From Paradoxes of QM to Applications

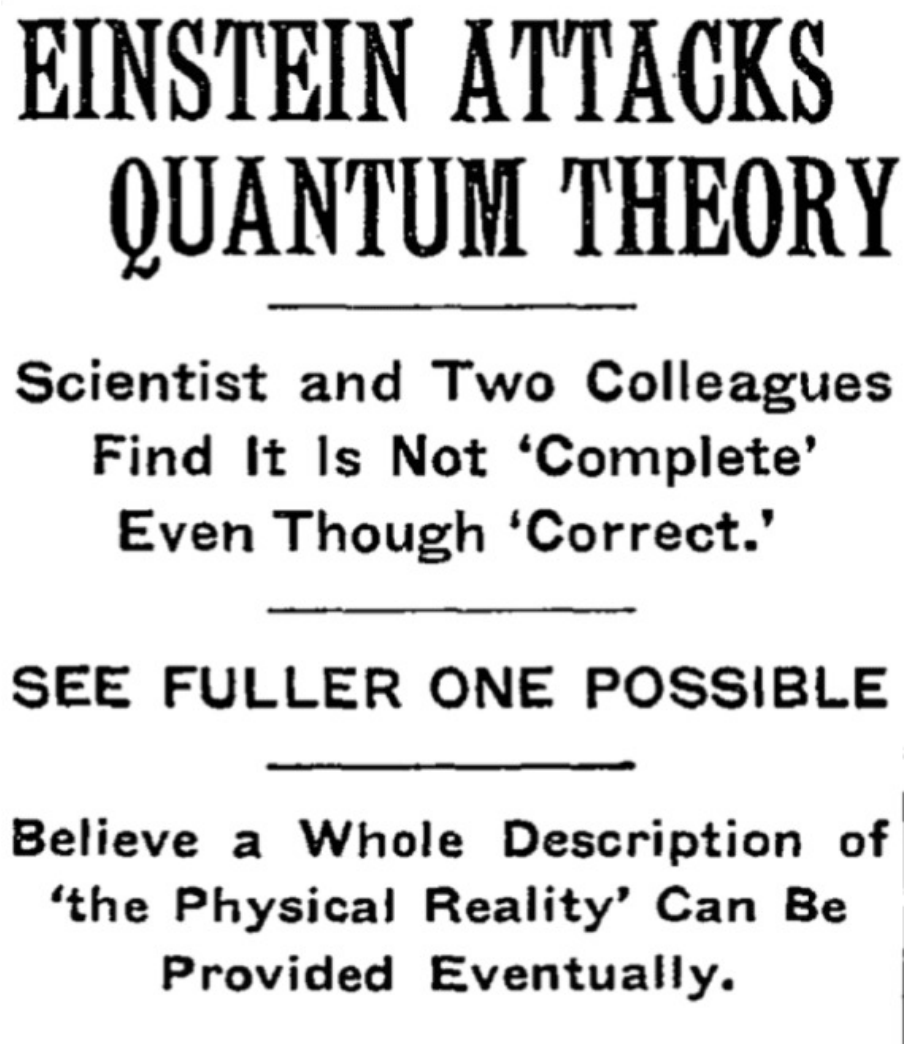
Karol Bartkiewicz

UAM

10 kwietnia 2025

Plan

Introduction



EINSTEIN ATTACKS
QUANTUM THEORY

Scientist and Two Colleagues
Find It Is Not 'Complete'
Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of
'the Physical Reality' Can Be
Provided Eventually.

