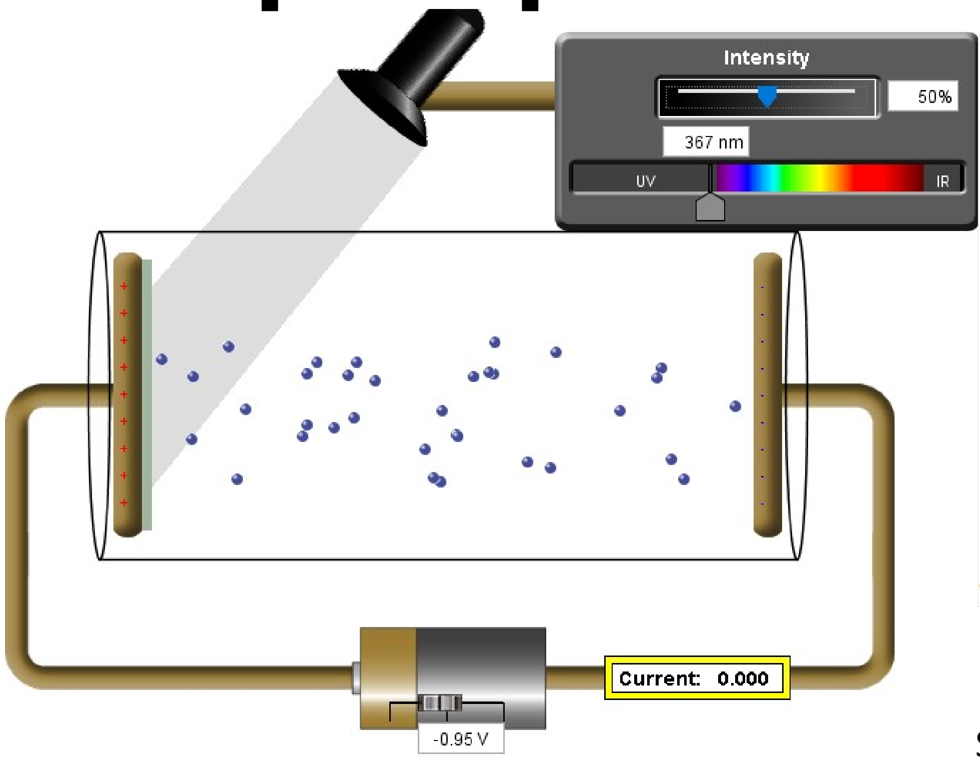
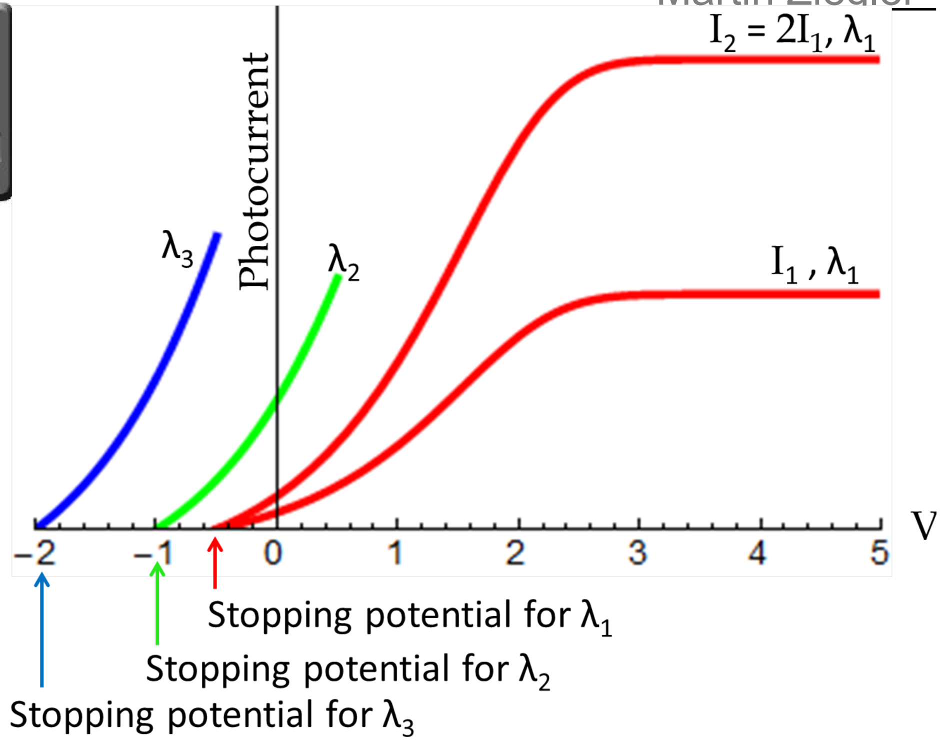
§11 Quantum Computing

- Recap: Experimental Physical Evidence
- Math Background: States and Operators
- Pure vs. Mixed States, Entanglement&EPR
- Qubits and Primitive Gates
- Quantum Circuits and Parallelism
- Quantum Phase Estimation
- Shor's Hybrid Algorithm

Recap: Experimental Physics

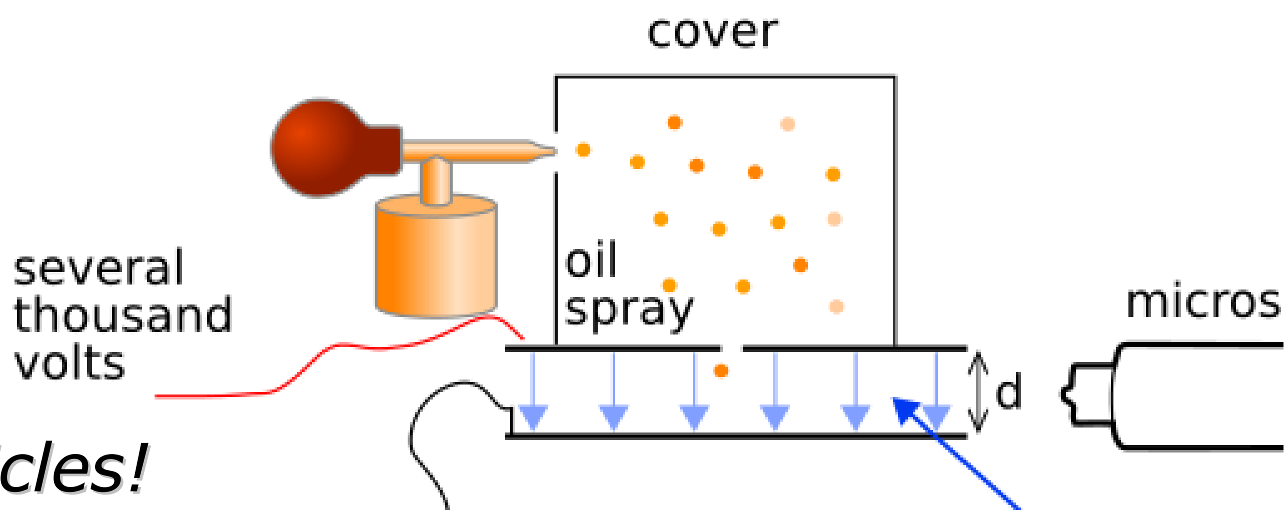




Einstein (1905):

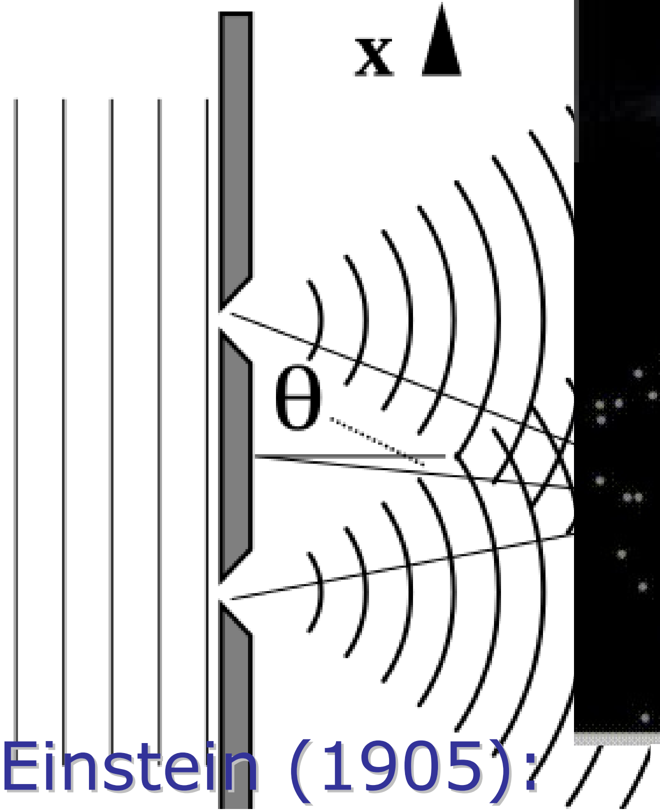
And so is *light!*

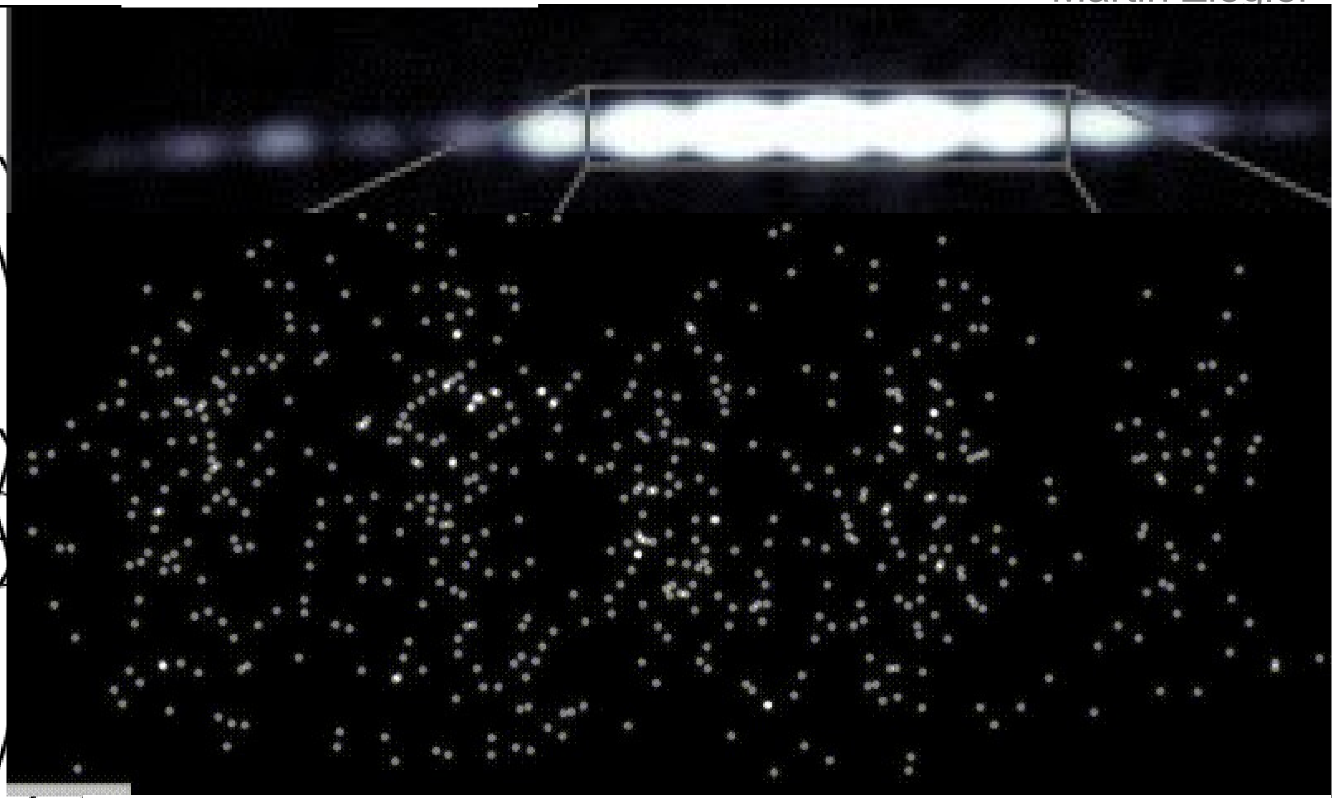
Robert Millikan "Oil drop" (1909):



