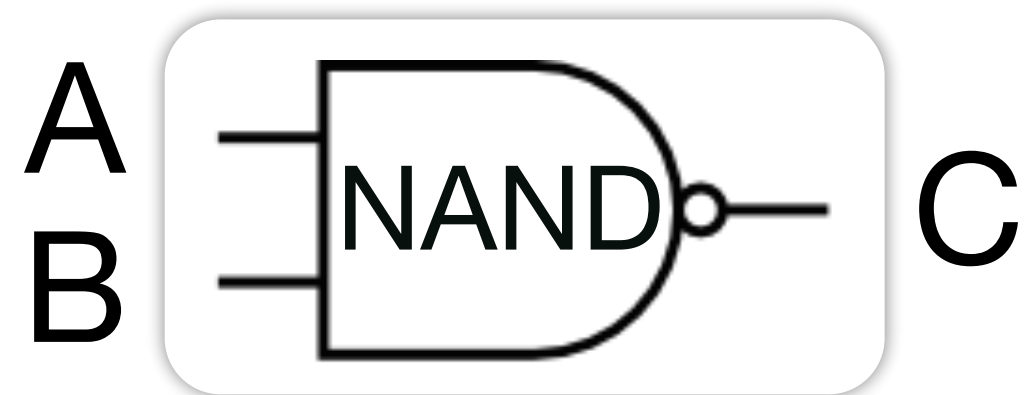
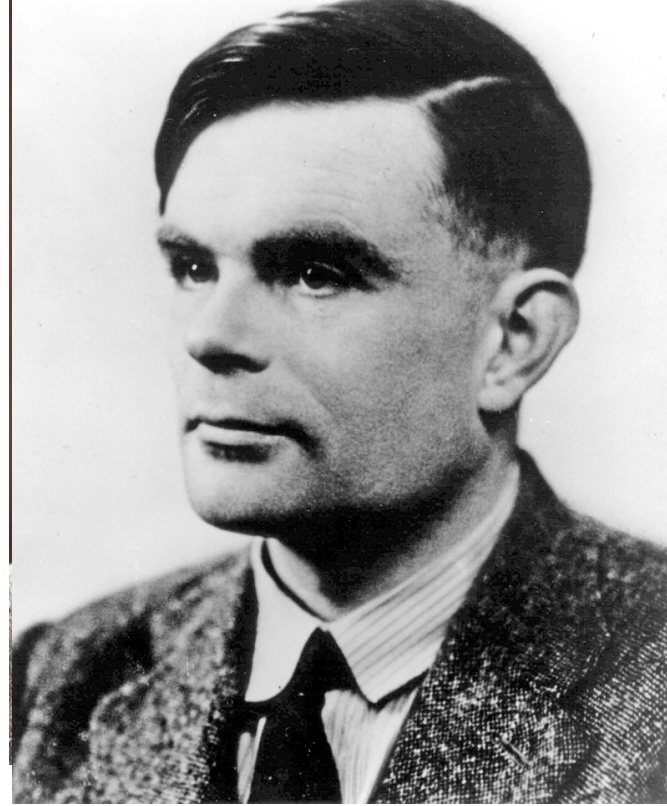
This implies either $\langle\psi|\phi\rangle = 0$ or $\langle\psi|\phi\rangle = 1$

U only exists if the states are orthogonal - so we can only copy classical information.

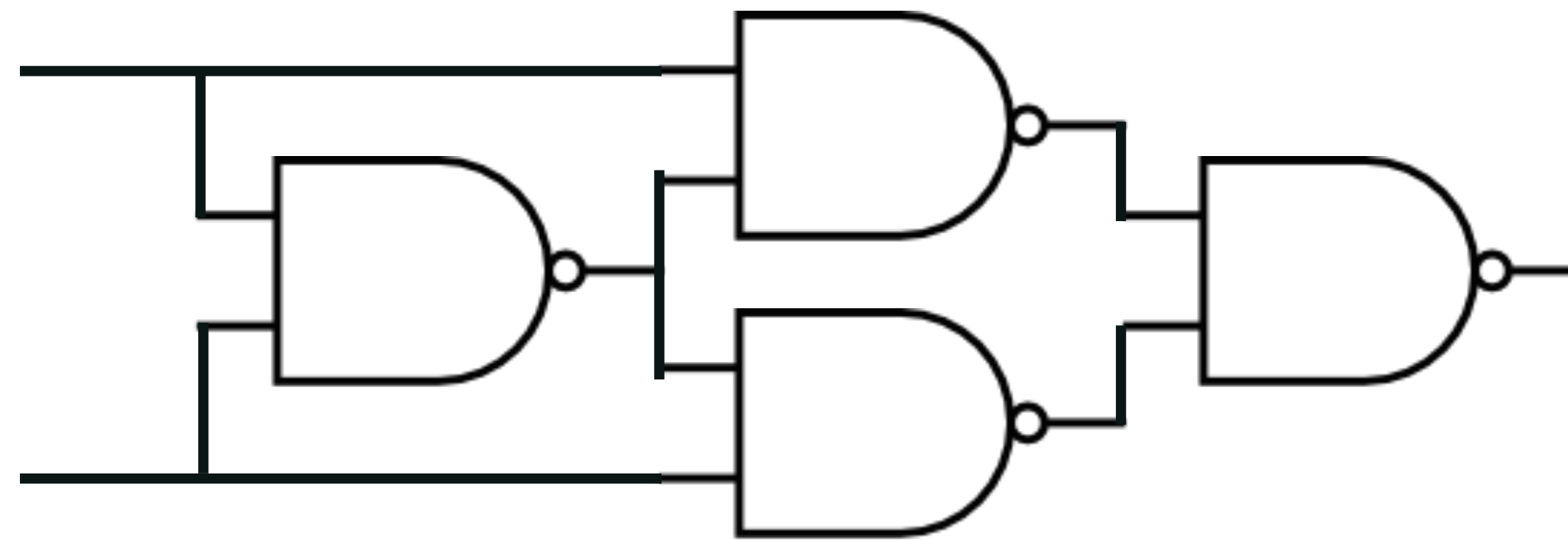
Universality in Classical Computation

How many kinds of gate must I build?

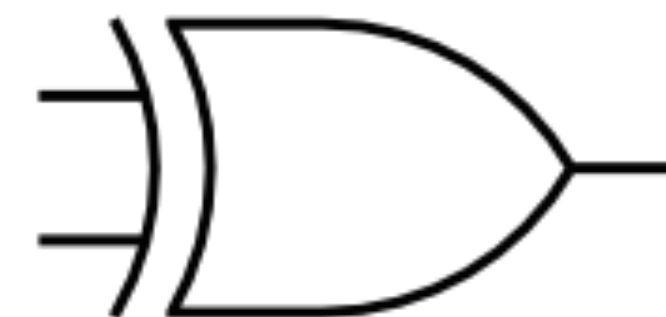
Classically: ONE! NAND is universal



A	B	C
0	0	1
0	1	1
1	0	1
1	1	0

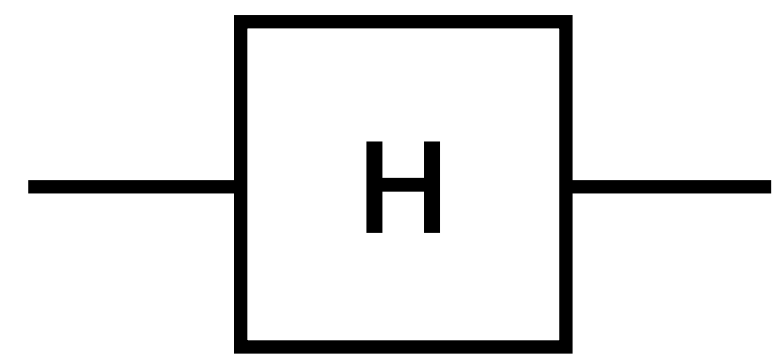


=



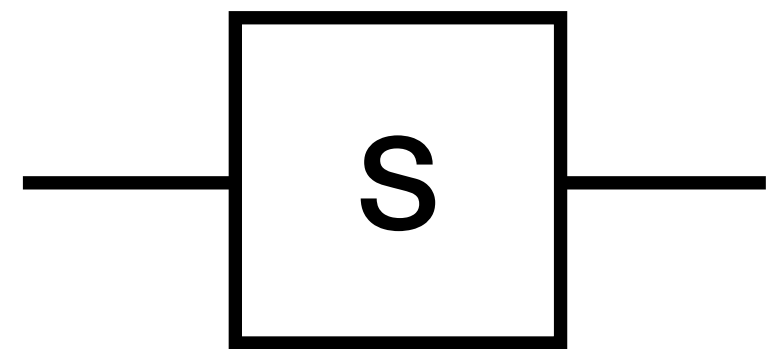
One Qubit Quantum Gates

Hadamard



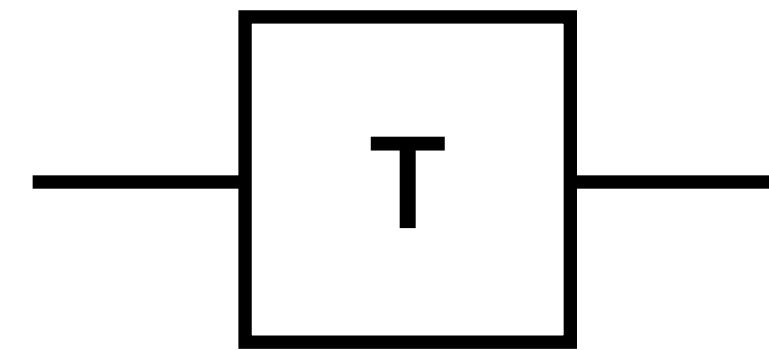
$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