The New York Times, 4.05.1935

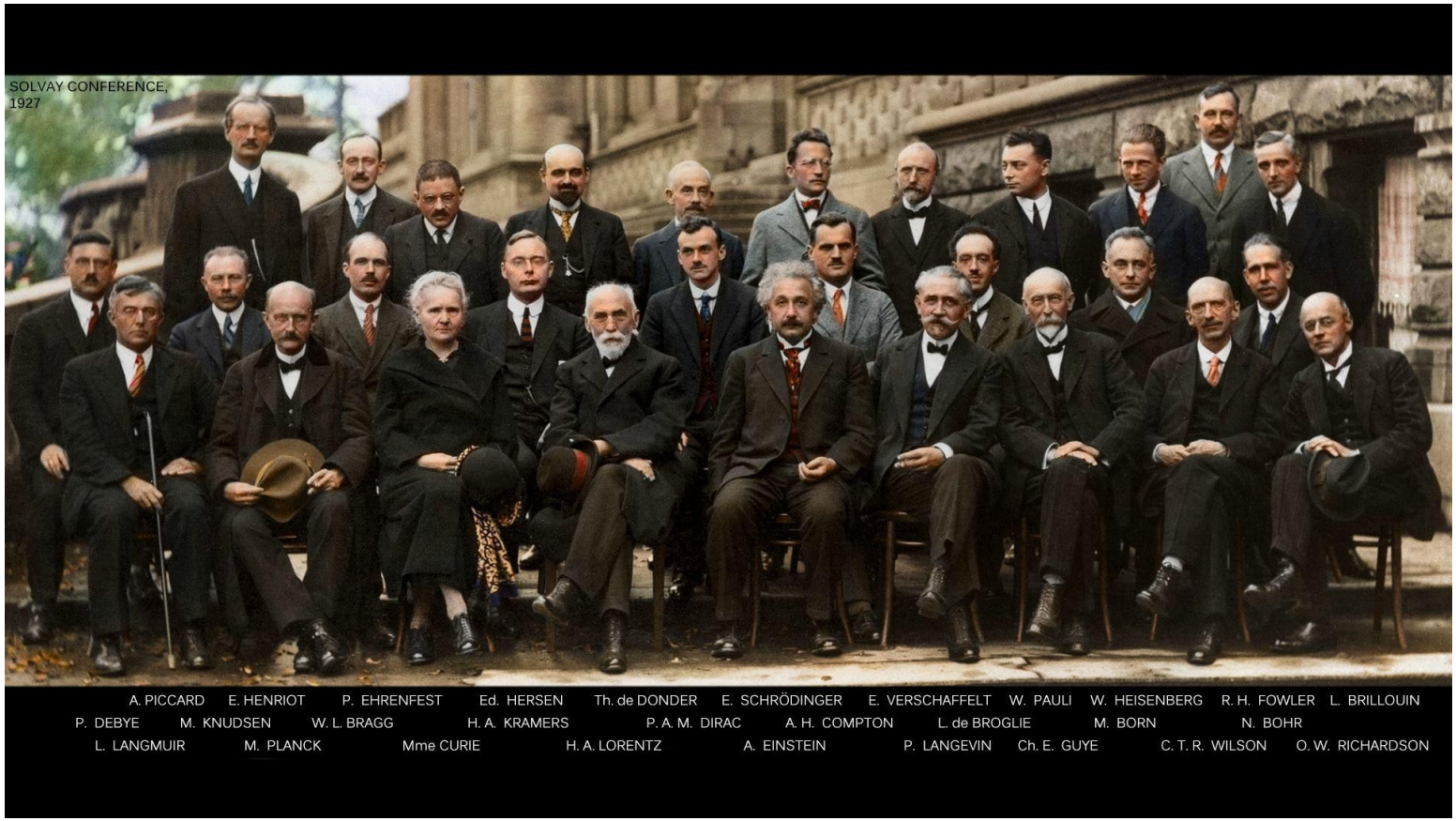
Introduction

- „God does not play dice" – A. Einstein
- „Stop telling God what to do" – N. Bohr

Einstein and Bohr at Solvay conference (1927)

History

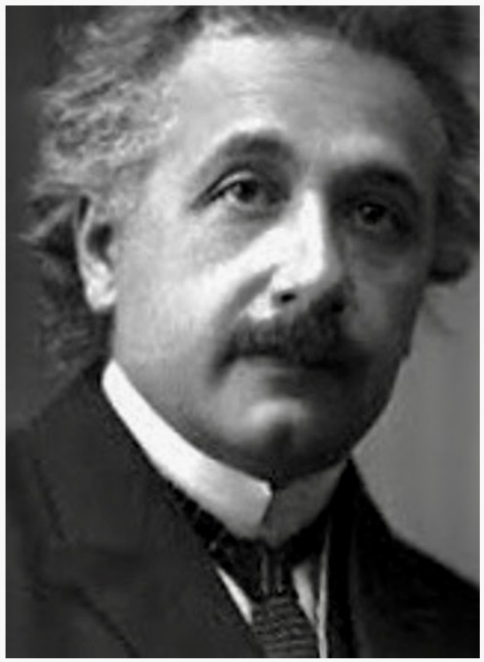
- 1900: Quantization of energy (M. Planck)
- 1905: Quantum of light (A. Einstein)
- 1925-26: Matrix and wave mechanics (Heisenberg, Schrödinger)



Einstein and Bohr at Solvay conference (1927)

