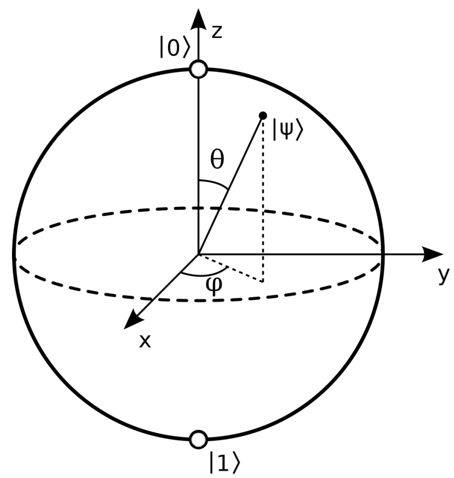
QSIT: Theory

Quantum Systems for Information Technology
Theory Part

Matthias Christandl
Quantum Information Theory
Institute for Theoretical Physics
ETH Zurich



What is it?

- All-round theory course for quantum information
(heavy-theory course given by Prof. Renner)
- target audience: experimental physicists
current or future
Bachelor/Master/PhD

0. Introduction

Content

- What is Quantum Information and Computation?
- What is Entanglement?
- What is a Bell Inequality?
- What is Quantum Tomography?
- What is Shor's Algorithm?
- What is Quantum Error Correction?

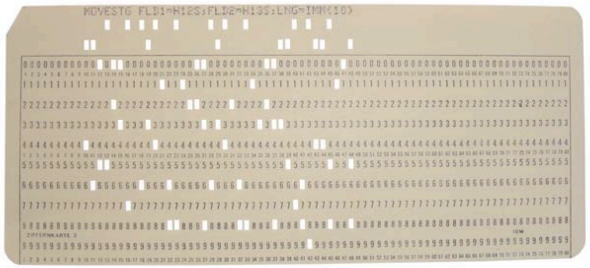
Testat

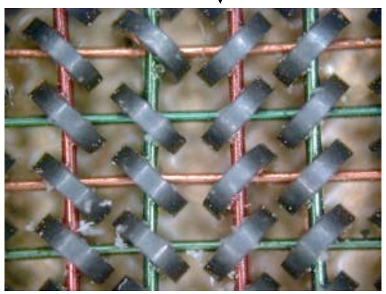
- active participation in the course and exercises
- 75% of exercises

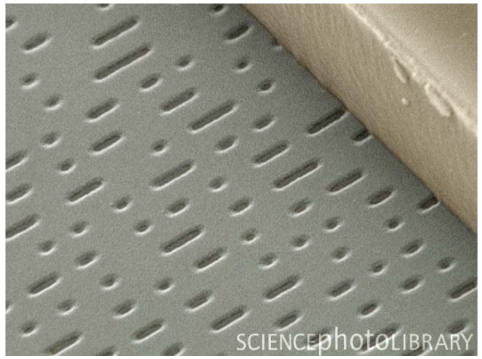
I. Quantum Information

Information

- Shannon, 1948
- Concept „information“ independent of physical implementation
- string of bits $\boxed{01011010100}$



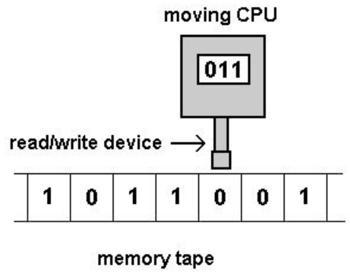




- all physical information can be represented in this way → Information Theory

Computation

- Turing, 1948
- Concept „computation“ independent of physical implementation
- Turing machine



- Church-Turing thesis:
  all physical computation can be represented by a Turing machine → Computer Science

Quantum Mechanics

- Shannon & Turing's notions (1948)
  based on classical physics
  information has always definite value

01011010100

Shannon/Turing do not directly apply!

- Quantum Mechanics (1900s)
  atoms not governed by classical physics

Shannon/Turing can in principle not apply!

- State of system ↔ wave function

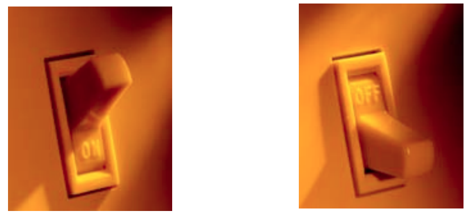
  definite measurement values do not exist prior to measurement, *in principle!*
  Einstein, Podolsky & Rosen (1935), Bell (1967), Kochen & Specker (1967)

Need for theory of information and computation that applies to QM

The Bit

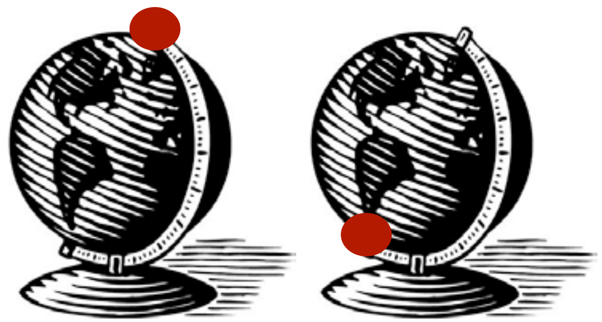
- The bit = unit of information

  on/off



  heads/tails

  north pole/ south pole

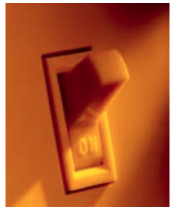


- variable $x \in \{0, 1\}$

The Bit

- random bit

  child plays with switch




  toss of a coin

  travel lottery


- random variable X
  range $\{0, 1\}$

$$p(0) = \mathrm{prob}[X = 0]$$
$$p(1) = \mathrm{prob}[X = 1]$$

The Quantum Bit or Qubit

$$'0' \rightarrow |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad '1' \rightarrow |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

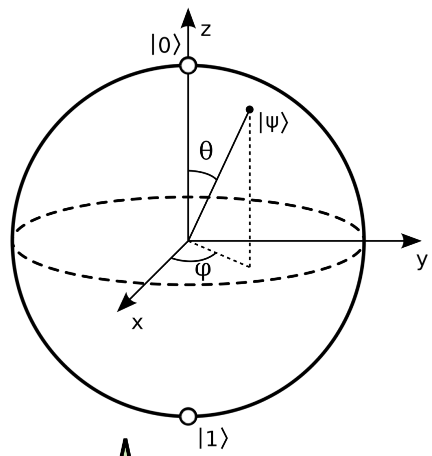
state of a qubit

- superposition principle $\quad |\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$
- probability amplitudes
- normalisation $\quad |\alpha|^2 + |\beta|^2 = 1$
- angles $\quad |\psi\rangle = \cancel{e^{i\gamma}}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$

infinitely many states

overall phase does not matter

- in nature: polarisation of photon
  electron / nuclear spin 1/2
  ground vs excited state



Bloch sphere representation

Measuring a Qubit

- Qubit = Bloch vector
- Bloch vector = infinite amount of information

$$\theta = \theta_0\theta_1\theta_2\ldots$$

$$\phi = \phi_0\phi_1\phi_2\ldots$$

binary expansion

$\log_2(4/\Delta^2)$

precision on Bloch sphere, see Christandl & Renner, PRL 2012

- Can qubit store an infinite amount of information?
- No! Measurement retrieves only one bit!
- State of qubit after measurement = outcome

Measuring a Qubit

- Observable= self-adjoint operator

here, 2x2 Hermitian matrix,

$$A = a_0|\phi_0\rangle\langle\phi_0| + a_1|\phi_1\rangle\langle\phi_1|$$

spectral theorem   eigenvalues (real)   eigenvectors (orthonormal)

outcome   post-measurement state

$$|\psi\rangle \longrightarrow \boxed{\text{measurement of A}} \longrightarrow i, |\phi_i\rangle$$

$$\begin{aligned}\text{prob}[\text{outcome} = i] &= |\langle\psi|\phi_i\rangle|^2 \\ &= \text{tr}|\psi\rangle\langle\psi||\phi_i\rangle\langle\phi_i| \\ &= \cos^2\frac{\theta_i}{2}\end{aligned}$$

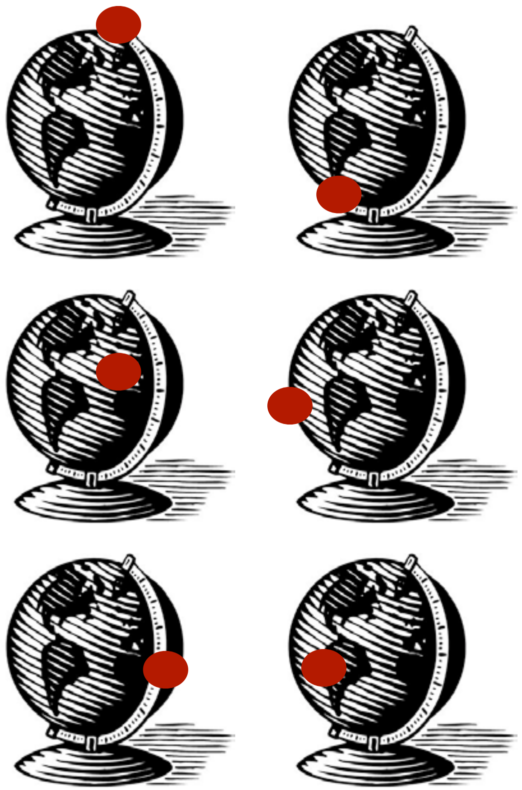
enclosed angle

- Measurement:
probabilistic and disturbing!
only 1 bit information,
but we can choose which!

Qubit

- $|\phi_0\rangle, |\phi_1\rangle$ orthonormal, i.e. antipodal

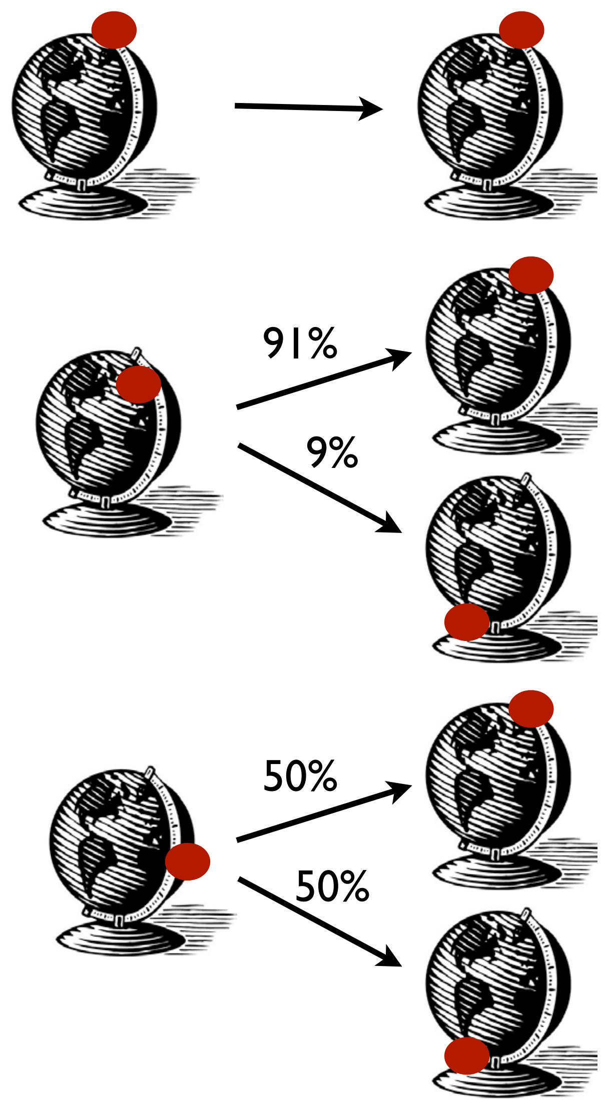
  $\Rightarrow$ measure, if state is in one of two antipodes:



- North or south pole?
- Madrid or Wellington?
- Bangkok or Lima?