S gate



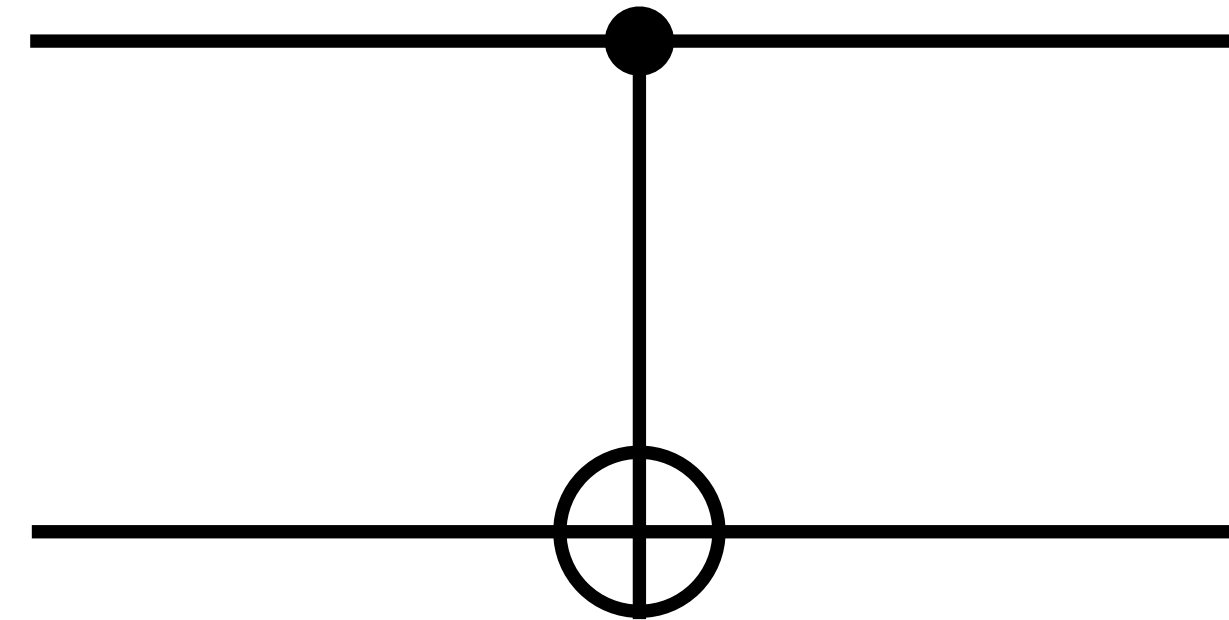
$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

T gate



$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

CNOT

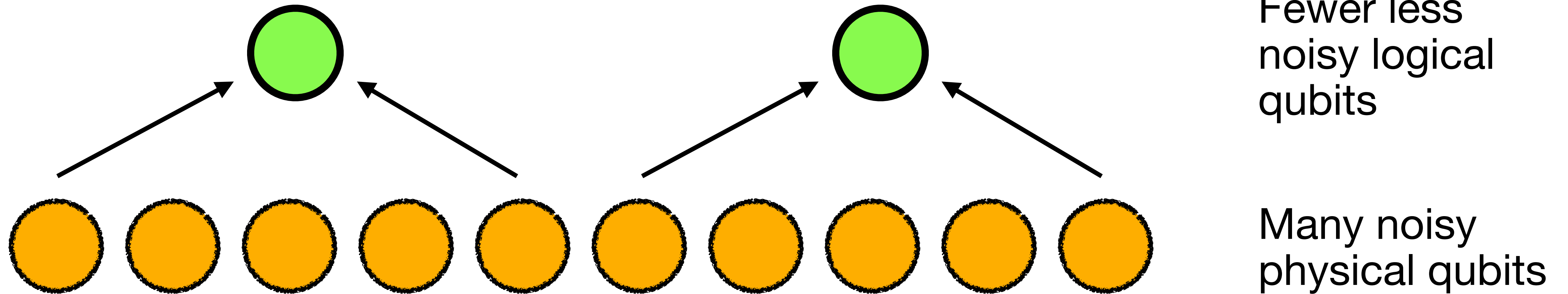


Clifford Gates - easy to simulate classically
Not universal!