History

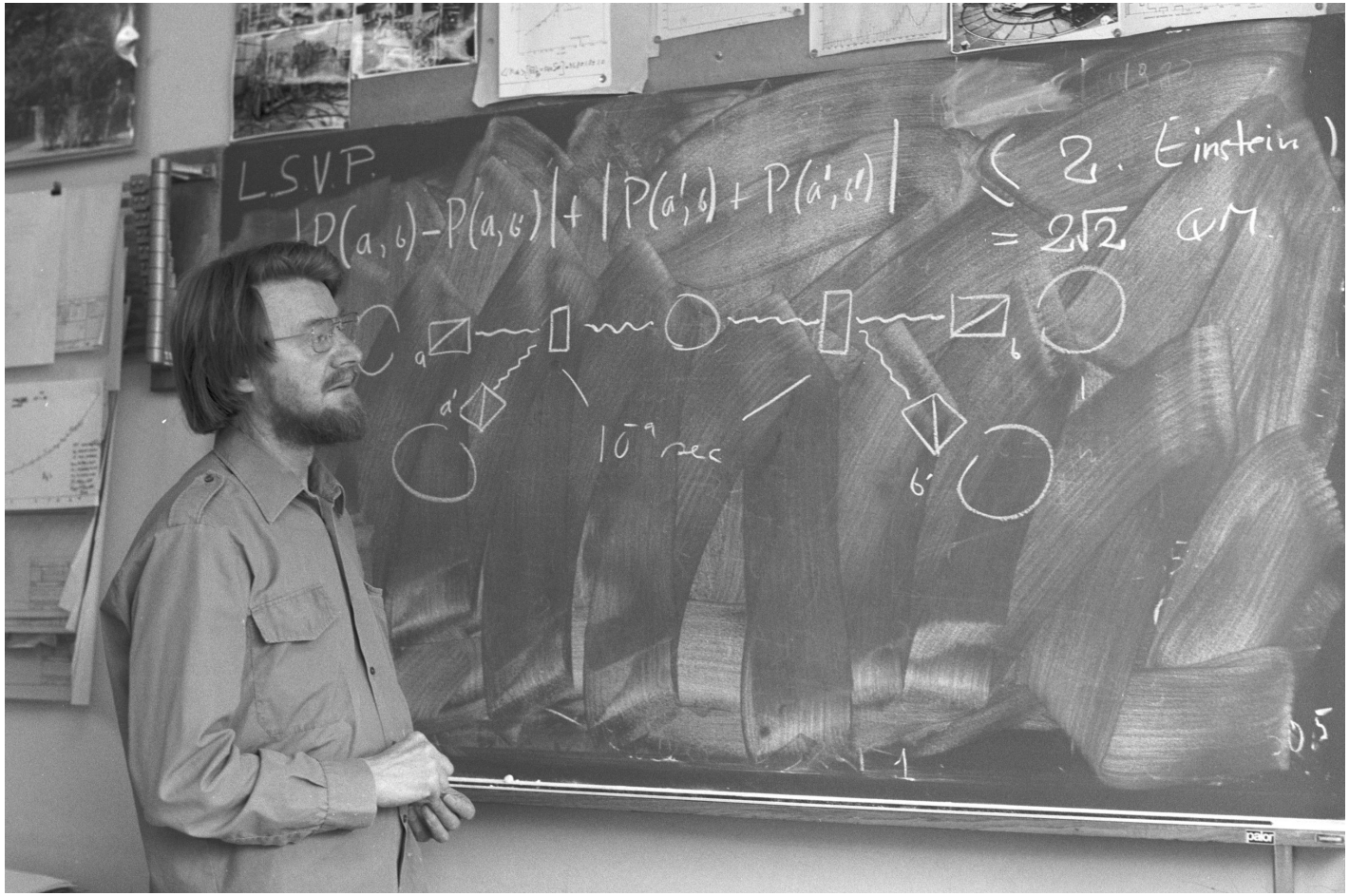
- 1935: EPR – questioning the completeness of quantum mechanics



EPR: Albert Einstein, Boris Podolsky, Nathan Rosen

History

- 1964: Bell's theorem – the ability to test "quantum strangeness"



John Bell (1982)

