KAIST

School of **Computing**

*Un*conventional Computing

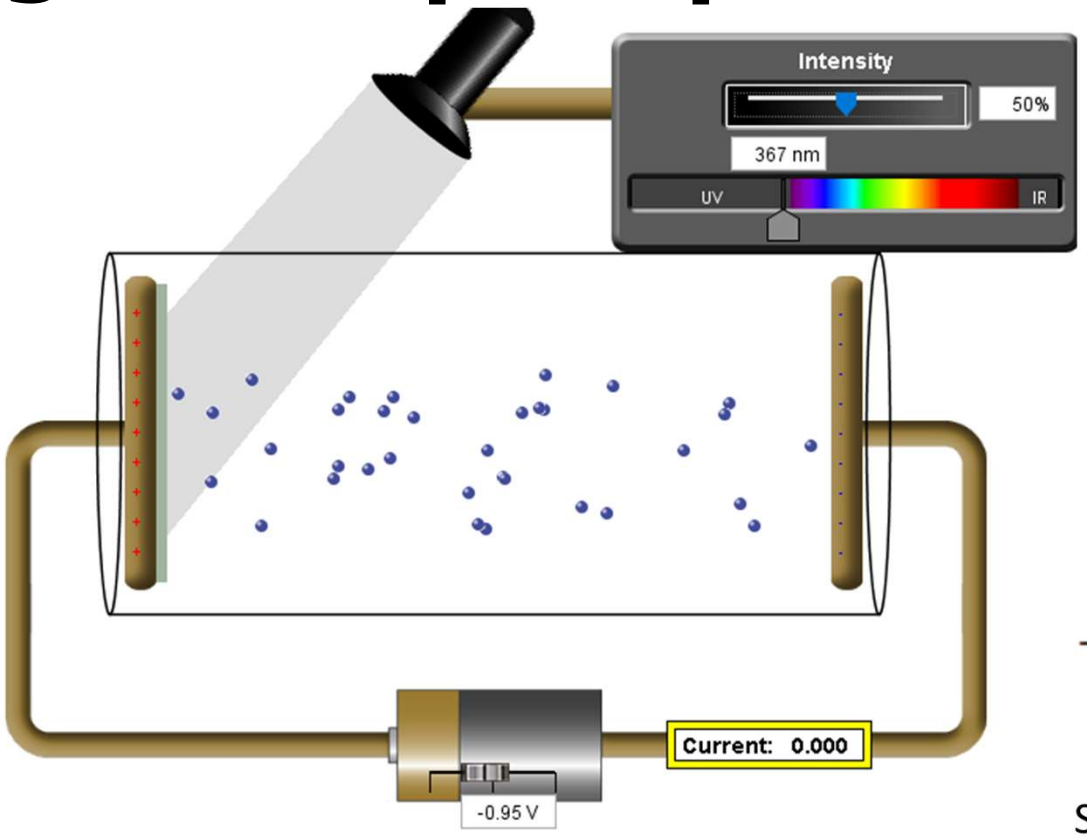
Martin Ziegler

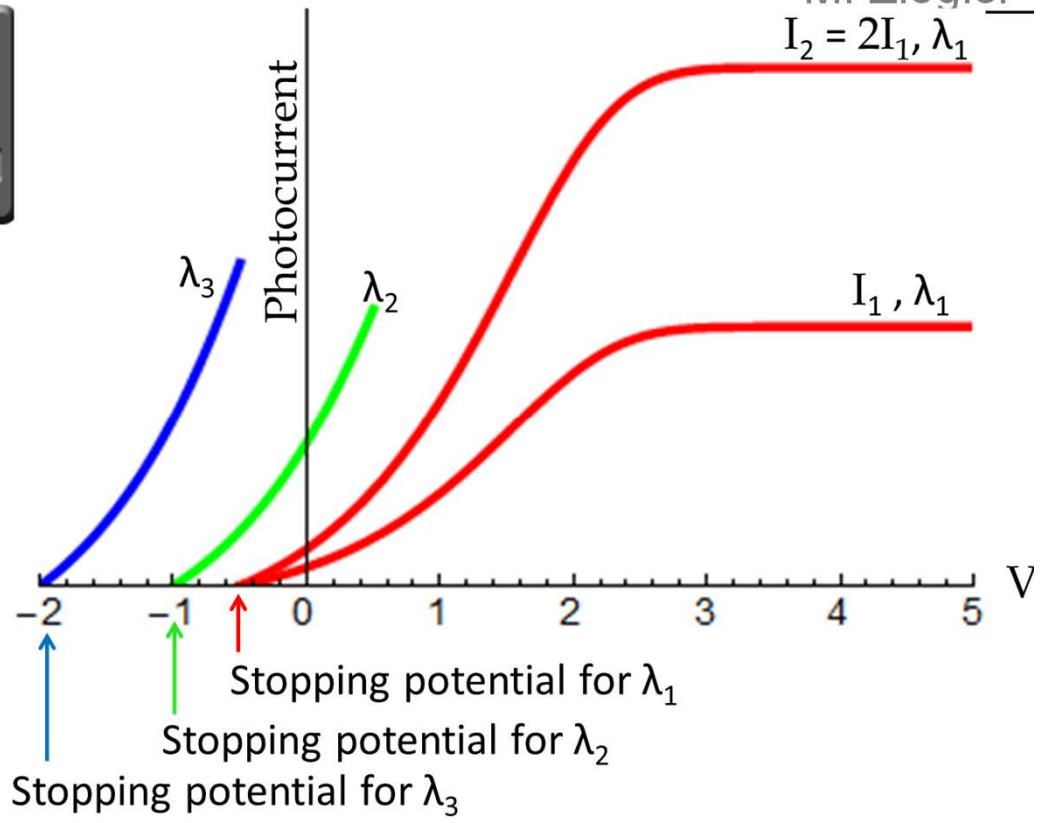
CS492A in Fall 2024

§4 Quantum Computing

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

§4 Recap: Experimental Physics





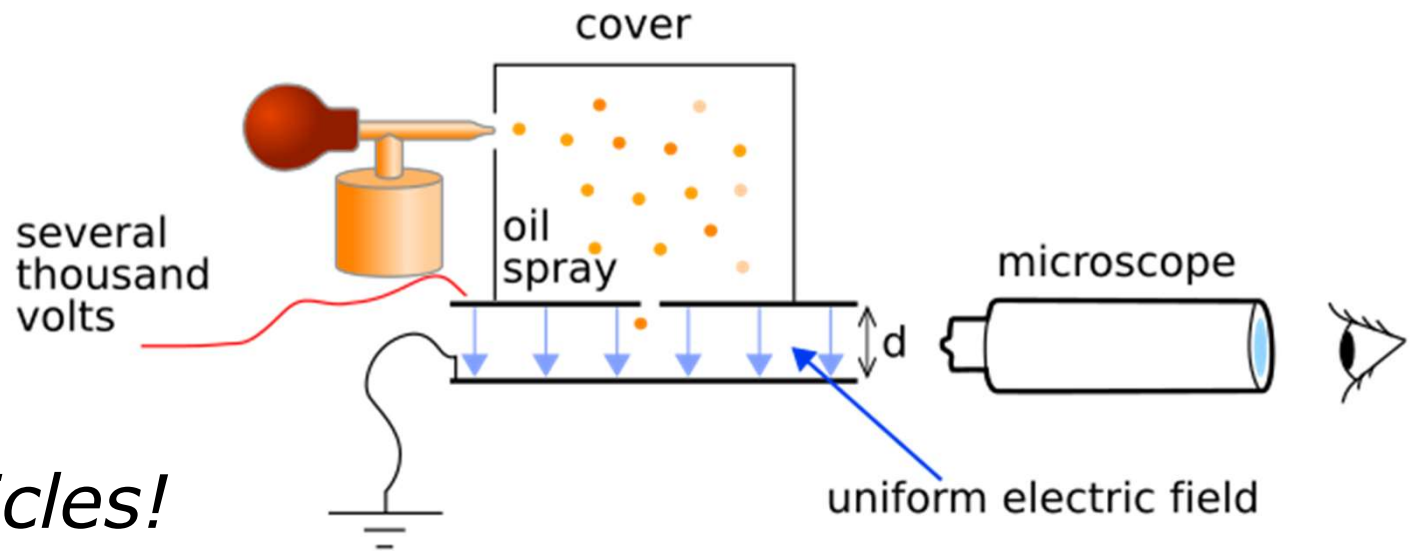
Einstein (1905):