Only need to add T gate to make a universal set



Logical qubits

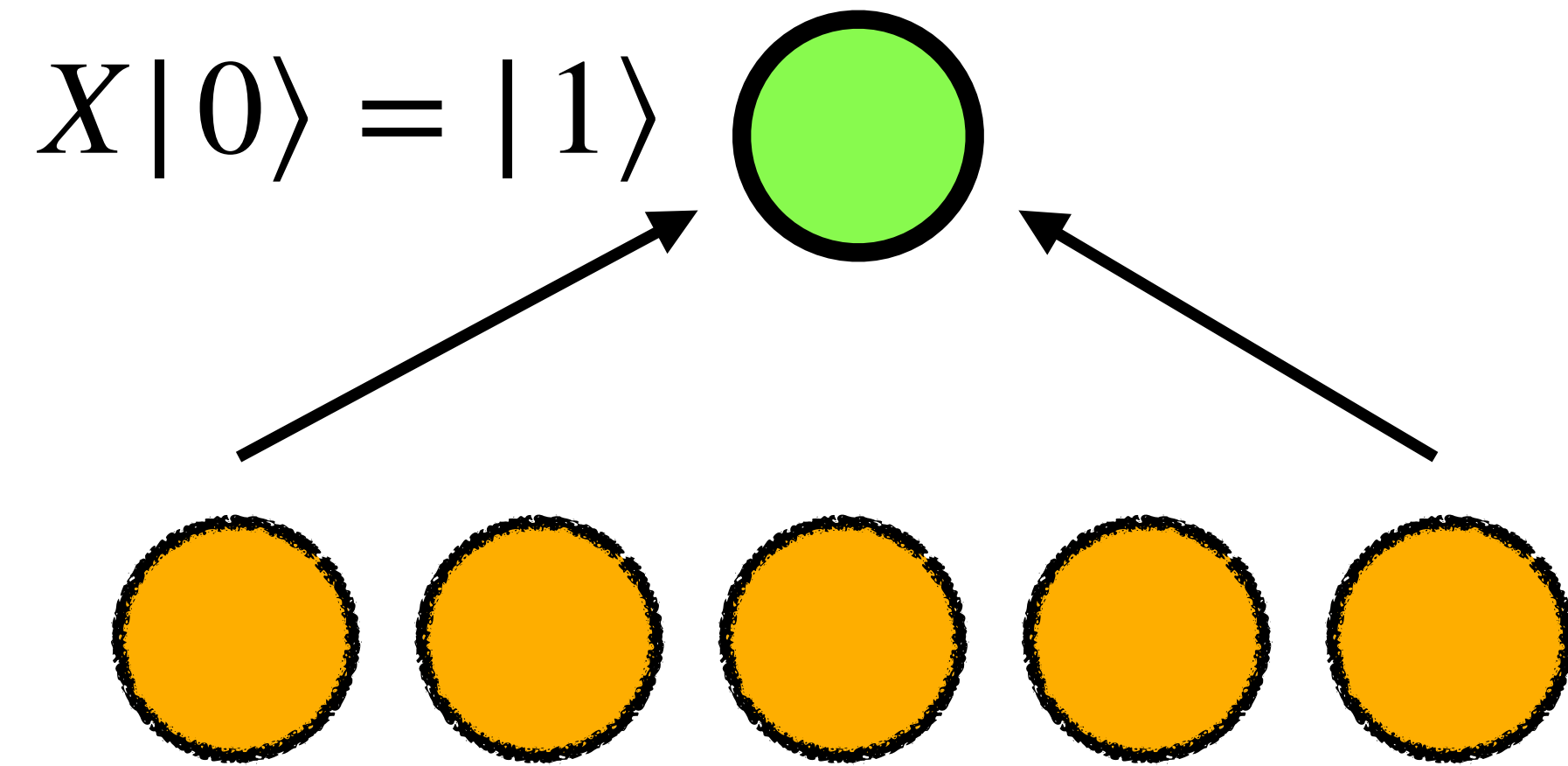


Logical $|0\rangle$ and $|1\rangle$ are entangled states of the physical qubits

Errors can be detected and corrected without disturbing logical information

Physical noise must be below a threshold that depends on the code

Fault tolerant gates



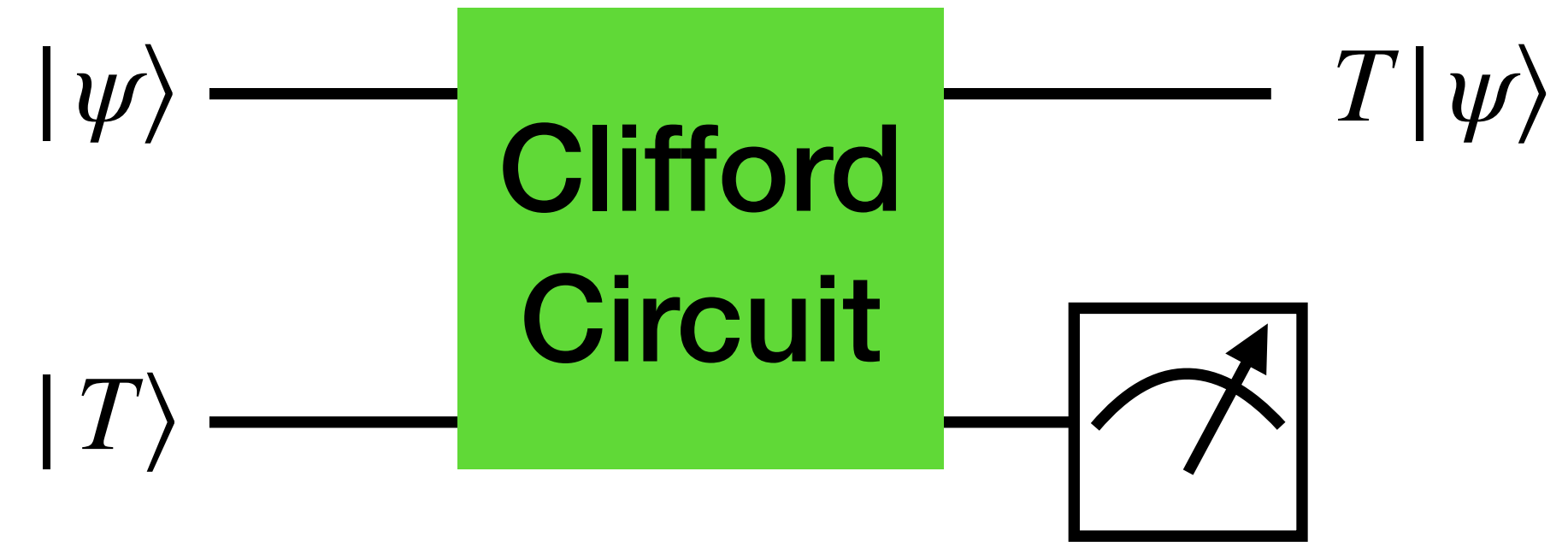
Transversal Gates: Easy!

Clifford gates are transversal

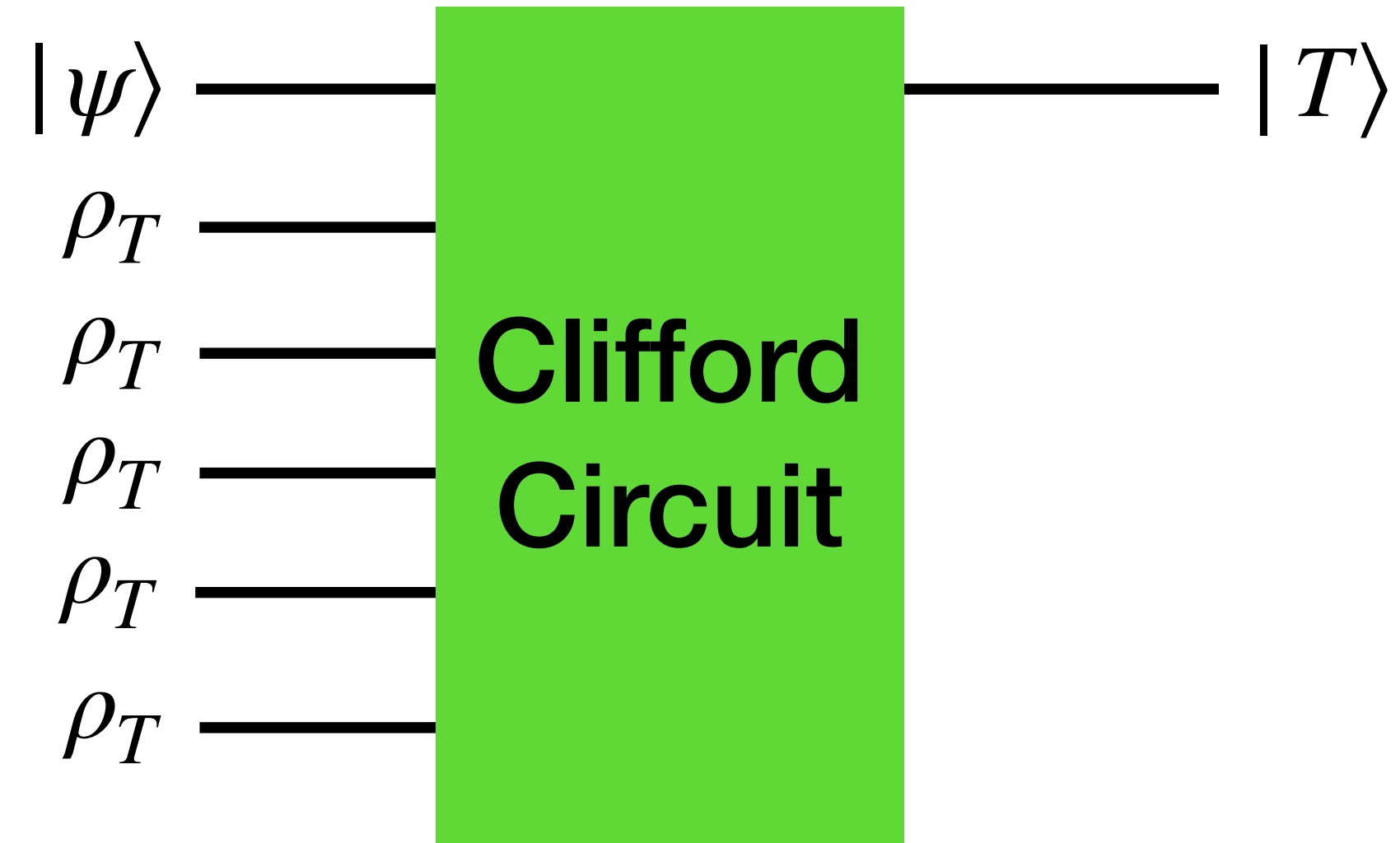
T-gates are not transversal

T-gates are Hard!