History

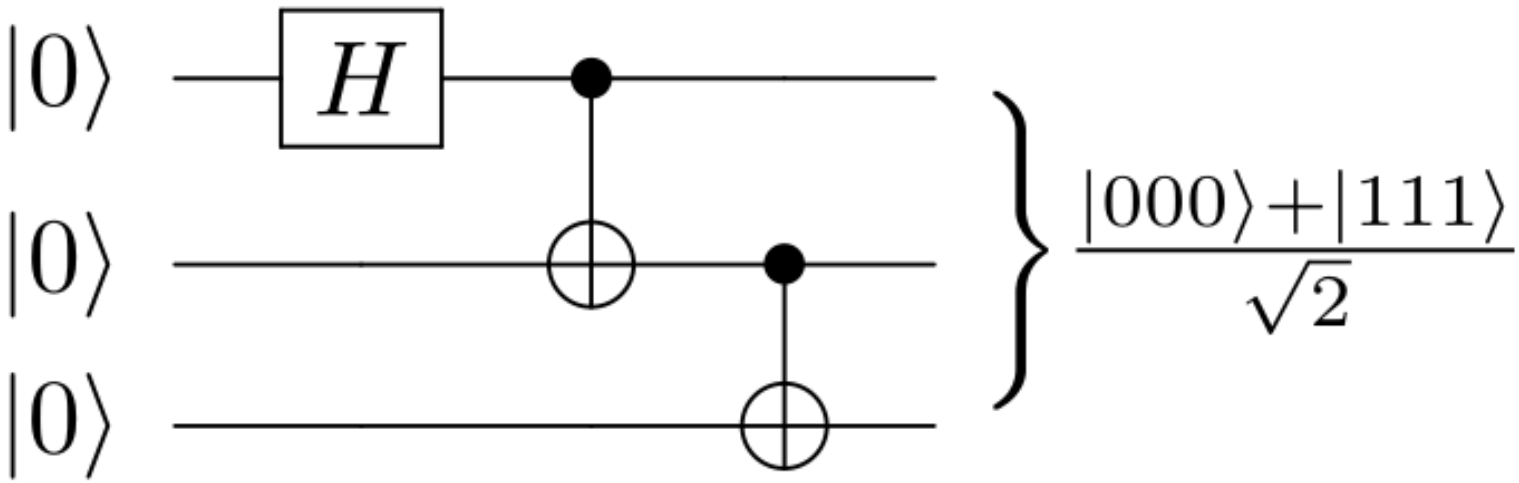
- 1967: Kochen–Specker theorem – nonexistence of the hidden variable

u_1	(0, 0, 0, 1)	(0, 0, 0, 1)	(1, –1, 1, –1)	(1, –1, 1, –1)	(0, 0, 1, 0)	(1, –1, –1, 1)	(1, 1, –1, 1)	(1, 1, –1, 1)	(1, 1, 1, –1)
u_2	(0, 0, 1, 0)	(0, 1, 0, 0)	(1, –1, –1, 1)	(1, 1, 1, 1)	(0, 1, 0, 0)	(1, 1, 1, 1)	(1, 1, 1, –1)	(–1, 1, 1, 1)	(–1, 1, 1, 1)
u_3	(1, 1, 0, 0)	(1, 0, 1, 0)	(1, 1, 0, 0)	(1, 0, –1, 0)	(1, 0, 0, 1)	(1, 0, 0, –1)	(1, –1, 0, 0)	(1, 0, 1, 0)	(1, 0, 0, 1)
u_4	(1, –1, 0, 0)	(1, 0, –1, 0)	(0, 0, 1, 1)	(0, 1, 0, –1)	(1, 0, 0, –1)	(0, 1, –1, 0)	(0, 0, 1, 1)	(0, 1, 0, –1)	(0, 1, –1, 0)

(Cabello et al. 2013) We cannot assign values 1 or 0 to the basis vectors in such a way that:
(a) value 1 appears in each column only once, the remaining values are 0;
(b) vectors marked with the same colors correspond to the same values – 1 or 0.

History

- 1989: GHZ paradox – stronger nonlocality test



Quantum circuit generating a GHZ state
(Daniel Greenberger, Michael Horne, Anton Zeilinger) for Mermin-GHZ (1990) experiment

Classical vs. quantum description

Classical physics:

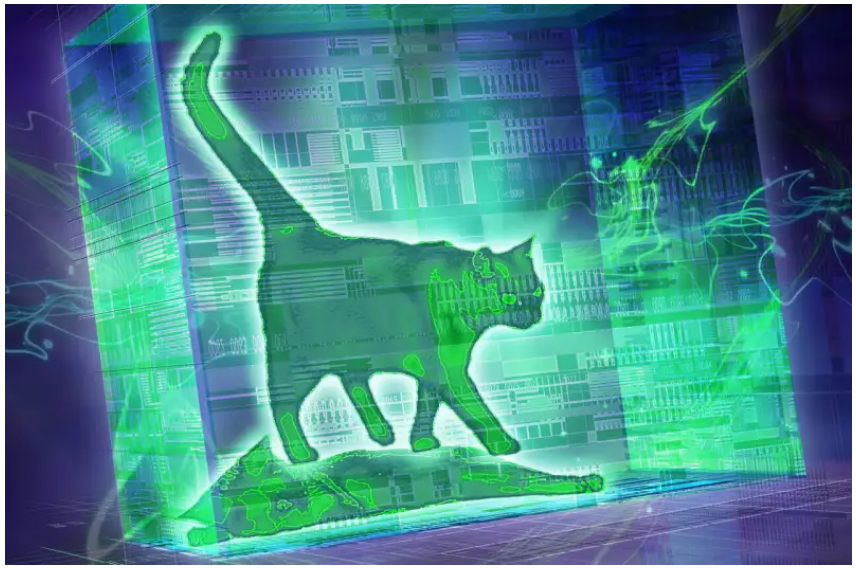
- Deterministic
- Realistic (measurement-independent reality)
- Local (interactions at limited speed)
- Accurate measurements

Quantum physics:

- Probabilistic
- Problems with the realism of the observables
- Nonlocality
- Uncertainty principle

Does quantum mechanics provide a complete description of reality?

