# Quantum Information: Part II

# *UC 2011*

Mika Hirvensalo

mikhirve@utu.fi

Department of Mathematics

University of Turku

FI-20014 Turku, Finland

# Structure of Quantum Mechanics

- State of a physical system: Unit-trace, positive operator $T$:

$$T = \lambda_1 \, |\boldsymbol{x}_1\rangle\langle\boldsymbol{x}_1\,| + \ldots + \lambda_n \, |\boldsymbol{x}_n\rangle\langle\boldsymbol{x}_n\,|,$$

  where $\lambda_i \geq 0$, $\lambda_1 + \ldots + \lambda_n = 1$ (density matrix).

- Observable: Self-adjoint operator $A$:

$$A = \mu_1 \, |\boldsymbol{y}_1\rangle\langle\boldsymbol{y}_1\,| + \ldots + \mu_n \, |\boldsymbol{y}_n\rangle\langle\boldsymbol{y}_n\,|,$$

  where $\mu_i \in \mathbb{R}$ are the potential values of $A$

- Minimal interpretation:

$$\mathbb{P}(\mu_i) = \mathrm{Tr}(T \, |\boldsymbol{y}_i\rangle\langle\boldsymbol{y}_i\,|)$$

  is the probability of seeing value $\mu_i$ if $A$ is observed when the system is in state $T$.

# Projection Postulate

For a state

$$T = \lambda_1 \, |\boldsymbol{x}_1\rangle\langle\boldsymbol{x}_1| + \ldots + \lambda_n \, |\boldsymbol{x}_n\rangle\langle\boldsymbol{x}_n|,$$

and observable

$$A = \mu_1 \, |\boldsymbol{y}_1\rangle\langle\boldsymbol{y}_1| + \ldots + \mu_n \, |\boldsymbol{y}_n\rangle\langle\boldsymbol{y}_n|$$

$$\mathbb{P}(\mu_i) = \mathrm{Tr}(T \, |\boldsymbol{y}_i\rangle\langle\boldsymbol{y}_i|).$$

If $\mu_i$ was observed, the post-observation state is

$$\frac{|\boldsymbol{y}_i\rangle\langle\boldsymbol{y}_i| \, T \, |\boldsymbol{y}_i\rangle\langle\boldsymbol{y}_i|}{\mathrm{Tr}(T \, |\boldsymbol{y}_i\rangle\langle\boldsymbol{y}_i|)}$$

(Projection postulate)

# Example

Let $n = 2$ (quantum bit), $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$$T = \frac{1}{2} \,|0\rangle\langle 0|\, + \frac{1}{2} \,|1\rangle\langle 1|= \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

and

$$A = \sigma_z = 1 \cdot \,|0\rangle\langle 0|\, - 1 \cdot \,|1\rangle\langle 1|\,.$$

Then

$$\begin{aligned} \mathbb{P}(1) &= \text{Tr}(T \,|0\rangle\langle 0|) = \text{Tr}(\frac{1}{2} \,|0\rangle\langle 0|) = \frac{1}{2}, \text{ and} \\ \mathbb{P}(-1) &= \text{Tr}(T \,|0\rangle\langle 0|) = \text{Tr}(\frac{1}{2} \,|0\rangle\langle 0|) = \frac{1}{2}. \end{aligned}$$

# Example

$$T = 1 \cdot \, |0\rangle\langle 0| \, + 0 \cdot \, |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

and

$$A = \sigma_z = 1 \cdot \, |0\rangle\langle 0| \, - 1 \cdot \, |1\rangle\langle 1| \, .$$

Then

$$\begin{aligned} \mathbb{P}(1) &= \text{Tr}(T \, |0\rangle\langle 0|) = \text{Tr}(1 \, |0\rangle\langle 0|) = 1, \text{ and} \\ \mathbb{P}(-1) &= \text{Tr}(T \, |1\rangle\langle 1|) = \text{Tr}(0) = 0. \end{aligned}$$

# Example

$$T = \frac{1}{2}\,|\,0\rangle\langle 0\,| + \frac{1}{2}\,|\,1\rangle\langle 1\,| = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

and

$$A = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 1\cdot\,|\,\boldsymbol{y}_1\rangle\langle\boldsymbol{y}_1\,| - 1\cdot\,|\,\boldsymbol{y}_2\rangle\langle\boldsymbol{y}_2\,|,$$

where $\boldsymbol{y}_1 = \frac{1}{\sqrt{2}}(1,1)$ and $\boldsymbol{y}_2 = \frac{1}{\sqrt{2}}(1,-1)$. Then

$$\begin{aligned} \mathbb{P}(1) &= \mathrm{Tr}(T\,|\,\boldsymbol{y}_1\rangle\langle\boldsymbol{y}_1\,|) = \frac{1}{2}, \text{ and} \\ \mathbb{P}(-1) &= \mathrm{Tr}(T\,|\,\boldsymbol{y}_2\rangle\langle\boldsymbol{y}_2\,|) = \frac{1}{2}. \end{aligned}$$