Electrons are *particles!*

Recap: Experimental Physics





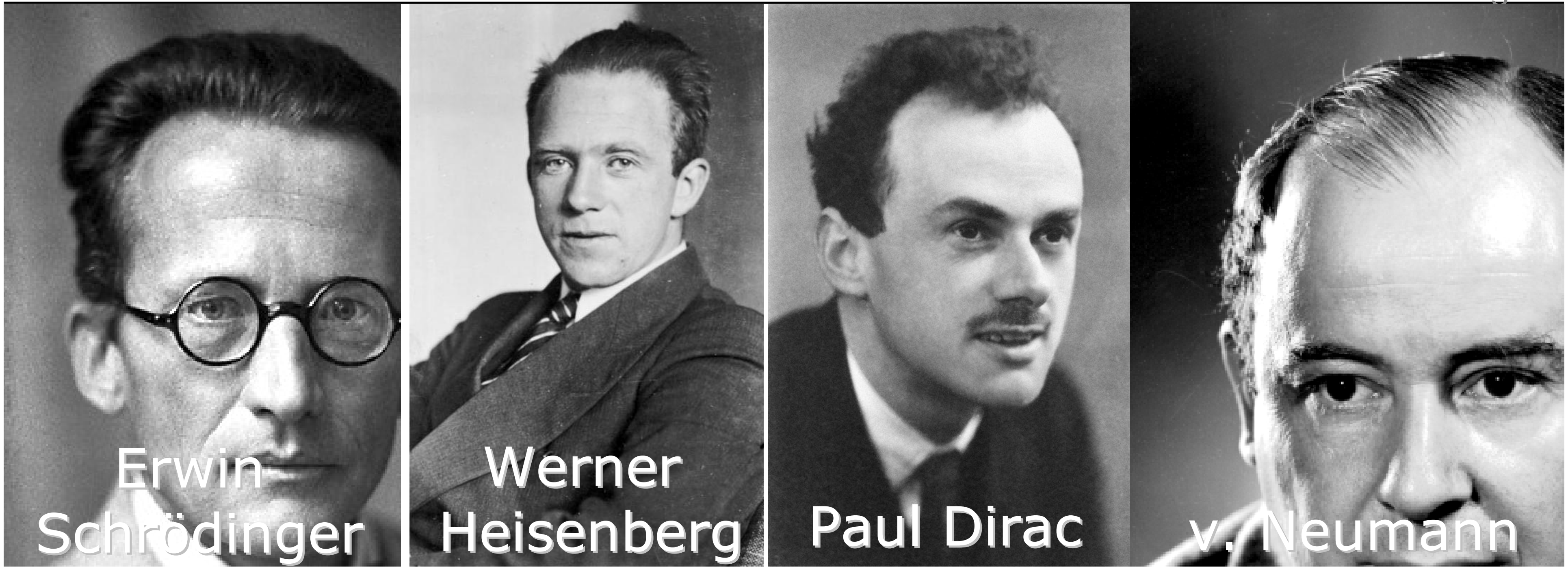
Einstein (1905):
And so is *light*!

Robert Millikan
"Oil drop" (1909):
Electrons are *particles*!

Claus Jönsson (1959):
And so are *electrons!*

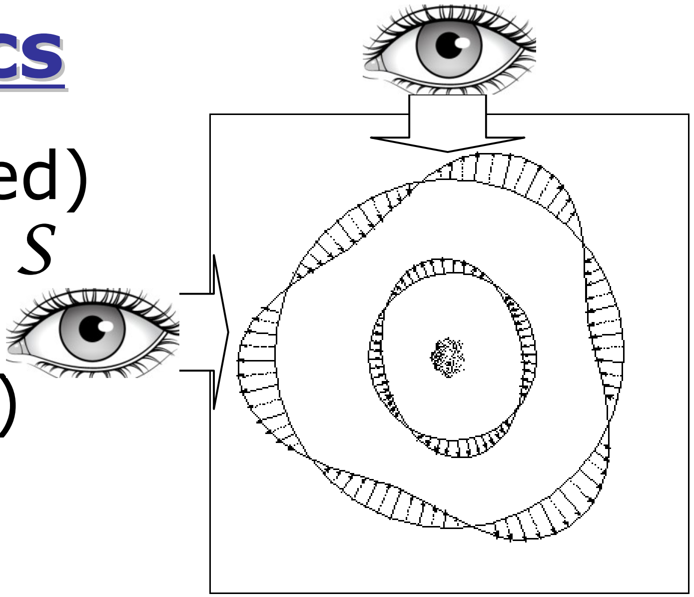
Thomas Young (1801):
Light is a *wave!*

Basic Quantum Mechanics

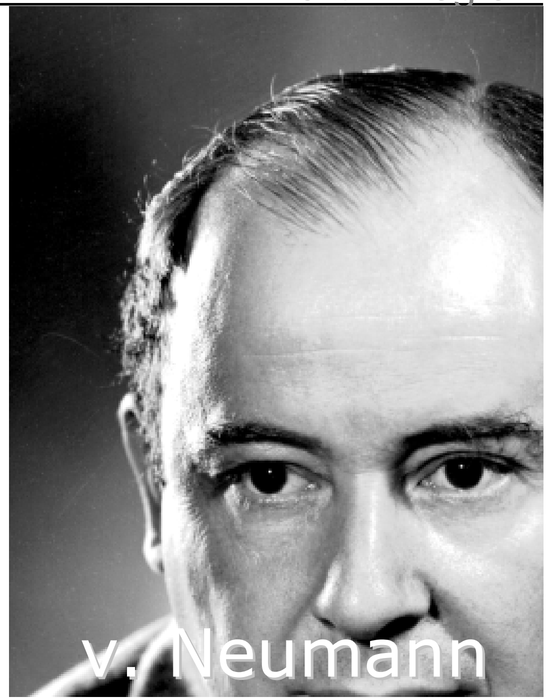


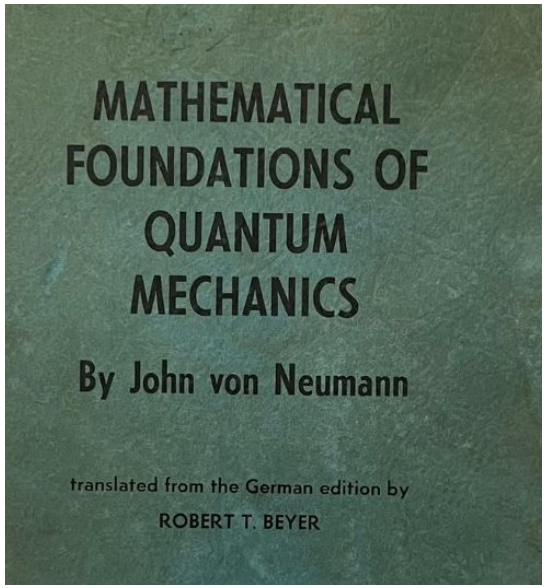
- NOT *Path Integral* (Richard Feynman)
- NOT *Quantum Field Theory* (Dyson, Feynman, Schwinger, Tomonaga)
- NOT *Relativistic* Quantum Mechanics

Math of Quantum Mechanics



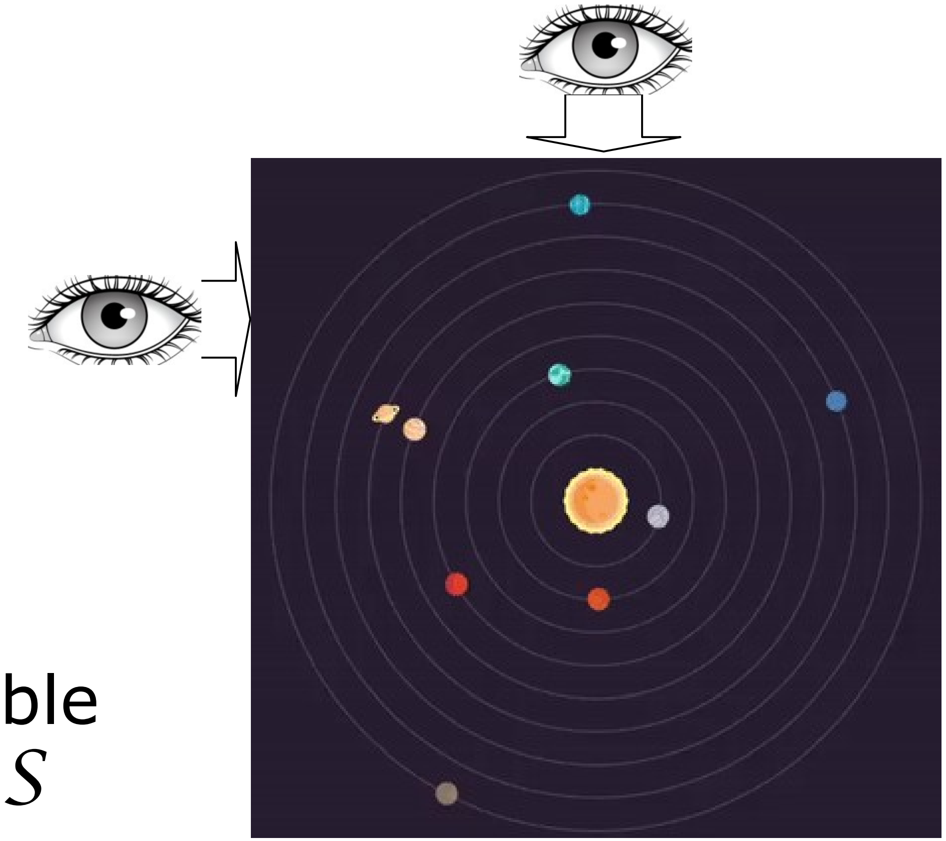
Physics	Math
I (isolated) system $\mathcal{S}$	Hilbert Space $\mathcal{H}$
II (pure) states s, s' of $\mathcal{S}$	normal vectors $\psi, \psi' \in \mathcal{H}$
III observable $\mathcal{A}$, $\mathcal{A}'$ of $\mathcal{S}$	Hermit. operator A, A' on $\mathcal{H}$
IV measurement of $\mathcal{A}$	eigenvalue a of A
V time evolution $s(0) \to s(t)$	Schrödinger Eq. $i\hbar\, \mathrm{d}/\mathrm{d}t\, \psi(t) = \boldsymbol{H}\, \psi(t)$





Math of *Newton* Mechanics

Physics	Math
I (isolated) system S	Euclid. phase space $\mathbb{R}^{6p}$
II (pure) states s, s' of S	vectors $\bar{u}, \bar{u}' \in \mathbb{R}^{6p}$
III observable $\mathcal{A}$, $\mathcal{A}'$ of S	projections $\boldsymbol{A}, \boldsymbol{A}': \mathbb{R}^{6p} \to \mathbb{R}$
IV measurement of $\mathcal{A}$	value $a = \boldsymbol{A}(\bar{u})$
V time evolution $s(0) \to s(t)$	Newton's Law/Eq. $\mathrm{d}/\mathrm{d}t\ \bar{u}(t) = \ldots$