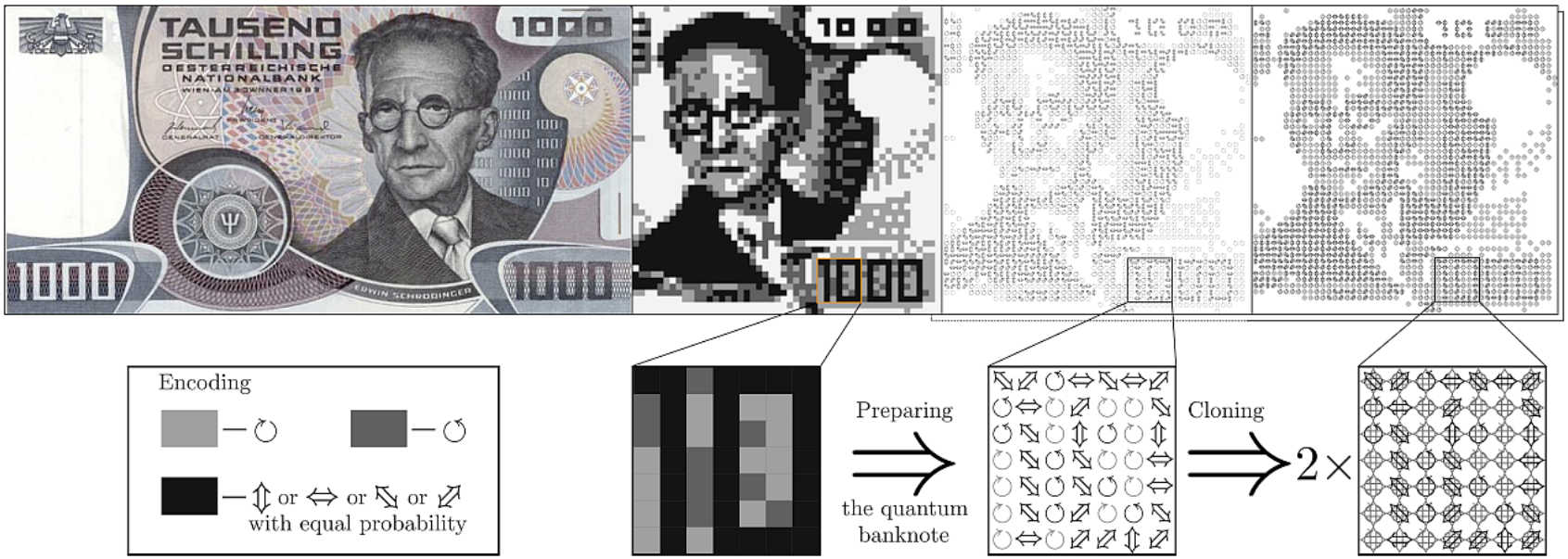
Quantum measurement



$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\text{dead}\rangle + |\text{alive}\rangle) \tag{1}$$

- The wavefunction collapses at the moment of measurement
- Interpretations: Copenhagen, multiverse, decoherence...
- The problem of quantum/classical threshold
- The EPR paradox (1935): nonlocality or incompleteness of quantum mechanics

Quantum Money



Quantum currency: No safe bets (Nature Physics, 02.03.2017)

Polacy... fałszują kwantowe pieniądze (PAP, 08.03.2017)