And so is *light!*

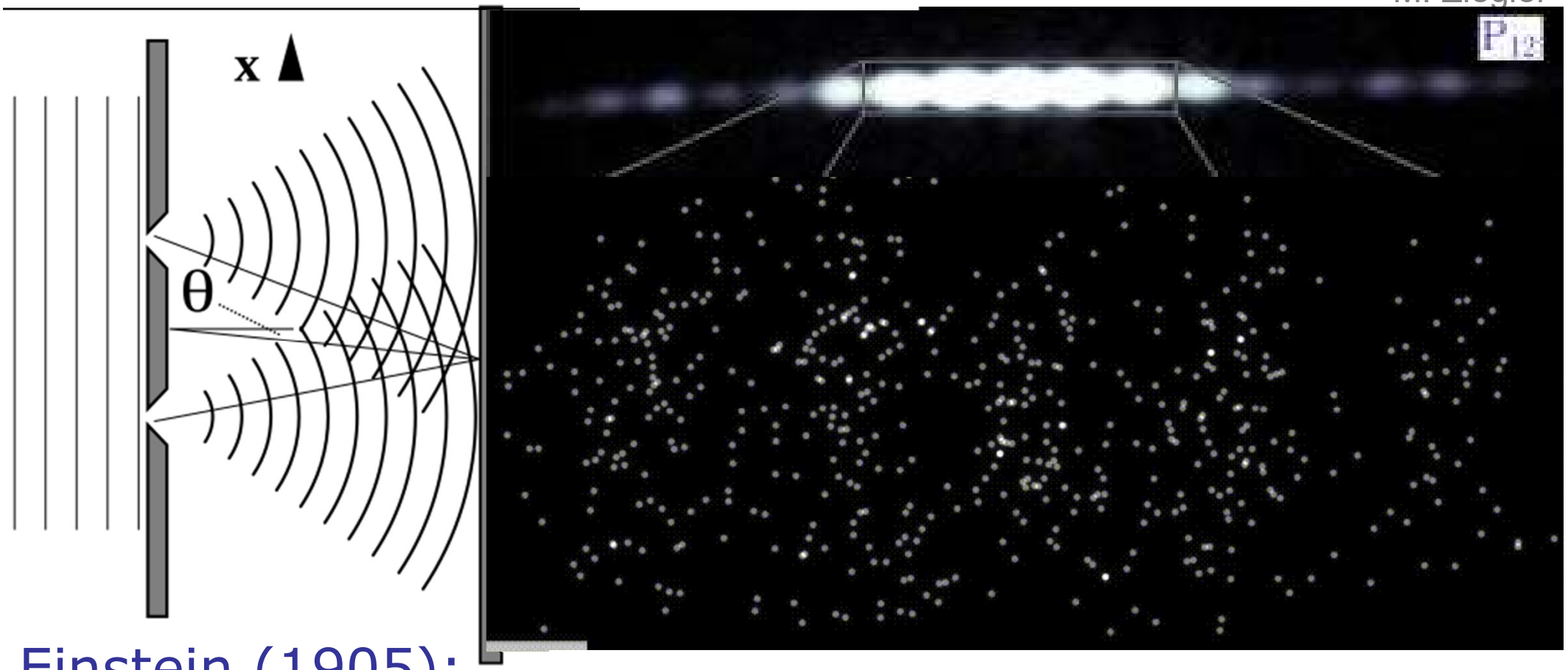
Robert Millikan

"Oil drop" (1909):

Electrons are *particles!*



§4 Recap: Experimental Physics



Einstein (1905):

And so is *light*!

Robert Millikan

"Oil drop" (1909):

Electrons are *particles*!

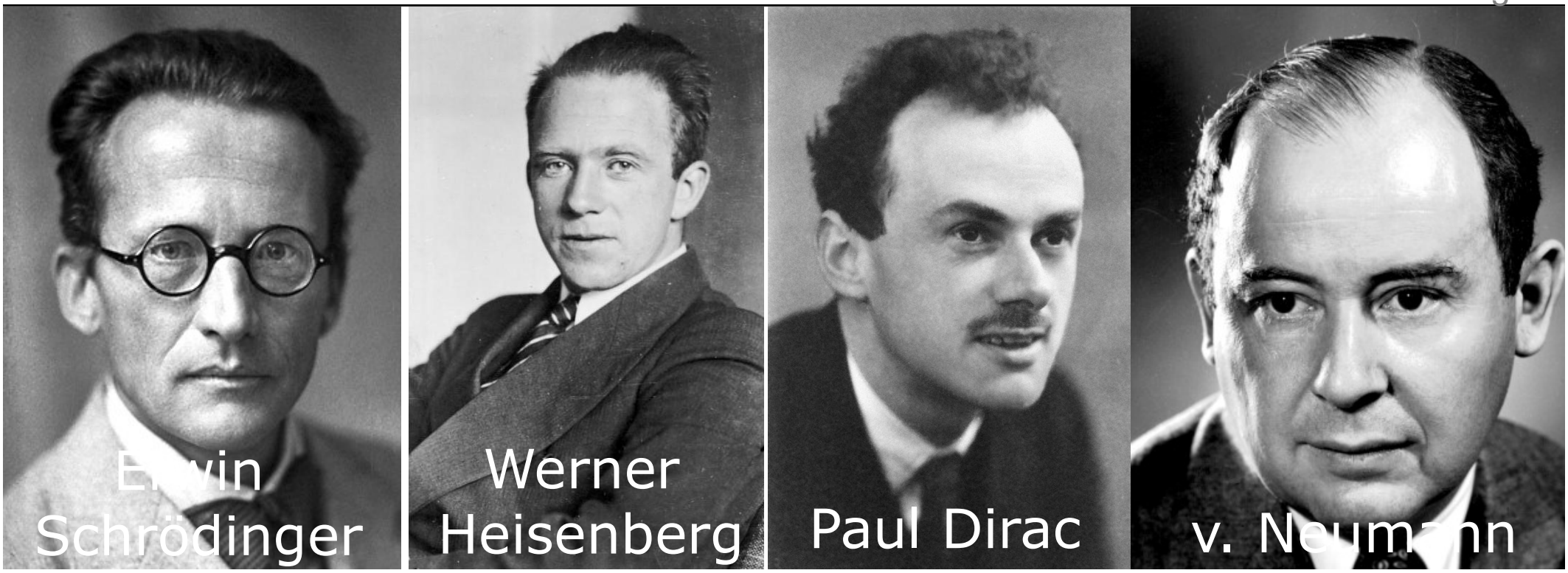
Claus Jönsson (1959):

And so are *electrons!*

Thomas Young (1801):

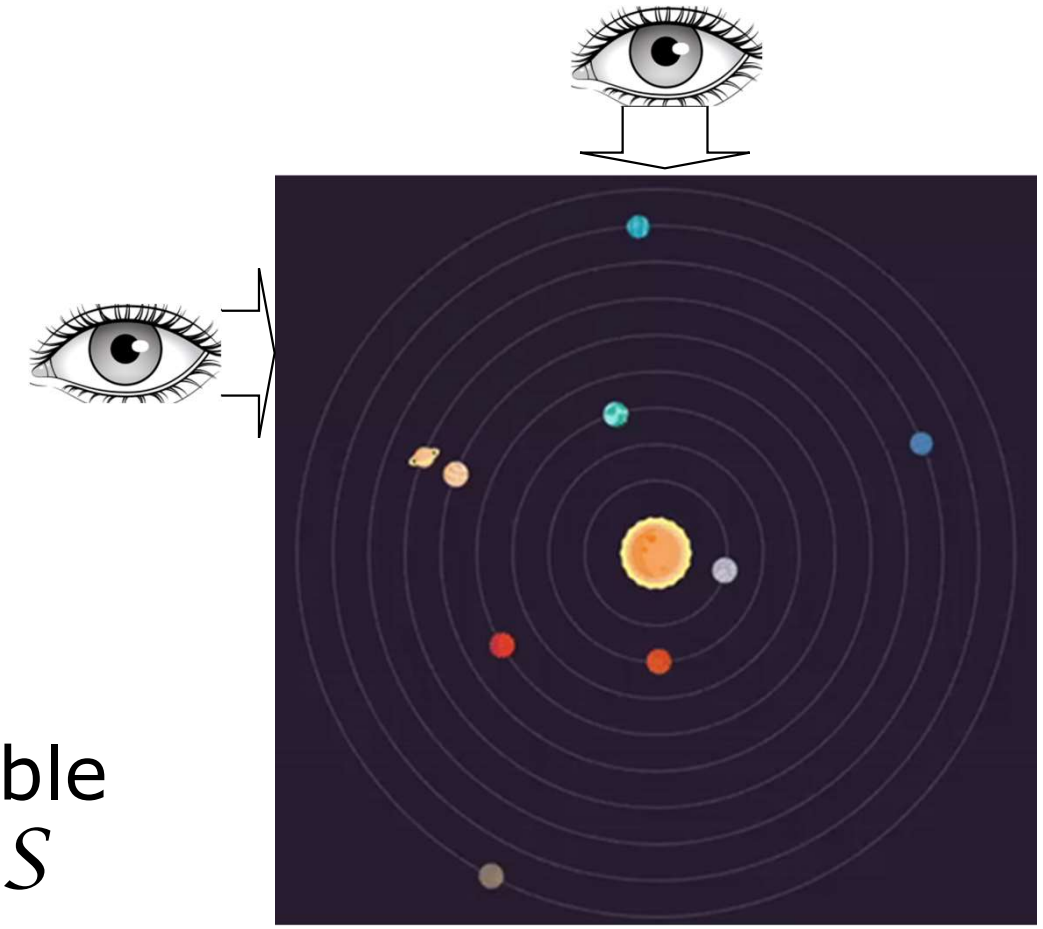
Light is a *wave!*

§4 *Basic* Quantum Mechanics



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

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

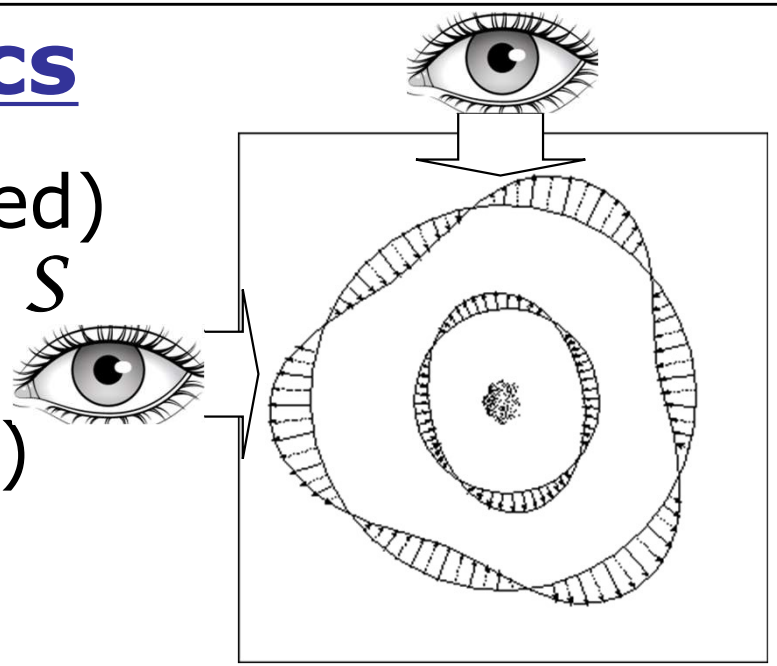
projections $A, A' : \mathbb{R}^{6p} \to \mathbb{R}$