Qubit

- State: North pole
  Measurement: North or south pole?
  Result: North pole
- State: Copenhagen
  Measurement: North or south pole?
  Result: North pole ($\text{Cos}^2\ 35°/2 \approx 91\%$)
- State: Singapore
  Measurement: North or south pole?
  Result: North pole ($\text{Cos}^2\ 90°/2 = 50\%$)



The projector

$|\psi\rangle$ → measurement of A → $i, |\phi_i\rangle$

$$\text{prob}[\text{outcome} = i] = |\langle\psi|\phi_i\rangle|^2$$
$$= \text{tr}|\psi\rangle\langle\psi||\phi_i\rangle\langle\phi_i|$$

observable consequences depend only on projector $|\psi\rangle\langle\psi|$

projector, trace = 1

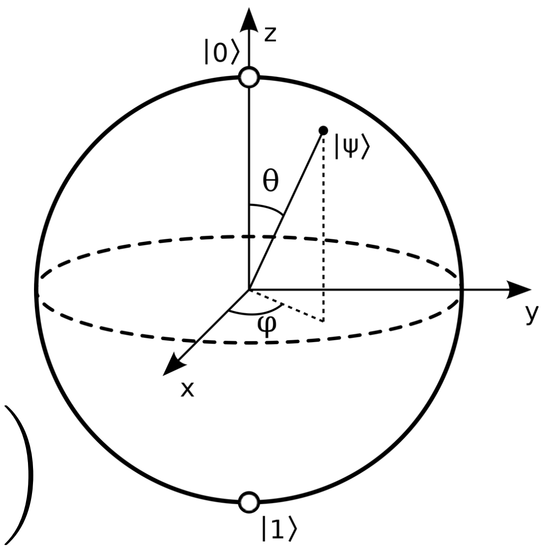
$$|\psi\rangle\langle\psi| = \frac{1}{2}\left(\mathbf{1} + \vec{r}\cdot\vec{\sigma}\right)$$

$$\vec{r}\cdot\vec{\sigma} = r_x\sigma_x + r_y\sigma_y + r_z\sigma_z$$

$$||r||_2 = 1$$

Pauli matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

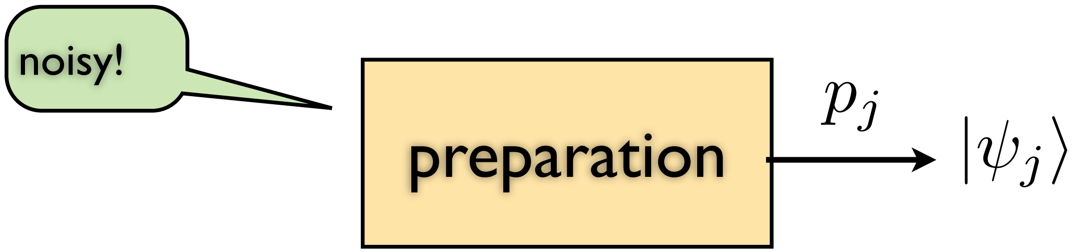


Mixed qubit

Mixed states: the problem

Incompleteness knowledge of the system:

we may have state $|\psi_j\rangle$ with probability p_j

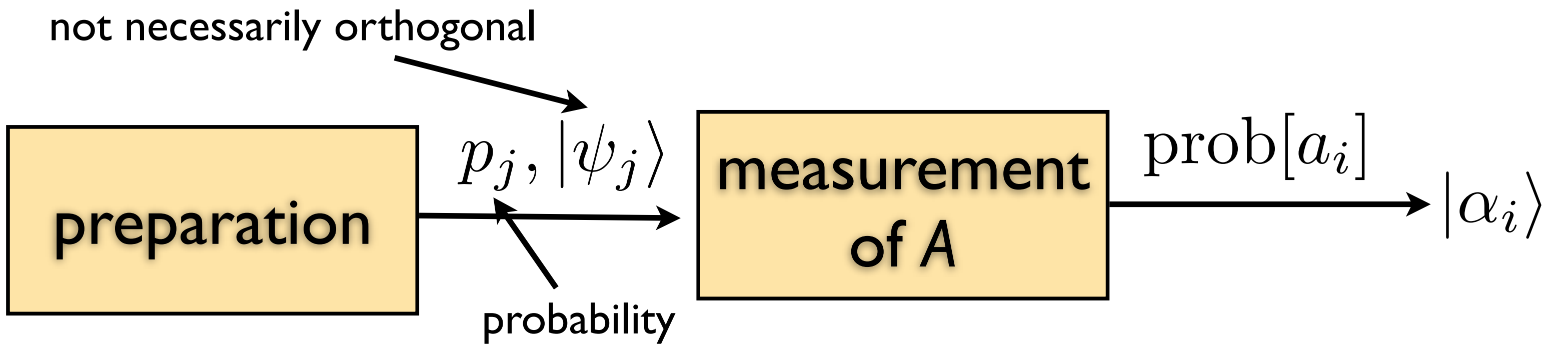


How to represent our knowledge of the state?

Let us see what happens if we measure the state...

Observable	Outcomes	Post-measurement states
A	$\{a_i\}$	$\{\|\alpha_i\rangle\}$

Mixed states: derivation



Probability of obtaining outcome a_i

$$
\begin{aligned}
\text{prob}[a_i] &= \sum_j p_j |\langle \alpha_i | \psi_j \rangle|^2 \\
&= \sum_j \text{tr}\Big[|\psi_j\rangle\langle\psi_j| \; |\alpha_i\rangle\langle\alpha_i| \Big] \\
&= \text{tr}\left[\underbrace{\left(\sum_j p_j |\psi_j\rangle\langle\psi_j| \right)}_{=\rho} |\alpha_i\rangle\langle\alpha_i| \right]
\end{aligned}
$$

The probability is only dependent on ρ

Density matrix

Incomplete knowledge of the system:

we may have state $|\psi_j\rangle$ with probability p_j

Description by density matrix

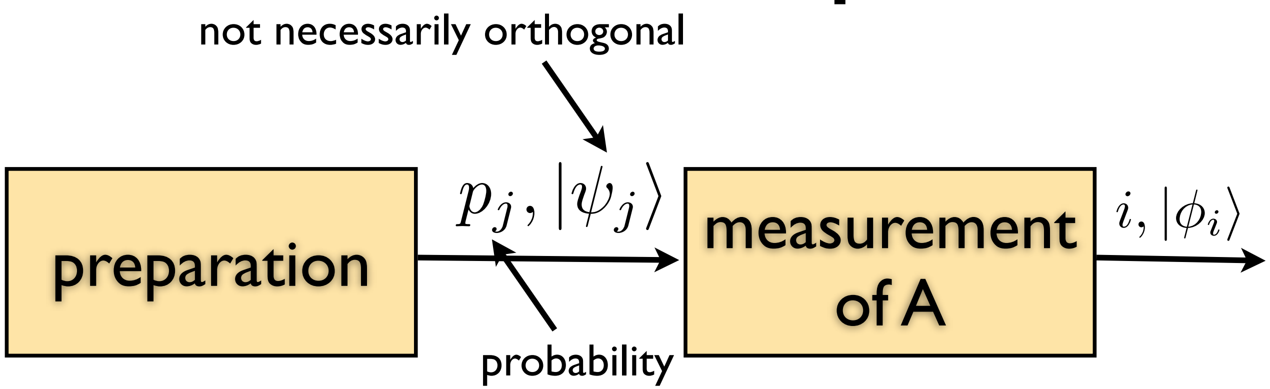
$$\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$$

Special case of a pure state: perfect knowledge

we have state $|\psi\rangle$ with probability 1

$$\rho = |\psi\rangle\langle\psi|$$

Bloch representation

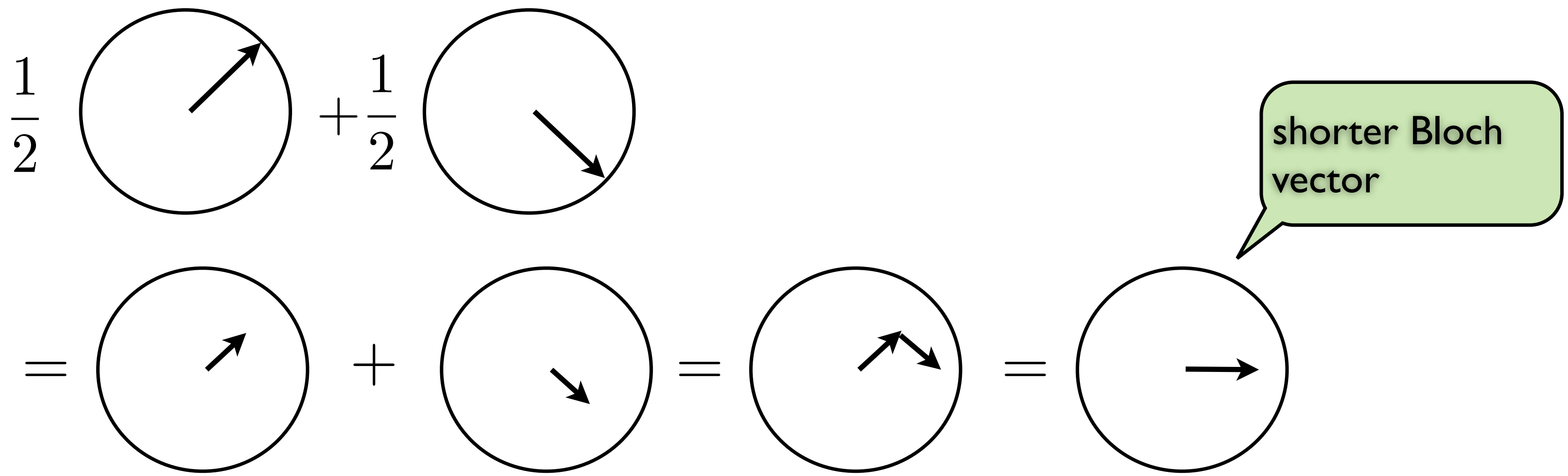


$$\mathrm{prob}[\mathrm{outcome} = i]$$

$$= \sum_i p_j \mathrm{tr} |\psi_j\rangle\langle\psi_j||\phi_i\rangle\langle\phi_i|$$

$$= \mathrm{tr}(\underbrace{\sum_i p_j |\psi_j\rangle\langle\psi_j|}_{=\rho})|\phi_i\rangle\langle\phi_i|$$

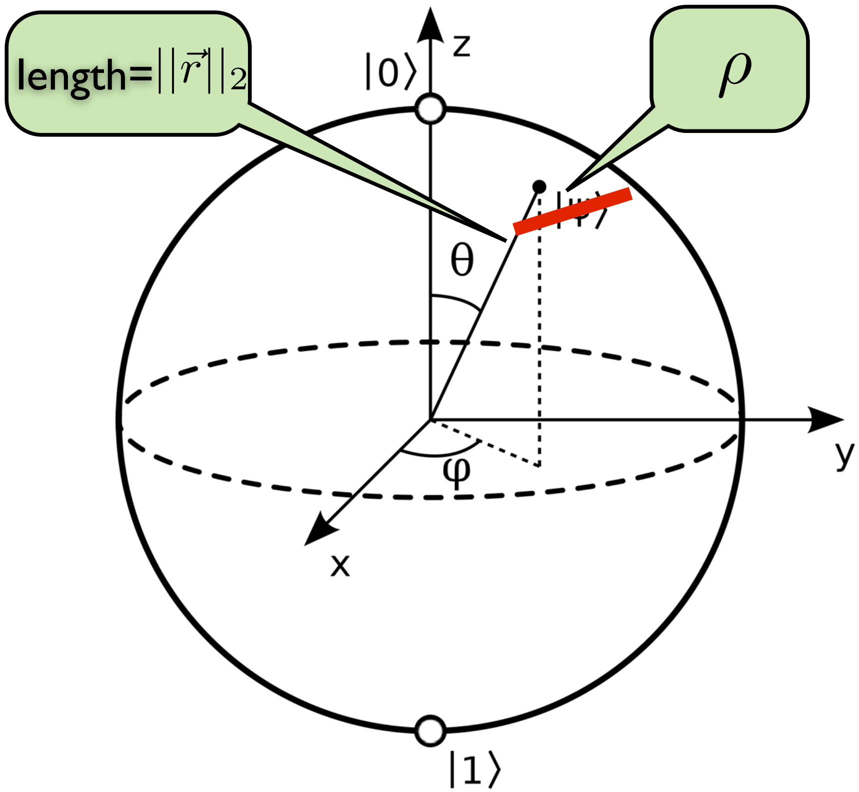
average of the Bloch vectors



Bloch ball

$$\rho = \frac{1}{2}\left(\mathbf{1} + \vec{r}\cdot\vec{\sigma}\right) \qquad \vec{r}\cdot\vec{\sigma} = \sum_i r_i \sigma_i$$

Pauli matrices



noise leads to shortening of Bloch vector

Properties of density matrices

In general,

$$\boxed{\rho \geq 0, \quad \mathrm{tr}\,\rho = 1}$$

positive semidefinite
(non-negative eigenvalues)

On the other hand, any state has an eigenvector decomposition

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \quad \forall \rho \in \mathcal{S}(\mathcal{H})$$

The density matrix describes all
the physical properties of a state!

How mixed is a state?

Measure of information: purity $\mathrm{tr}(\rho^2)$

Examples

$$\rho = |\psi\rangle\langle\psi| \quad \Rightarrow \quad \mathrm{tr}(\rho^2) = 1$$

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \quad \Rightarrow \quad \mathrm{tr}(\rho^2) = \frac{1}{2}$$

Other measures: entropies (later...)