Math of *Newton* Mechanics

Physics

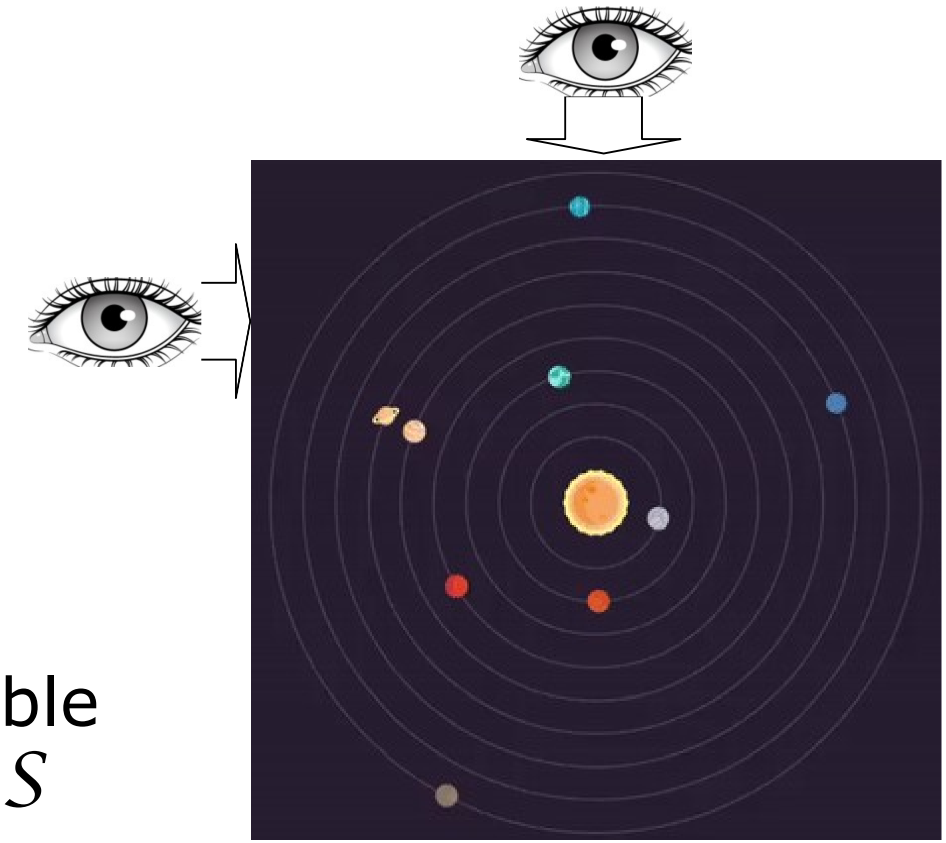
I (isolated) system S

II (pure) states s, s' of S

III observable $\mathcal{A}$, $\mathcal{A}'$ of S

IV measurement of $\mathcal{A}$

V time evolution $s(0) \to s(t)$



Math

Euclid. phase space $\mathbb{R}^{6p}$

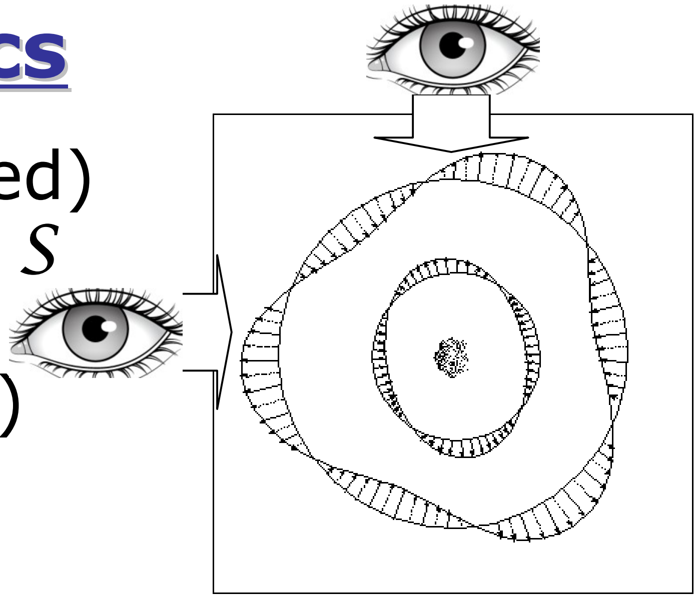
vectors $\bar{u}, \bar{u}' \in \mathbb{R}^{6p}$

projections $\boldsymbol{A}, \boldsymbol{A}': \mathbb{R}^{6p} \to \mathbb{R}$

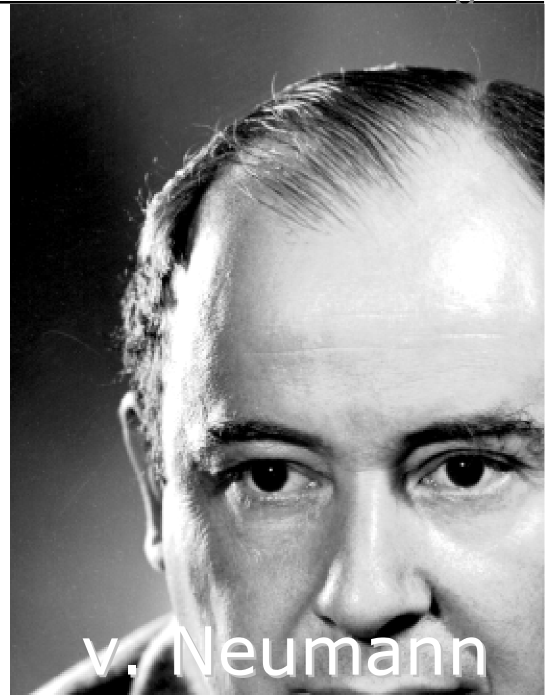
value $a = \boldsymbol{A}(\bar{u})$

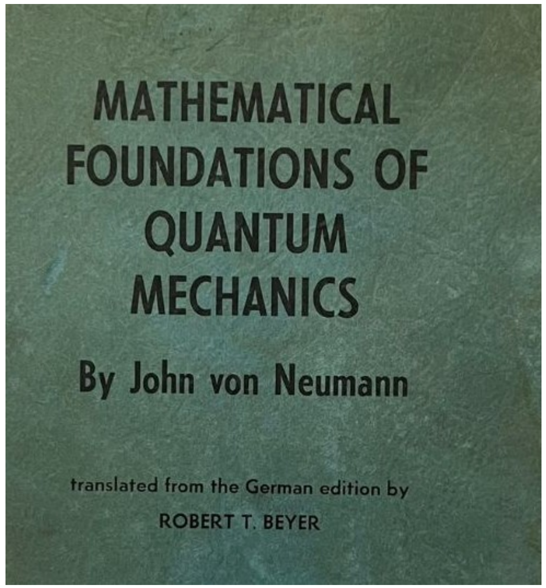
Newton's Law/Eq. $\mathrm{d}/\mathrm{d}t\ \bar{u}(t) = \ldots$

Math of Quantum Mechanics



Physics	**Math**
I (isolated) system $\mathcal{S}$	Hilbert Space $\mathcal{H}$
II (pure) states s,s' of $\mathcal{S}$	normal vectors $\psi,\psi'\in\mathcal{H}$
III observable $\mathcal{A}\,,\,\mathcal{A}'$ of $\mathcal{S}$	Hermit. operator $\boldsymbol{A},\boldsymbol{A}'$ on $\mathcal{H}$
IV measurement of $\mathcal{A}$	eigenvalue a of $\boldsymbol{A}$
V time evolution $s(0)\ \to\ s(t)$	Schrödinger Eq. $i\hbar\ \mathrm{d}/\mathrm{d}t\ \psi(t) = \boldsymbol{H}\ \psi(t)$





Axioms of Quantum Mechanics

Ia. To any (isolated) physical system S corresponds a complex Hilbert space $\mathcal{H}$ called the *state space*.

Ib. The state space of a system S composed from (connected) sub-systems S_j is the *tensor product* $\mathcal{H} = \otimes_j \mathcal{H}_j$ of the state spaces associated with components S_j

IIa. A *pure* state $s=s(t)$ of S at time t corresponds to a *unit* (=norm**1**) vector $\psi = \psi(t) \in \mathcal{H}$.

IIb. A statistical *ensemble* (=mix) of pure states/ vectors s_k/ψ_k with weights $w_k \in [0;1]$ corresponds to a *density* (=pos.semid. trace**1**) *operator* $\rho = \sum_k w_k \cdot |\psi_k\rangle\langle\psi_k|$

Axioms of Quantum Mechanics

III. Any physical observable $\mathcal{A}$ on $\mathcal{S}$ corresponds to a Hermitian operator $\boldsymbol{A}$ on $\mathcal{H}$.

IVa. When $\mathcal{S}$ is in *pure* state ψ, measuring $\mathcal{A}$ produces eigenvalue a of $\boldsymbol{A}$ with **probability** $\boxed{|\langle\psi_a|\psi\rangle|^2}$, where ψ_a is any unit eigenvector of $\boldsymbol{A}$ to eigenvalue a.

IVa'. After this measurement, $\mathcal{S}$ will be in state $\psi'=\psi_a$

IVb When $\mathcal{S}$ is in *mixed* state with density $\boldsymbol{\rho}$, measuring $\mathcal{A}$ produces eigenvalue a with **probability** $\langle\psi_a|\, \boldsymbol{\rho}\, \psi_a\rangle$.

IVb'. After this measurement,
$\mathcal{S}$ will be in a state with density $\boldsymbol{\rho}' = |\psi_a\rangle\langle\psi_a|\, \boldsymbol{\rho}\, \psi_a\rangle\langle\psi_a|$

Density (=pos.semid. trace**1**) *operator* $\rho = \sum_k w_k \cdot |\psi_k\rangle\langle\psi_k|$

Axioms of Quantum Mechanics

III. A physical observable $\mathcal{A}$ on $\mathcal{S}$ corresponds to a Hermitian operator $\boldsymbol{A}$ on $\mathcal{H}$.

IVa. When $\mathcal{S}$ is in *pure* state ψ, measuring $\mathcal{A}$ produces eigenvalue a of $\boldsymbol{A}$ with **probability** $|\langle\psi_a|\psi\rangle|^2$,
where ψ_a is any unit eigenvector of $\boldsymbol{A}$ to eigenvalue a.

IVa'. After this measurement, $\mathcal{S}$ will be in state $\psi'=\psi_a$

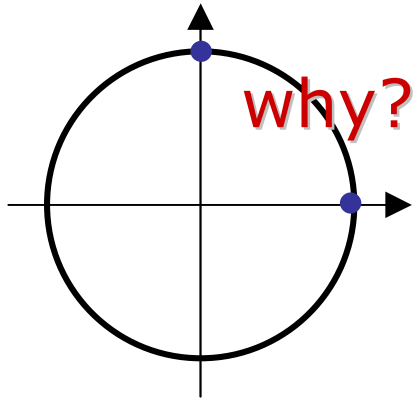
IIa. A *pure* state $s=s(t)$ of $\mathcal{S}$ at time t corresponds to a *unit* (=norm**1**) vector $\psi = \psi(t) \in \mathcal{H}$.

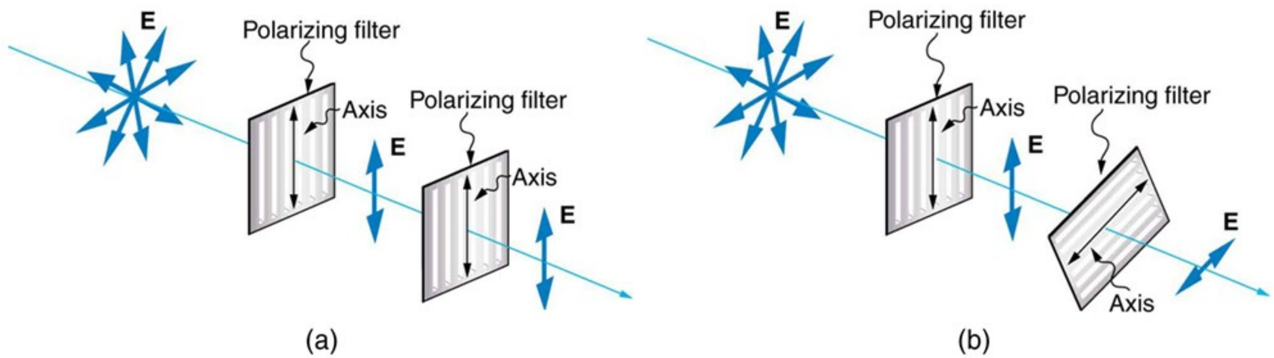
$\boldsymbol{H}$ Hamilton operator from observable "*energy*" (**III**)

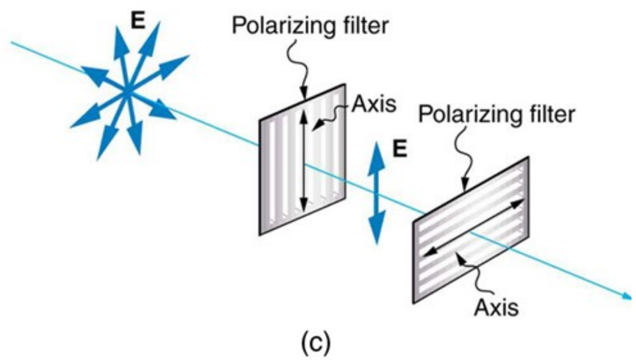
V. The time evolution of a *pure* state $\psi(0) \to \psi(t) \in \mathcal{H}$
is $\psi(t)= \boldsymbol{U}(t)\, \psi(0)$, $\boldsymbol{U}(t)= e^{-i\int \boldsymbol{H}(t)\mathrm{d}t/\hbar}$ unitary

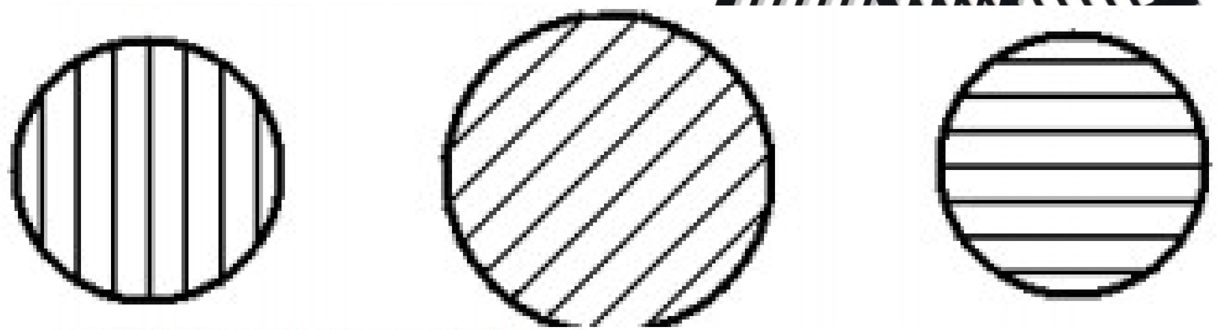
Illustration/Justification

Example *Polarized light*: $\mathcal{H}=\mathbb{C}^2$ (qubit)