Entangled states

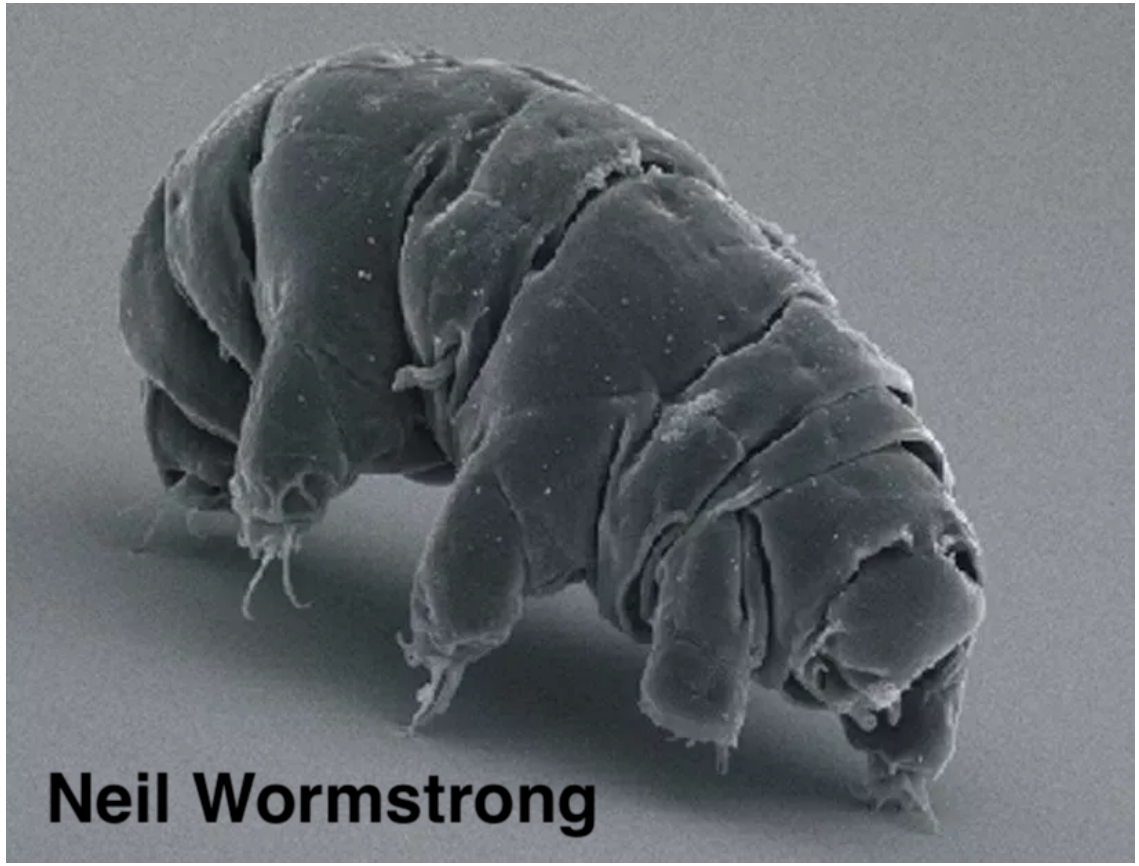
- Entangled states of two particles:

$$\left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) \tag{2}$$

- EPR paradox: measuring the first particle immediately sets the state of the second particle (distance independent)
- The information might be transferred faster than c
- Superluminal communication is impossible (nocloning theorem, nosignaling theorem)

Quantum entanglement suggests the existence of nonlocal correlations!

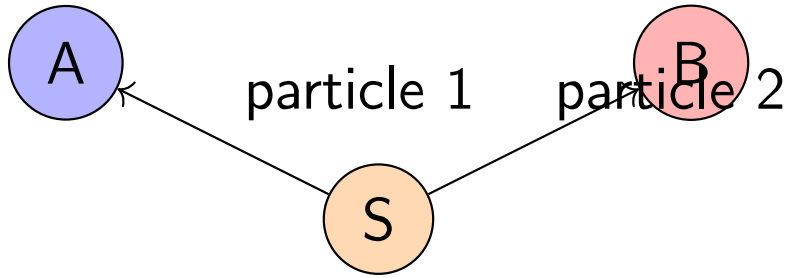
Neil Wormstrong



Niesporczak - Neil Wormstrong - przeżył splątanie kwantowe? Trwa dyskusja (PAP, 31.12.2021)

Experimental Setup

- Source emits entangled particle pairs
- Alice and Bob receive one particle each
- Alice can measure in direction a or a'
- Bob can measure in direction b or b'
- Results are binary: ± 1



Measurement Operators

- Alice's measurement settings: a and a'
- Bob's measurement settings: b and b'
- Measurement outcomes: $A(a) = \pm 1$, $A(a') = \pm 1$, $B(b) = \pm 1$, $B(b') = \pm 1$
- In local hidden variable theories, these outcomes are determined by some hidden variable λ
- For a single run with fixed λ, Alice's measurement cannot depend on Bob's choice of setting and vice versa

The CHSH Inequality: Setup

Define the CHSH operator

$$S = A(a)B(b) + A(a)B(b') + A(a')B(b) - A(a')B(b') \tag{3}$$

For a specific hidden variable λ

- Each measurement outcome $A(a)$, $A(a')$, $B(b)$, $B(b')$ is predetermined
- Each outcome equals ± 1
- These values must satisfy certain mathematical constraints

Deriving the Bell-CHSH Inequality: Step 1

For any specific hidden variable λ, let's use the notation:

$$A_a = A(a, \lambda) = \pm 1 \tag{4}$$
$$A_{a'} = A(a', \lambda) = \pm 1 \tag{5}$$
$$B_b = B(b, \lambda) = \pm 1 \tag{6}$$
$$B_{b'} = B(b', \lambda) = \pm 1 \tag{7}$$