Composed systems

Several Qubits

Hilbert space of 1 qubit

$$\mathcal{H}_1 = \mathbb{C}^2 = \text{span}\left\{|0\rangle, |1\rangle\right\} = \text{span}\left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\}$$

Hilbert space of n Qubits

$$\begin{aligned}\mathcal{H}_n &= \mathcal{H}_1 \otimes \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_1 = \mathcal{H}_1^{\otimes n}\\ &= \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2 = \mathbb{C}^{2^{\otimes n}}\\ &= \text{span}\left\{|i_1\ i_2 \ldots i_n\rangle\right\}_{i_j \in \{0,1\}}\\ &= \mathbb{C}^{2^n}\end{aligned}$$

Example: 2 qubits

$$
\begin{aligned}
\mathcal{H}_2 &= \mathbb{C}^2 \otimes \mathbb{C}^2 \\
&= \mathrm{span}\left\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\right\} \\
&= \mathrm{span}\left\{\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix}\right\} \\
&= \mathrm{span}\left\{\begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right\}
\end{aligned}
$$

Examples of normalized states

$$|\phi\rangle = |0\rangle \otimes |1\rangle =: |0\rangle|1\rangle =: |01\rangle$$

simplifying notation

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

d-dimensional systems

Hilbert space of dimension d

$$\mathcal{H} = \mathbb{C}^d = \mathrm{span}\left\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\right\}$$

Example: $d = 3$

$$\mathcal{H} = \mathbb{C}^3 = \mathrm{span}\left\{|0\rangle, |1\rangle, |2\rangle\right\}$$

$$|\psi\rangle = \frac{|0\rangle + |1\rangle - |2\rangle}{\sqrt{3}}$$

Mixed states on many qubits

Example: 2 qubits. Source prepares

- state $|\phi\rangle = |01\rangle$ with probability p
- state $|\psi\rangle = \dfrac{|01\rangle - |10\rangle}{\sqrt{2}}$ with probability $1-p$

Density matrix

$$\begin{aligned}
\rho &= p\ |\phi\rangle\langle\phi| + (1-p)\ |\psi\rangle\langle\psi| \\
&= p\ |01\rangle\langle 01| + (1-p)\ \frac{(|01\rangle - |10\rangle)(\langle 01| - \langle 10|)}{2} \\
&= \frac{1+p}{2}\ |01\rangle\langle 01| + \frac{1-p}{2}\,(-|01\rangle\langle 10| - |10\rangle\langle 01| + |10\rangle\langle 10|) \\
&= \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1+p & p-1 & 0 \\ 0 & p-1 & 1-p & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}
\end{aligned}$$

Density matrix of many qubits

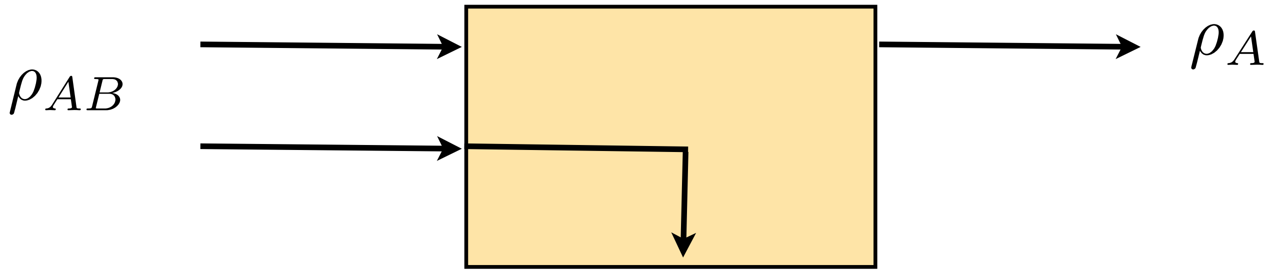
Mixed state of n qubits can be expanded in terms of Pauli matrices

$$\rho = \frac{1}{2^n} \sum_{i_j \in \{0,x,y,z\}} \underbrace{r_{i_1 \ldots i_n}}_{\in \mathbb{R}} \sigma_{i_1} \otimes \ldots \otimes \sigma_{i_n} \in \mathcal{M}_{2^n \times 2^n} \text{ with } \sigma_0 = \mathbb{1}$$

analogue of Bloch vector (not all vectors are allowed!)

Mixed states by forgetting: partial trace

If we forget (or do not have access to) the state of system *B*



Density matrix of *A* is given by the partial trace of ρ_{AB} over system *B*

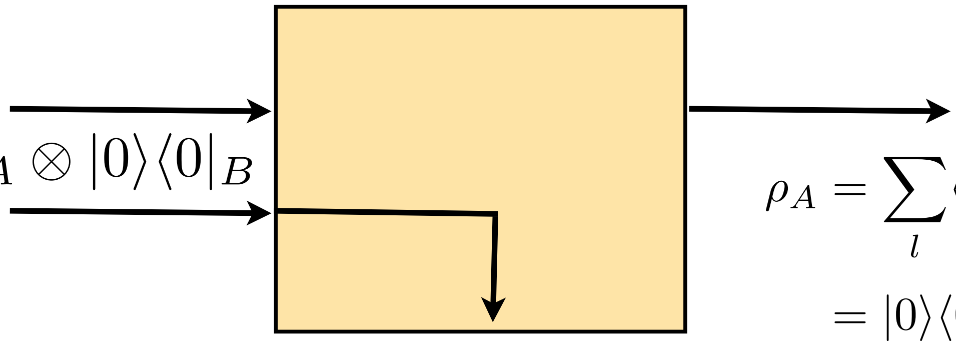
$$\rho_A = \mathrm{tr}_B\left(\rho_{AB}\right) = \sum_{k=0}^{|B|-1} \left(\mathbb{1}_A \otimes \langle k|_B\right)\ \rho_{AB}\ \left(\mathbb{1}_A \otimes |k\rangle_B\right)$$

Measurement statistics on *A* do not change

$$\mathrm{tr}\left(\rho_{AB}|\alpha\rangle\langle\alpha|_A \otimes \mathbb{1}_B\right) = \mathrm{tr}\left(\rho_A|\alpha\rangle\langle\alpha|_A\right)$$

Examples

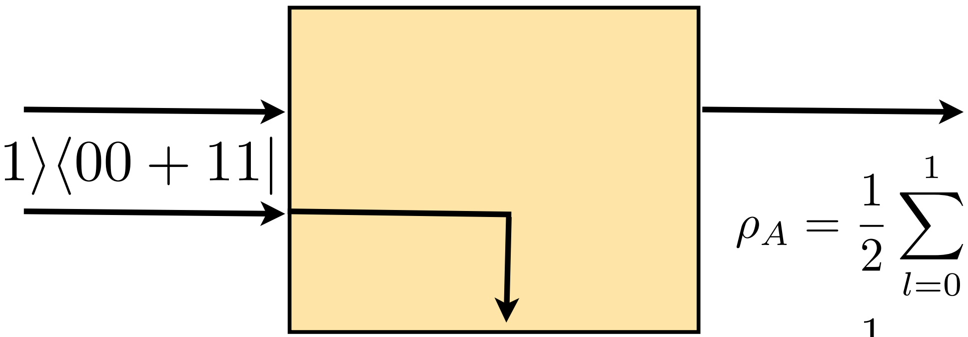
$$\rho_{AB} = |0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B$$



$$\rho_A = \sum_l \langle l|_B |0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B |l\rangle_B$$

$$= |0\rangle\langle 0| \sum_l \langle l|0\rangle\langle 0|l\rangle = |0\rangle\langle 0|$$

$$\rho_{AB} = \frac{1}{2}|00+11\rangle\langle 00+11|$$



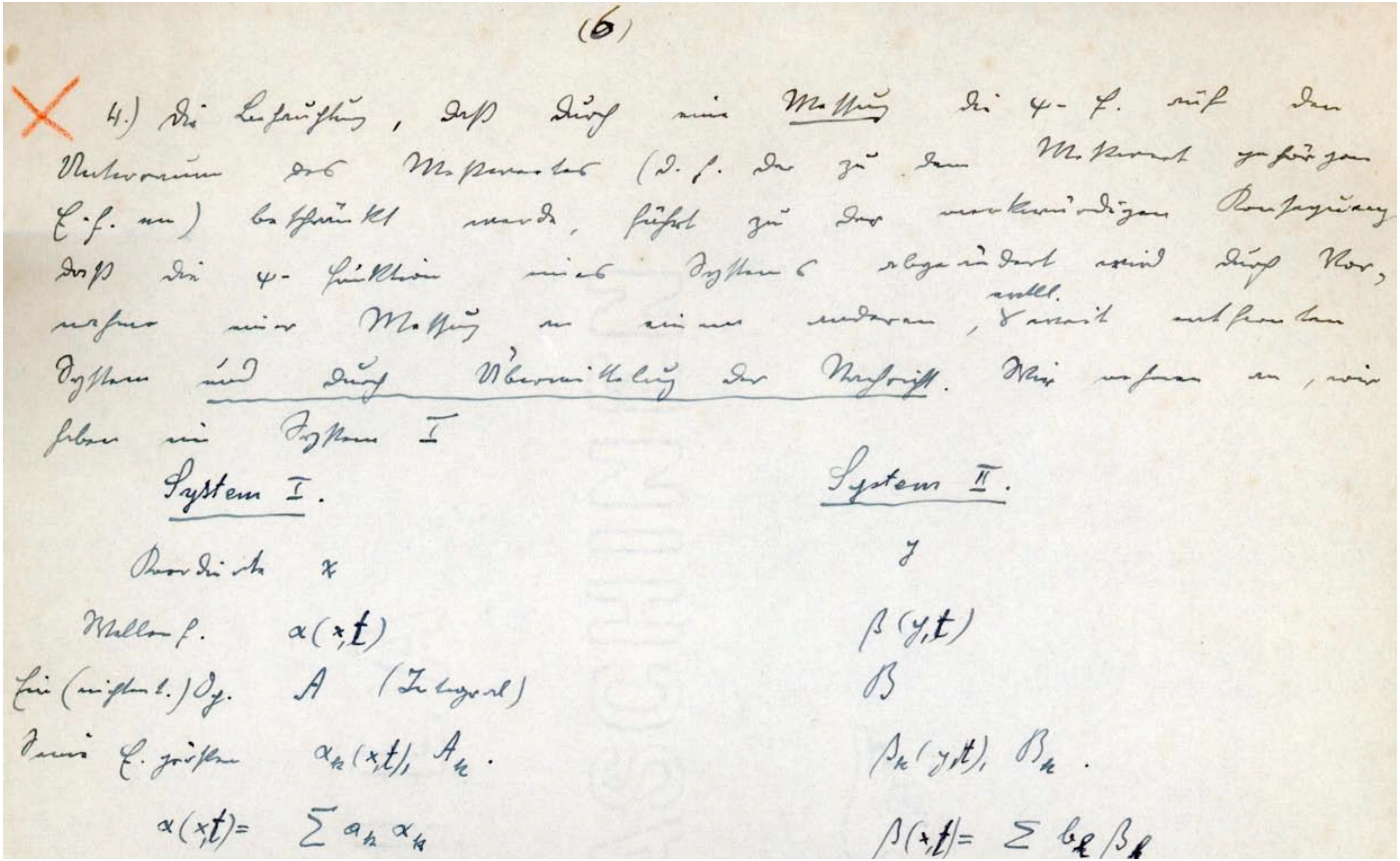
$$\rho_A = \frac{1}{2}\sum_{l=0}^{1} \langle l|_B |00+11\rangle\langle 00+11||l\rangle_B$$

$$= \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right)$$

We obtained a mixed state of one qubit from a (pure) state of two qubits by forgetting one qubit!

Entanglement

Schrödinger 1932

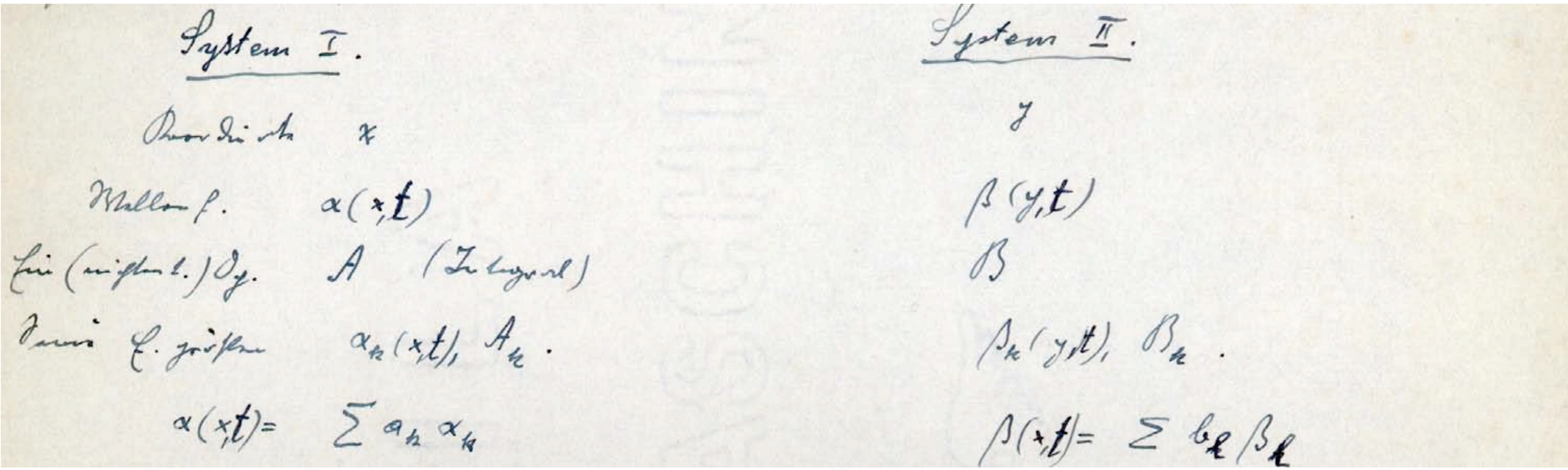

(6)

4.) Die Behauptung, daß durch eine Messung die ψ-F. auf den
Unterraum des Messwertes (d. h. die zu dem Messwert gehörigen
E.-f. en) beschränkt werde, führt zu der merkwürdigen Konsequenz
daß die ψ-Funktion eines Systems abgeändert wird durch Vor-,
nehmen einer Messung an einem anderen, damit mittel. verbundenen
System und durch Übermittelung der Vorschrift. Wir nehmen an, wir
haben ein System I

	System I.	System II.
Koordinate	x	y
Wellen f.	$\alpha(x,t)$	$\beta(y,t)$
Ein (vollständ.) Sy.	A (Integral)	B
Deren E. größen	$\alpha_k(x,t)$, A_k.	$\beta_k(y,t)$, B_k.
	$\alpha(x,t) = \sum a_k \alpha_k$	$\beta(x,t) = \sum b_k \beta_k$

Schrödinger 1932

The claim that the measurement restricts the ψ-function to the subspace belonging to the measurement result has the strange consequence that the ψ-function of a system is changed by the performance of a measurement on a different, far separated system and through the transmission of the message.