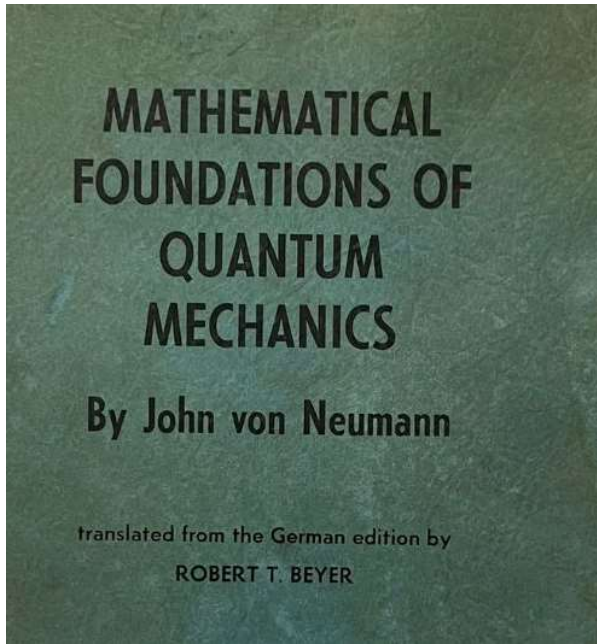
value $a = A(\bar{u})$

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

§4 *Math* of Quantum Mechanics

Physics	Math
I (isolated) system S	Hilbert Space $\mathcal{H}$
II (pure) states s,s' of S	normal vectors $\psi,\psi' \in \mathcal{H}$
III observable $\mathcal{A}$, $\mathcal{A}'$ of 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. $i\hbar\, \mathrm{d}/\mathrm{d}t\, \psi(t) = H\, \psi(t)$





§4 *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* $\rho = \sum_k w_k \cdot |\psi_k\rangle\langle\psi_k|$

§4 *Axioms* of Quantum Mechanics

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

IVa. When $\mathcal{S}$ 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, $\mathcal{S}$ 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* $\rho = \sum_k w_k \cdot |\psi_k\rangle\langle\psi_k|$

§4 *Axioms* of Quantum Mechanics

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

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 $\psi'=\psi_a$

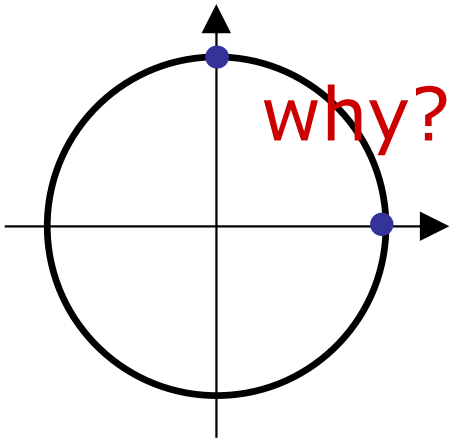
IIa. A *pure* state $s=s(t)$ of S at time t corresponds to a *unit* (=norm**1**) vector $\psi=\psi(t)\in\mathcal{H}$.

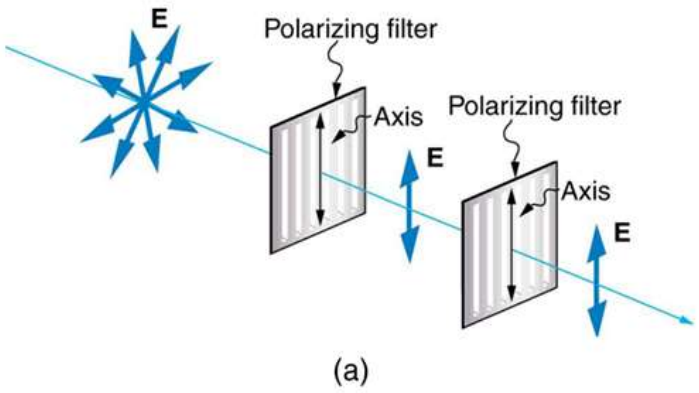
H Hamilton operator from observable "*energy*" (**III**)

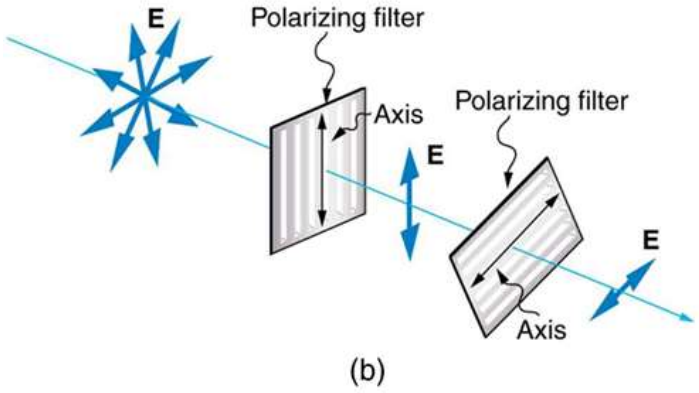
V. The time evolution of a *pure* state $\psi(0)\to\psi(t)\in\mathcal{H}$ is $\psi(t)=U(t)\,\psi(0)$, $U(t)=e^{-i\int H(t)\mathrm{d}t/\hbar}$ unitary

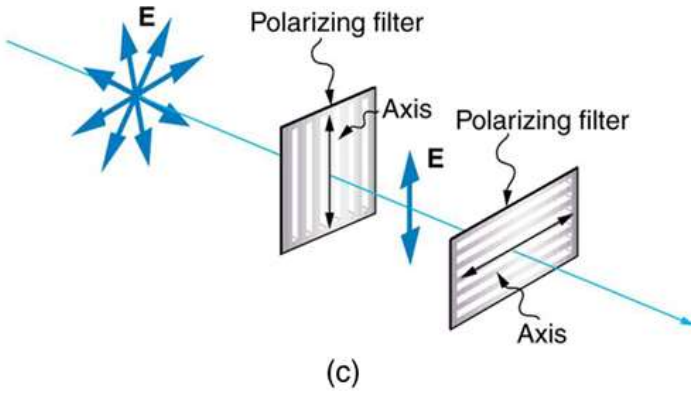
§4 Illustration/Justification

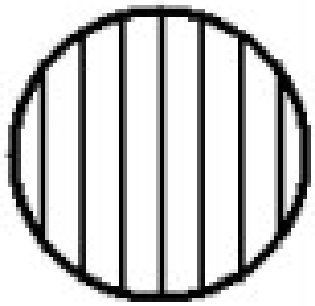
Example *Polarized light*: $\mathcal{H}=\mathbb{C}^2$ (qubit)

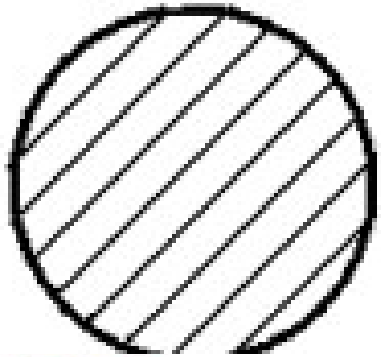


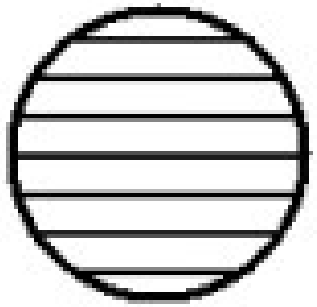










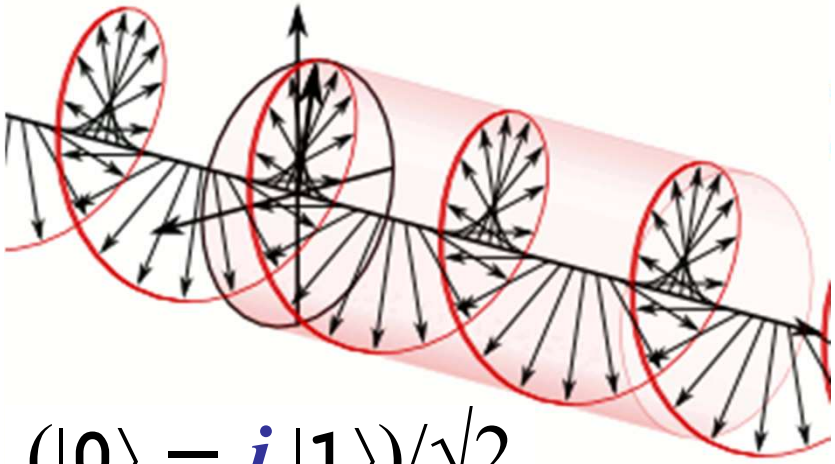


(d)

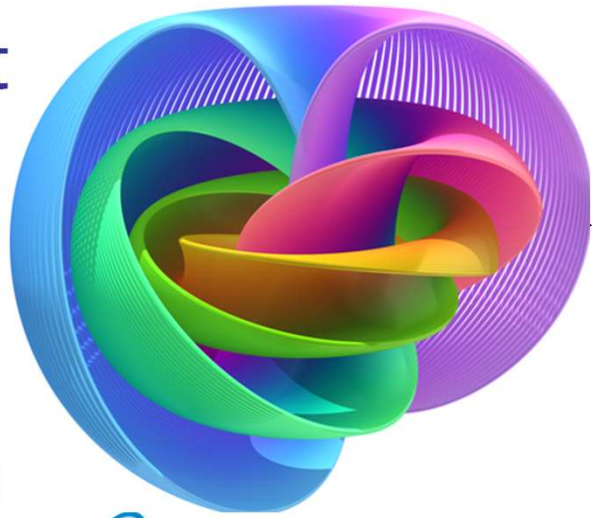
Ia. To any (isolated) physical system S corresponds a complex Hilbert space $\mathcal{H}$ called the *state space*.