The CHSH expression becomes:

$$S(\lambda) = A_a B_b + A_a B_{b'} + A_{a'} B_b - A_{a'} B_{b'} \tag{8}$$

Deriving the Bell-CHSH Inequality: Step 2

Rearranging:

$$S(\lambda) = A_a B_b + A_a B_{b'} + A_{a'} B_b - A_{a'} B_{b'} \tag{9}$$
$$= A_a(B_b + B_{b'}) + A_{a'}(B_b - B_{b'}) \tag{10}$$

Note that either:

- $B_b = B_{b'}$ implying $B_b + B_{b'} = \pm 2$ and $B_b - B_{b'} = 0$, or
- $B_b = -B_{b'}$ implying $B_b + B_{b'} = 0$ and $B_b - B_{b'} = \pm 2$

Deriving the Bell-CHSH Inequality: Step 3

In both cases, we get:

$$|S(\lambda)| = |A_a(B_b + B_{b'}) + A_{a'}(B_b - B_{b'})| \tag{11}$$
$$\leq |A_a(B_b + B_{b'})| + |A_{a'}(B_b - B_{b'})| \tag{12}$$
$$\leq 2 \tag{13}$$

Since $|A_a| = |A_{a'}| = 1$ and at most one of $(B_b + B_{b'})$ or $(B_b - B_{b'})$ can be ± 2 (the other being 0).

Deriving the Bell-CHSH Inequality: Step 4

For any probability distribution $\rho(\lambda)$ of hidden variables:

$$|S| = \left| \int S(\lambda)\rho(\lambda)d\lambda \right| \tag{14}$$

$$\leq \int |S(\lambda)|\rho(\lambda)d\lambda \tag{15}$$

$$\leq \int 2\rho(\lambda)d\lambda = 2 \tag{16}$$

Therefore, for any local hidden variable theory:

$$\boxed{|S| = |E(a,b) + E(a,b') + E(a',b) - E(a',b')| \leq 2} \tag{17}$$

where $E(a,b)$ is the expected correlation between measurements with settings a and b.

Quantum Mechanical Prediction

The entangled state

Consider the singlet state of two spin-$\frac{1}{2}$ particles:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) \tag{18}$$

Quantum correlation

For measurements along directions $\vec{a}$ and $\vec{b}$:

$$E(a,b) = -\vec{a}\cdot\vec{b} = -\cos(\theta_{ab}) \tag{19}$$

where θ_{ab} is the angle between directions $\vec{a}$ and $\vec{b}$.

Quantum Violation of Bell-CHSH

Optimal measurement settings

Choose measurement directions in a plane with angles:

$$\vec{a} = (1, 0, 0) \qquad \vec{a'} = (0, 1, 0) \tag{20}$$

$$\vec{b} = \frac{1}{\sqrt{2}}(1, 1, 0) \qquad \vec{b'} = \frac{1}{\sqrt{2}}(-1, 1, 0) \tag{21}$$

Calculation

$$E(a, b) = -\cos(\pi/4) = -\frac{1}{\sqrt{2}} \qquad E(a, b') = -\cos(3\pi/4) = \frac{1}{\sqrt{2}} \tag{22}$$

$$E(a', b) = -\cos(\pi/4) = -\frac{1}{\sqrt{2}} \tag{23}$$

$$E(a', b') = -\cos(\pi/4) = -\frac{1}{\sqrt{2}} \tag{24}$$

Quantum Violation of Bell-CHSH (continued)

CHSH value in quantum mechanics

$$S = E(a,b) + E(a,b') + E(a',b) - E(a',b') \tag{25}$$
$$= -\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \left(-\frac{1}{\sqrt{2}}\right) - \left(-\frac{1}{\sqrt{2}}\right) \tag{26}$$
$$= -\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \tag{27}$$
$$= \frac{2\sqrt{2}}{2} = \sqrt{2} \approx 2.83 \tag{28}$$

The Bell-CHSH inequality is violated!

$$S = 2\sqrt{2} > 2 \tag{29}$$

This violates the CHSH inequality, showing that quantum mechanics is incompatible with local hidden variable theories.

Maximum Quantum Violation

Tsirelson's bound

The maximum possible quantum violation of the CHSH inequality is:

$$|S| \leq 2\sqrt{2} \approx 2.83 \tag{30}$$

- Local hidden variables: $|S| \leq 2$
- Quantum mechanics: $|S| \leq 2\sqrt{2}$
- No-signaling theories: $|S| \leq 4$

The quantum bound is strictly between the classical and no-signaling bounds.