Schrödinger 1932

If we think of the two systems as a whole the ψ-function of this joint system is given by

$$\psi(x,y) = \sum_k \sum_l a_k b_l \alpha_k \beta_l$$

If we couple the systems for a short while and decouple them afterwards, the ψ-function acquires the form

$$\psi(x,y) = \sum_k \sum_l c_{kl} \alpha_k \beta_l$$

where in general $c_{kl} : c_{km} = c_{k'l} : c_{k'm}$ is not true. There remains a dependence, even if we separate the systems widely.

Schrödinger 1932

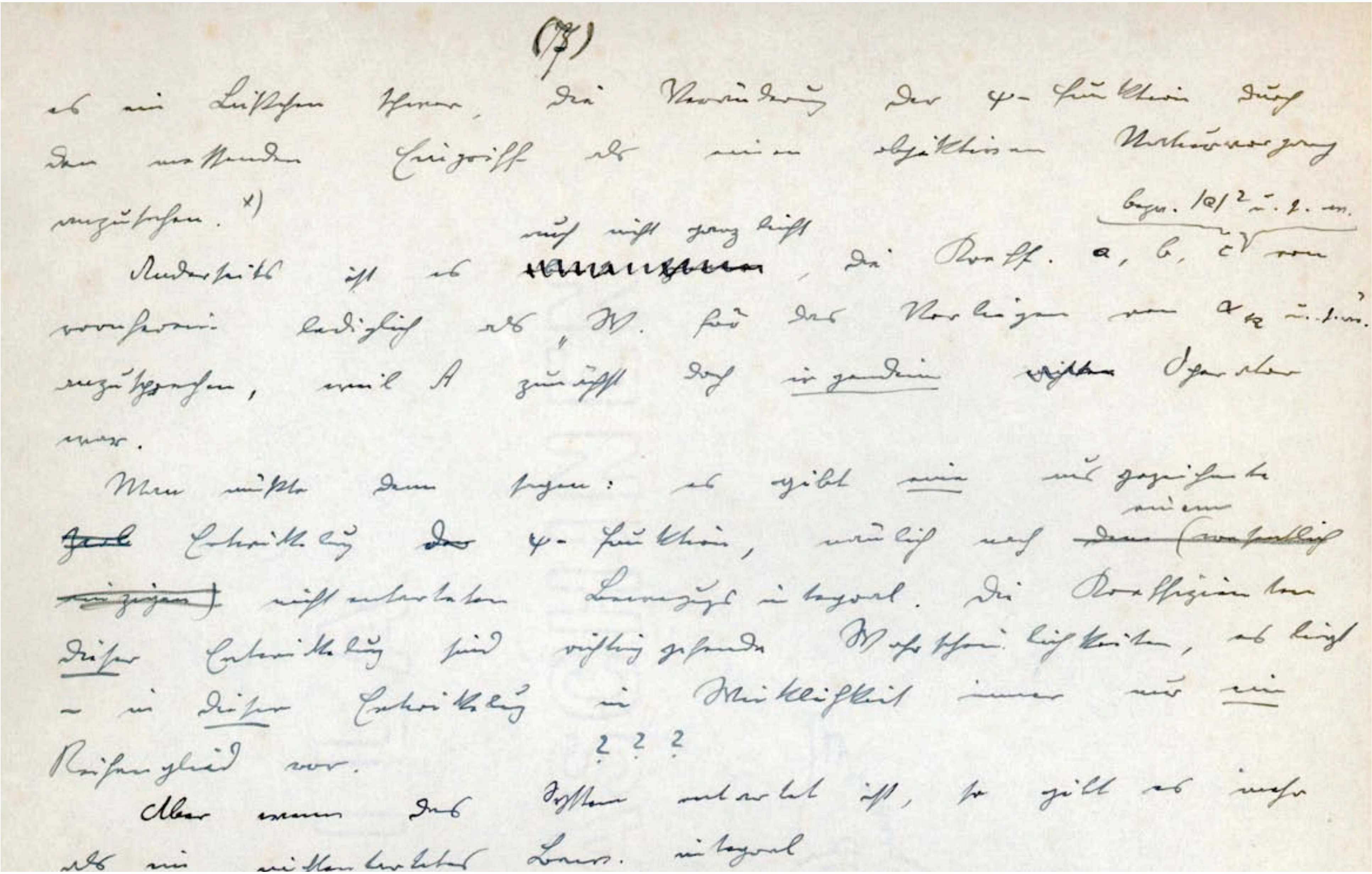
A subsequent measurement of the quantity B on system II transforms the joint ψ-function into

$$\psi(x, y) = C \cdot \sum_k c_{k\ell}\, \alpha_k \beta_\ell$$

which depends on the measured $\mathcal{B}_\ell$. This makes it a bit difficult to view the change in the ψ-function as a *Naturvorgang**

*the matter becomes even more strange, if we do not measure B on the American system, but if we measure a different, with B non-commuting integral.

Schrödinger 1932



Pure State Entanglement

Two systems A and B, finite-dimensional

$$A \cong \mathbb{C}^d, d \in \mathbb{N}, |A| := d, \qquad B \cong \mathbb{C}^{|B|}$$

Joint system

$$AB := A \otimes B \cong \mathbb{C}^{|A|} \otimes \mathbb{C}^{|B|} \cong \mathbb{C}^{|AB|}$$

$|\Psi\rangle_{AB} \in AB$ is called **separable** if $|\Psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi'\rangle_B$

otherwise it is called **entangled.**

Example: $|\Psi\rangle_{AB} = |0\rangle_A \otimes |0\rangle_B$ separable

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$$ entangled

Examples

$$|\psi\rangle = \frac{1}{\sqrt{2}} |00 + 11\rangle$$

Entangled state of n qubits

$$|\psi\rangle = \sum c_{i_1 i_2 \ldots i_n} |i_1\rangle |i_2\rangle \ldots |i_n\rangle$$

$$\text{with } c_{i_1 i_2 \ldots i_n} \in \mathbb{C} \text{ such that } \sum |c_{i_1 i_2 \ldots i_n}|^2 = 1$$

(Not equal to n Bloch spheres!)

When measuring n qubits one can extract at most n bits of information, Holevo‘s theorem (Holevo‘s theorem)

Mixed-State Entanglement

The density operator ρ is *separable* iff it can be decomposed into product states

$$\rho_{AB} = \sum_i p_i \ |\psi_i\rangle\langle\psi_i|_A \otimes |\psi_i\rangle\langle\psi_i|_B$$

Equivalent: for some probabilities p_i and density matrices ρ_A^i and ρ_B^i

$$\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i$$

Werner, 1989

If a state is not separable, we say it is entangled.

Example: Bell state

The wave function

$$\psi = \frac{1}{\sqrt{2}} |00\rangle + |11\rangle$$

corresponds to the density operator

$$\begin{aligned}
\rho &= \frac{1}{2} |00 + 11\rangle \langle 00 + 11| \\
&= \frac{1}{2}(|00\rangle \langle 00| + |00\rangle \langle 11| + |11\rangle \langle 00| + |11\rangle \langle 11| \\
&= \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

which is entangled.

Further Examples

Separable states

$$
\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}
\quad
\begin{pmatrix} \frac{1}{3} & 0 & 0 & \frac{1}{6} \\ 0 & \frac{1}{6} & 0 & 0 \\ 0 & 0 & \frac{1}{6} & 0 \\ \frac{1}{6} & 0 & 0 & \frac{1}{3} \end{pmatrix}
\quad
\begin{pmatrix} \frac{1}{4} & 0 & 0 & 0 \\ 0 & \frac{1}{4} & 0 & 0 \\ 0 & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{4} \end{pmatrix}
$$

Entangled state

$$
\begin{pmatrix} \frac{1}{8} & 0 & 0 & \frac{2}{8} \\ 0 & \frac{1}{8} & 0 & 0 \\ 0 & 0 & \frac{1}{8} & 0 \\ \frac{2}{8} & 0 & 0 & \frac{1}{8} \end{pmatrix}
$$

Entanglement Criteria

Excursion to current research

The Peres-Horodecki Criterion

$$\underbrace{\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i}_{\text{separable}} \xrightarrow{\text{transpose B}} \underbrace{\rho_{AB}^{\Gamma} = \sum_i p_i \rho_A^i \otimes (\rho_B^i)^T}_{\text{positive semidefinite}}$$

separable

positive semidefinite

Separability $\Rightarrow$ PPT (positive partial transpose)

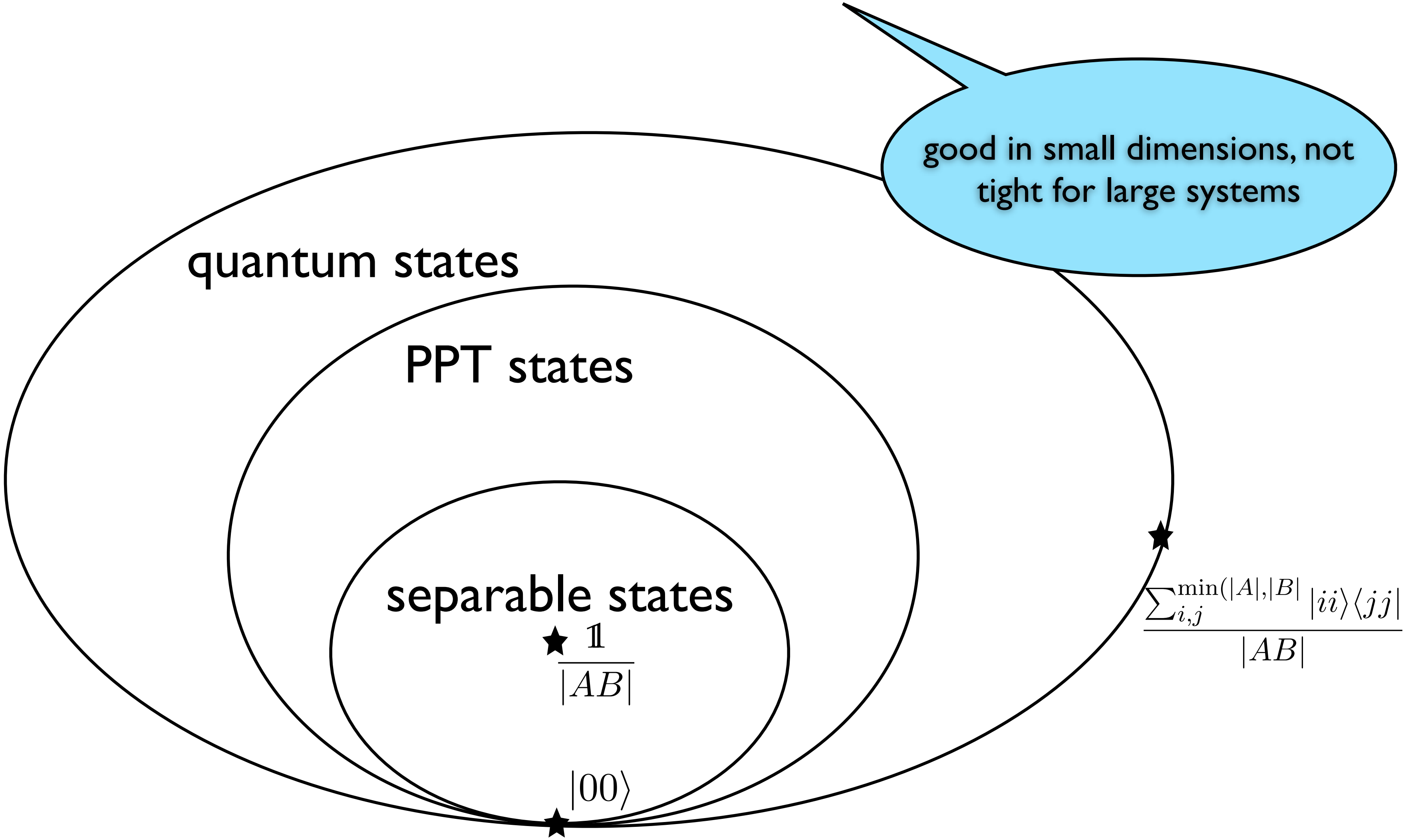
Separability $\not\Leftarrow$ PPT

$$\rho_{AB} = \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{pmatrix} \xrightarrow{\text{transpose B}} \rho_{AB}^{\Gamma} = \begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}$$

entangled

not positive semi-definite
entangled

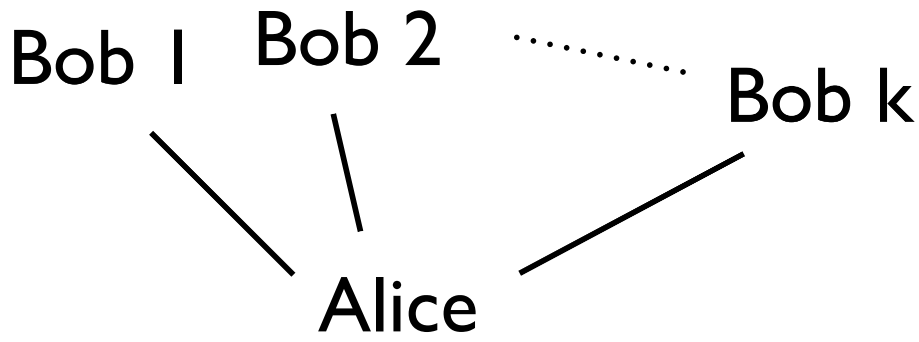
The Peres-Horodecki Criterion



A Hierarchy of Criteria

$$\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i \quad \substack{\Longrightarrow \\ \Longleftarrow} \quad \rho_{AB} \text{ has symmetric extension to arbitrarily many Bobs}$$