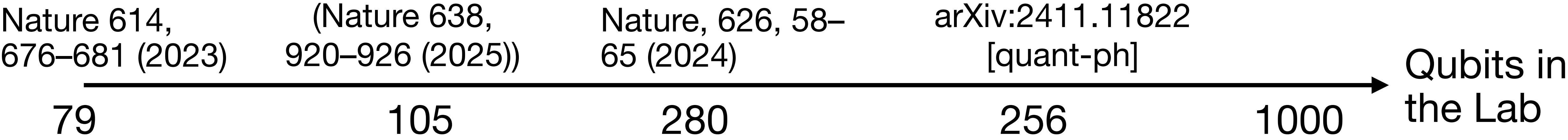
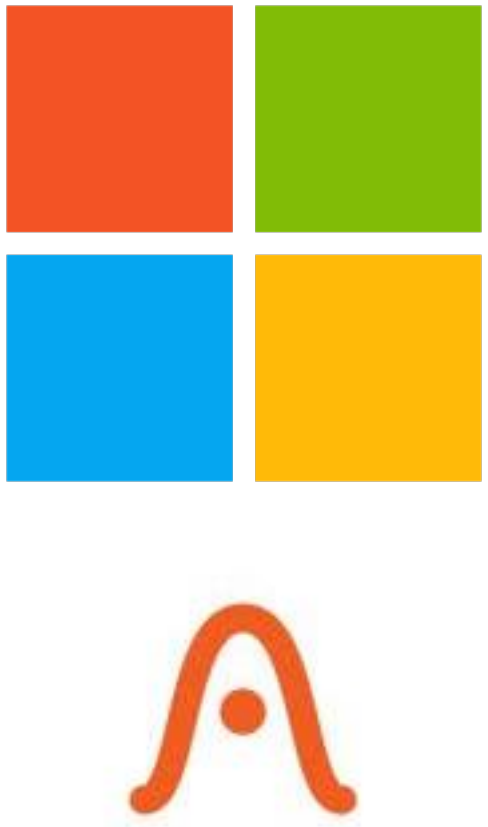
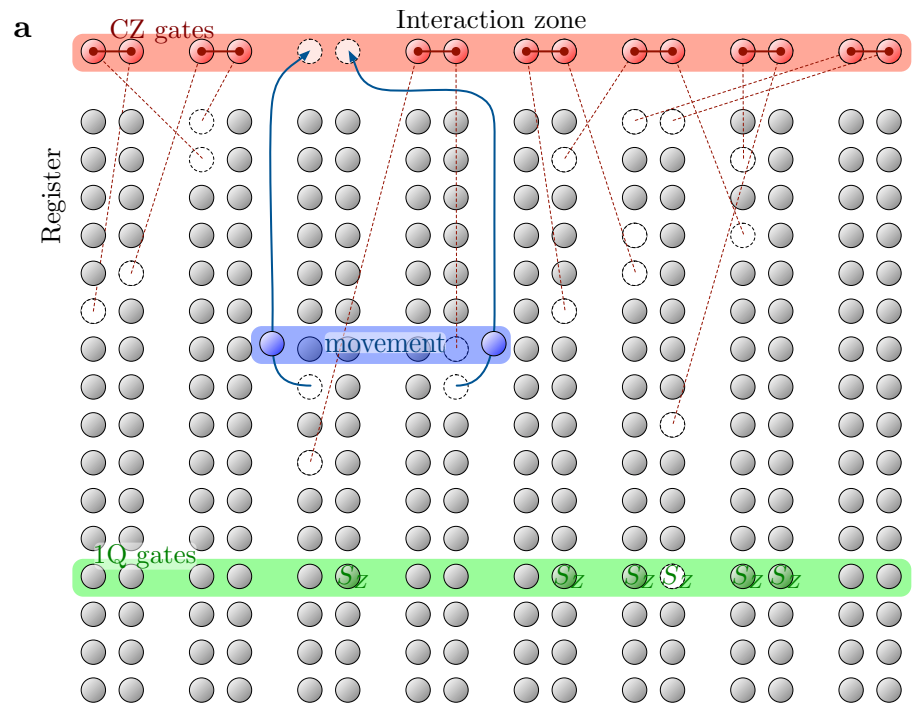
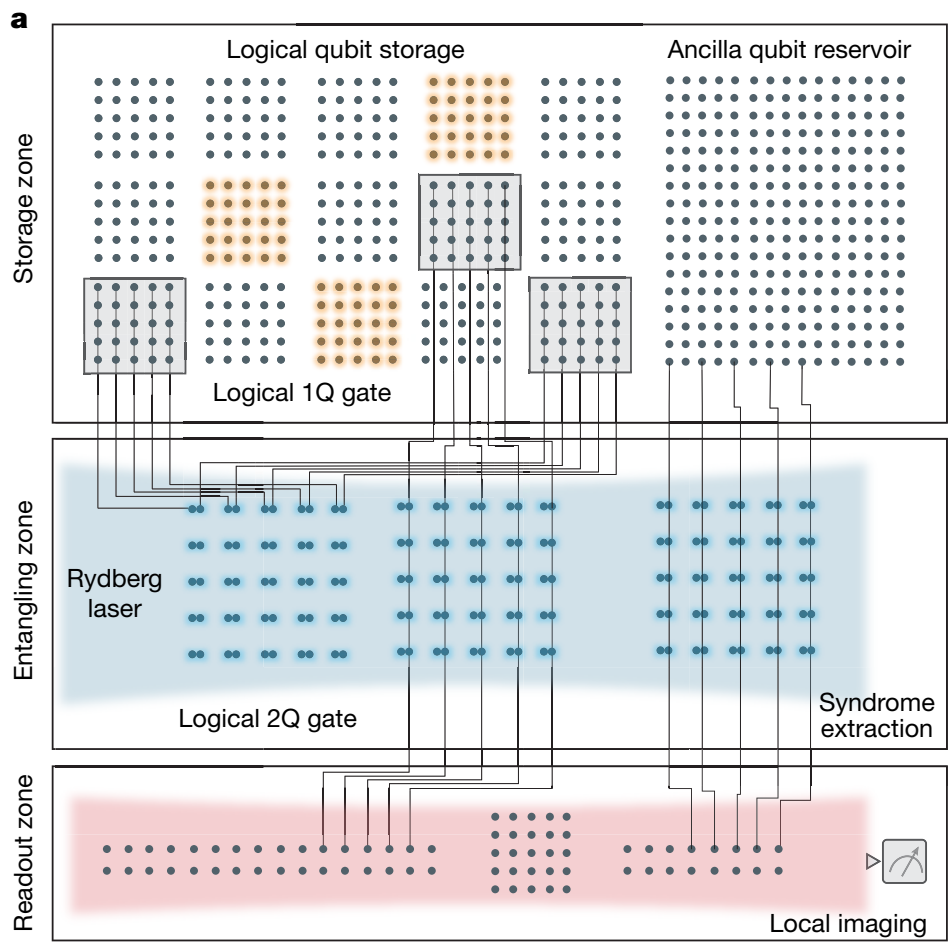
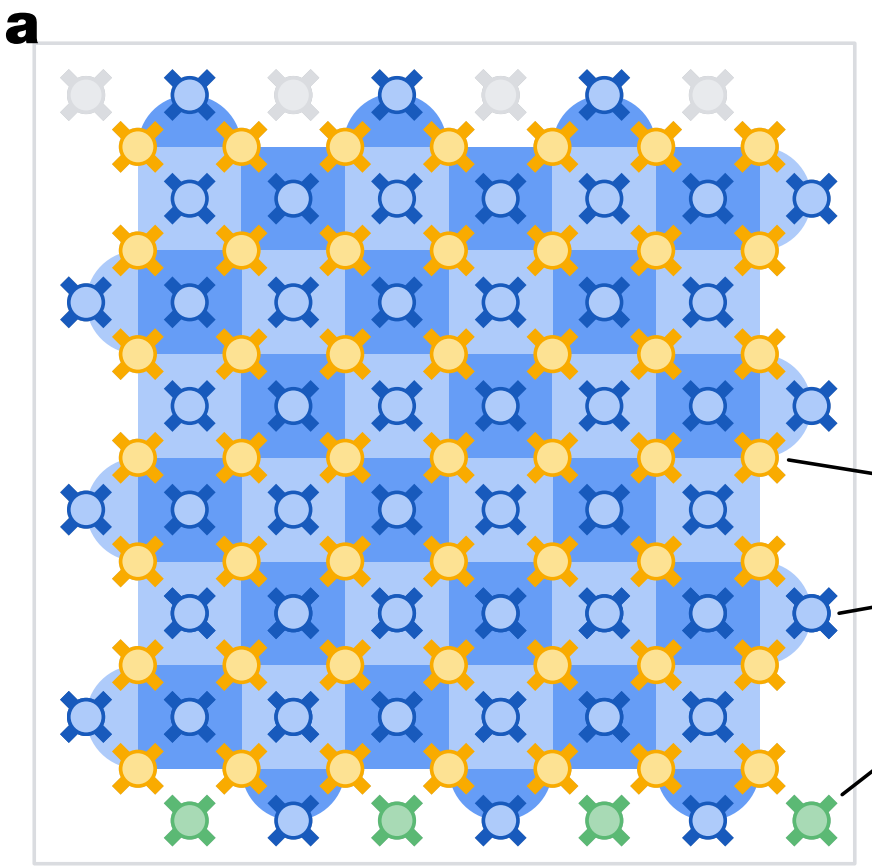
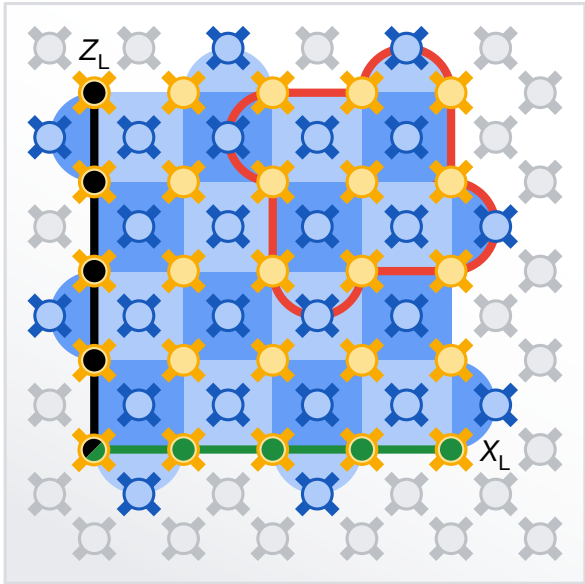
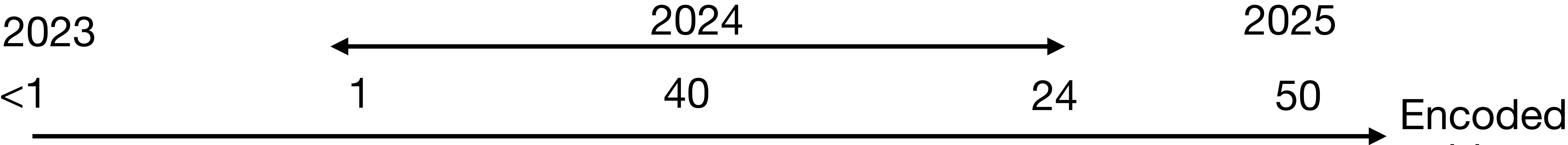
State Injection:



Magic state distillation



Where are we now?