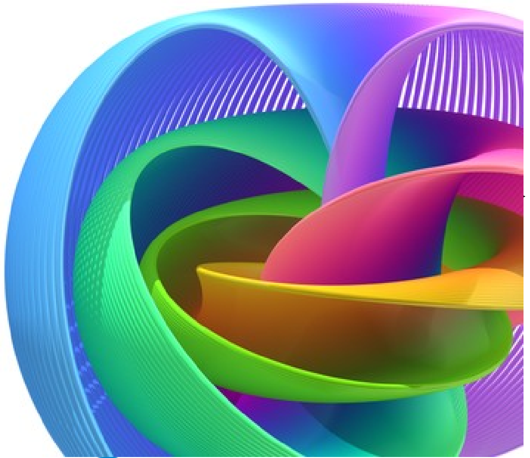


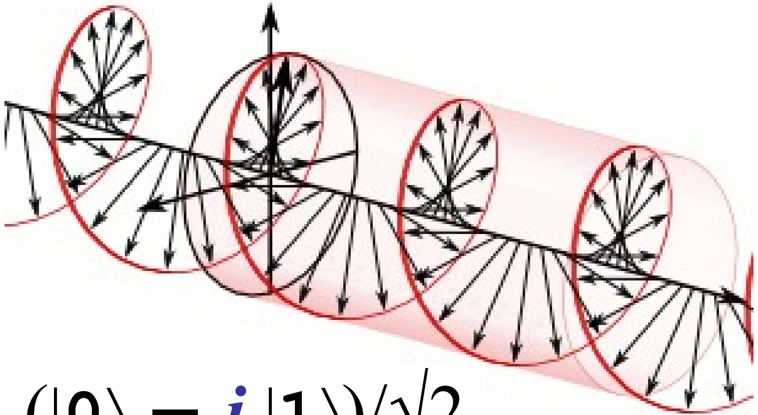
(d)

Ia. To any (isolated) physical system S corresponds a complex Hilbert space $\mathcal{H}$ called the *state space*.

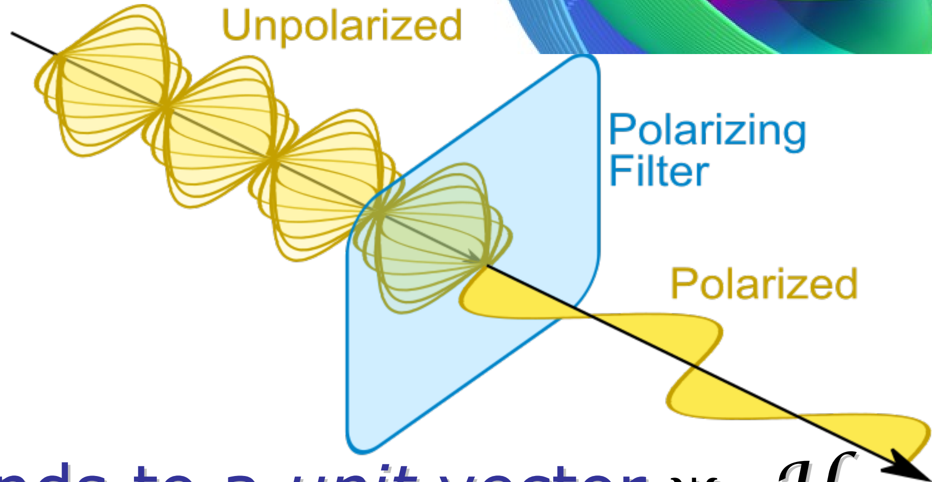
Pure vs. Mixed States

Example *Polarized light*: $\mathcal{H}=\mathbb{C}^2$ (qubit ortho-basis $(0,1) =: |\mathbf{0}\rangle$ and $(1,0) =: |\mathbf{1}\rangle$





$(|\mathbf{0}\rangle - \boldsymbol{i}\,|\mathbf{1}\rangle)/\sqrt{2}$



IIa. A *pure* state corresponds to a *unit* vector $\psi\in\mathcal{H}$.

IIb. A statistical *ensemble* (=mix) of pure states/ vectors s_k/ψ_k with weights $w_k\in[0;1]$ corresponds to a *density* (=pos.semid. trace**1**) *operator* $\rho = \sum_k w_k\cdot|\psi_k\rangle\langle\psi_k|$

Qubit Register

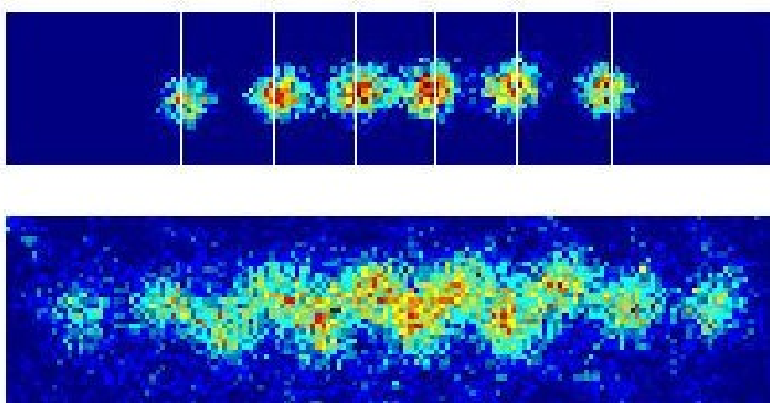
b) Particle spin: $\mathcal{H}=\mathbb{C}^2$ (qubit),

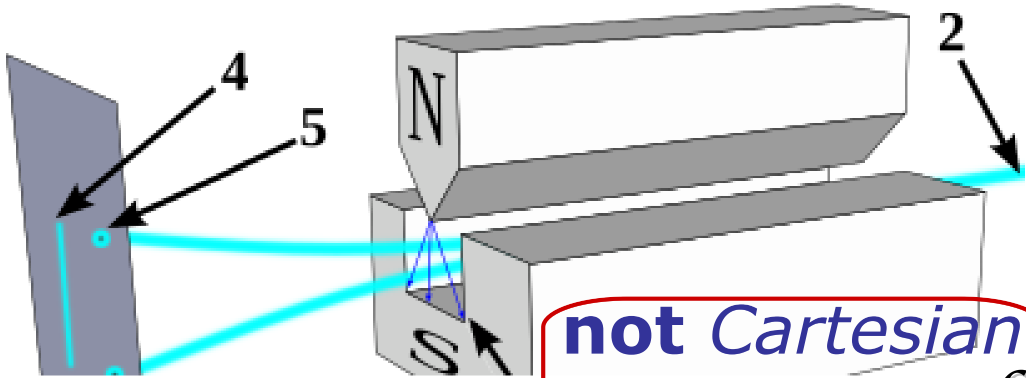
entanglement

ortho-basis $(0,1) =: |\mathtt{0}\rangle$ and $(1,0) =: |\mathtt{1}\rangle$

c) $\otimes^n \mathbb{C}^2$ (n qubit**s**) has complex dimension 2^n

with ortho-basis $|\mathtt{0...0}\rangle$ ... $|\mathtt{1...1}\rangle$





not *Cartesian* product $\prod_j \mathcal{H}_j$

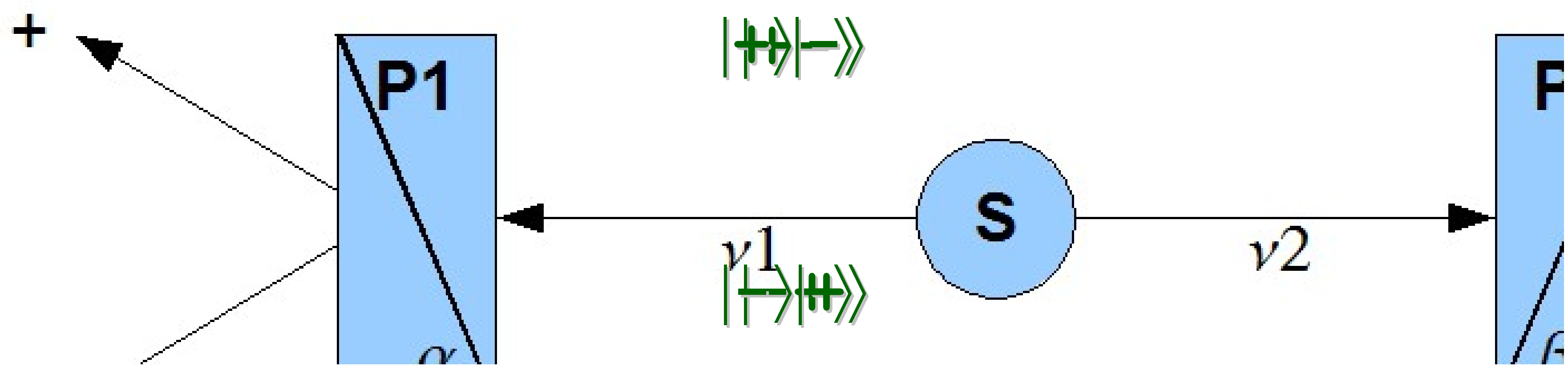
Ib. The state space of a system S composed from (connected) sub-systems S_j is the *tensor product* $\mathcal{H} = \otimes_j \mathcal{H}_j$ of the state spaces associated with components S_j

Entanglement & *EPR*

Einstein Podolski Rosen'35

d) Two particles: $\mathcal{H}=\mathbb{C}^4$ (double qubit)

ortho-basis $|{+}{+}\rangle$, $|{+}{-}\rangle$, $|{-}{+}\rangle$, $|{-}{-}\rangle$



IVa. When S is in *pure* state ψ, measuring $\mathcal{A}$ produces eigenvalue a of A with **probability** $|\langle\psi_a|\psi\rangle|^2$, where ψ_a is any unit eigenvector of A to eigenvalue a.

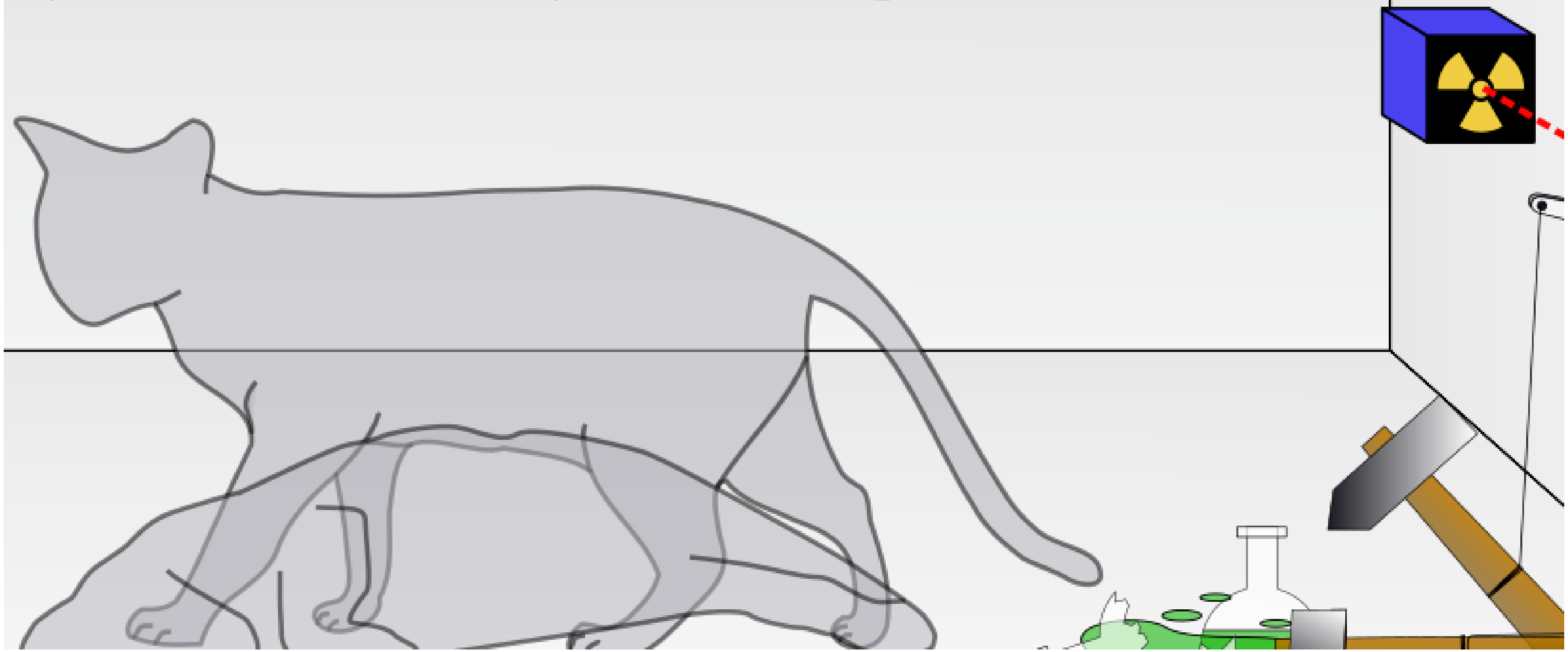
IVa'. After this measurement, S will be in state $\psi'=\psi_a$