# Remark

The *expected value* of observable $A$ in state $T$ is

$$\begin{aligned} \mathbb{E}_T(A) &= \sum_{i=1}^{n} \mu_i \mathbb{P}(\mu_i) \\ &= \sum_{i=1}^{n} \mu_i \mathsf{Tr}(T \,|\boldsymbol{y}_i\rangle\langle\boldsymbol{y}_i|) \\ &= \mathsf{Tr}(TA). \end{aligned}$$

# The State Set Structure

- If $T_1$ and $T_2$ are states, and $\lambda \in (0, 1)$, then also $\lambda T_1 + (1 - \lambda)T_2$ is. (convexity)
- $T$ is *extremal* if $T = \lambda T_1 + (1 - \lambda)T_2$ with $\lambda \in (0, 1)$ implies $T_1 = T_2$.
- Extremals are called *pure or vector states*
- Lemma: $T$ is pure if and only if $T = | \boldsymbol{x} \rangle\langle \boldsymbol{x} |$ for some unit-length $\boldsymbol{x}$.
- For a pure state $T = | \boldsymbol{x} \rangle\langle \boldsymbol{x} |$ and observable $A = \sum_{i=1}^{n} \mu_i \, | \boldsymbol{y}_i \rangle\langle \boldsymbol{y}_i |$

$$\mathbb{P}(\mu_i) = \mathrm{Tr}(T \, | \boldsymbol{y}_i \rangle\langle \boldsymbol{y}_i |) = |\langle \boldsymbol{x} \mid \boldsymbol{y}_i \rangle|^2 .$$

# Pure states

Let $T = |\boldsymbol{x}\rangle\langle\boldsymbol{x}|$ be a pure state and

$$A = \mu_1 \, |\boldsymbol{y}_1\rangle\langle\boldsymbol{y}_1| + \ldots + \mu_n \, |\boldsymbol{y}_n\rangle\langle\boldsymbol{y}_n|$$

an observable. In representation

$$\boldsymbol{x} = \alpha_1 \boldsymbol{y}_1 + \ldots + \alpha_n \boldsymbol{y}_n$$

$\alpha_i = \langle \boldsymbol{y}_i \mid \boldsymbol{x} \rangle$ (amplitude of $\boldsymbol{y}_i$), so

$$\mathbb{P}(\mu_i) = |\alpha_i|^2 \, .$$

Corollary: For each pure state $T$ there is a nontrivial observable $A$ such that $\mathbb{P}(\mu_1) = 1$ for a potential value $\mu_1$ of $A$.

# Remark

For a pure state $T = |\boldsymbol{x}\rangle\langle\boldsymbol{x}|$ the expected value of observable $A$ is

$$\mathbb{E}_T(A) = \mathrm{Tr}(TA) = \mathrm{Tr}(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|\, A) = \langle\boldsymbol{x} \mid A\boldsymbol{x}\rangle.$$

# Example

Let $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

vector $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ corresponds to a state

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \otimes (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}) = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix},$$

but vector representation gives that for
$A = 1\cdot |0\rangle\langle 0| - 1\cdot |1\rangle\langle 1|$ we have

$$\mathbb{P}(1) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} = \mathbb{P}(-1).$$

# Example

Let $\boldsymbol{y}_1 = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\boldsymbol{y}_2 = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, and

$$A = 1\ |\boldsymbol{y}_1\rangle\langle\boldsymbol{y}_1|\ -1\cdot\ |\boldsymbol{y}_2\rangle\langle\boldsymbol{y}_2|\ .$$

Vector state $\boldsymbol{x} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ can then be written as

$$\boldsymbol{x} = 1 \cdot \boldsymbol{y}_1 + 0 \cdot \boldsymbol{y}_2,$$

so

$$\mathbb{P}(1) = 1 \quad \text{and} \quad \mathbb{P}(-1) = 0.$$

# Quantum Bit (Qubit)

Quantum Bit = Two-level quantum system

- $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ is called *computational basis*.
- Computational basis $\leftrightarrow$ preferred observable

$$A = v_0 \, |0\rangle\langle 0| + v_1 \, |1\rangle\langle 1|, \qquad (v_0 \neq v_1)$$