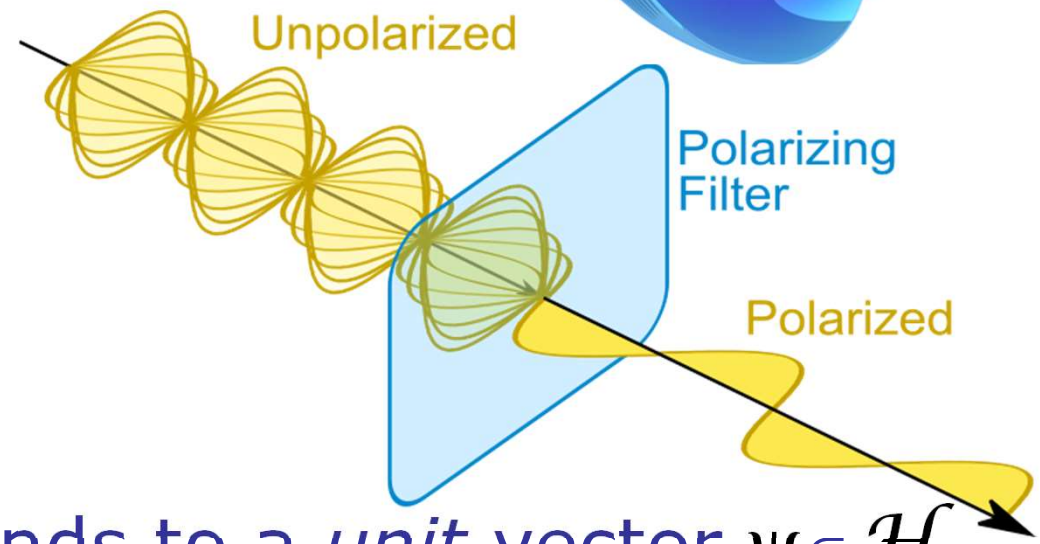
§4 Pure vs. Mixed States

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



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





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* $\rho = \sum_k w_k\cdot|\psi_k\rangle\langle\psi_k|$

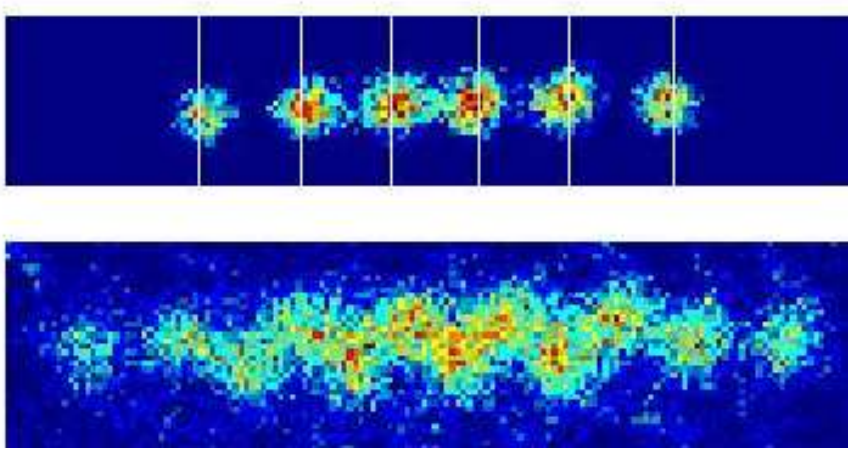
§4 Qubit Register

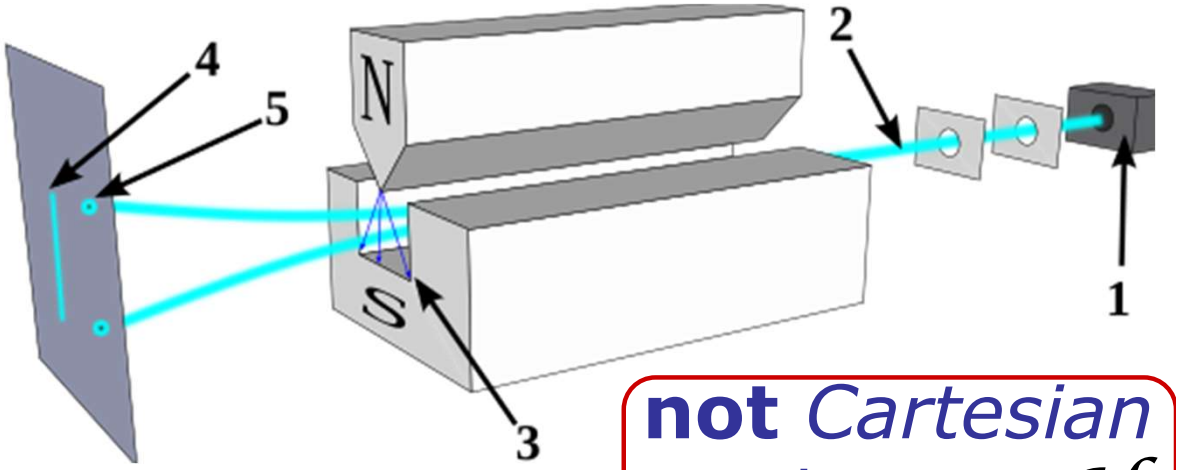
b) Particle spin: $\mathcal{H}=\mathbb{C}^2$ (qubit), *entanglement*

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

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

with ortho-basis $|\mathbf{0}\ldots\mathbf{0}\rangle$ … $|\mathbf{1}\ldots\mathbf{1}\rangle$





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

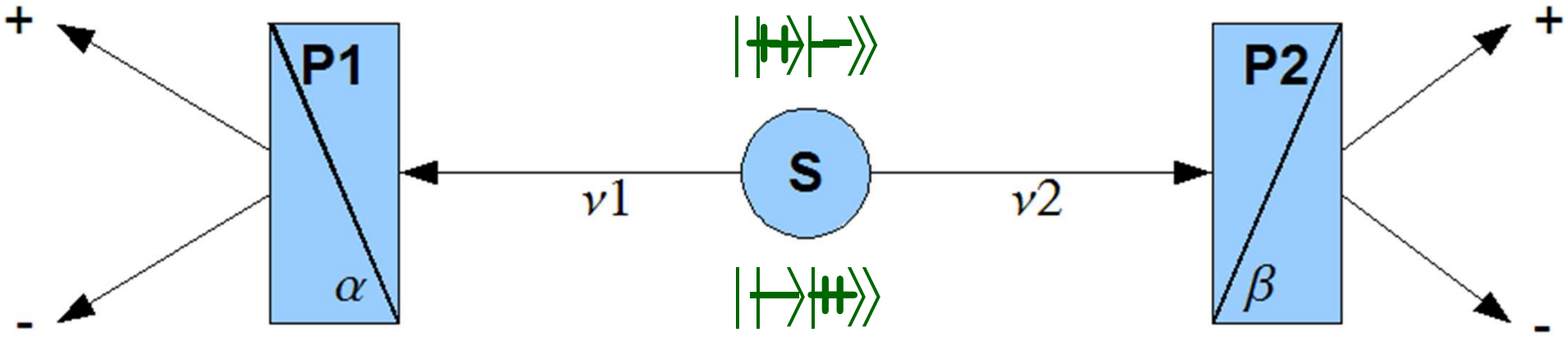
Ib. The state space of a system S composed from (connected) sub-systems S_j is the *tensor product* $\mathcal{H} = \otimes_j \mathcal{H}_j$ of the state spaces associated with components S_j

§4 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.