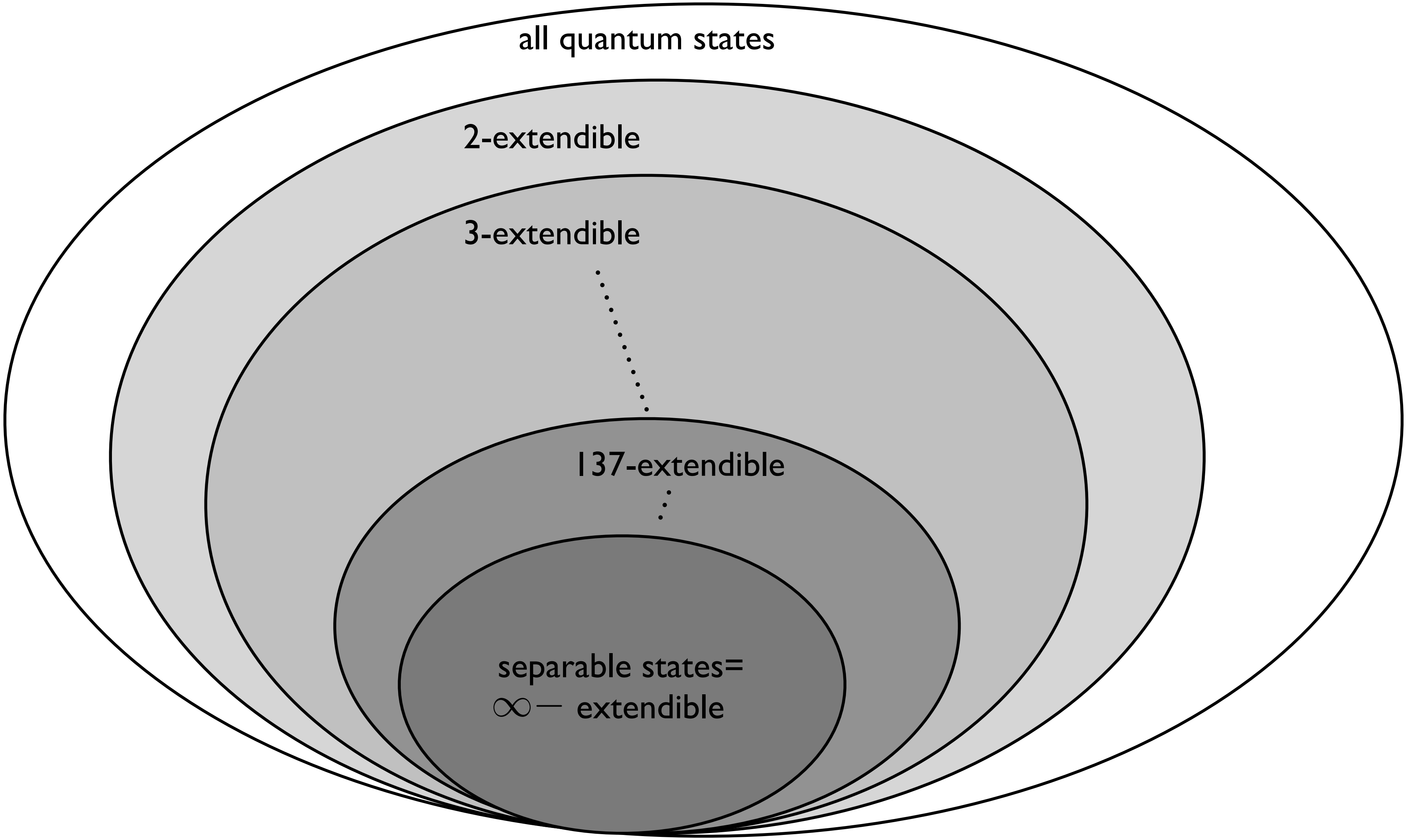
separable



$$\rho_{AB_1B_2\cdots B_k} = \sum_i p_i \rho_A^i \otimes \rho_{B_1}^i \otimes \rho_{B_2}^i \otimes \cdots \otimes \rho_{B_k}^i$$

de Finetti (1937); Diaconis & Freedman; Størmer, Hudson & Moody; Raggio & Werner; Caves, Fuchs & Schack; König & Renner, Christandl, König, Mitchison & Renner (2006)

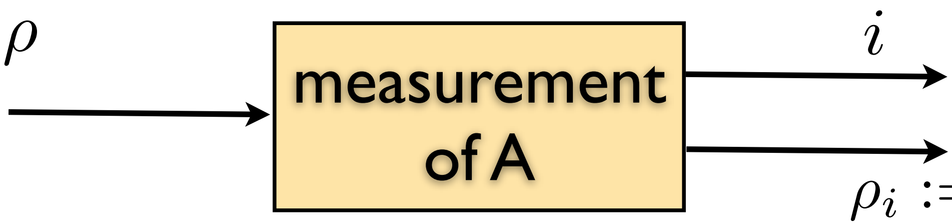
An active research field!



How close to separable is ρ_{AB} if a k-extension is found?
How long does it take to check if a k-extension exists?

Measurements and Time Evolution

Measurements



$$\rho_i := \frac{P_i \rho P_i}{\mathrm{prob}[i]}$$

$$\mathrm{prob}[i] = \mathrm{tr} P_i \rho$$

independent of eigenvalue

$$A = \sum_i a_i P_i$$

projector on to eigenspace
to i‘th eigenvalue

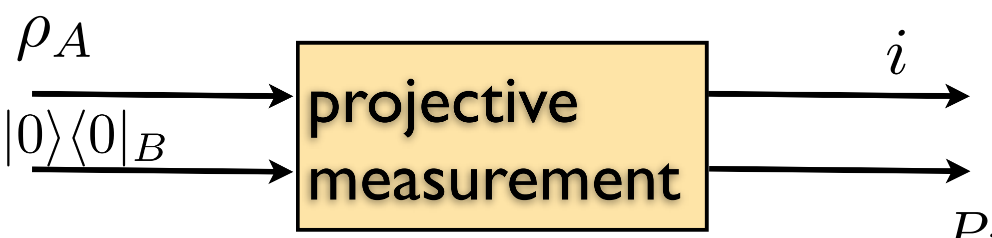
Labelling with eigenvalues often convenient,
but not necessary

projective measurement $\longleftrightarrow$ set of orthogonal projectors that sum to identity

$$\{P_i\}, P_i = P_i^\dagger, P_i^2 = P_i, \sum_i P_i = \mathrm{id}$$

Is this the most general measurement?

POVMs



$$\mathrm{prob}[i] = \mathrm{tr} P_i(\rho_A \otimes |0\rangle\langle 0|_B)$$
$$= \mathrm{tr}_A Q_i \rho_A$$

$$\rho_i := \frac{P_i(\rho_A \otimes |0\rangle\langle 0|_B)P_i}{\mathrm{prob}[i]}$$

$$Q_i = \langle 0|_B P_i |0\rangle_B$$

POVM

positive operator-valued measure

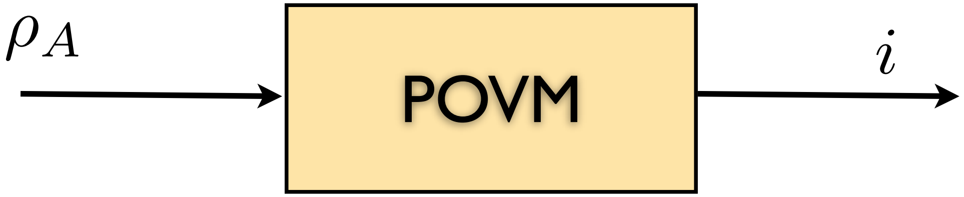
$\longleftrightarrow$ **set of positive-semidefinite operators that sum to identity**

$$\{Q_i\}, Q_i \geq 0, \sum_i Q_i = \mathrm{id}$$

$$\langle\phi|Q_i|\phi\rangle = \langle\phi|_A\langle 0|_B P_i|\phi\rangle_A|0\rangle_B \geq 0$$

$$\sum_i Q_i = \sum_i \langle 0|_B P_i|0\rangle_B$$
$$= \langle 0|_B(\sum_i P_i)|0\rangle_B$$
$$= \langle 0|_B \mathrm{id}_{AB}|0\rangle_B = \mathrm{id}_A$$

POVMs: Examples



$$\mathrm{prob}[i] = \mathrm{tr}_A Q_i \rho_A$$

$$\{Q_i\}, Q_i \geq 0, \sum_i Q_i = \mathrm{id}$$

Example 1: Mixture of two projective measurements

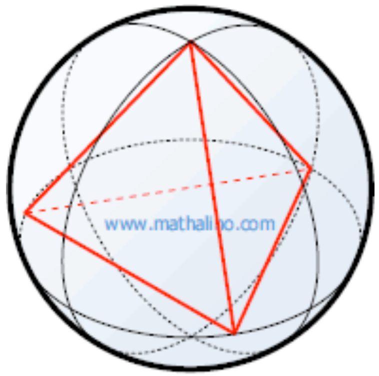
$$Q_0 = \frac{1}{2}|0\rangle\langle 0|, Q_1 = \frac{1}{2}|1\rangle\langle 1|, Q_3 = \frac{1}{2}|-\rangle\langle -|, Q_4 = \frac{1}{2}|-\rangle\langle -|$$

with 50% probability measure in z-direction
with 50% probability meaure in x-direction

Example 2: Tetrahedron

$$Q_i = \frac{1}{2}|\alpha_i\rangle\langle\alpha_i| = \frac{1}{2}\frac{1}{2}(\mathrm{id} + \vec{a}_i \cdot \vec{\sigma})$$

$$a_{0/1} = \sqrt{\frac{2}{3}}(\pm 1, 0, -\frac{1}{\sqrt{2}}), a_{2/3} = \sqrt{\frac{2}{3}}(0, \pm 1, \frac{1}{\sqrt{2}})$$



Time Evolution

$|\psi\rangle$ → time evolution → $e^{-iHt}|\psi\rangle$

with time-independent Hamiltonian
for a fixed amount of time

without loss of generality
(discretisation)

ρ → U → $U_t \rho U_t^\dagger$

Example: Qubit rotation

$$U_t = e^{it\vec{e}\cdot\frac{\vec{\sigma}}{2}} \qquad U_t \rho U_t^\dagger = \frac{1}{2}(\mathrm{id} + U_t(\vec{r}\cdot\vec{\sigma})U_t^\dagger) = \frac{1}{2}(\mathrm{id} + (R_t\vec{r})\cdot\vec{\sigma})$$

unit vector

Wunderformel

$R(\vec{e}, t)$

rotations in the Bloch sphere

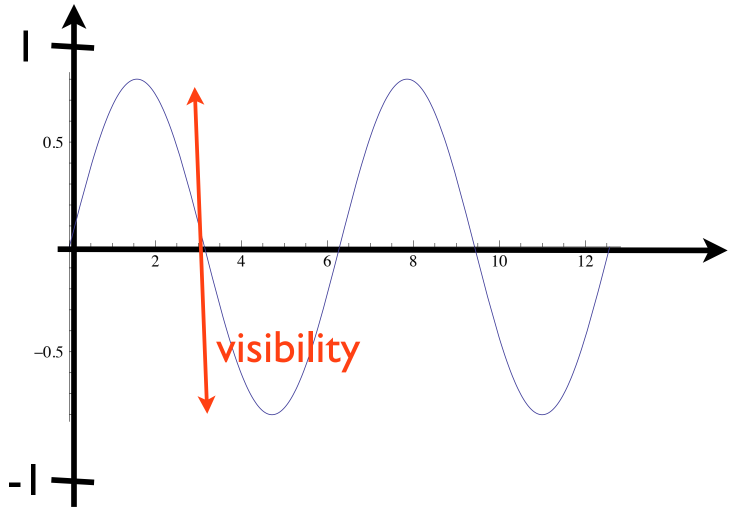
Rotations in the Bloch sphere

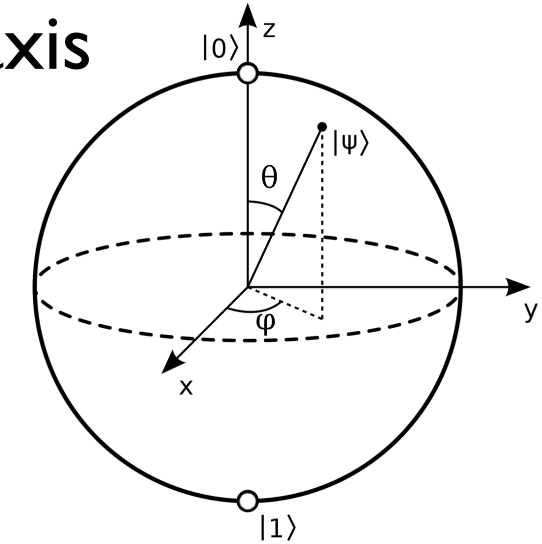
$$U_t = e^{it\vec{e}\cdot\frac{\vec{\sigma}}{2}} \qquad U_t \rho U_t^\dagger = \frac{1}{2}(\mathrm{id} + U_t(\vec{r}\cdot\vec{\sigma})U_t^\dagger) = \frac{1}{2}(\mathrm{id} + (R_t\vec{r})\cdot\vec{\sigma})$$