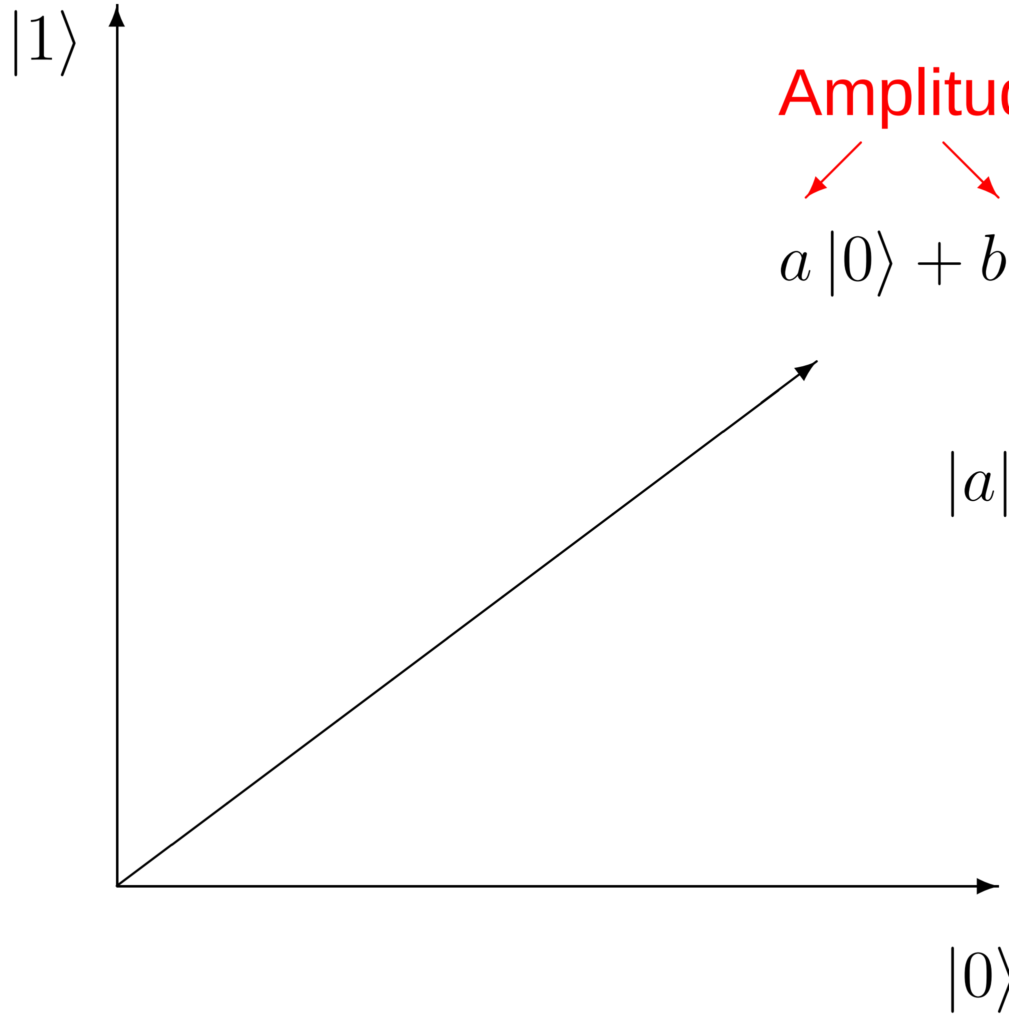
"*(Vector) state*

$$\psi = \alpha_0 \, |0\rangle + \alpha_1 \, |1\rangle \,,$$

*observed*" refers to observable $A$:

$$\mathbb{P}(|0\rangle) = \mathbb{P}(v_0) = |\alpha_0|^2 \quad \text{and} \quad \mathbb{P}(|1\rangle) = \mathbb{P}(v_1) = |\alpha_1|^2$$

# Quantum Bit (Qubit)




Amplitudes

$a\,|0\rangle + b\,|1\rangle$

Superposition of $|0\rangle$ and $|1\rangle$

$|a|^2 + |b|^2 = 1$

Measurement of

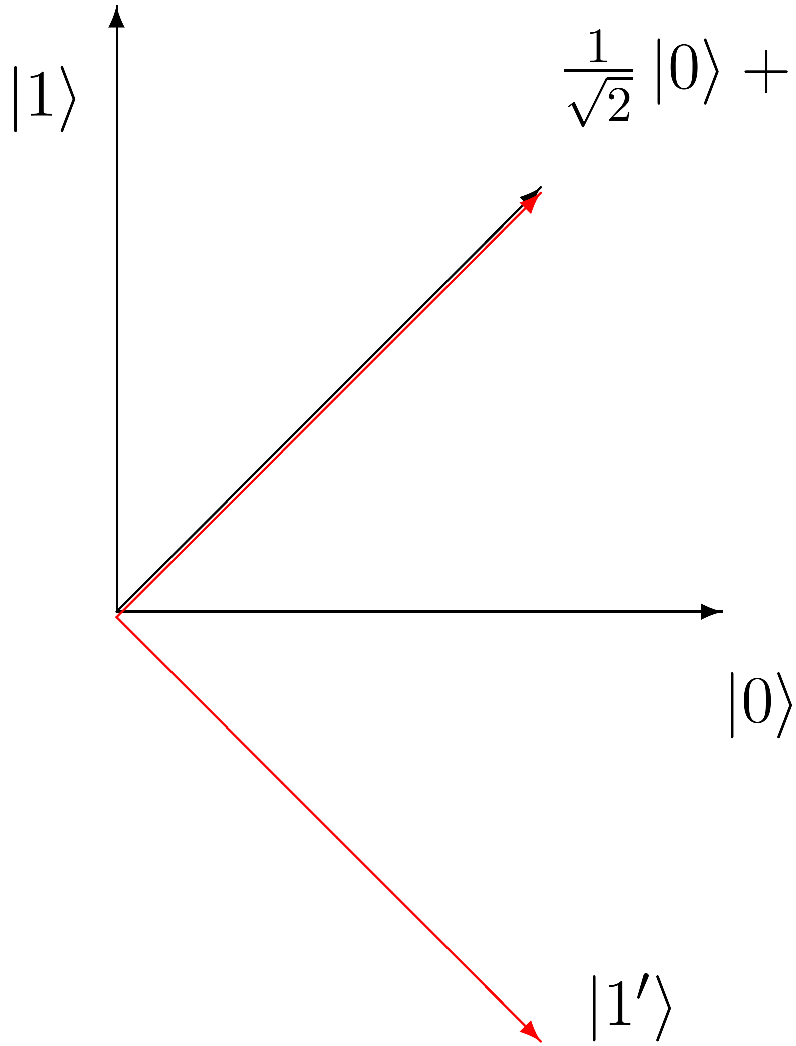
$v_0\ |0\rangle\langle 0|\ + v_1\ |0\rangle\langle 0|$:

$\mathbb{P}(v_0) = |a|^2$, $\mathbb{P}(v_1) = |b|^2$

Minimal interpretation!

# Quantum Bit (Qubit)

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad = |0'\rangle$$




Basis 1:

$\{|0\rangle, |1\rangle\}$

$$\mathbb{P}(0) = \frac{1}{2}$$

Basis 2:

$$\{\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |0'\rangle,$$
$$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |1'\rangle\}$$

$$\mathbb{P}(0') = 1$$

# Compound Systems

- Down $\rightarrow$ Up: Tensor product construction: $T = T_1 \otimes T_2$, $A = A_1 \otimes A_2$
- Up $\rightarrow$ Down: Partial trace:
  $T_1 = \mathrm{Tr}_1(T) \iff \mathrm{Tr}(T(A_1 \otimes I)) = \mathrm{Tr}(T_1 A_1)$ for each $A_1$
- Example: Pure state

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Or:

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \end{pmatrix}$$

# Compound Systems

A vector

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

corresponds to a pure state

$$T = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \otimes (\frac{1}{\sqrt{2}}, 0, 0, \frac{1}{\sqrt{2}}) = \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{pmatrix}$$

Subsystem states:

$$T_1 = T_2 = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

# von Neumann Entropy

$$S = -\mathsf{Tr}(T \log T),$$

where

$$\begin{aligned} f(T) &= f(\lambda_1 \,|\boldsymbol{x}_1\rangle\langle\boldsymbol{x}_1| + \ldots + \lambda_n \,|\boldsymbol{x}_n\rangle\langle\boldsymbol{x}_n|) \\ &= f(\lambda_1)\,|\boldsymbol{x}_1\rangle\langle\boldsymbol{x}_1| + \ldots + f(\lambda_n)\,|\boldsymbol{x}_n\rangle\langle\boldsymbol{x}_n| \,. \end{aligned}$$

For

$$T = p_1 \,|\boldsymbol{x}_1\rangle\langle\boldsymbol{x}_1| + \ldots + p_n \,|\boldsymbol{x}_n\rangle\langle\boldsymbol{x}_n|$$

$$T \log T = p_1 \log p_1 \,|\boldsymbol{x}_1\rangle\langle\boldsymbol{x}_1| + \ldots + p_n \log p_n \,|\boldsymbol{x}_n\rangle\langle\boldsymbol{x}_n|$$

and

$$S(T) = -\mathsf{Tr}(T \log T) = -(p_1 \log p_1 + \ldots + p_n \log p_n).$$

# von Neumann Entropy

For a pure state $T = |\boldsymbol{x}\rangle\langle\boldsymbol{x}|$

$$S(T) = -1 \cdot \log 1 = 0.$$

Example: Let $A$ and $B$ be qubits with joint state $T = |\boldsymbol{x}\rangle\langle\boldsymbol{x}|$, where $\boldsymbol{x} = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.

- $S(T) = 0$, but for subsystem states $S(T_1) = S(T_2) = 1$.
- Conditional entropy
  $S(T_1 \mid T_2) = S(T_1, T_2) - S(T_2) = 0 - 1 = -1$
- Mutual information:

$$I(T_1 : T_2) = S(T_1) - S(T_1 \mid T_2) = 1 - (-1) = 2$$

# Compound Systems

Vector state $\boldsymbol{x}$ is *decomposable*, if $\boldsymbol{x} = \boldsymbol{x}_1 \otimes \boldsymbol{x}_2$ for subsystem states $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$. Otherwise, state is *entangled*. Example:

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

is decomposable, whereas

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

is entangled.