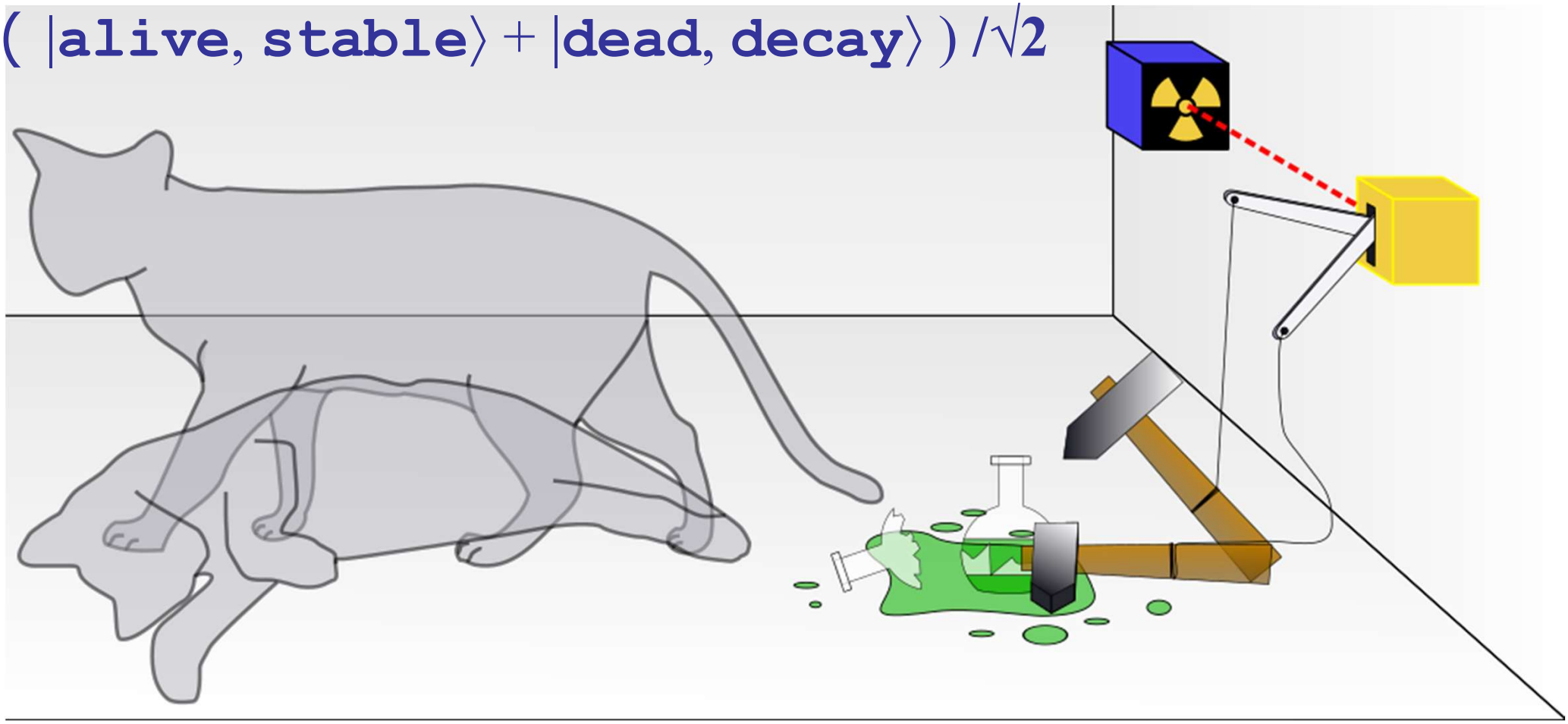
IVa'. After this measurement, S will be in state $\psi'=\psi_a$

§4 Schrödinger's Cat

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

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

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



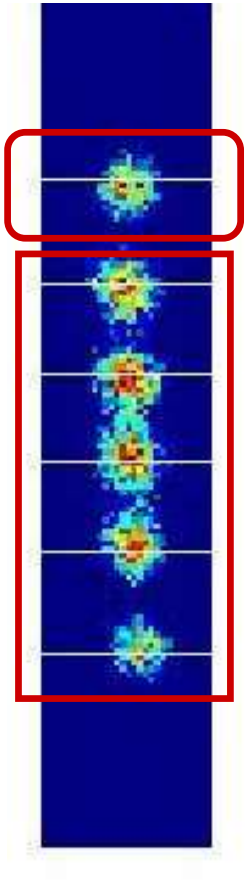
IVa'. After this measurement, S will be in state $\psi'=\psi_a$

§4 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 $U_Z = \begin{pmatrix} +1 & 0 \\ 0 & -1 \end{pmatrix}$ $|0\rangle \to +\,|0\rangle$, $|1\rangle \to -\,|1\rangle$

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

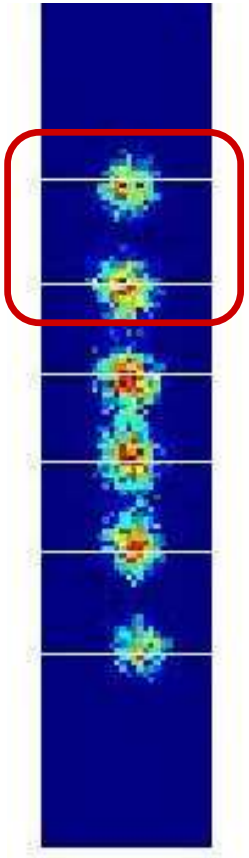
$P_\pi = ?$

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

§4 Quantum *Gates*: on 2 qubits

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

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



CNOT

1			
	1		
			1
		1	

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

SWAP

1			
		1	
	1		
			1

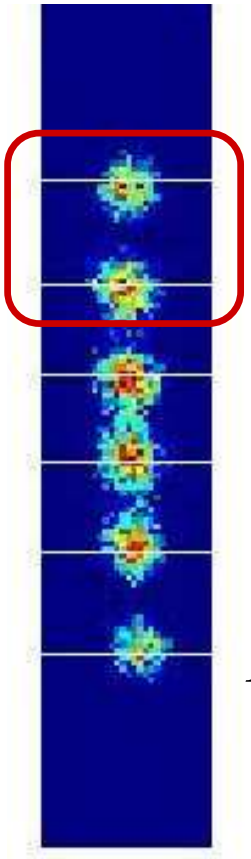
$|00\rangle \rightarrow |00\rangle$
$|01\rangle \rightarrow |10\rangle$
$|10\rangle \rightarrow |01\rangle$
$|11\rangle \rightarrow |11\rangle$

Quantum gates are *unitary*

§4 Hadamard *Gate*: on *n* qubits

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

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



H
H
H
H
H
H

in parallel

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

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

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

$$H\otimes H = \begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}/2$$

$\otimes$ id $\otimes\ldots\otimes$ id (*n*-2)–fold

$= (1,1,\ldots,1) / 2^{n/2}$

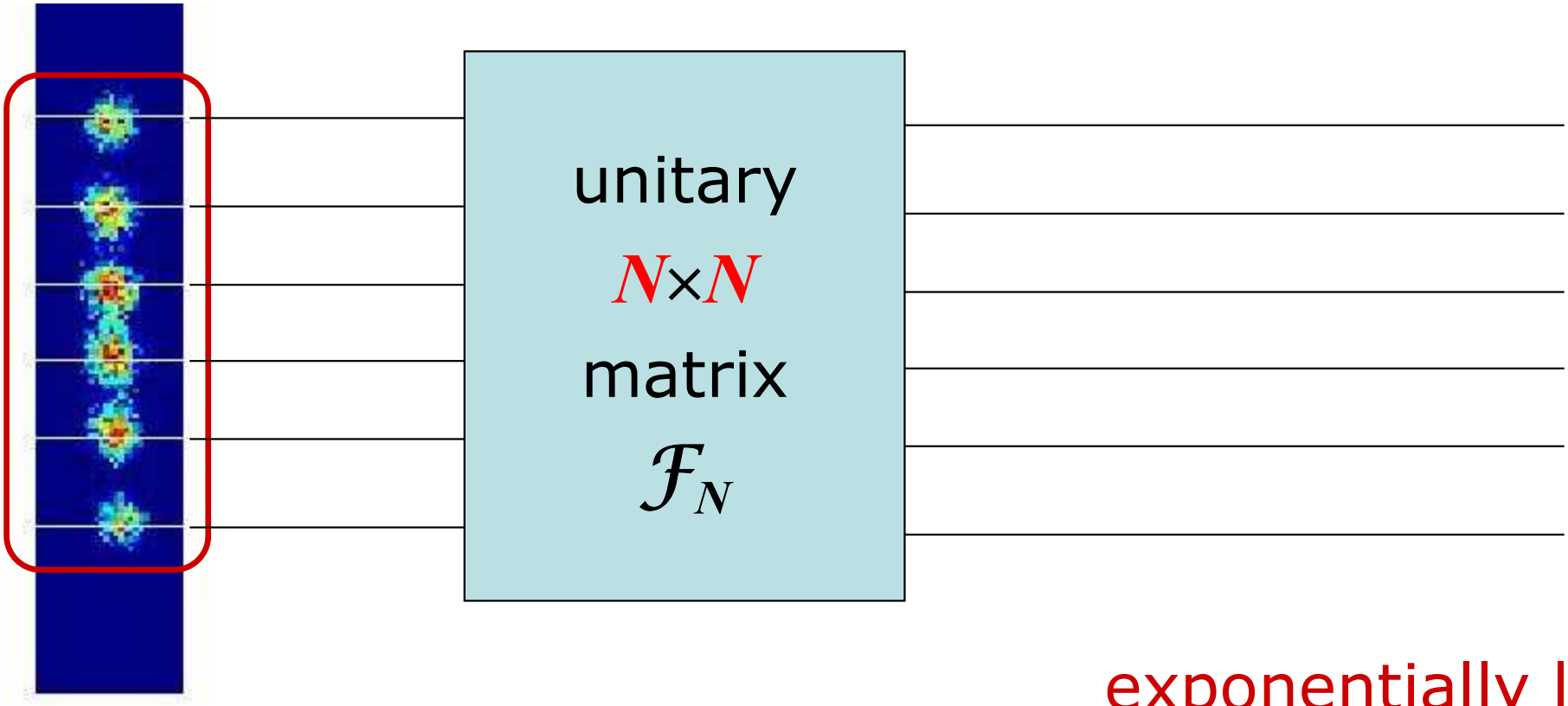
$H\otimes\ldots\otimes H$ (*n*–fold)