Schrödinger's Cat

e) Two *macroscopic* objects? $\mathcal{H}=\mathbb{C}^4$ (double qubit)

ortho-basis $(|\texttt{alive}\rangle , |\texttt{dead}\rangle) \times (|\texttt{decay}\rangle , |\texttt{stable}\rangle)$

$(|\texttt{alive}, \texttt{stable}\rangle + |\texttt{dead}, \texttt{decay}\rangle) /\sqrt{2}$



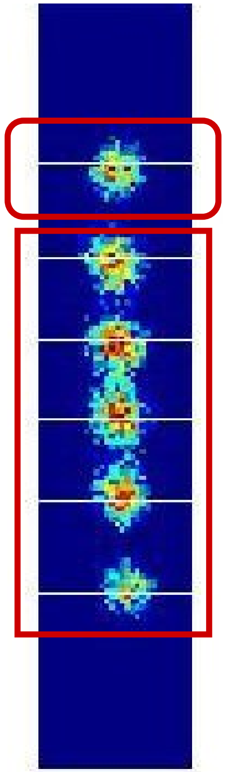
IVa'. After this measurement, S will be in state $\psi'=\psi_a$

Quantum *Gates*: on 1 qubit

a/b) One qubit state space $\mathcal{H}=\mathbb{C}^2$

basis $(0,1) =: |0\rangle$ and $(1,0) =: |1\rangle$

phase $P_\varphi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$



Pauli-X (="*NOT*") $U_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $|0\rangle \to |1\rangle$, $|1\rangle \to |0\rangle$

Pauli-Y $U_Y = \begin{pmatrix} 0 & -i \\ +i & 0 \end{pmatrix}$ $|0\rangle \to -i\,|1\rangle$, $|1\rangle \to +i\,|0\rangle$

Pauli-Z $P_\pi = U_Z = \begin{pmatrix} +1 & 0 \\ 0 & -1 \end{pmatrix}$ $|0\rangle \to +\,|0\rangle$, $|1\rangle \to -\,|1\rangle$

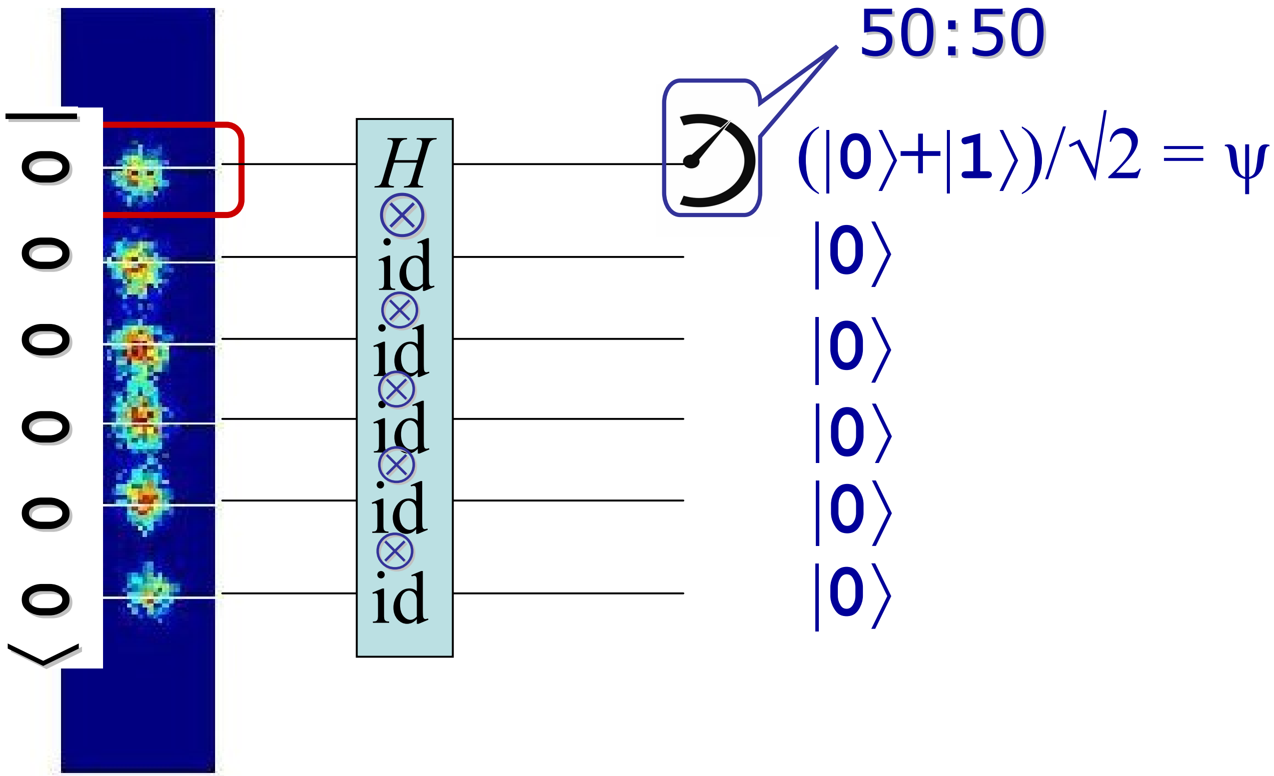
$\otimes\,\mathrm{id} \otimes \ldots \otimes \mathrm{id}$ $(n\text{-}1)$–fold

Quantum gates are *unitary* $\Rightarrow$ ***reversible!***

***Hadamard* Gate:** on 1 qubit

a/b) One qubit state space $\mathbb{C}^2$
with ortho-basis $|0\rangle$, $|1\rangle$

$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} / \sqrt{2}$$



$a = 0 \,/\, 1$

$\psi_0 = |0\rangle$

$\psi_1 = |1\rangle$

$|0\rangle \rightarrow (|0\rangle+|1\rangle)/\sqrt{2}$

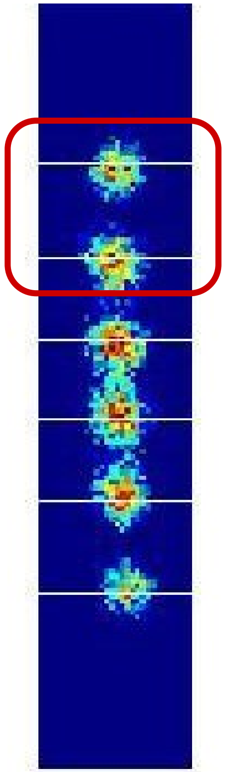
$|1\rangle \rightarrow (|0\rangle-|1\rangle)/\sqrt{2}$

IVa. When in *pure* state ψ, measuring produces eigenvalue a with **probability** $|\langle\psi_a|\psi\rangle|^2$, ψ_a eigenvector

Quantum *Gates*: on 2 qubits

d) Two qubits state space $\mathcal{H}=\mathbb{C}^4$

with ortho-basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$



CNOT

$$\begin{array}{|c|c|c|c|}\hline 1 & & & \\ \hline & 1 & & \\ \hline & & & 1 \\ \hline & & 1 & \\ \hline \end{array}$$

$$|00\rangle \to |00\rangle$$
$$|01\rangle \to |01\rangle$$
$$|10\rangle \to |11\rangle$$
$$|11\rangle \to |10\rangle$$

SWAP

$$\begin{array}{|c|c|c|c|}\hline 1 & & & \\ \hline & & 1 & \\ \hline & 1 & & \\ \hline & & & 1 \\ \hline \end{array}$$

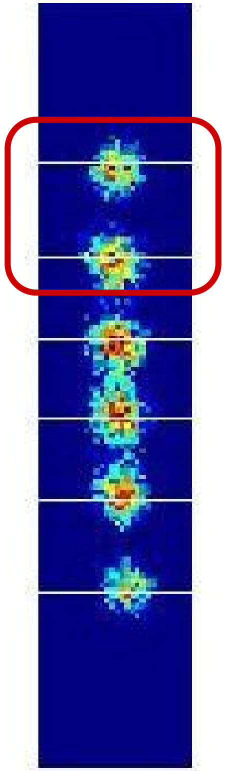
$$|00\rangle \to |00\rangle$$
$$|01\rangle \to |10\rangle$$
$$|10\rangle \to |01\rangle$$
$$|11\rangle \to |11\rangle$$

Quantum gates are *unitary*

Hadamard on 2 and on *n* qubits

c) $\mathcal{H}=\otimes^n \mathbb{C}^2$ (n qubit**s**) has complex dimension $N=2^n$

with ortho-basis $|$**0...0**$\rangle$ … $|$**1...1**$\rangle$



$H \otimes H \otimes H \otimes H \otimes H \otimes H$

concurrent→

$H=$

1	1
1	-1

$/\sqrt{2}$

$H \otimes H =$

1	1	1	1
1	-1	1	-1
1	1	-1	-1
1	-1	-1	+1

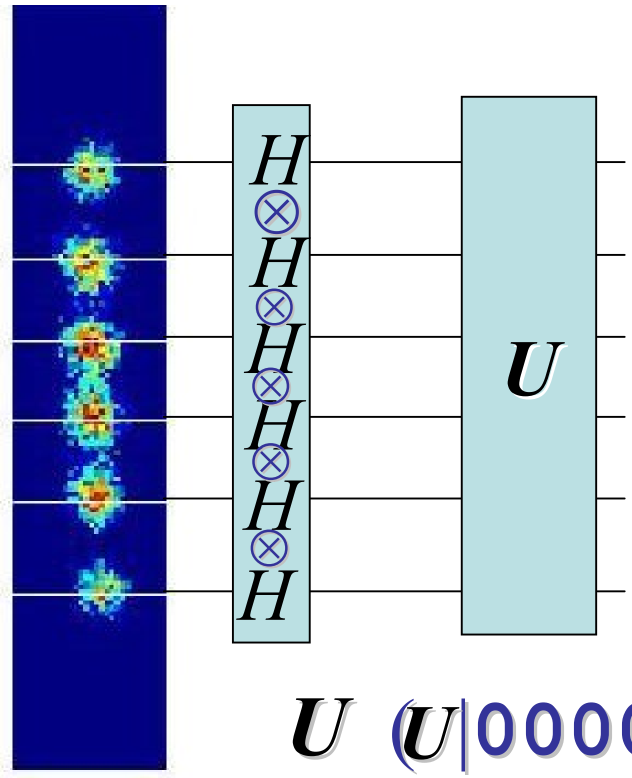
$/2$

$|0...0\rangle \to \sum_{0\leq J<2^n} |\,\mathrm{bin}(J)\,\rangle \;/\; 2^{n/2}$

Quantum *Parallelism*

c) $\mathcal{H}=\otimes^n\,\mathbb{C}^2$ (n qubit**s**) has complex dimension $\boldsymbol{N=2^n}$

with ortho-basis $|0\ldots0\rangle$ … $|1\ldots1\rangle$



sequential→

quantum parallelism (N-fold!)

concurrent→ (n-fold)