Nature 614,
676–681 (2023)

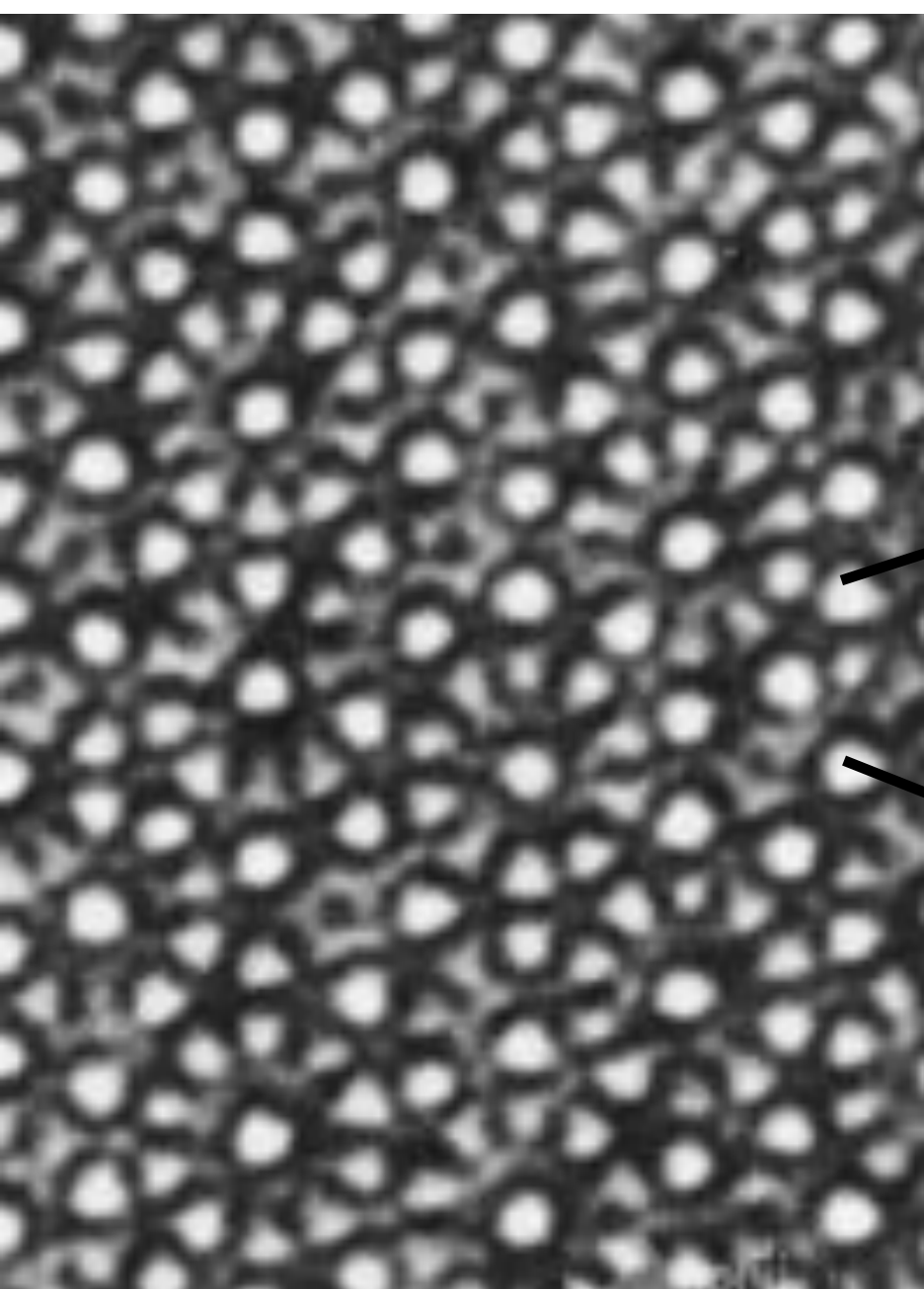
(Nature 638,
920–926 (2025))

Nature, 626, 58–
65 (2024)

arXiv:2411.11822
[quant-ph]

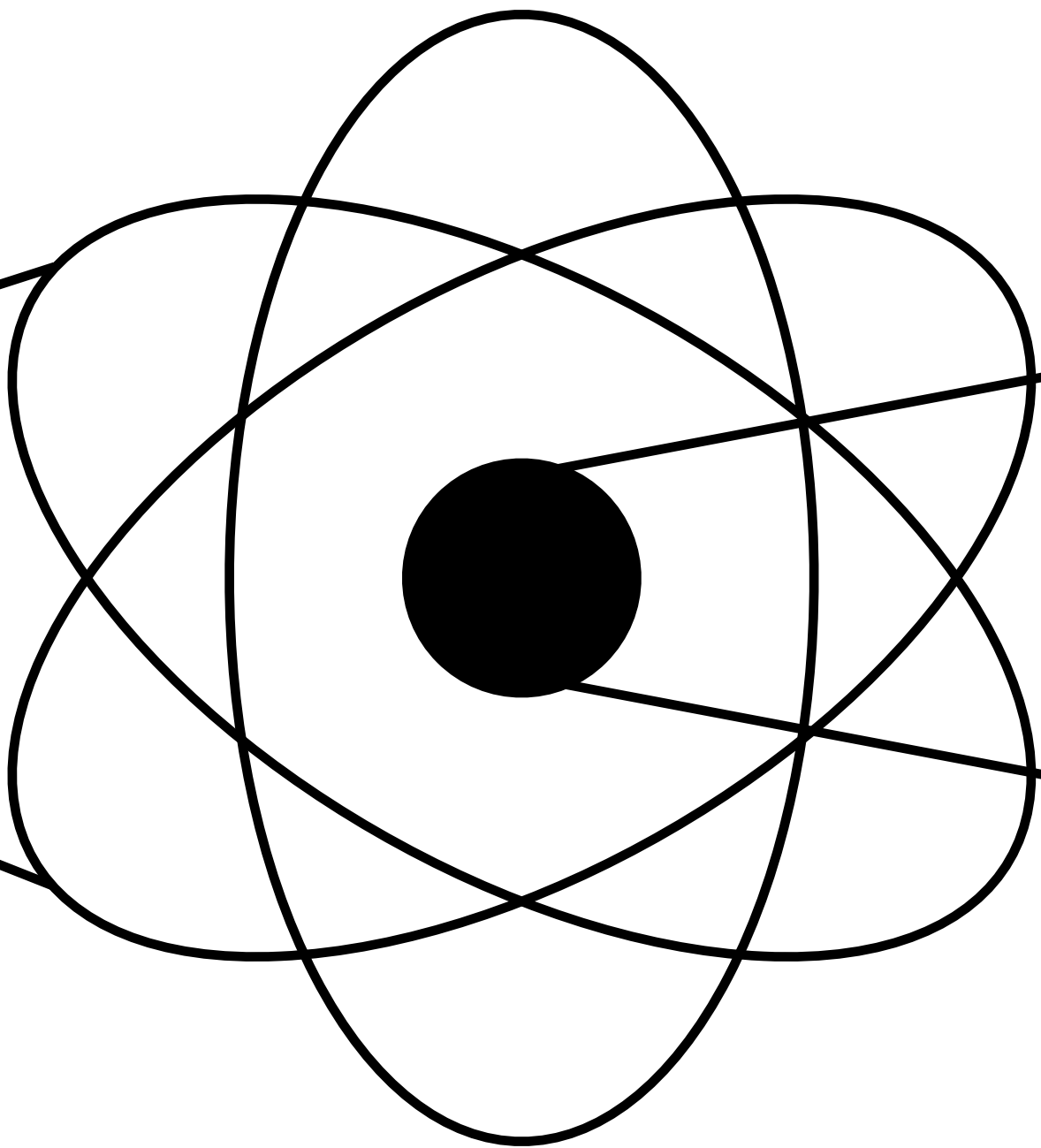
Application: Quantum simulation of the structure of matter