# Compound Systems

For pure state

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

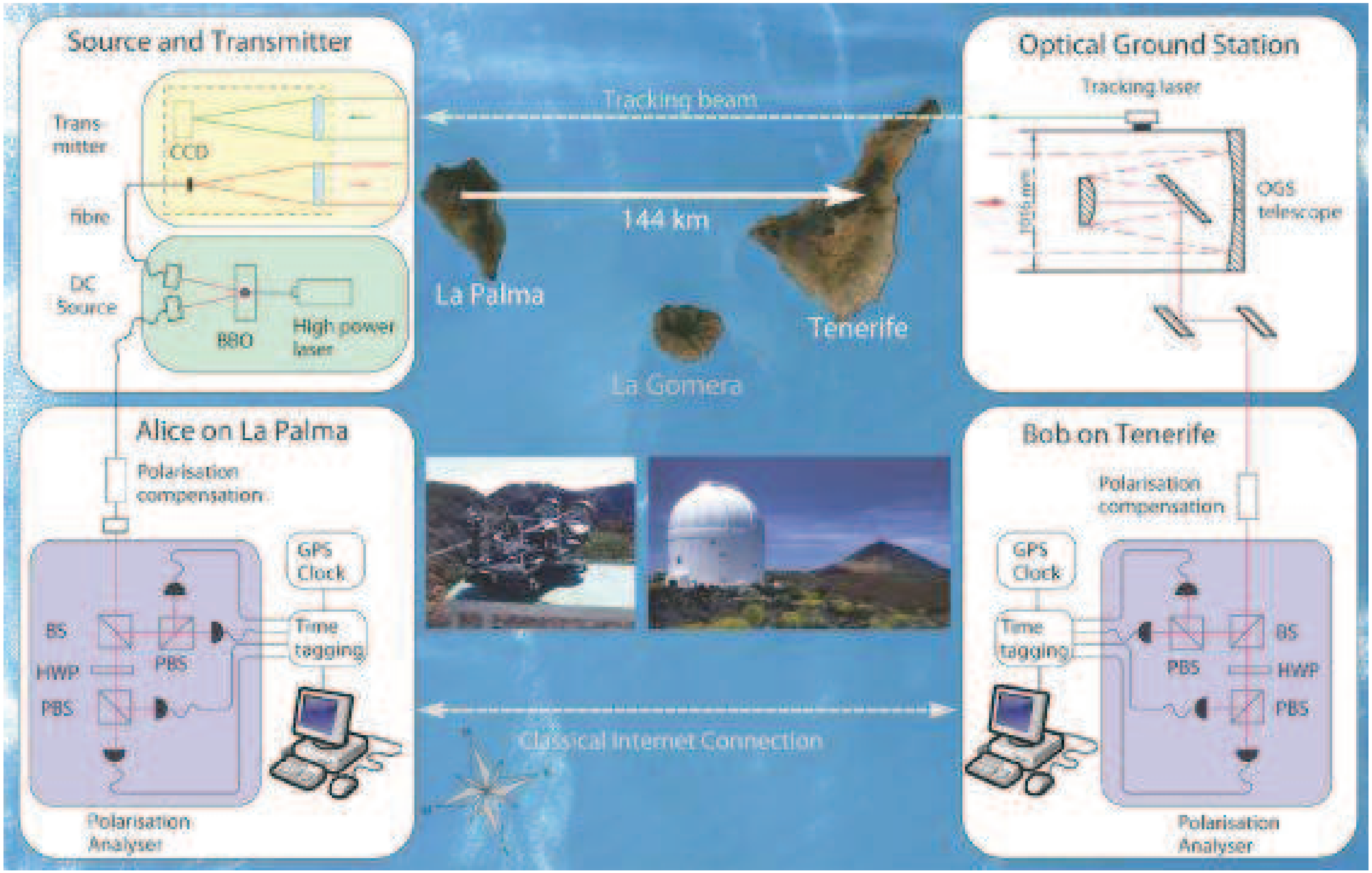
$$\mathbb{P}(|00\rangle) = \mathbb{P}(|11\rangle) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2},$$

and

$$\mathbb{P}(|01\rangle) = \mathbb{P}(|10\rangle) = 0$$

(perfect correlation)

# Compound Systems




Experiment on Canary islands 2007

# Compound Systems

Correlation over distance also possible in classical mechanics:

$$\frac{1}{2}[00] + \frac{1}{2}[11]$$

But

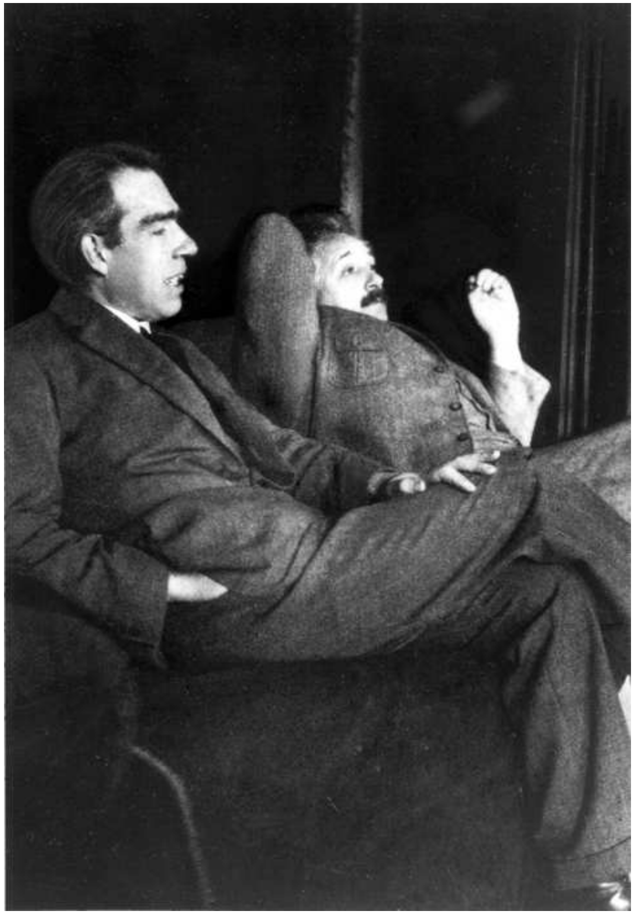
$$\frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle$$

violates a *Bell inequality*.

For classical case:

$$\begin{aligned} I(A:B) &= H(A) - H(A \mid B) \\ &= H(A) + H(B) - H(A,B) = 1 + 1 - 1 = 1. \end{aligned}$$

# EPR Paradox



Einstein, Podolsky, Rosen: Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

Physical Review 47, 777–780 (1935)

Niels Bohr (1885–1962) & Albert Einstein (1879–1955)

# EPR Paradox (Bohm formulation)

- Einstein: The physical world is <u>local</u> and <u>realistic</u>
- Assume distant qubits in state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
- Quantum mechanics: neither qubit has definite pre-observation value
- Observe the first qubit

$\Rightarrow$ The value of the second qubit is known certainly (without “touching” or “disturbing” it)

$\Rightarrow$ The value if the second qubit is “an element of reality”

$\Rightarrow$ Quantum mechanics is an incomplete theory

# John Bell

John Steward Bell (1928–1990)

Bell inequalities

# Bell Inequalities

Itamar Pitowsky: Quantum Probability – Quantum Logic, Springer (1989)

- Ballot box of 100 balls
- Each red or blue, wooden or plastic
- 80 red, 60 wooden
- 30 red <u>and</u> wooden?
- Then 80+60-30=110 are red <u>or</u> wooden. No way!

In other words: $(0.8, 0.6, 0.3)$ does *not* express probabilities $(p_1, p_2, p_{12})$ of two events and their intersection.

Reason: $\mathbb{P}(1 \vee 2) = p_1 + p_2 - p_{12}$ is a probability, too.

# Bell Inequalities

Lemma: $(p_1, p_2, p_{12})$ is an “eligible” probability vector if and only if

$$0 \leq p_{12} \leq p_1, p_2 \leq 1 \quad \text{and} \quad 0 \leq p_1 + p_2 - p_{12} \leq 1$$

Bell inequalities!
Idea of proof:

- Correlation polytope in $\mathbb{R}^3$
- Formed from collection $\{\{1\}, \{2\}, \{1,2\}\}$ as follows: $(e_1, e_2) \mapsto (e_1, e_2, e_1 e_2)$, where $e_1, e_2 \in \{0, 1\}$.
- Extremals: $(0,0,0)$, $(1,0,0)$, $(0,1,0)$, $(1,1,1)$.
- Polytope: Convex hull of the extremals
- $(p_1, p_2, p_{12})$ is an eligible probability if and only if it is in the convex hull

# Bell Inequalities

Now

$$
\begin{aligned}
& (p_1, p_2, p_{12}) \\
= \quad & (1 - p_2 - p_2 + p_{12})(0,0,0) \\
+ \quad & (p_2 - p_{12})(0,1,0) \\
+ \quad & (p_1 - p_{12})(1,0,0) \\
+ \quad & p_{12}(1,1,1).
\end{aligned}
$$

However, the representation is not generally unique.

# Bell Inequalities

Example: $\{\{1\},\{3\},\{1,3\},\{1,4\},\{2,3\},\{2,4\}\}$ generates a correlation polytope in $\mathbb{R}^6$ with extremals

$$\{(e_1, e_3, e_1e_3, e_1e_4, e_2e_3, e_2e_4) \mid e_i \in \{0,1\}\}$$

Easy to verify:

$$e_1e_4 + e_1e_3 + e_2e_3 - e_2e_4 - e_1 - e_3 \in \{-1, 0\}$$

for each extremal.

$$\Rightarrow -1 \leq p_{14} + p_{13} + p_{23} - p_{24} - p_1 - p_3 \leq 0$$

is satisfied for each “eligible” vector $(p_1, p_3, p_{13}, p_{14}, p_{23}, p_{24})$ (another Bell inequality).