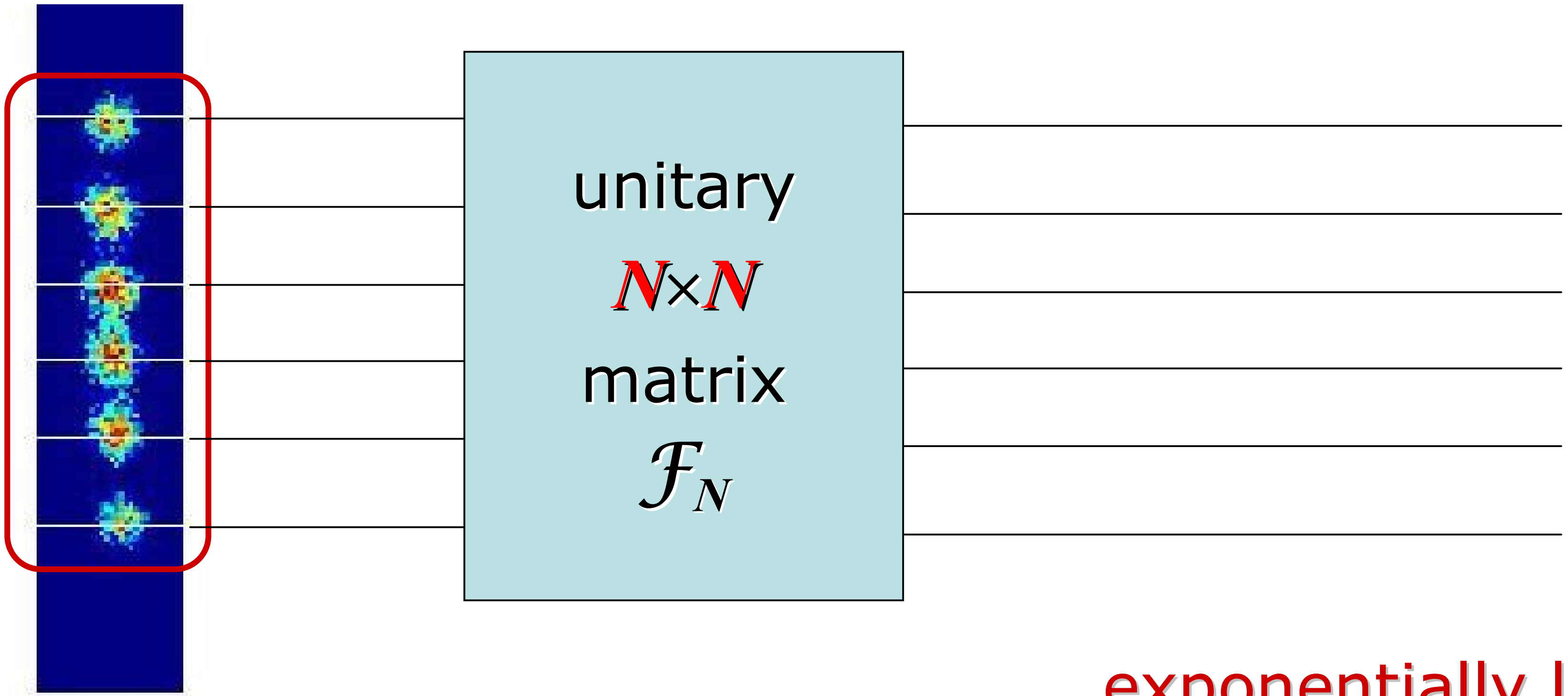
e.g. $n=4$: $\boldsymbol{U}\;(\boldsymbol{U}|0000\rangle+\boldsymbol{U}|0001\rangle+\boldsymbol{U}|0010\rangle+\boldsymbol{U}|0011\rangle+\ldots$
$+\boldsymbol{U}|1100\rangle+\boldsymbol{U}|1101\rangle+\boldsymbol{U}|1110\rangle+\boldsymbol{U}|1111\rangle)\;/4$

$\sum_{0\leq J<2^n} \boldsymbol{U}\;|\,\mathrm{bin}(J)\,\rangle\;/\;2^{n/2}$

Quantum Fourier Transform

c) $\mathcal{H}=\otimes^n\,\mathbb{C}^2$ (n qubit**s**) has complex dimension $N=2^n$

$\mathcal{F}_N$: $|\mathrm{bin}(K)\rangle \to \boxed{\sum_{0\leq J<N}} \exp(2\pi i JK/N)\,|\mathrm{bin}(J)\rangle\,/\sqrt{N}, \qquad 0\leq K<N$



exponentially large

quantum circuit

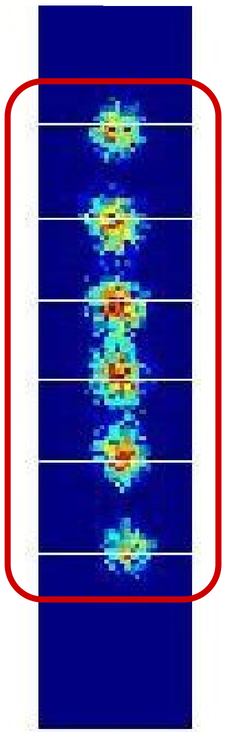
Quantum gates are *unitary*

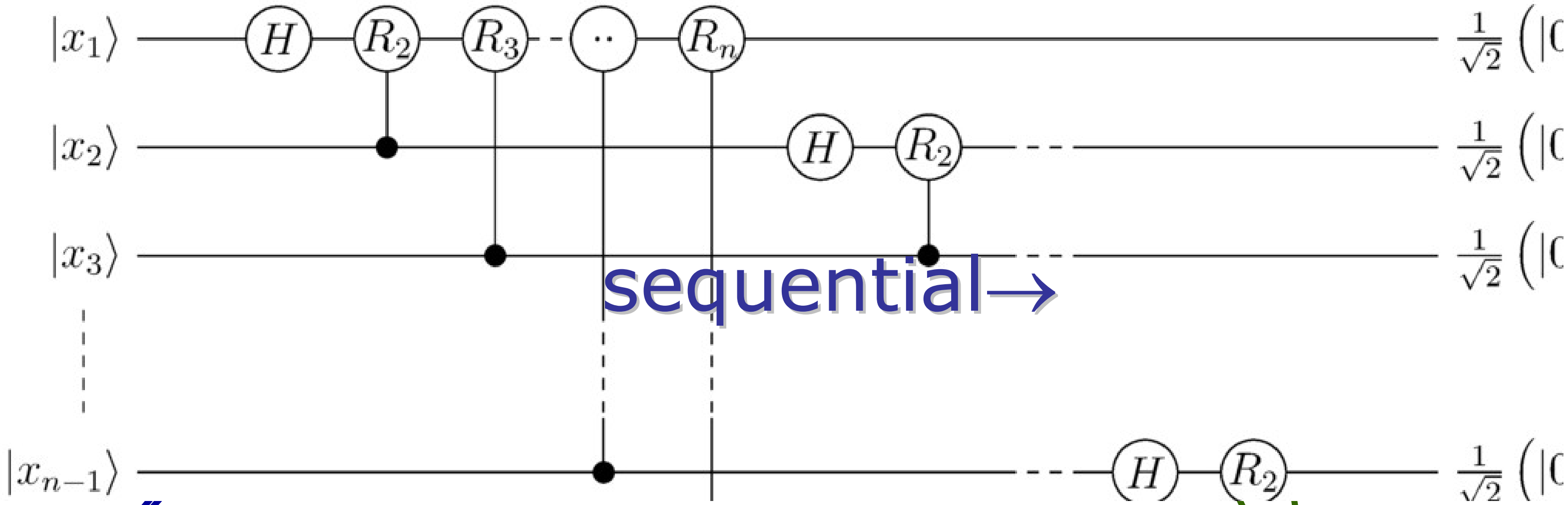
Fast **Quantum Fourier Trafo**

c) $\mathcal{H}=\otimes^n \mathbb{C}^2$ (n qubit**s**) has complex dimension $N=2^n$

$$\mathcal{F}_N\text{:}\ \ |x_1x_2\ldots x_n\rangle \to \big(\,|0\rangle+\exp(2\pi i\,\boxed{[0.x_n]})\,|1\rangle\,\big)\otimes\ldots$$

$$\ldots\otimes\boxed{\big(\,|0\rangle+\exp(2\pi i\,[0.x_1\ldots x_n])\,|1\rangle\,\big)}\,/\sqrt{N}$$





sequential→

$[0.x_1\ldots x_m] := x_1/2 + x_2/4 + \ldots$

tensor factorization

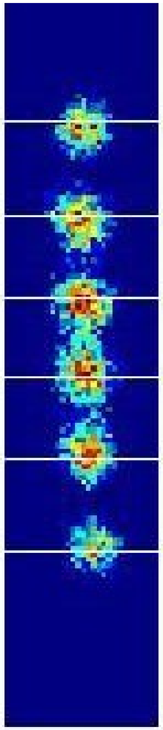
controlled
phase $R_k=$

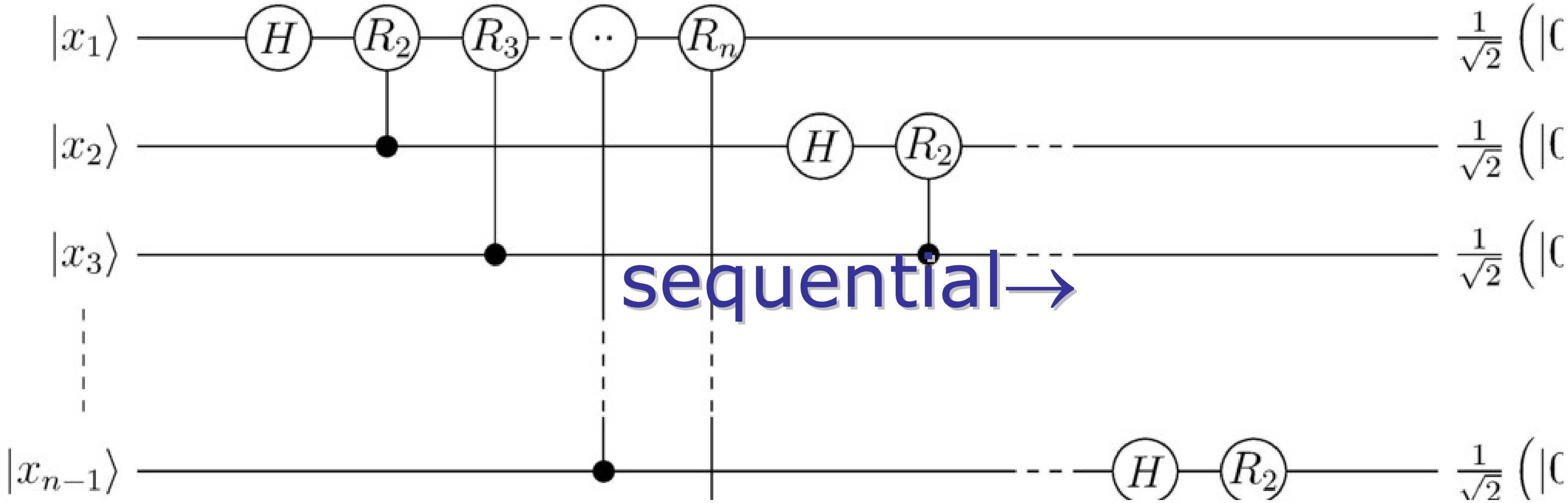
$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & e^{2\pi i 2^{-k}} \end{pmatrix}$$

Quantum Fourier *Circuit*

c) $\mathcal{H}=\otimes^n\,\mathbb{C}^2$ (n qubit**s**) has complex dimension $N=2^n$

$\mathcal{F}_N$: $|\mathrm{bin}(K)\rangle \to \sum_{0\le J<N} \exp(2\pi i JK/N)\,|\mathrm{bin}(J)\rangle/\sqrt{N}, \quad 0\le K<N$





sequential→

polynomial

size = $O(n^2)$

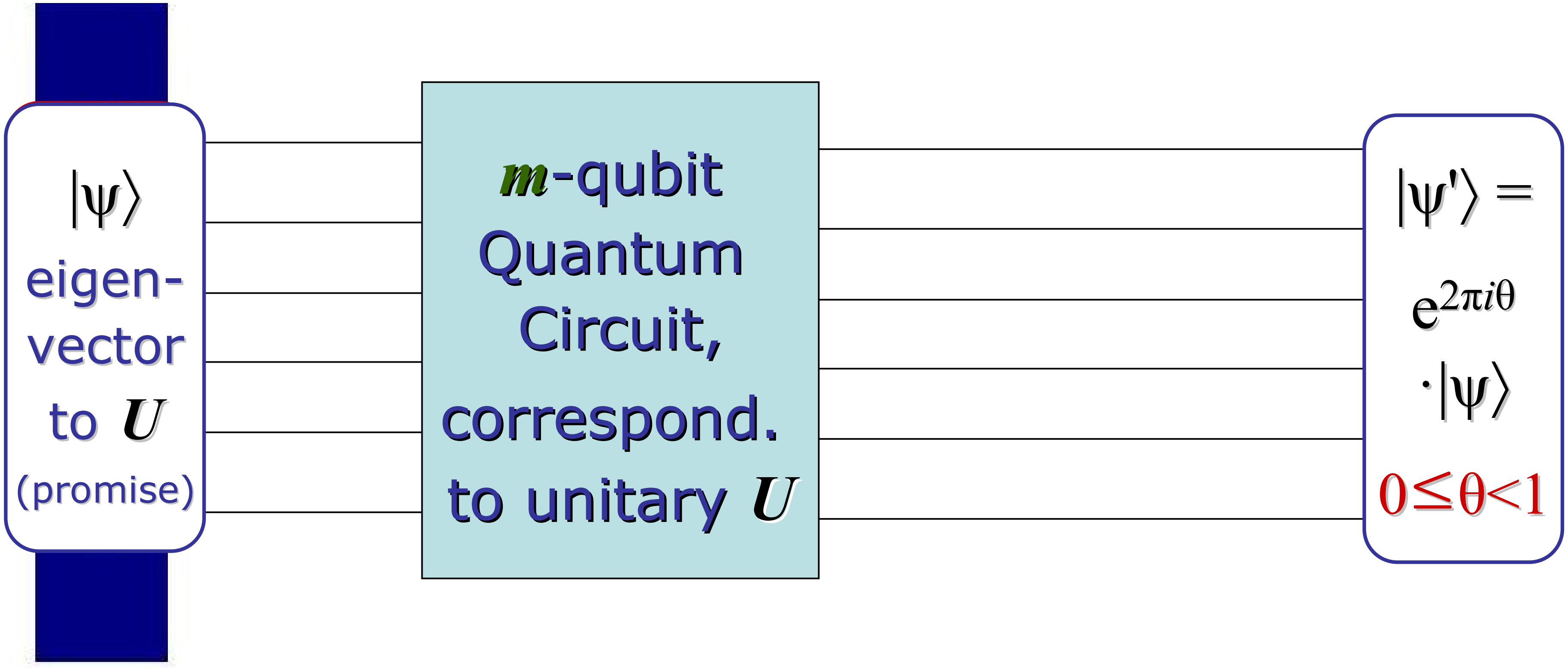
depth = $O(n)$

$\otimes$ (parallel) of unitary is unitary

$\circ$ (sequential) of unitary is unitary

Quantum *Phase Estimation* Problem

Goal: approximate θ **!**



Quantum circuits are *unitary*

Peter Shor's *Hybrid* Algorithm

Input: Composite $X \in \mathbb{N}$.