$|0\ldots0\rangle \to \sum_{0\le J<2^n} |\,\mathrm{bin}(J)\,\rangle / 2^{n/2}$

§4 *Quantum* Fourier Transform

c) $\mathcal{H}=\bigotimes^n \mathbb{C}^2$ (n qubits) has complex dimension $N=2^n$

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



exponentially large

quantum circuit

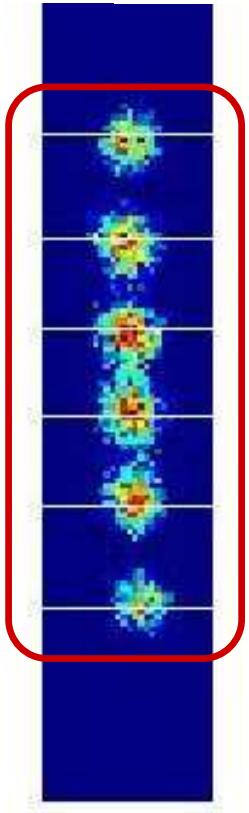
Quantum gates are *unitary*

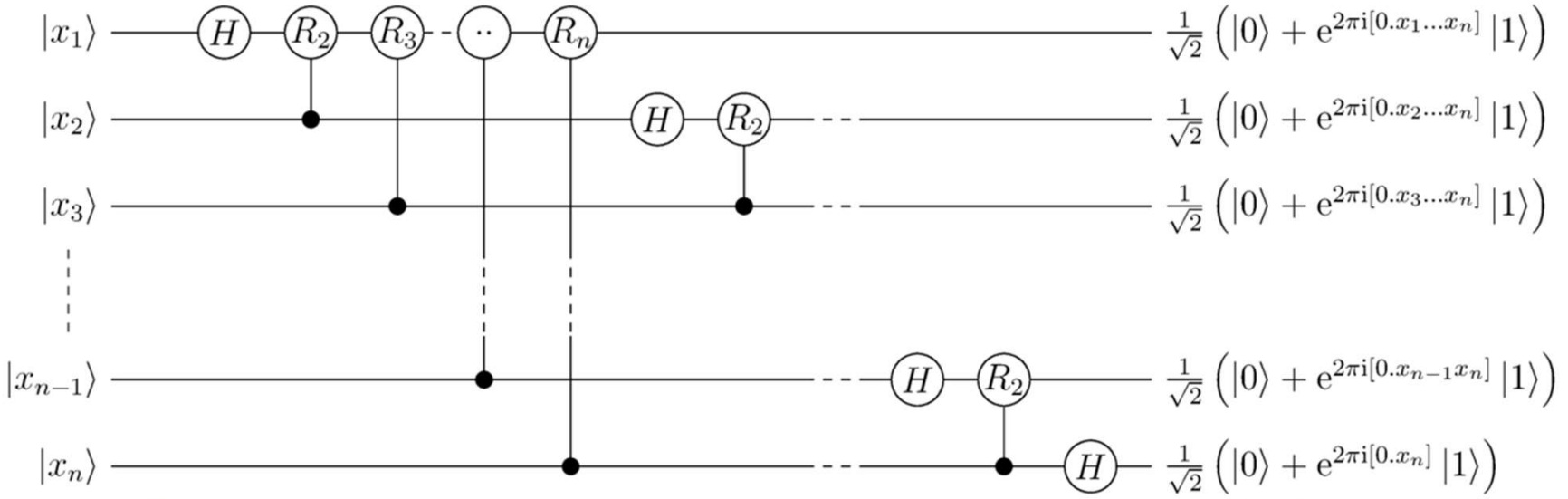
§4 *Fast* Quantum Fourier Trafo

c) $\mathcal{H}=\bigotimes^n \mathbb{C}^2$ (n qubits) has complex dimension $N=2^n$

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

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





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

tensor factorization

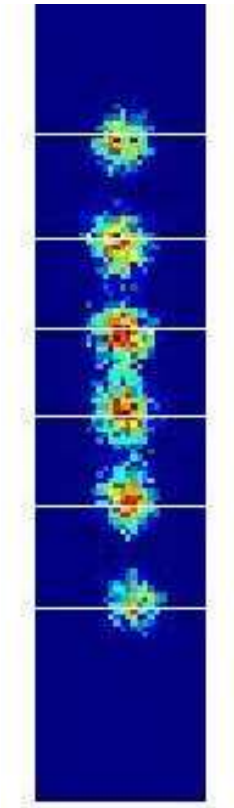
controlled phase $R_k=$

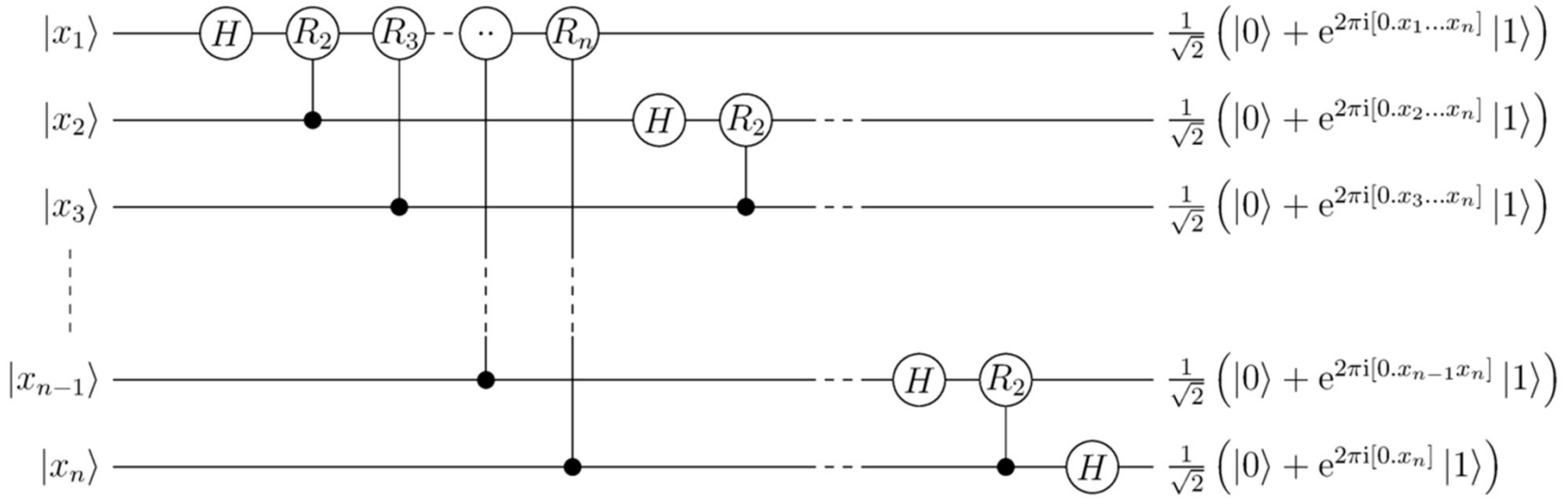
1			
	1		
		1	
			$e^{2\pi i 2^{-k}}$

§4 Quantum Fourier *Circuit*

c) $\mathcal{H}=\bigotimes^n \mathbb{C}^2$ (n qubits) has complex dimension $N=2^n$