Example: magnetic field in x-direction, qubit in z-direction

qubit rotates around x-axis

$\mathrm{tr}\sigma_z\rho_t$





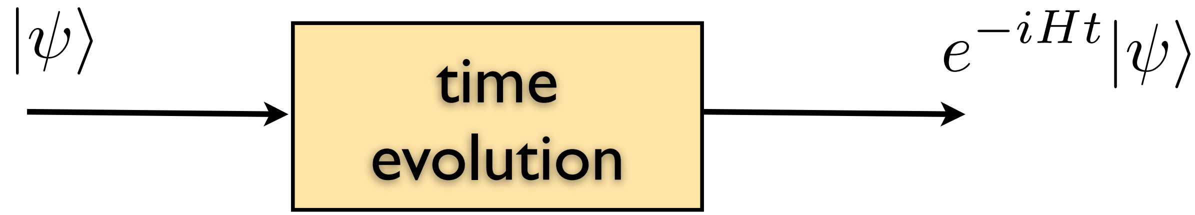
$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$$

Example: Hadamard transform

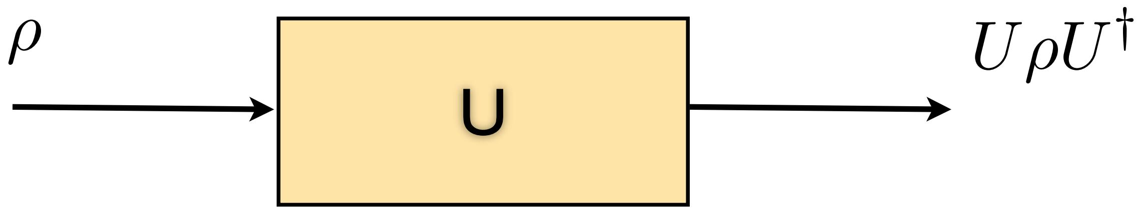
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{\sigma_x + \sigma_z}{\sqrt{2}} = ie^{i\pi(\frac{1}{\sqrt{2}},0,\frac{1}{\sqrt{2}})\cdot\frac{\vec{\sigma}}{2}}$$

Time Evolution



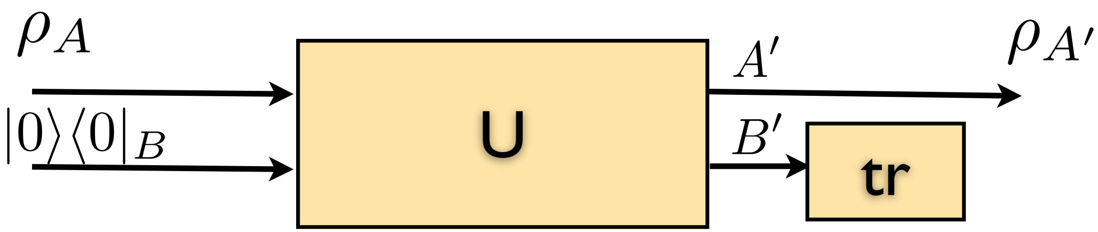
with time-independent Hamiltonian
for a fixed amount of time

without loss of generality
(discretisation)



Is this the most general evolution?

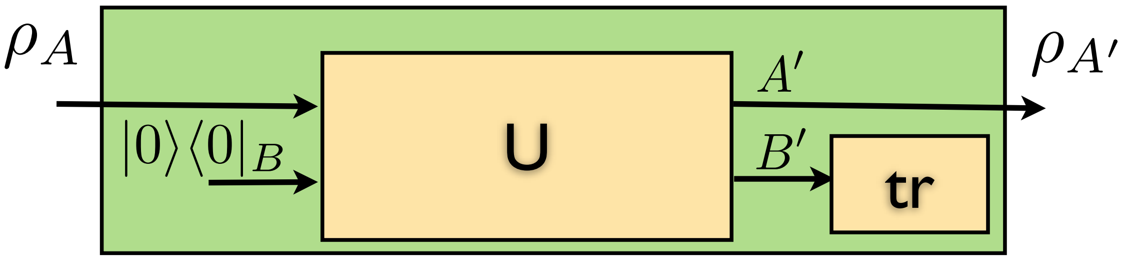
No: partial trace & measurement



$$\mathrm{tr}_{B'} U(\rho_A \otimes |0\rangle\langle 0|_B)U^\dagger$$

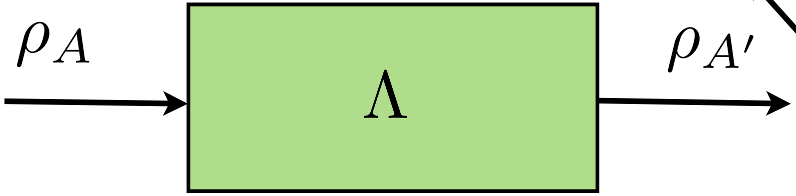
Physical Operations as CPTP Maps

CPTP maps



$$\mathrm{tr}_{B'} U(\rho_A \otimes |0\rangle\langle 0|_B) U^\dagger$$

completely positive trace-preserving map



$$\mathrm{tr}\Lambda(\rho_A) = \mathrm{tr}\rho_A$$

$$\Lambda(\rho_A) \geq 0, \text{for all } \rho_A \geq 0$$

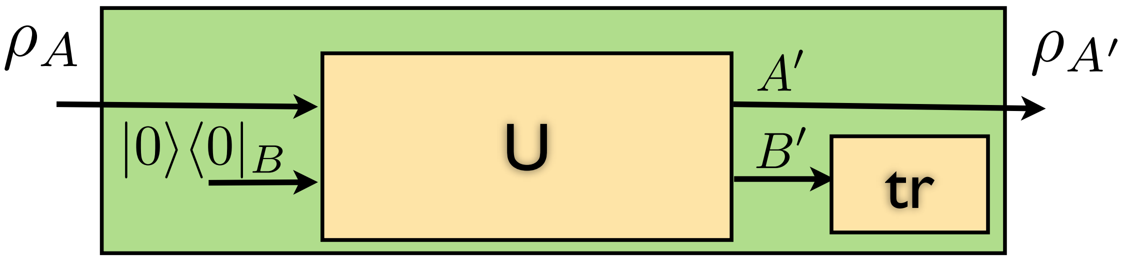
$$\Lambda \otimes \mathrm{id}_C(\rho_{AC}) \geq 0, \text{for all } \rho_{AC} \geq 0$$

for all C

Stinespring: Every CPTP map is of this form!

implies: every state evolution is unitary

Operator-Sum Representation

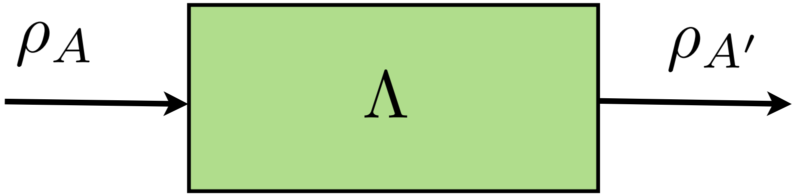


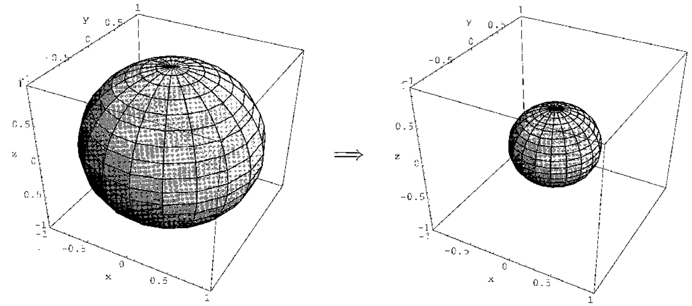
$$\Lambda(\rho_A) = \mathrm{tr}_{B'} U(\rho_A \otimes |0\rangle\langle 0|_B)U^\dagger = \sum_i \langle i|_{B'} U |0\rangle_B \rho_A \langle 0|_B U^\dagger |i\rangle_{B'}$$

$$= \sum_i E_i \rho_A E_i^\dagger$$

Kraus operators:
matrices, mapping A into A‘

CPTP maps: Examples





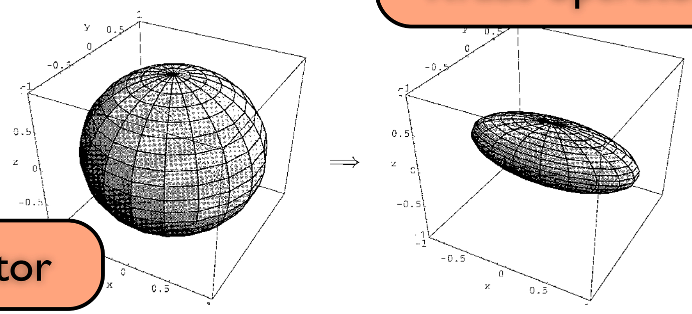
Depolarising channel

$$\Lambda(\rho) = (1-p)\rho + p\frac{1}{2}\mathbf{1} = (1-\frac{3}{4}p)\rho + \frac{1}{4}p(X\rho X + Y\rho Y + Z\rho Z)$$

Kraus operator

Bit flip channel

$$\Lambda(\rho) = (1-p)\rho + pX\rho X$$



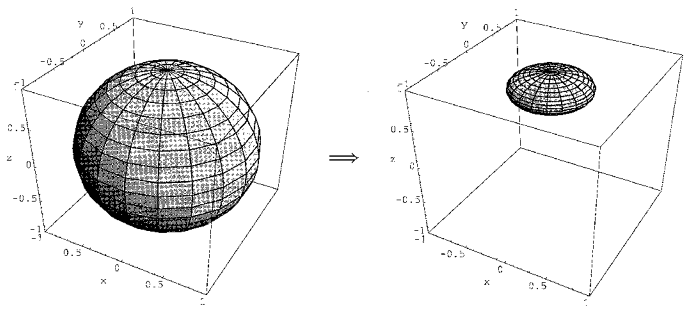
Phase flip channel

$$\Lambda(\rho) = (1-p)\rho + pZ\rho Z$$

Kraus operator

Amplitude damping channel

$$\Lambda(\rho) = E_0\rho E_0^\dagger + E_1\rho E_1^\dagger$$

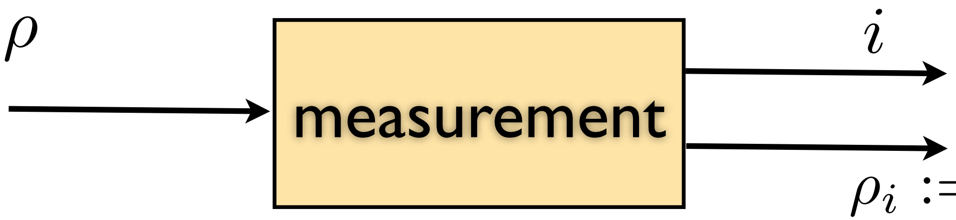


$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix} \qquad E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$$

Nielsen-Chuang, CUP 2001

Measurements as CPTP maps

for simplicity for projective ones only



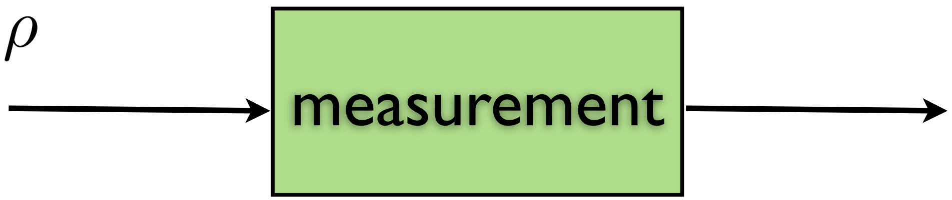
$$\rho_i := \frac{P_i \rho P_i}{\mathrm{prob}[i]} \qquad \mathrm{prob}[i] = \mathrm{tr} P_i \rho$$

$$\begin{aligned}\Lambda(\rho) &= \sum_i p_i |i\rangle\langle i| \otimes \rho_i \\ &= \sum_i |i\rangle\langle i| \otimes P_i \rho P_i\end{aligned}$$

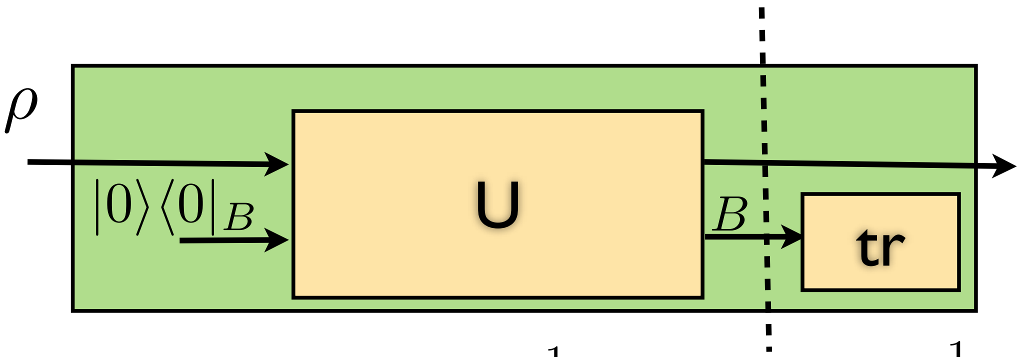
Example: z-axis

$$\Lambda(\rho) = (\mathrm{tr}|0\rangle\langle 0|\rho)|0\rangle\langle 0| + (\mathrm{tr}|1\rangle\langle 1|\rho)|1\rangle\langle 1| = \left(\begin{array}{cc} p_0 & 0 \\ 0 & p_1 \end{array} \right)$$

Entangled with Environment



$$\Lambda(\rho) = p_1|0\rangle\langle 0| + p_1|1\rangle\langle 1|$$



$\frac{1}{2}(|00\rangle + |11\rangle)$ $\qquad$ $\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$

decoherence is entanglement with environment

$$U = |00\rangle\langle 00| + |11\rangle\langle 10| + |01\rangle\langle 01| + |10\rangle\langle 11|$$

$$\rho = |+\rangle\langle +| \qquad |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Distinguishing Quantum States

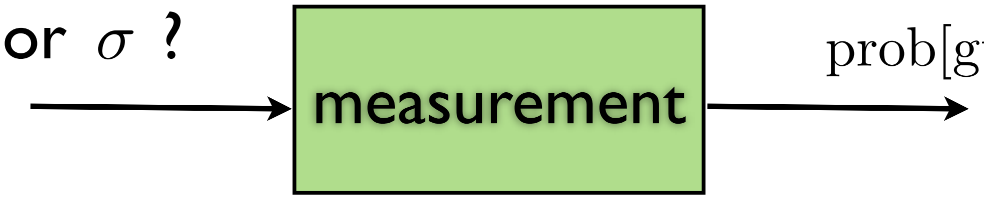
Distances

overlap or fidelity for pure states $|\langle\phi|\psi\rangle|$

overlap or fidelity for mixed states $F(\rho,\sigma) = \mathrm{tr}\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}$

symmetric!