# CHSH Inequality

- Two communicating parties Alice and Bob (distance large)
- Alice chooses to measure $A_1$ or $A_2$, Bob $B_1$ or $B_2$ (all $\pm 1$-valued observables)
- For fixed $i, j \in \{-1, 1\}$ let $p_1 = \mathbb{P}(i \mid A_1)$, $p_2 = \mathbb{P}(i \mid A_2)$, $p_3 = \mathbb{P}(j \mid B_1)$, $p_4 = \mathbb{P}(j \mid B_2)$.
- Locality: $p_1 = \mathbb{P}(i \mid A_1) = \mathbb{P}(i \mid A_1, B_1) = \mathbb{P}(i \mid A_1, B_2)$, $p_3 = \mathbb{P}(j \mid B_1) = \mathbb{P}(j \mid A_1, B_1) = \mathbb{P}(j \mid A_2, B_1)$, etc.
- Also, $p_{13} = \mathbb{P}(i, j \mid A_1, B_1)$, $p_{14} = \mathbb{P}(i, j \mid A_1, B_2)$, $p_{23} = \mathbb{P}(i, j \mid A_2, B_1)$, $p_{24} = \mathbb{P}(i, j \mid A_2, B_2)$.

# CHSH Inequality

- For fixed $i, j \in \{-1, 1\}$ let $p_1 = \mathbb{P}(i \mid A_1)$, $p_2 = \mathbb{P}(i \mid A_2)$, $p_3 = \mathbb{P}(j \mid B_1)$, $p_4 = \mathbb{P}(j \mid B_2)$.
- Locality: $p_1 = \mathbb{P}(i \mid A_1) = \mathbb{P}(i \mid A_1, B_1) = \mathbb{P}(i \mid A_1, B_2)$, $p_3 = \mathbb{P}(j \mid B_1) = \mathbb{P}(j \mid A_1, B_1) = \mathbb{P}(j \mid A_2, B_1)$, etc.
- Also, $p_{13} = \mathbb{P}(i, j \mid A_1, B_1)$, $p_{14} = \mathbb{P}(i, j \mid A_1, B_2)$, $p_{23} = \mathbb{P}(i, j \mid A_2, B_1)$, $p_{24} = \mathbb{P}(i, j \mid A_2, B_2)$.

Bell:

$$\begin{aligned} -1 \quad &\leq \quad \mathbb{P}(i, j \mid A_1, B_1) + \mathbb{P}(i, j \mid A_1, B_2) + \mathbb{P}(i, j \mid A_2, B_1) \\ &- \quad \mathbb{P}(i, j \mid A_2, B_2) - \mathbb{P}(i \mid A_1) - \mathbb{P}(j \mid B_1) \leq 0 \end{aligned}$$

Multiply with $ij$ for all $i, j \in \{-1, 1\}$ and sum:

# CHSH Inequality

$$\begin{aligned} -1 &\leq \mathbb{P}(i,j \mid A_1,B_1) + \mathbb{P}(i,j \mid A_1,B_2) + \mathbb{P}(i,j \mid A_2,B_1) \\ &- \mathbb{P}(i,j \mid A_2,B_2) - \mathbb{P}(i \mid A_1) - \mathbb{P}(j \mid B_1) \leq 0 \end{aligned}$$

Multiply with $ij$ for all $i,j \in \{-1,1\}$ and sum:

$$-2 \leq \mathbb{E}(A_1B_1) + \mathbb{E}(A_1B_2) + \mathbb{E}(A_2B_1) - \mathbb{E}(A_2B_2) \leq 2$$

(CHSH inequality). Here

$$\mathbb{E}(A_kB_l) = \sum_{i,j\in\{-1,+1\}} ij\mathbb{P}(i,j \mid A_k,B_l)$$

is the expected value (correlation).

# EPR Paradox Resolved

- Assume Alice and Bob share state $\boldsymbol{x} = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$.
- Define observables

$$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$B_1 = \frac{1}{\sqrt{2}}(A_1 + A_2), B_2 = \frac{1}{\sqrt{2}}(A_1 - A_2)$$

(eigenvalues = potential values =$\pm 1$)

- On state $\boldsymbol{x}$, $\mathbb{E}(A_1 B_1) = \langle \boldsymbol{x} \mid (A_1 \otimes B_1)\boldsymbol{x} \rangle$
- Likewise for $\mathbb{E}(A_1 B_2)$, etc.

# EPR Paradox Resolved

$$\mathbb{E}(A_1B_1) + \mathbb{E}(A_1B_2) + \mathbb{E}(A_2B_1) - \mathbb{E}(A_2B_2) = 2\sqrt{2},$$

which contradicts CHSH inequality

$$-2 \leq \mathbb{E}(A_1B_1) + \mathbb{E}(A_1B_2) + \mathbb{E}(A_2B_1) - \mathbb{E}(A_2B_2) \leq 2.$$

Conclusion:

Locality, realism, and quantum mechanics form a contradictory set of assumptions.