Materials



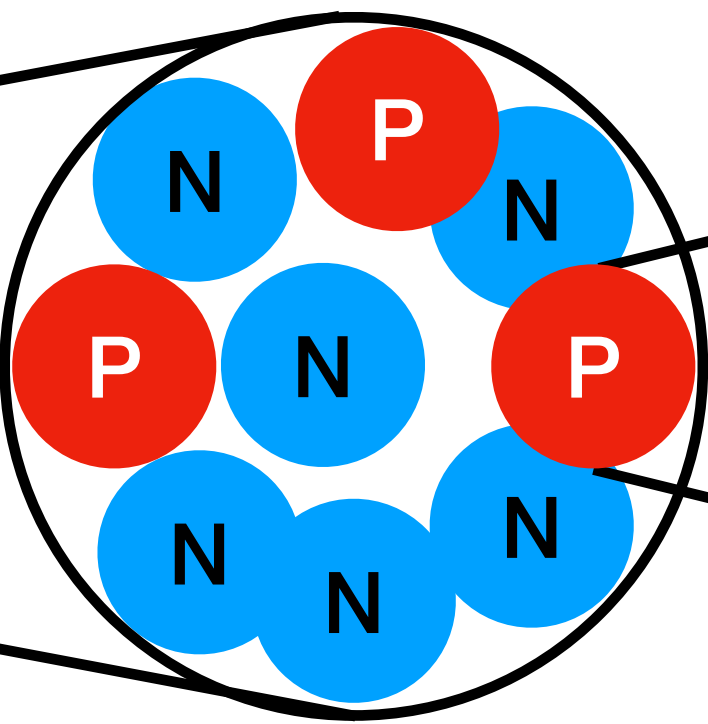
meV

Electronic Structure



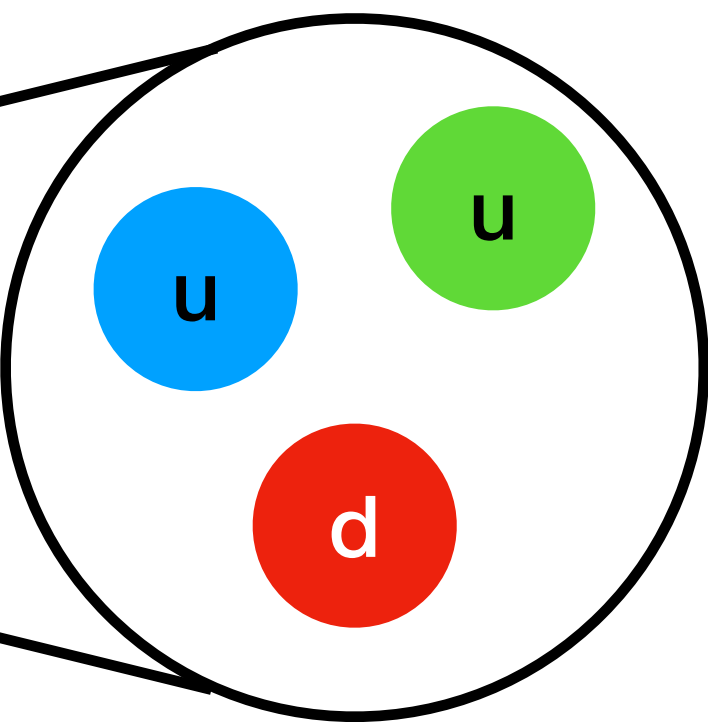
eV
 10^{-10} m

Nuclear Structure



GeV
 10^{-15} m

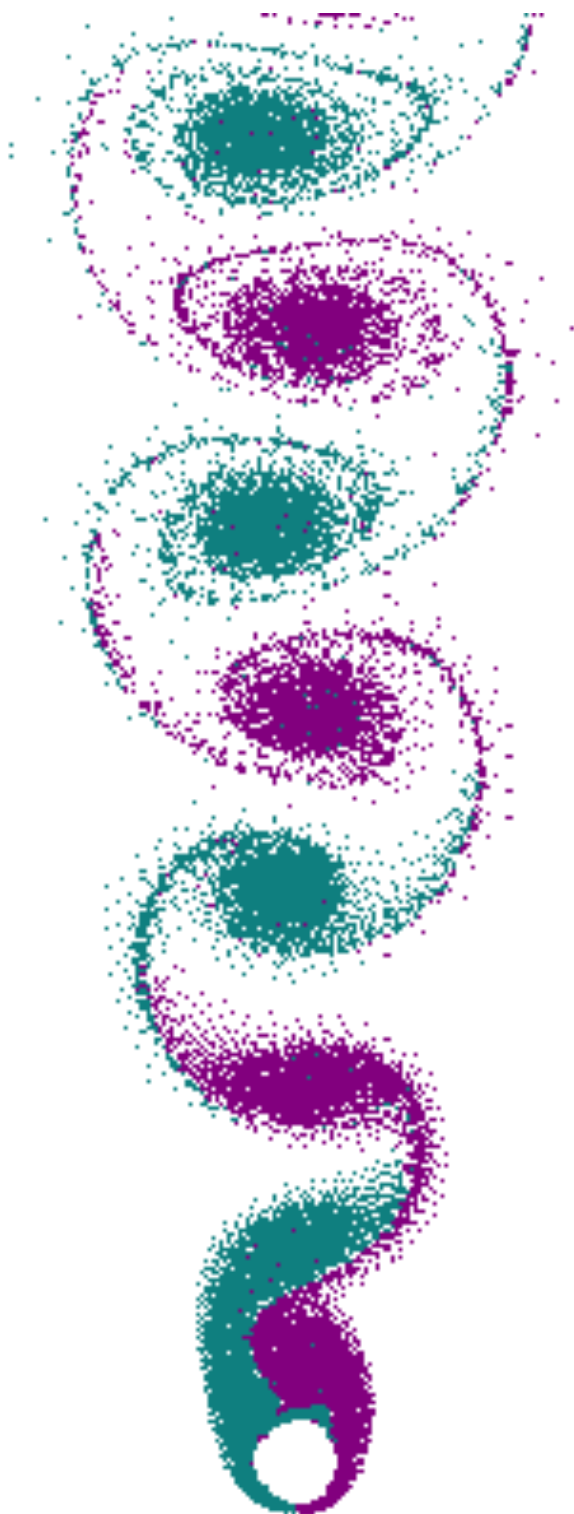
Hadronization



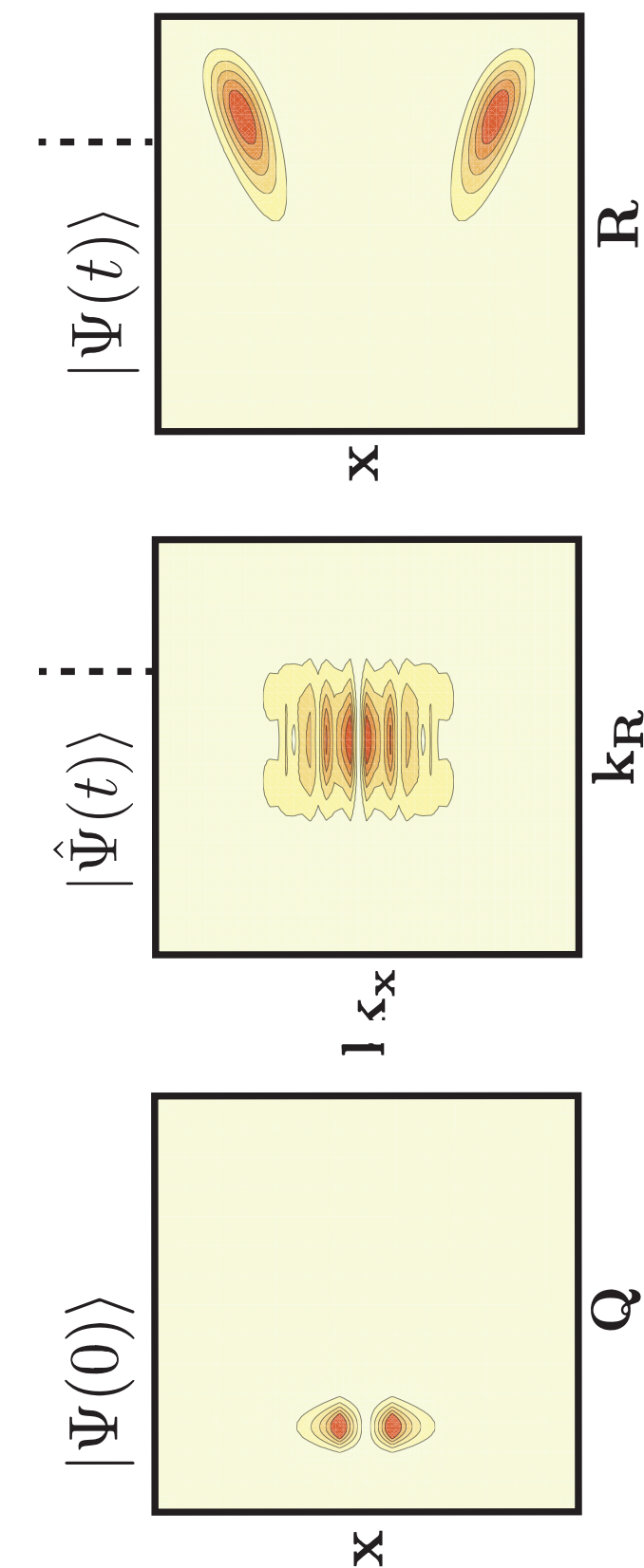
>10 GeV
 $<10^{-17}$ m

Application: Quantum simulation of the dynamics of matter

Hydrodynamics