Output: some nontrivial factor F of X.

W.l.o.g: X odd, and not a prime power.

(*) *classical* random analysis/ Number Theory

1. Pick a random number A.
2. Use Euclid to calculate $F := \gcd(X, A)$
3. If $F \neq 1$, then F is a nontrivial factor of X: done!
4. Otherwise, use the **quantum subroutine** to find the $\boxed{\text{multiplicative order } R \text{ of } A \bmod X}$.
5. If R is odd, then go back to step 1. (*)
6. Calculate $F := \gcd(X, A^{R/2}+1)$. If $F \neq 1$, done!
7. Otherwise, go back to step 1. (*)

$R = \min\{\, K : A^K \equiv 1 \bmod X \,\}$

Modular Order and Phase Estimation

$M=2^m$

Def: $U\,|\mathrm{bin}(L)\rangle := |\mathrm{bin}(L\cdot A \bmod X)\rangle$ for $0\le L<X$

$U\,|\mathrm{bin}(L)\rangle := |\mathrm{bin}(L)\rangle$ for $X\le L<M$

where X denotes the m-bit integer to be factored and $1<A<X$ is an integer parameter coprime to X.

- U is *unitary*
- eigen*values* $\exp(2\pi i\theta)$, $0\le\theta<1$
- $U^K = I \;\Leftrightarrow\; A^K \equiv 1 \bmod X.$

$\theta_K = K/R,\; 0\le K<R$

- normed eigen*vector* $\psi_K := \sum_J \exp(-2\pi i JK/R)\,|\mathrm{bin}(A^J)\rangle \,/\, \sqrt{R}$
- $\sum_K \psi_K/\sqrt{R} \;=\; |0\ldots01\rangle$

(check**!**)

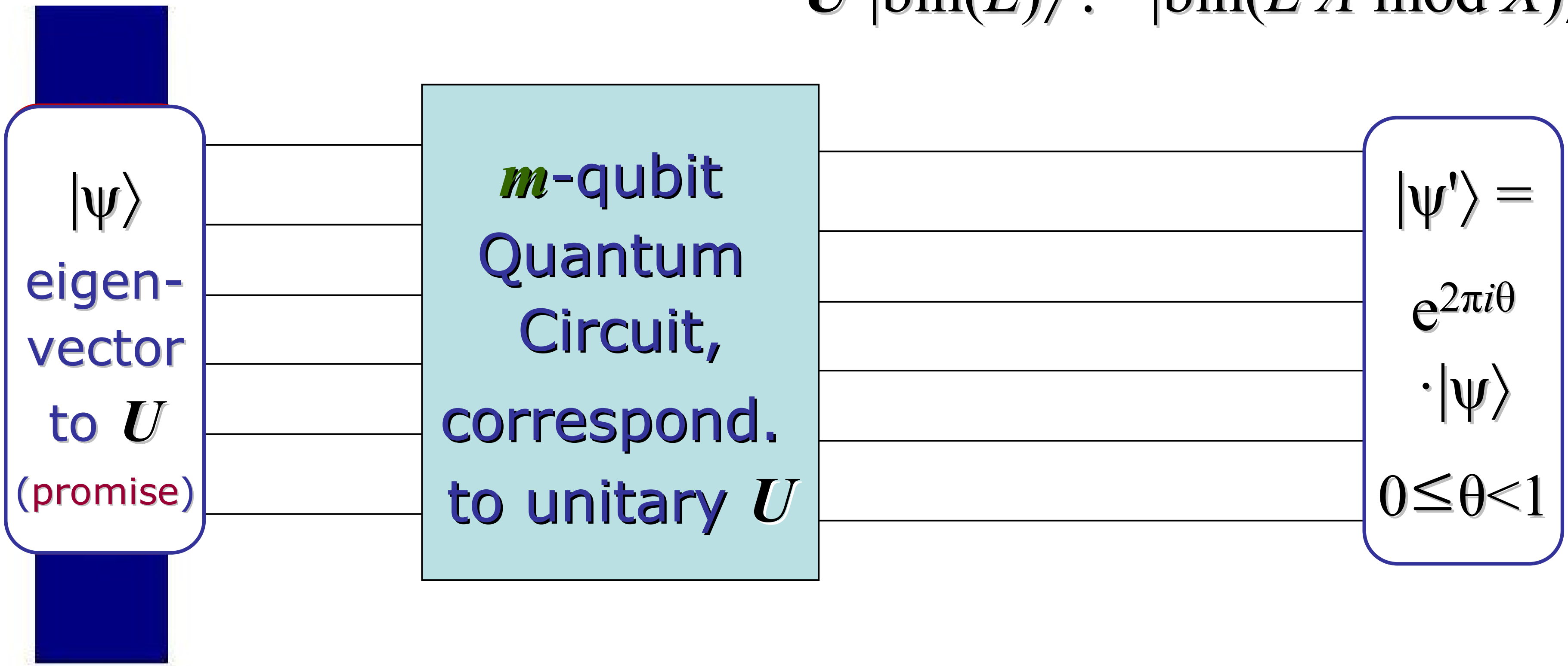
$R = \min\{\, K : A^K \equiv 1 \bmod X \,\}$

quantum subroutine to find multiplicativ. order R of $A \bmod X$

Quantum *Phase Estimation* Problem

Goal: approximate θ **!**

$U\,|\mathrm{bin}(L)\rangle := |\mathrm{bin}(L\cdot A \bmod X)\rangle$

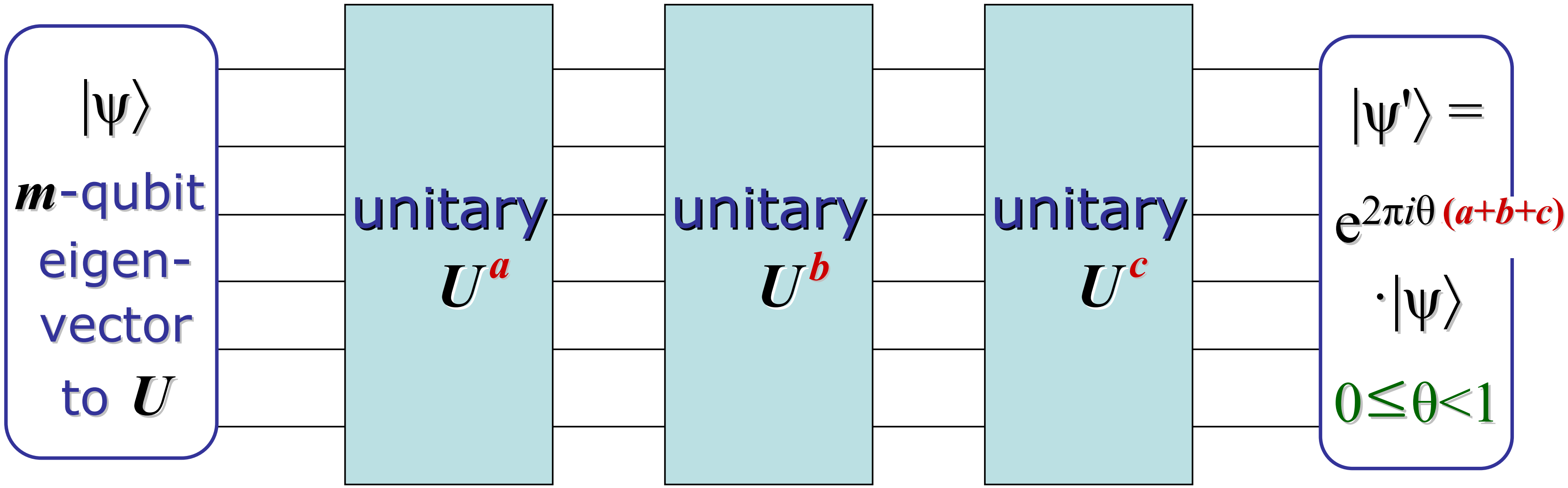


- normed eigen*vector* $\psi_K := \sum_J \exp(-2\pi i JK/R)\,|\mathrm{bin}(A^J)\rangle\,/\,\sqrt{R}$
- to eigen*value* $\exp(2\pi i\theta)$, $\theta = K/R$ • $\sum_K \psi_K/\sqrt{R} = |0\ldots01\rangle$