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





polynomial

size = $O(n^2)$

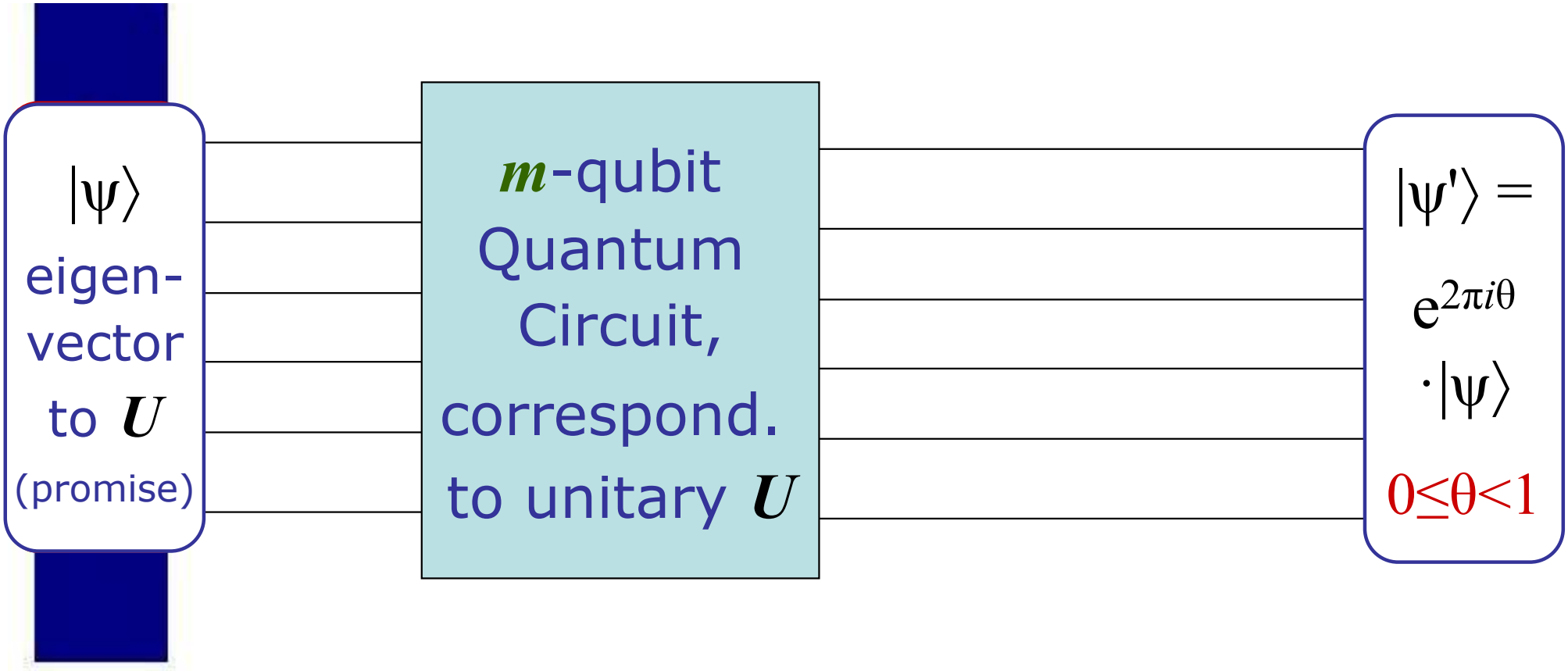
depth = $O(n)$

$\otimes$ (parallel) of unitary is unitary

$\circ$ (sequential) of unitary is unitary

§4 Quantum *Phase Estimation* Problem

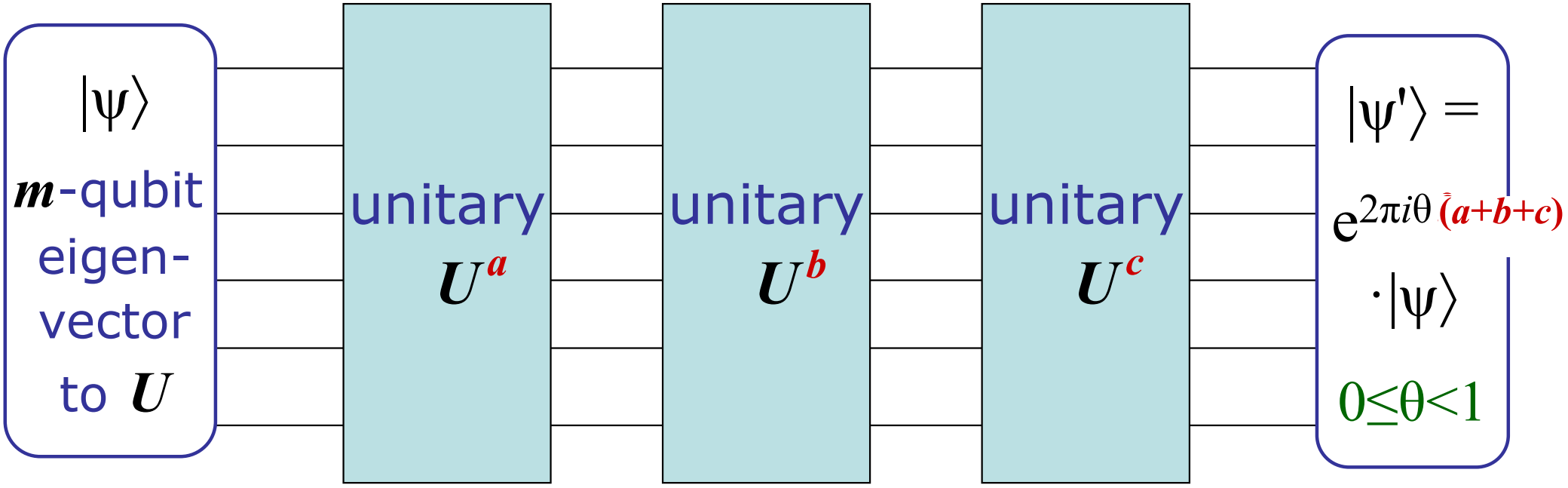
Goal: approximate θ **!**



Quantum circuits are *unitary*

§4 *Towards* Unitary Phase Estimation

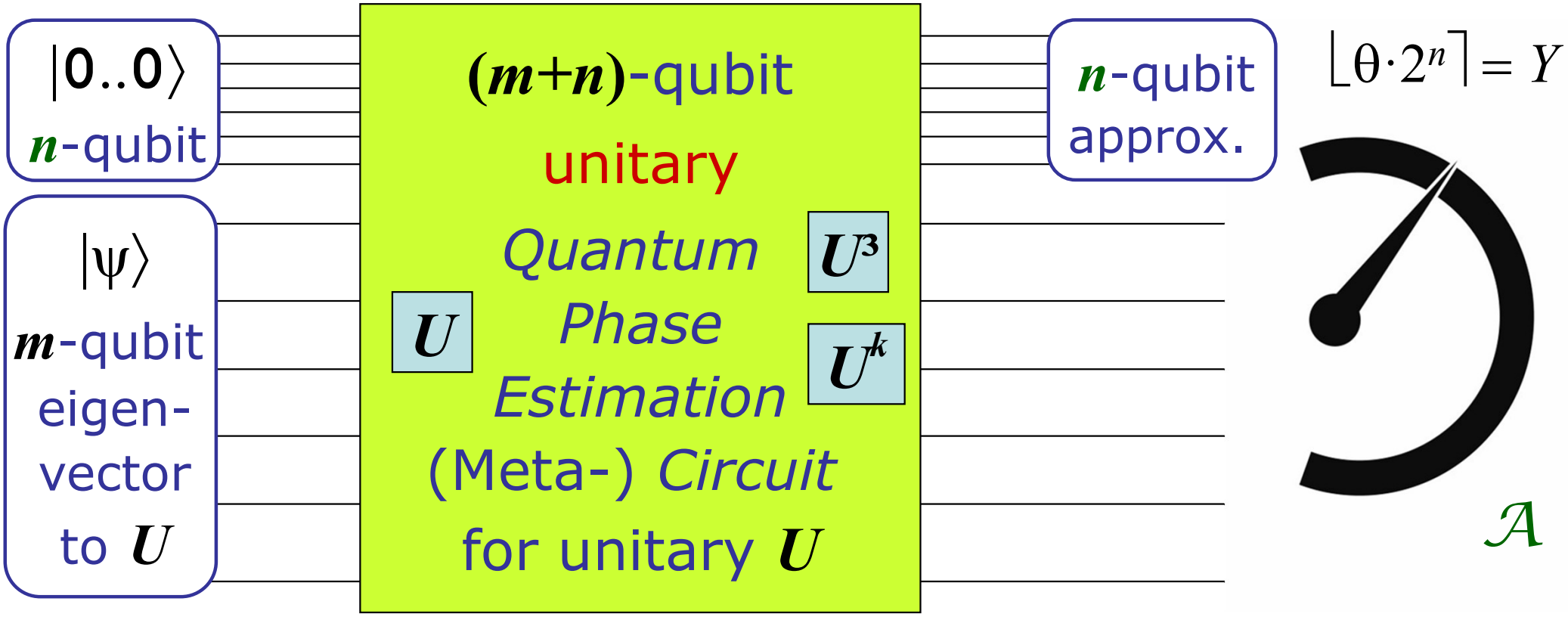
Goal: approximate θ to absolute error $1/2^n$



§4 Quantum Phase Estim. *Meta*-Circuit

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

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



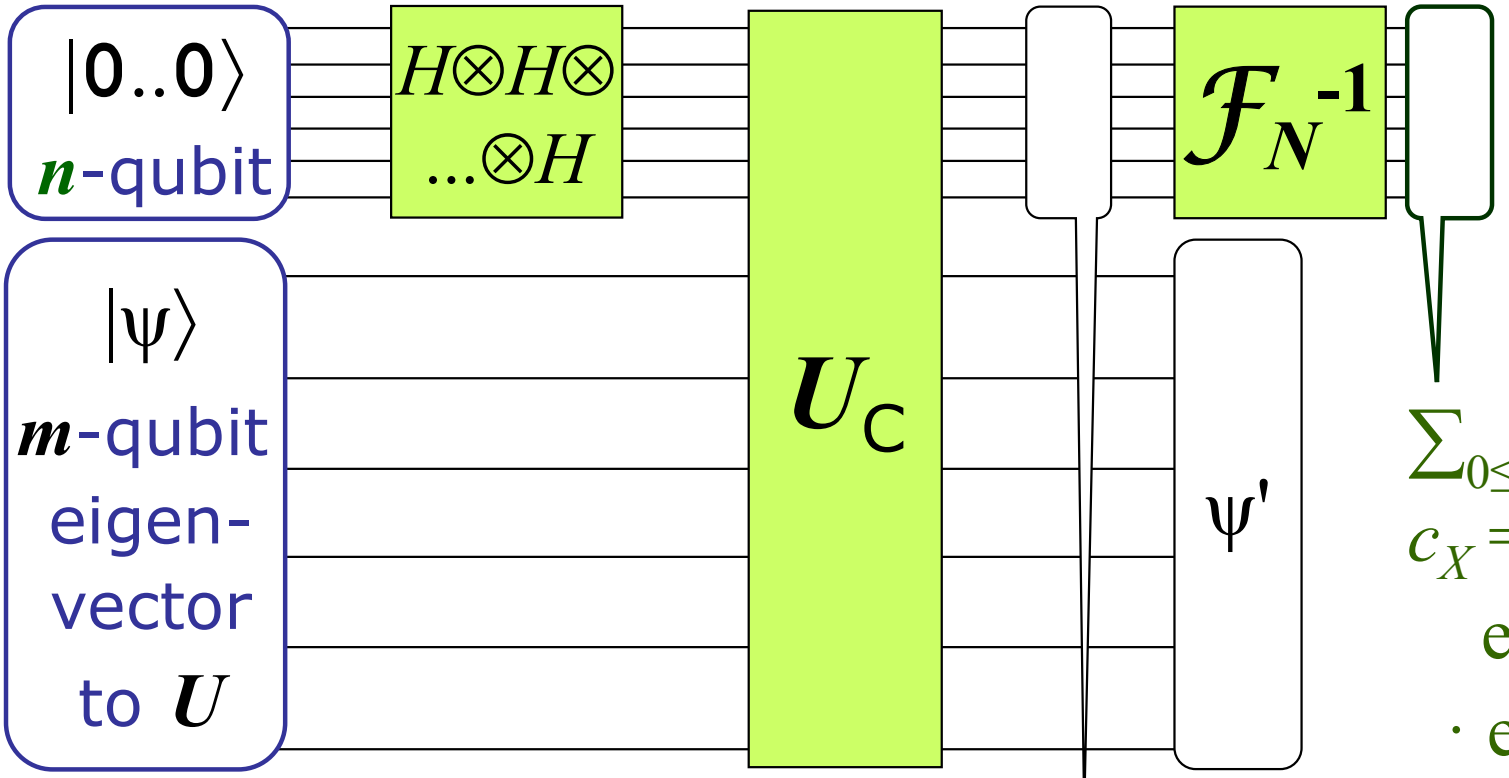
IVa. When S is in *pure* state ψ, measuring $\mathcal{A}$ produces eigenvalue a of A with **probability** $|\langle \psi_a | \psi \rangle|^2$, where ψ_a is any unit eigenvector of A to eigenvalue a.