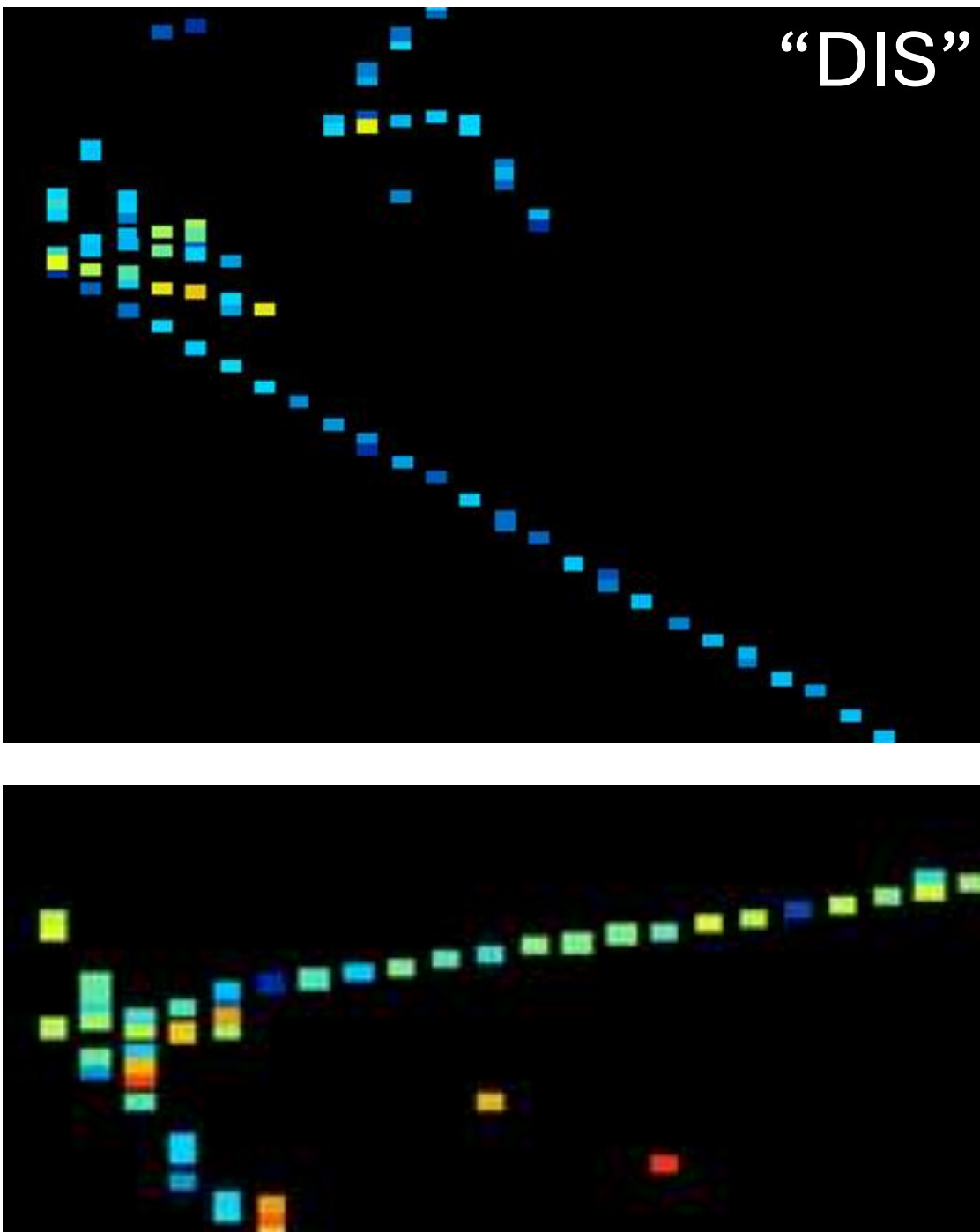


Chemical Dynamics



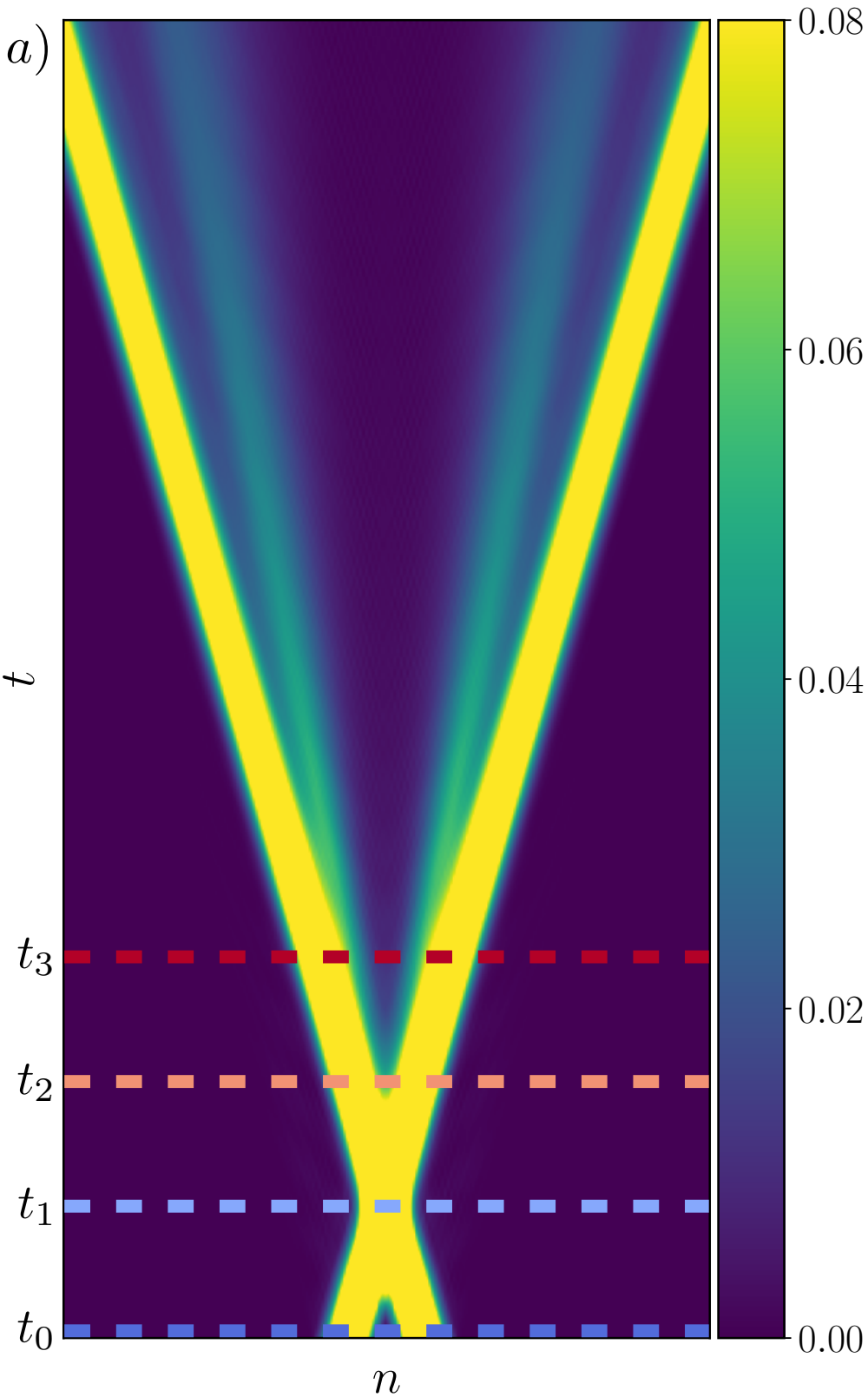
2603.19007v1

Nuclear Scattering



NOvA events

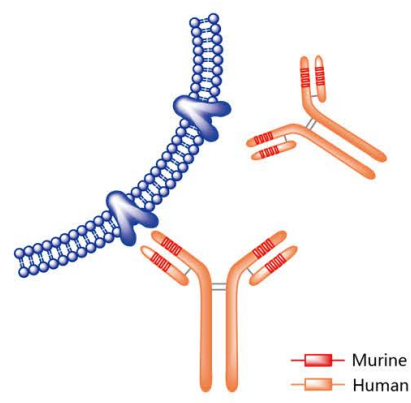
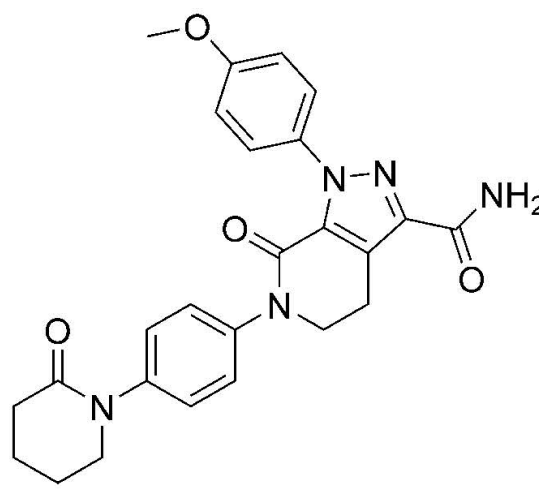
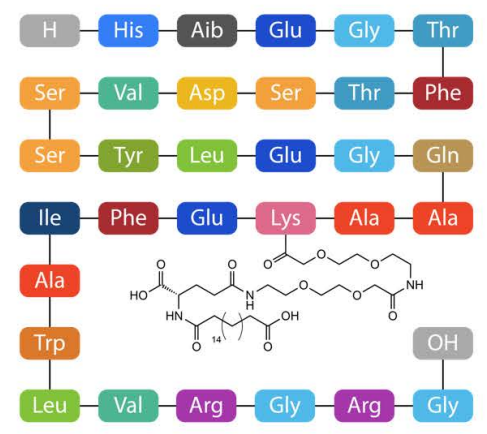
QFT Scattering



2505.03111

Quantum Advantage: do something useful with a quantum computer!