Towards Unitary Phase Estimation

Goal: approximate θ to absolute error $1/2^n$

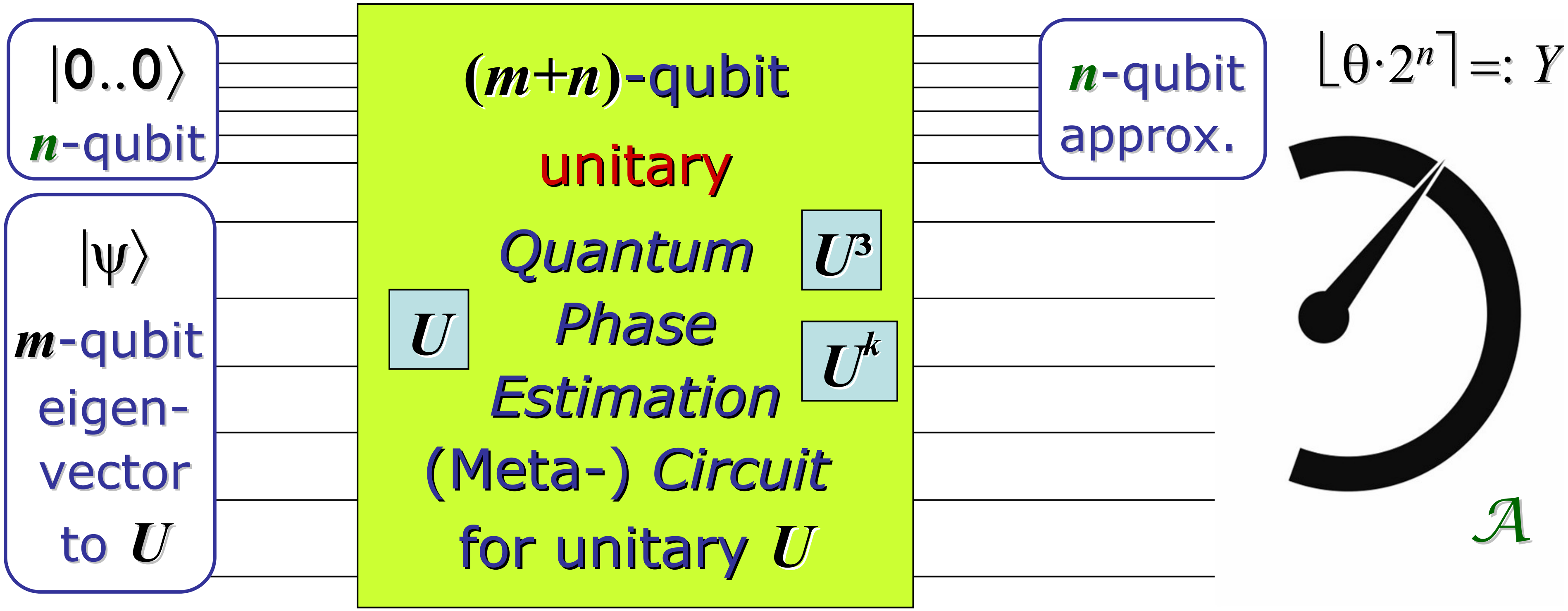
sequential→



Quantum Phase Estim. *Meta*-Circuit

$N=2^n$, $M=2^m$

Goal: compute $Y=\lfloor\theta\cdot 2^n\rceil$ with "high" probability



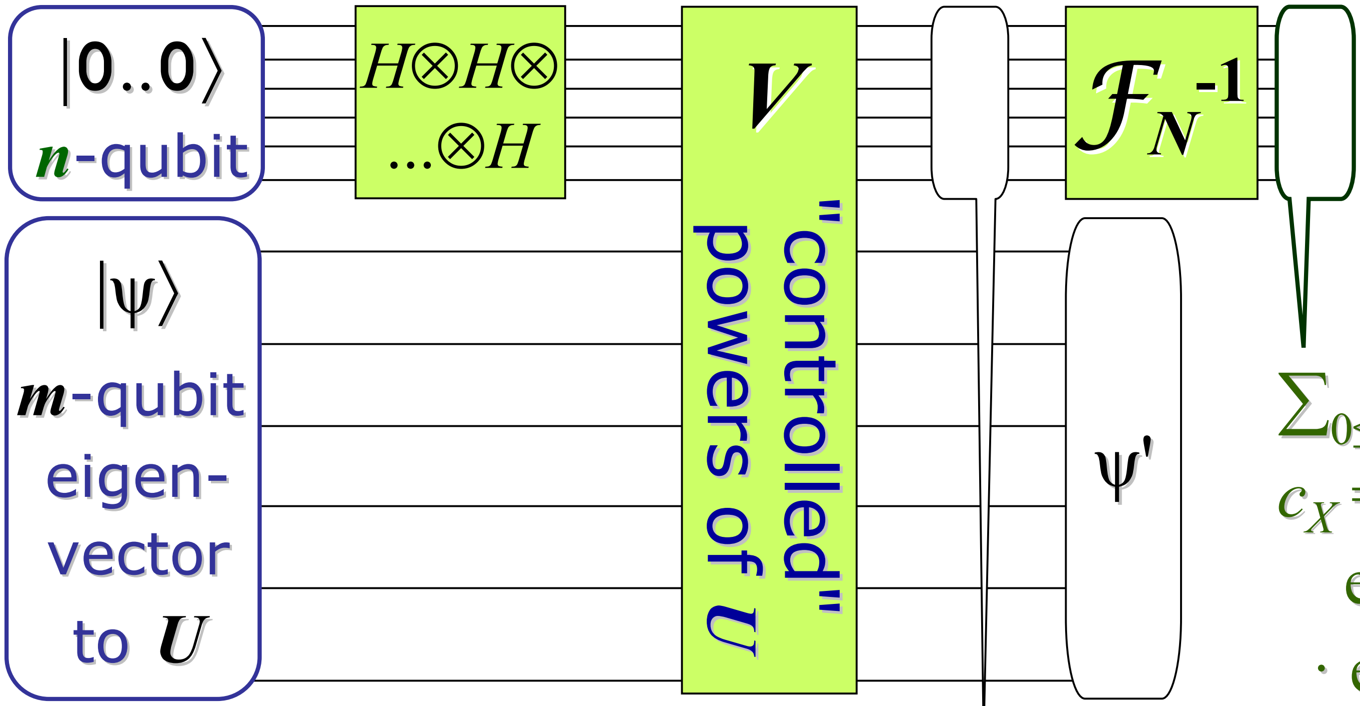
IVa. When S is in *pure* state ψ, measuring $\mathcal{A}$ produces eigenvalue a of A with **probability** $|\langle\psi_a|\psi\rangle|^2$,
where ψ_a is any unit eigenvector of A to eigenvalue a.

Quantum Phase Estim. *Meta*-Circuit

$N=2^n$ **Goal:** compute $\lfloor \theta \cdot 2^n \rceil$ **with "high" probability**

$$V = \sum_{0 \le K < N} |\mathrm{bin}(K)\rangle \langle \mathrm{bin}(K)| \otimes U^K, \quad |\mathrm{bin}(K)\rangle \otimes |\psi\rangle \to |\mathrm{bin}(K)\rangle \otimes |U^K|\psi\rangle$$

$$= \exp(2\pi i \theta K)\, |\psi\rangle$$



$Y = \lfloor \theta \cdot 2^n \rceil$

$\delta := \theta - Y/2^n$

$\Rightarrow |\delta| \le 2^{-(n+1)}$

$\sum_{0 \le X < N} c_X\, |\mathrm{bin}(X)\rangle$,

$c_X = \sum_{0 \le K < N} \exp(2\pi i K(Y-X)/N) \cdot \exp(2\pi i K \delta)\, /N$

V has exponential size!

$\sum_{0 \le K < N} \exp(2\pi i \theta K)\, |\mathrm{bin}(K)\rangle / \sqrt{N}$

Measurement yields $Y = \lfloor \theta \cdot 2^n \rceil$ with probability $|c_Y|^2 \ge 4/\pi^2$

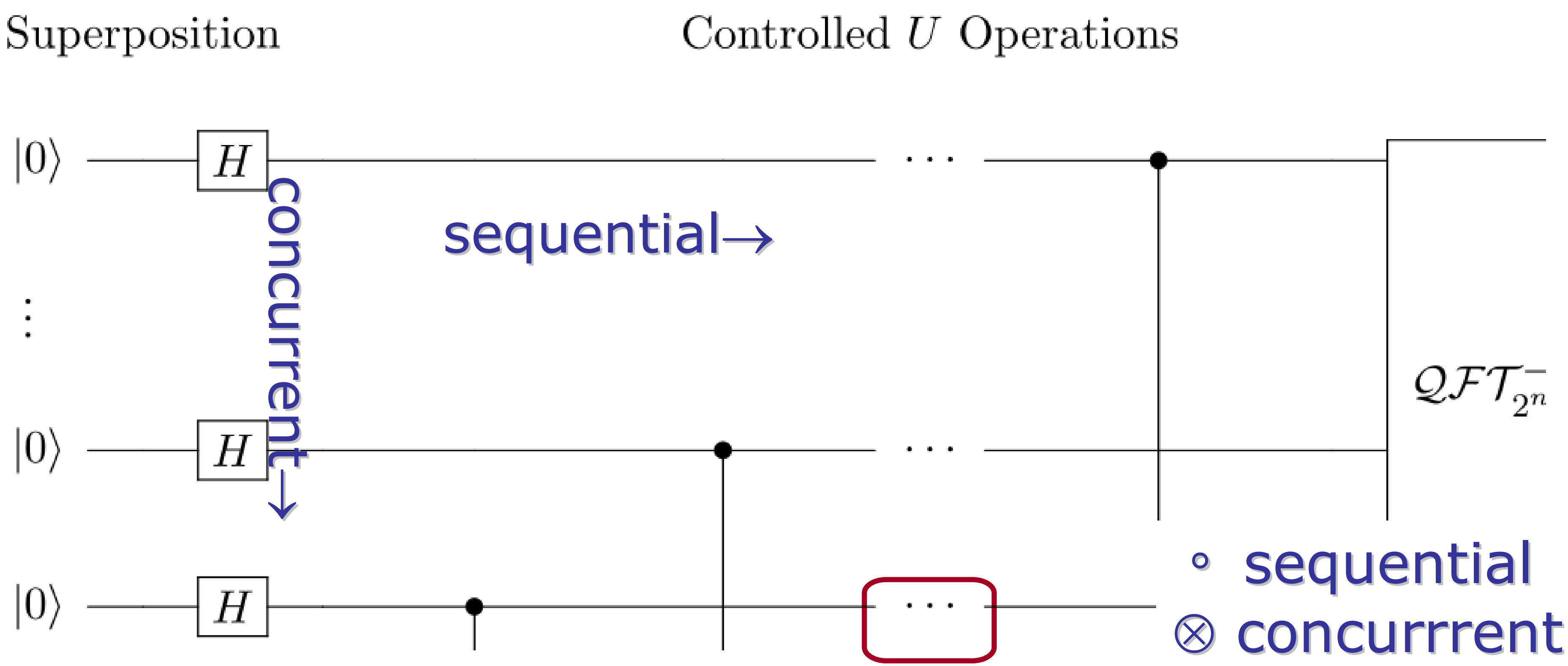
Quantum Phase Estim. *Meta*-Circuit

$N=2^n$ **Goal:** compute $\lfloor \theta \cdot 2^n \rceil$ **with "high" probability**

$$V = \sum_{0\le K<N} |\mathrm{bin}(K)\rangle\langle \mathrm{bin}(K)| \otimes U^K \quad = \prod_{0\le k<n} V_{2^k,k}$$

controlled *binary* power

where $V_{K,\ell}\,|x_0\ldots x_{n-1}\rangle \otimes |\psi\rangle := \boxed{|x_0\ldots x_{n-1}\rangle \otimes (U^{K\cdot x_\ell}}|\psi\rangle)$



Phase Estim. in Shor's Algorithm

$N=2^n$

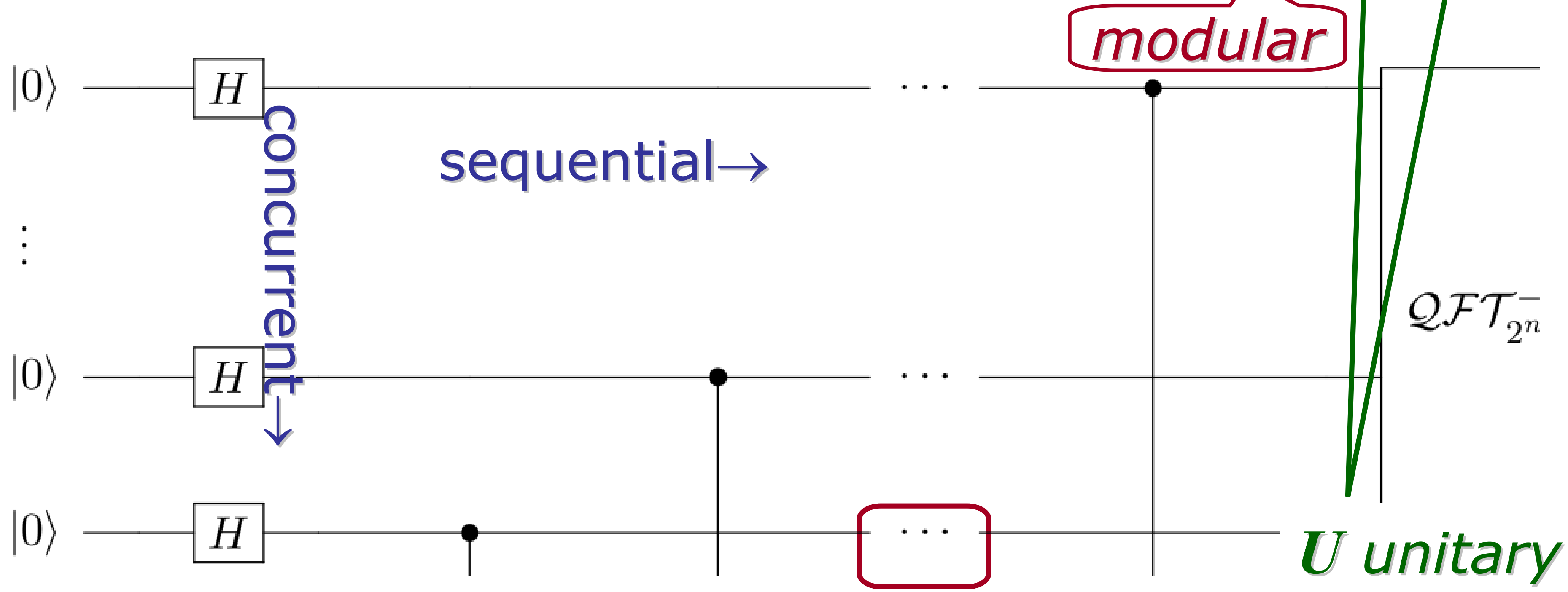
$M=2^m$

$U\,|\mathrm{bin}(L)\rangle := |\mathrm{bin}(L\cdot A \bmod X)\rangle$ for $0\leq L<X$

$U\,|\mathrm{bin}(L)\rangle := |\mathrm{bin}(L)\rangle$ for $X\leq L<M$

where X denotes the m-bit integer to be factored and $1<A<X$ is an integer parameter coprime to X.

$\Rightarrow U^{2^k}\,|\mathrm{bin}(L)\rangle = |\mathrm{bin}(L\cdot A^{2^k} \bmod X)\rangle$ repeated squaring



§11 Summary

- Recap: Experimental Physical Evidence
- Math Background: States and Operators
- Pure vs. Mixed States, Entanglement&EPR
- Qubits and Primitive Gates
- Quantum Circuits and Parallelism
- Quantum Phase Estimation
- Shor’s Hybrid Algorithm