ρ or σ ?



$$\text{prob[guess correctly]} = \frac{1}{2} + \frac{1}{4}||\rho - \sigma||_1$$

$$||\alpha||_1 = \mathrm{tr}\sqrt{\alpha\alpha^\dagger}$$

trace distance for mixed states $\frac{1}{2}||\rho - \sigma||_1$

Application of nonorthogonal states: The first idea for a quantum technology

Wiesner 1970's

This paper treats a class of codes made possible by restrictions on measurement related to the uncertainty principal. Two concrete examples and some general results are given.

Conjugate Coding *

Stephen Wiesner

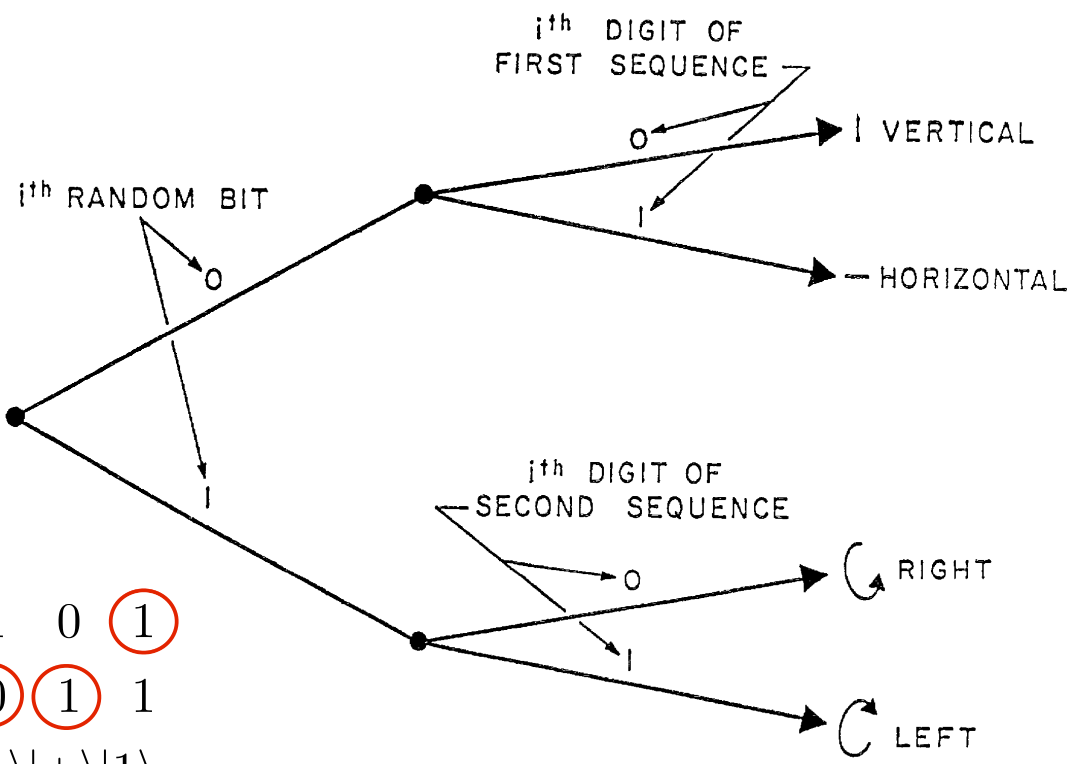
Columbia University, New York, N.Y.
Department of Physics

Wiesner Conjugate Coding

Example One: A means for transmitting two messages either but not both of which may be received.

half of the bits are received of one message, but nothing of the other

POLARIZATION OF i^{th} BURST



receiving first message= measuring vertical/ horizontal

receiving second message= measuring right/left

$0 \quad 1 \quad 0 \quad 1$

$1 \quad 0 \quad 1 \quad 1$

$|0\rangle|-\rangle|+\rangle|1\rangle$

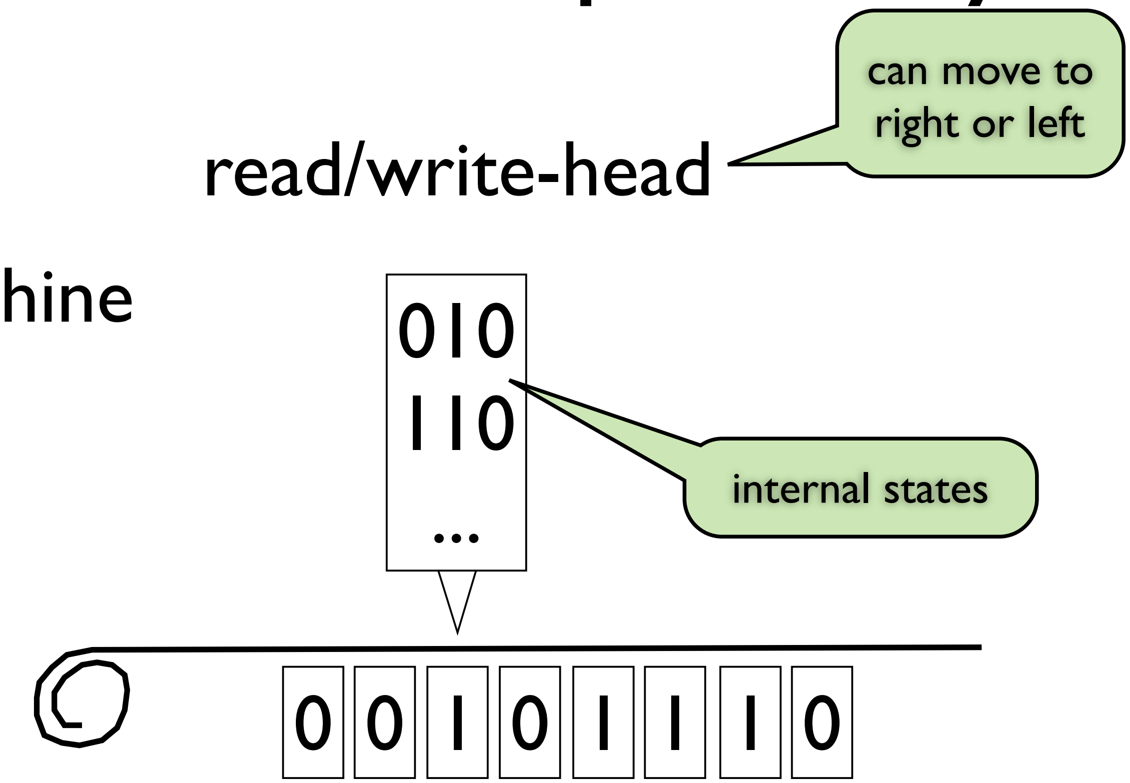
II. Quantum Computation

Computer Science: Computability

What is a computer?

Concept:

Universal Turing machine



Question:
Are all functions computable by the universal Turing machine?

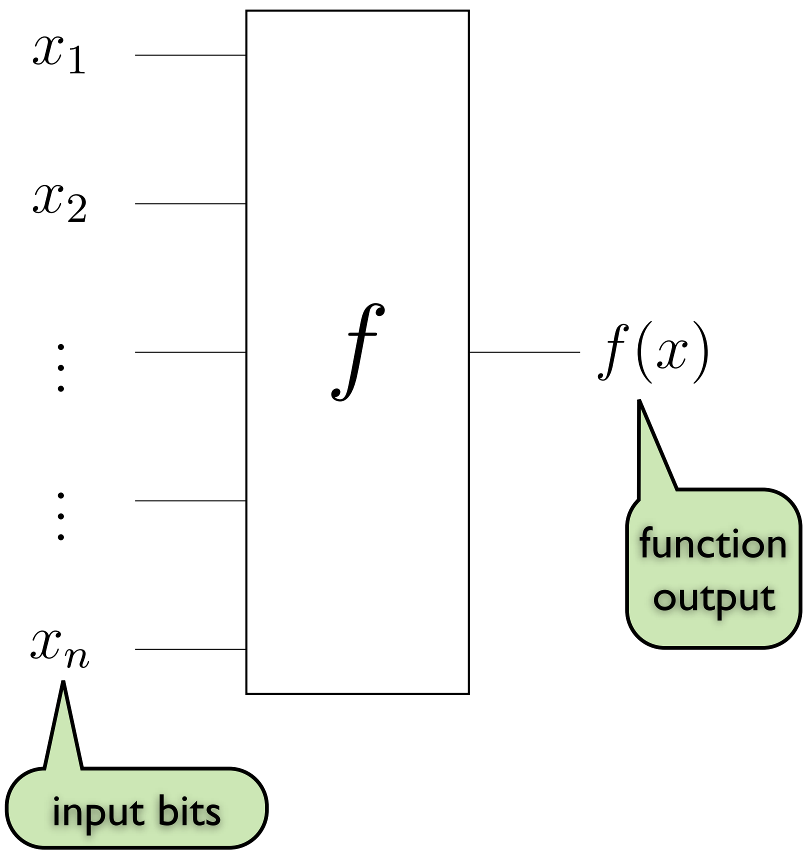
Answer: No!
Example: the function that asks whether the Turing machine halts for algorithm X on input 0

Circuit model

input length

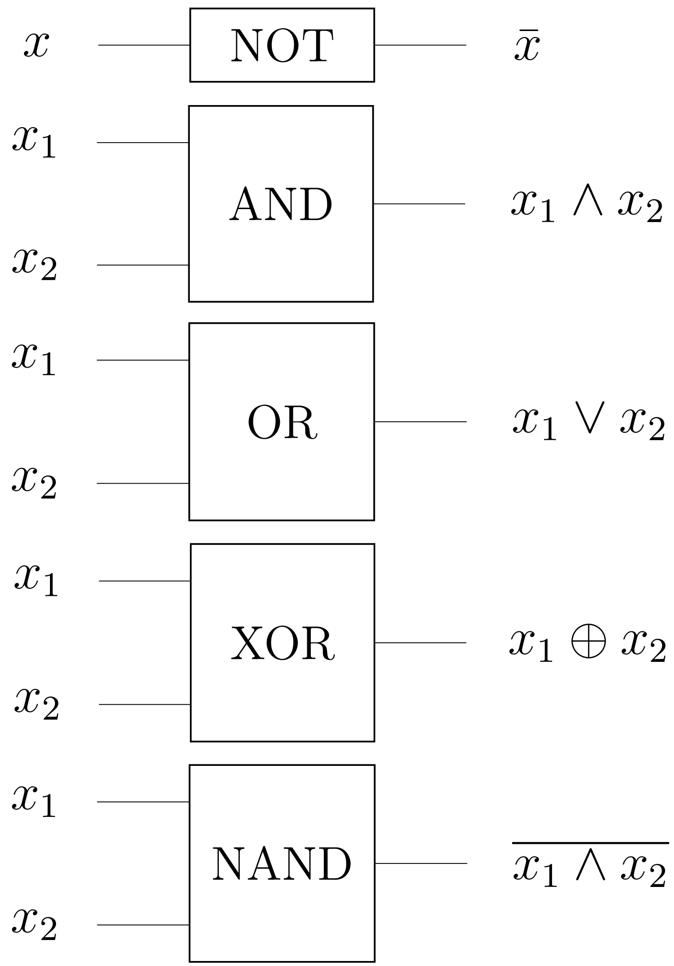
$$f : \{0,1\}^n \to \{0,1\}$$

Boolean function



Build-up for gates

Gate | **Truth table**



AND:

	0	1
0	0	0
1	0	1

OR:

	0	1
0	0	1
1	1	1

XOR:

	0	1
0	0	1
1	1	0

NAND:

	0	1
0	0	0
1	0	1

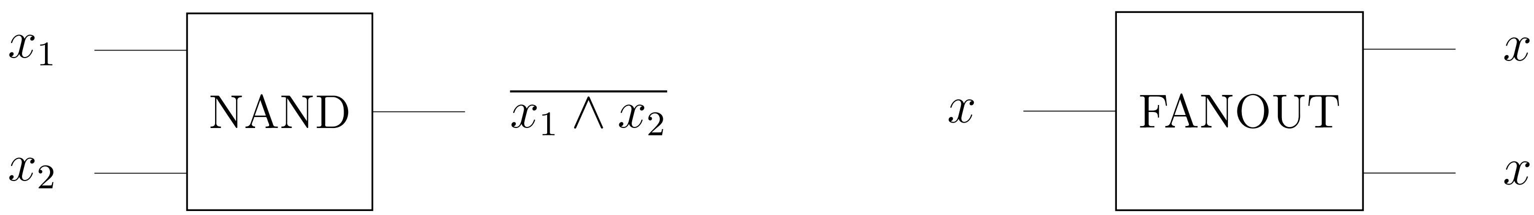
Classical universal set of gates

A set of gates is universal if for all n and for any Boolean function

$$f : \{0,1\}^n \to \{0,1\}$$

can be implemented by a circuit using only gates from the set and ancillas (additional wires with input bit 0).