Chemistry

1 Keytruda (Pembrolizumab)	2 Eliquis (Apixaban)	3 Ozempic (Semaglutide)
		
\$25.011 Billion Oncology	\$18.953 Billion Cardiology/Vascular Diseases	\$18.468 Billion Diabetes

\$25B

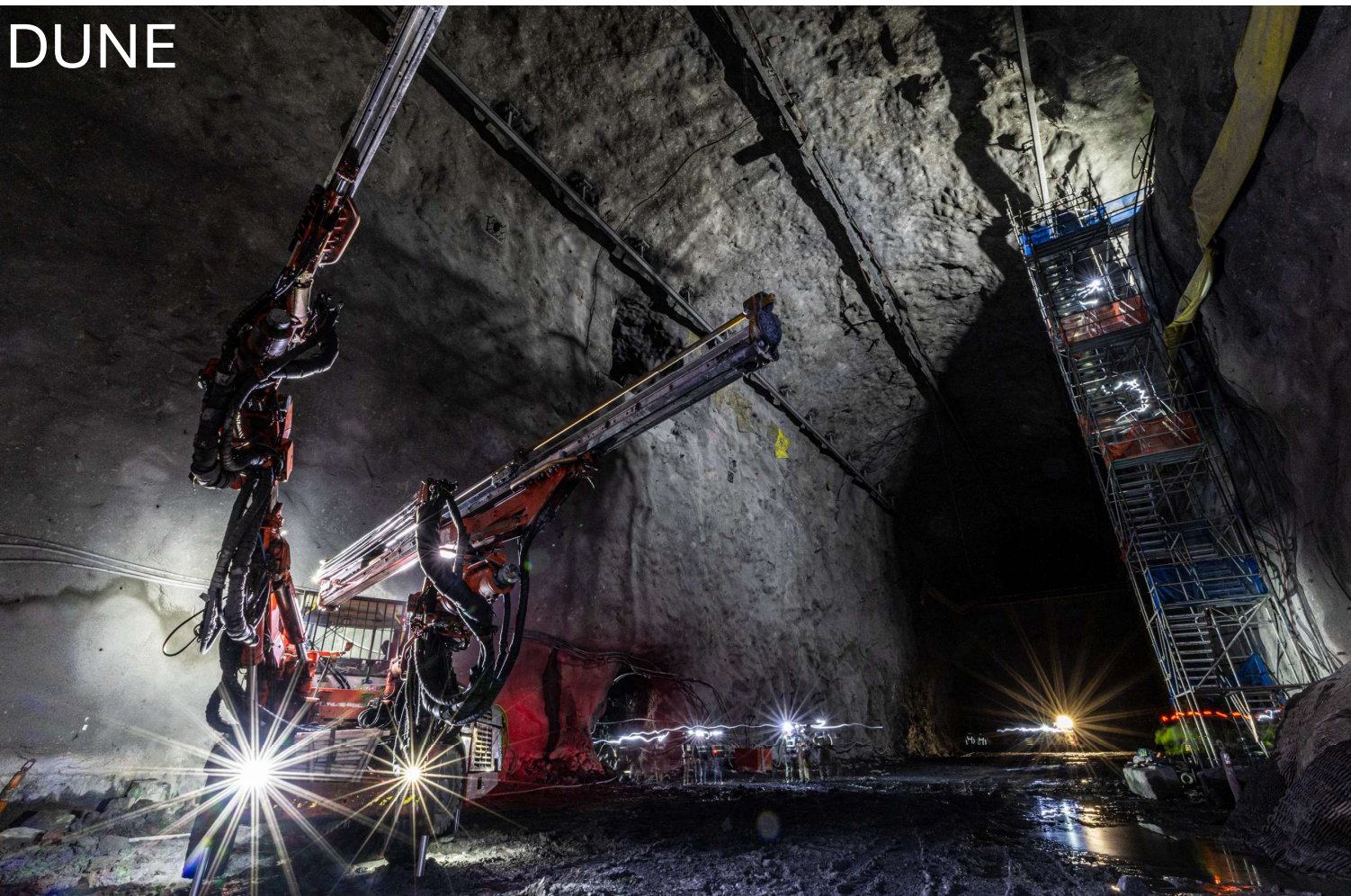
\$18B

\$18B

Top 166 molecules are all over \$1B in 2024 sales

From 2024 data compiled by <https://sites.arizona.edu/njardarson-lab/top200-posters/>

NP

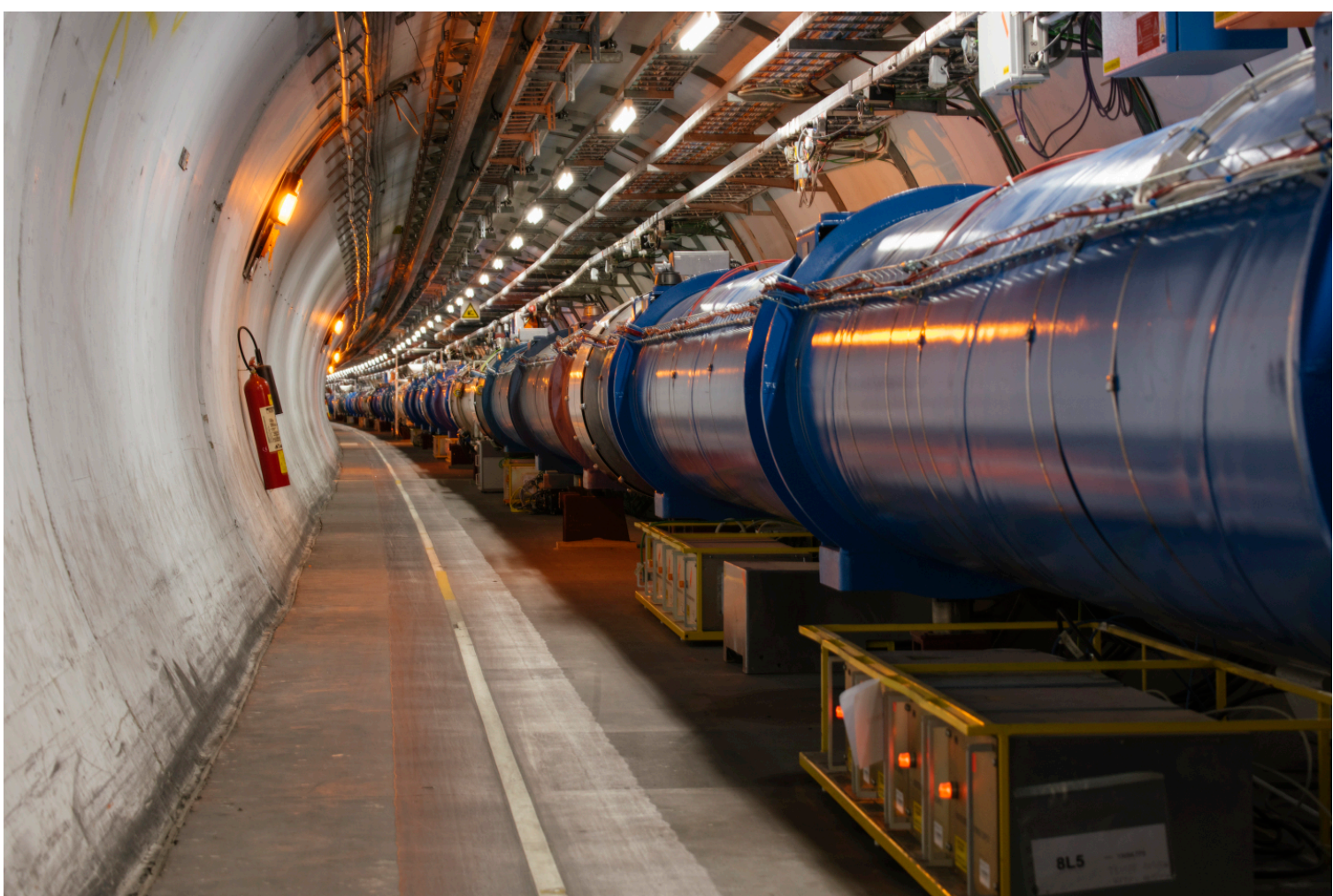


DUNE neutrino expt.

Liquid Argon detectors.

\$5B Phase I.

HEP



LHC: Construction \$5B,

Detectors \$15B

New accelerators ~\$20B