§4 Quantum Phase Estim. *Meta*-Circuit

$N=2^n$

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

$$U_C = \sum_{0 \le K < N} |\mathrm{bin}(K)\rangle \langle \mathrm{bin}(K)| \otimes U^K, \quad |\mathrm{bin}(K)\rangle \otimes |\psi\rangle \rightarrow |\mathrm{bin}(K)\rangle \otimes U^K|\psi\rangle = \exp(2\pi i \theta K)\,|\psi\rangle$$



$$Y = \lfloor \theta \cdot 2^n \rceil$$
$$\delta := (Y - X)/2^n$$
$$\Rightarrow |\delta| \le 2^{-(n+1)}$$

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

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

U_C has exponential size!

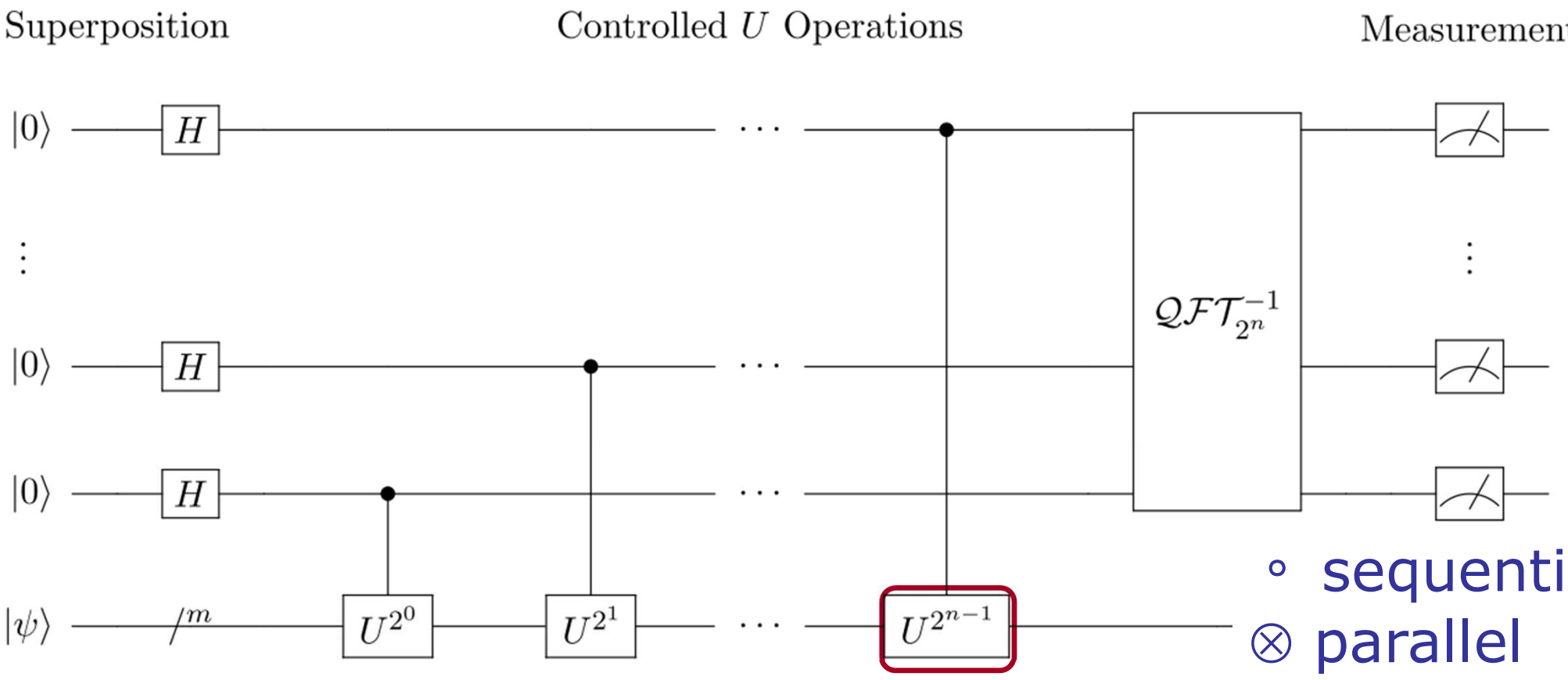
Measurement yields $Y = \lfloor \theta \cdot 2^n \rceil$ with probability $|c_Y|^2 \ge 4/\pi^2$

§4 Quantum Phase Estim. *Meta*-Circuit

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

$$U_C = \sum_{0 \le K < N} |\mathrm{bin}(K)\rangle \langle \mathrm{bin}(K)| \otimes U^K = \prod_{0 \le k < n} U^{2^k}{}_{C[k]}$$

where $U^K{}_{C[\ell]} |x_0 \ldots x_{n-1}\rangle \otimes |\psi\rangle := |x_0 \ldots x_{n-1}\rangle \otimes (U^{K \cdot x_\ell} |\psi\rangle)$



∘ sequential

⊗ parallel

§4 Phase Estim. in Shor's Algorithm

$N=2^n$

$M=2^m$

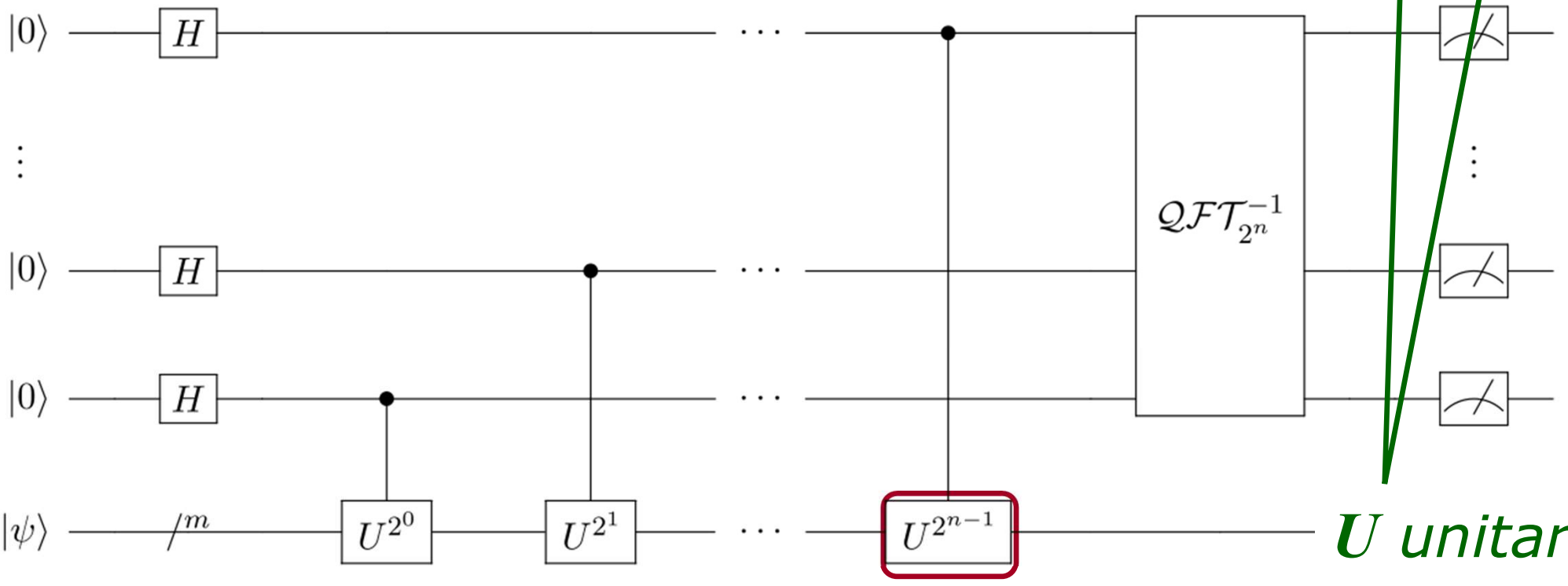
$$\boldsymbol{U}\,|\mathrm{bin}(L)\rangle := |\mathrm{bin}(L\cdot A \bmod X)\rangle \quad \text{for } 0\leq L<X$$

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

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

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

repeated squaring



U unitary