Theorem: $\{\mathrm{NAND},\ \mathrm{FANOUT}\}$ form a universal set.



However...

- exp(n) gates are needed to compute an arbitrary function.
- The NAND gate is irreversible.

Computational Complexity

Given a function of input size n,
how long does it take to compute it?

Equivalent formulations

How many steps does the Turing machine have to do?
How many gates are needed?

Examples of functions

Addition

$$
\begin{array}{rr}
 & x_1 x_2 \dots x_n \\
+ & y_1 y_2 \dots y_n \\
\hline
= & z_0 z_1 z_2 \dots z_n
\end{array}
$$

Multiplying and factoring

$$z_1 z_2 \dots z_n = x_1 x_2 \dots x_n \times y_1 y_2 \dots y_n$$

Examples of complexity

Problem	#gates to solve	#gates to verify
addition given two numbers, what is their sum?	$O(n)$	$O(n)$
multiplication given two numbers, what is their product?	$O(n^2)$	$O(n^2)$
factoring given a number, what are its factors?	$\exp(O(n^{\frac{1}{3}} \times \text{poly}(\log n)))$	$O(n^2)$
3-SAT given an expression $(\bar{x}_1 \vee x_2 \vee x_3) \wedge (x_2 \vee \bar{x}_3 \vee x_4) \wedge \ldots$ is there an assignment of variables that makes it true?	$\exp(O(n))$	$\text{poly}(n)$

a claimed solution

these are upper bounds (sufficient #gates, for the best known algorithms)

Complexity Classes of Decision Problems

P: functions solved with poly(n) circuits

NP: functions verified with poly(n) circuits

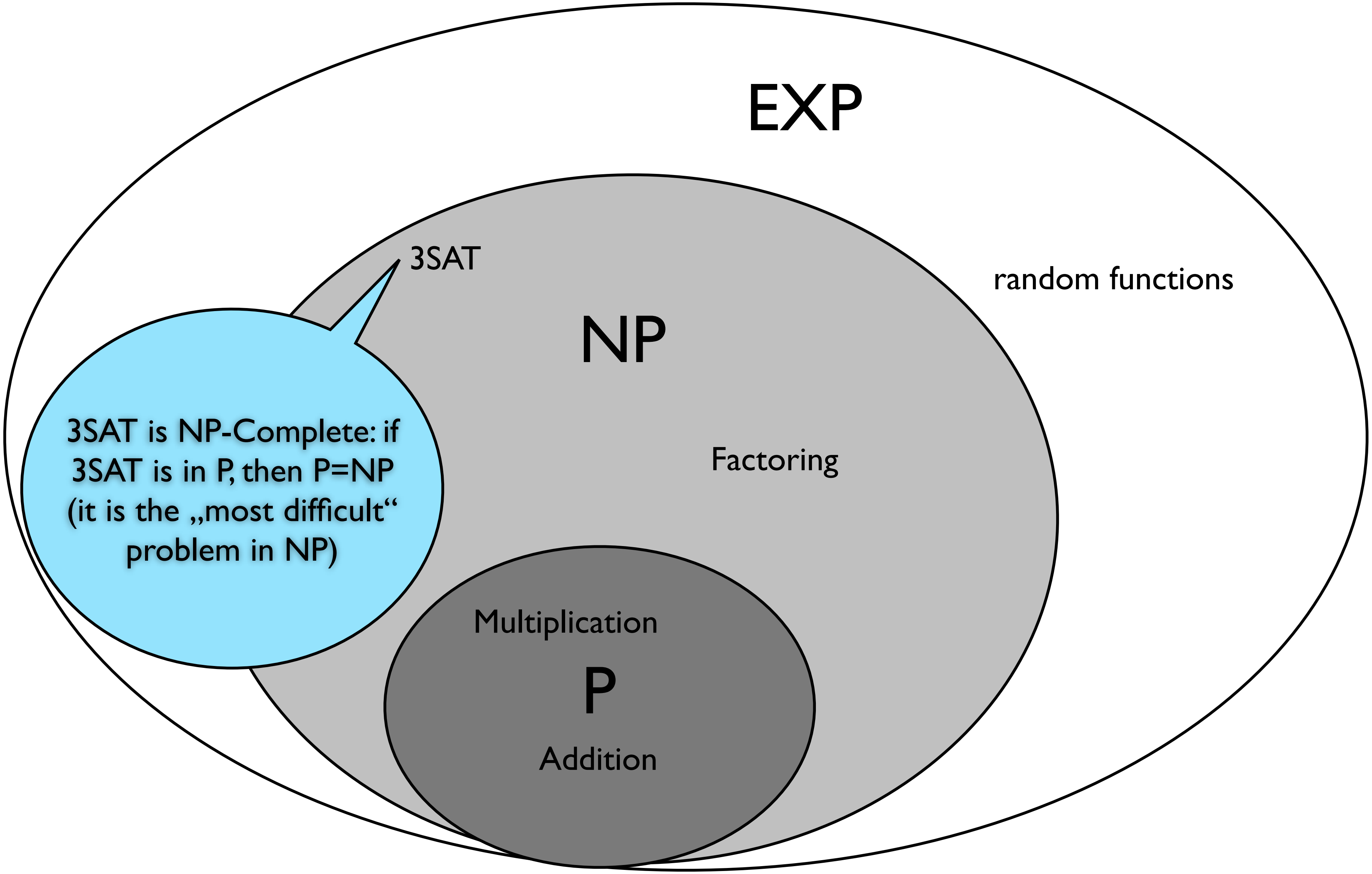
EXP: functions solved with exp(n) circuits

P is strictly smaller than EXP:

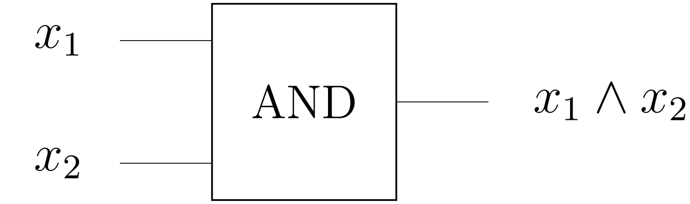
boolean functions with input size n : 2^{2^n}
(2 possible outputs for each of the 2^n input strings)

boolean functions implementable with circuit size $\mathrm{poly}(n)$:
$$\exp(\mathrm{poly}(n))$$

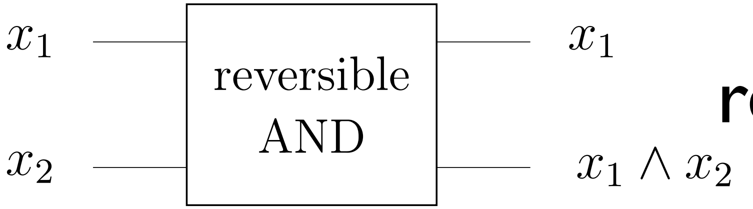
Complexity classes of Decision Problems



Reversible Computation



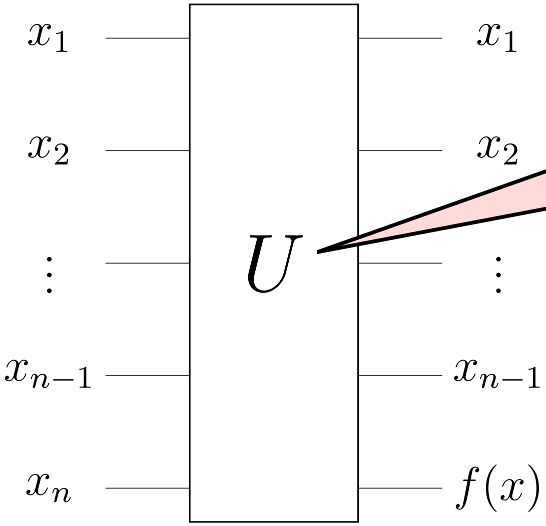
irreversible



reversible

Bennett: „Everything can be computed reversibly.“

Quantum computation



replace f by $U : (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$

potentially more possibilities than in classical computation

Single-qubit quantum gates

Pauli gates

$$\begin{matrix} |0\rangle \\ |1\rangle \end{matrix} \;—\boxed{\mathrm{X}}—\; \begin{matrix} |1\rangle \\ |0\rangle \end{matrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{matrix} |0\rangle \\ |1\rangle \end{matrix} \;—\boxed{\mathrm{Z}}—\; \begin{matrix} |0\rangle \\ -|1\rangle \end{matrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\begin{matrix} |0\rangle \\ |1\rangle \end{matrix} \;—\boxed{\mathrm{Y}}—\; \begin{matrix} -i|1\rangle \\ i|0\rangle \end{matrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Elementary rotations around x, y and z axes

(generated by the Pauli matrices)

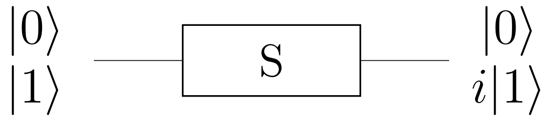
$$\begin{matrix} |0\rangle \\ |1\rangle \end{matrix} \;—\boxed{R_X(\theta)}—\; \begin{matrix} \cos(\frac{\theta}{2})|0\rangle - i\sin(\frac{\theta}{2})|1\rangle \\ -i\sin(\frac{\theta}{2})|0\rangle + \cos(\frac{\theta}{2})|1\rangle \end{matrix} \qquad R_x(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

$$\begin{matrix} |0\rangle \\ |1\rangle \end{matrix} \;—\boxed{R_Z(\theta)}—\; \begin{matrix} e^{-i\frac{\theta}{2}}|0\rangle \\ e^{i\frac{\theta}{2}}|1\rangle \end{matrix} \qquad R_z(\theta) = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}$$

$$\begin{matrix} |0\rangle \\ |1\rangle \end{matrix} \;—\boxed{R_Y(\theta)}—\; \begin{matrix} \cos\left(\frac{\theta}{2}\right)|0\rangle - \sin\left(\frac{\theta}{2}\right)|1\rangle \\ \sin\left(\frac{\theta}{2}\right)|0\rangle + \cos\left(\frac{\theta}{2}\right)|1\rangle \end{matrix} \qquad R_y(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

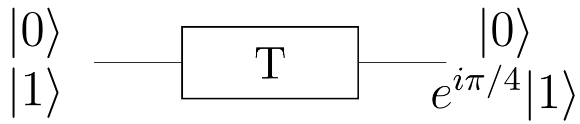
Single-qubit quantum gates

Phase gate



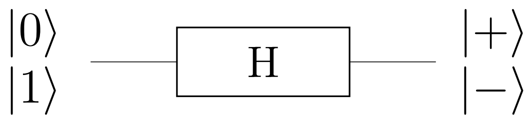
$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$\pi/8$ gate



$$T = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{pmatrix}$$

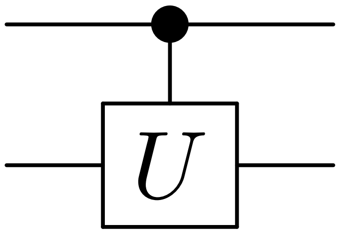
Hadamard gate



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

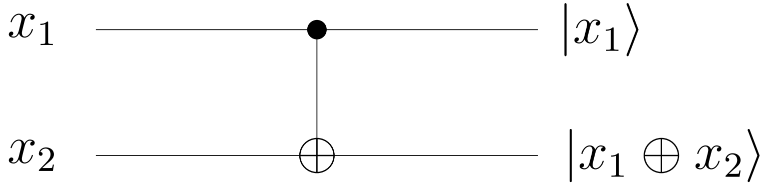
Controlled quantum gates

Controlled operation



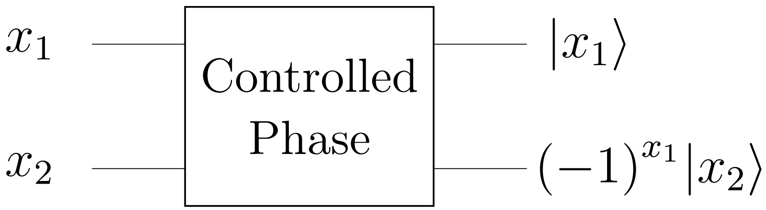
$$CU = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{pmatrix}$$

Controlled NOT Gate



$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Example: Controlled Phase Gate

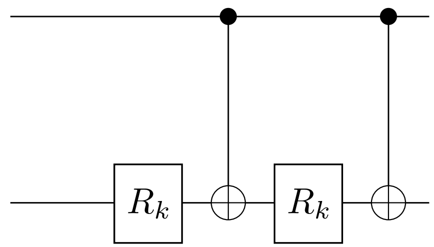


$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Universal quantum gates

A set of quantum gates is universal if any quantum operation acting on n qubits can be implemented by a circuit using only those gates and ancillas (additional qubits in state $|0\rangle$), for all *n*.

Theorem: CNOT and universal single qubit gates form a universal set (proof in exercise series 5).



Remark: This set is not finite (we need rotations for all angles).
However, it is possible to make a finite gate set approximately universal.

Quantum complexity classes

BQP is the class of functions $f^{(n)} : \{0,1\}^n \to \{0,1\}$
that can be computed with poly(n) quantum gates with

$$\mathrm{Prob}[success] \geq \frac{2}{3}$$

Theorem:

If an algorithm obtains the correct result with probability $\geq \dfrac{2}{3}$

we only need to repeat it $O(\log(1/\varepsilon))$ times
to succeed with probability $1 - \varepsilon$.

(proof uses majority vote and law of large numbers)

Quantum complexity classes