# Cryptography

Classical:

Recovering the encryption key is computationally difficult / impossible

Quantum:

Recovering the encryption key is physically difficult / impossible

# One-Time Pad

- Plaintext: $\boldsymbol{p} = 001110101011010110 0$
- Key: Random string $\boldsymbol{k} = 0101010110111001010$
- Cryptotext: $\boldsymbol{c} = \boldsymbol{p} \oplus \boldsymbol{k} = 0110111100001100110$
- To retrive the plaintext: $\boldsymbol{c} \oplus \boldsymbol{k} = \boldsymbol{p} \oplus \boldsymbol{k} \oplus \boldsymbol{k} = \boldsymbol{p}$
- If $\boldsymbol{c}_1 = \boldsymbol{p}_1 \oplus \boldsymbol{k}$ and $\boldsymbol{c}_2 = \boldsymbol{p}_2 \oplus \boldsymbol{k}$, then
  $\boldsymbol{c}_1 \oplus \boldsymbol{c}_2 = (\boldsymbol{p}_1 \oplus \boldsymbol{k}) \oplus (\boldsymbol{p}_2 \oplus \boldsymbol{k}) = \boldsymbol{p}_1 \oplus \boldsymbol{p}_2$

BB84: Protocol for key generation

# Protocol BB84

- Let $|0'\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, $|1'\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.
- $|0\rangle = \frac{1}{\sqrt{2}}|0'\rangle + \frac{1}{\sqrt{2}}|1'\rangle$, $|1\rangle = \frac{1}{\sqrt{2}}|0'\rangle - \frac{1}{\sqrt{2}}|1'\rangle$.
- $|\langle 0 \mid 0'\rangle|^2 = |\langle 0 \mid 1'\rangle|^2 = |\langle 1 \mid 0'\rangle|^2 = |\langle 1 \mid 1'\rangle|^2 = \frac{1}{2}$.

1. Alice selects a random bit string $x_1 \ldots x_n$
2. For $i = 1$ to $n$:
3. If $x_i = 0$, Alice sends $|0\rangle$ or $|0'\rangle$ ($50\% - 50\%$). If $x_i = 1$, Alice sends $|1\rangle$ or $|1'\rangle$ (Alice uses encoding $A = \{|0\rangle, |1\rangle\}$ and $A' = \{|0'\rangle, |1'\rangle\}$).
4. Bob selects observable $B = 1 \cdot |0\rangle\langle 0| - 1 \cdot |1\rangle\langle 1|$ or $B' = 1 \cdot |0'\rangle\langle 0'| - 1 \cdot |1'\rangle\langle 1'|$ ($50\% - 50\%$).

# Protocol BB84

- Let $|0'\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, $|1'\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.
- $|0\rangle = \frac{1}{\sqrt{2}}|0'\rangle + \frac{1}{\sqrt{2}}|1'\rangle$, $|1\rangle = \frac{1}{\sqrt{2}}|0'\rangle - \frac{1}{\sqrt{2}}|1'\rangle$.

5. If e.g. Alice's qubit is $|0'\rangle$ and Bob selected observable $B$, he sees zero with $50\%$ probability. If Bob selected observable $B'$, he sees zero with $100\%$ probability.
6. For approximately $1/2$ of the sent qubits we have correspondence $A \leftrightarrow B$ and $A' \leftrightarrow B'$.

# Protocol BB84

7. Alice and Bob publish lists $A_1, \ldots, A_n$ and $B_1, \ldots, B_n$, telling Alice's codings $\{|0\rangle, |1\rangle\}$ or $\{|0'\rangle, |1'\rangle\}$ and the observables used by Bob.
8. Alice ja Bob pick from sequence $x_1, \ldots, x_n$ the bits $y_1, \ldots, y_k$, where Alice's coding corresponds to Bobs basis ($k \approx n/2$). Alice's and Bob's bits should coincide.
9. Alice chooses randomly indices $i_1, \ldots, i_l \leq k$ ($l = k/2$) and publishes those.
10. Alice and Bob publish the bits corresponding to the indices and compare the bits.
11. If the published bits coincide, Alice and Bob conclude that the communication has been secret, and use the unpublished bits as an encryption key.

# Protocol BB84

1. Eavesdropper (Eve), (A special case):
2. If Eve uses basis $B$ and Alice encoding $A$, the quantum bit does not change when Eve observes.
3. If Eve uses basis $B'$ and Alice encoding $A$, the quantum bit will change when Even observes: $|0\rangle \mapsto |0'\rangle$ with $50\%$ probability, and $|0\rangle \mapsto |1'\rangle$ with $50\%$ probability.
4. The probability of not changing the bit is $50\%$.

General case:
Dominic Mayers: Unconditional Security in Quantum Cryptography. Journal of the ACM 48:3, 351–406 (2001)

# http://www.idquantique.com/

# http://www.idquantique.com/