Experimental Tests

- Aspect et al. (1982): First convincing violation of Bell's inequality
- Many subsequent experiments have confirmed the quantum prediction
- Loophole-free Bell tests:
  - Locality loophole: Ensure measurements are space-like separated
  - Detection loophole: Ensure high detection efficiency
  - Freedom-of-choice loophole: Ensure independent random selection of measurement settings
- Hensen et al. (2015), Giustina et al. (2015), Shalm et al. (2015): First loophole-free Bell tests

Implications

Philosophical implications

- Local realism is untenable
- Must give up either:
  - Locality: Accept faster-than-light influences
  - Realism: Accept that properties don't exist until measured
  - Both: Embrace quantum weirdness

Practical applications

- Quantum cryptography
- Quantum random number generation
- Device-independent quantum protocols
- Foundations for quantum computing

References

- Bell, J. S. (1964). On the Einstein Podolsky Rosen Paradox. Physics, 1(3), 195-200.
- Clauser, J. F., Horne, M. A., Shimony, A., & Holt, R. A. (1969). Proposed experiment to test local hidden-variable theories. Physical Review Letters, 23(15), 880.
- Aspect, A., Dalibard, J., & Roger, G. (1982). Experimental test of Bell's inequalities using time-varying analyzers. Physical Review Letters, 49(25), 1804.
- Hensen, B. et al. (2015). Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometers. Nature, 526(7575), 682-686.

From Bell to GHZ

- Bell's theorem (1964): Statistical incompatibility between local realism and quantum mechanics
- Greenberger, Horne, and Zeilinger (1989): Developed a more direct contradiction
- Mermin (1990): Simplified the argument, making it more accessible
- Result: A direct logical contradiction between local realism and quantum mechanics without using statistics

Why GHZ is Special

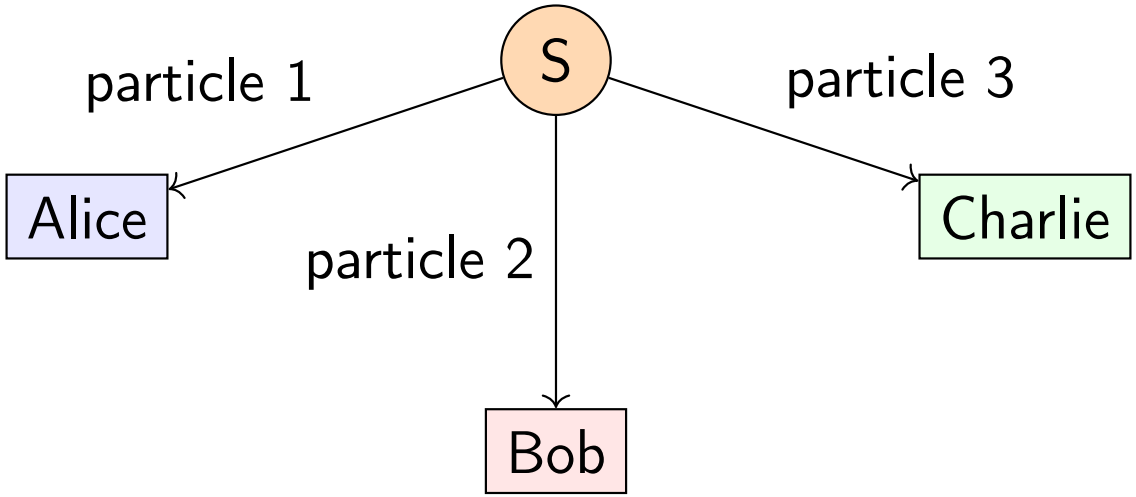
Bell's Inequality:

- Requires statistical analysis
- Uses two entangled particles
- Shows that local realism predicts bounds on correlations
- QM predicts violations of these bounds

GHZ Paradox:

- Provides a direct contradiction
- Uses three or more entangled particles
- Shows that local realism makes definite predictions
- QM predicts the exact opposite

Experimental Setup



- Three-particle entangled state prepared at source S
- Each particle sent to a different observer
- Each observer can choose to measure their particle in X or Y basis
- Each measurement yields result +1 or -1

The GHZ State

Three-particle GHZ state

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) \tag{31}$$

- A maximally entangled state of three qubits
- Cannot be factorized into product of individual states
- Exhibits "all-or-nothing"correlations
- Similar to Bell state but with three particles

Measurement Settings and Observables

Each observer can measure in one of two bases:

- X-basis: Measures spin along x-axis (σ_x)
- Y-basis: Measures spin along y-axis (σ_y)

Pauli matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{32}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{33}$$

Measurement outcomes

Each measurement yields eigenvalue +1 or -1

Quantum Predictions: Key Cases

Case 1: All measure X (XXX)

$$\langle \mathrm{GHZ} | \sigma_x^A \otimes \sigma_x^B \otimes \sigma_x^C | \mathrm{GHZ} \rangle = -1 \tag{34}$$

When all three observers measure in X-basis, the product of results is always -1

Quantum Predictions: Key Cases

Case 2: One X, two Y (XYY, YXY, YYX)

$$\langle \mathrm{GHZ}|\sigma_x^A \otimes \sigma_y^B \otimes \sigma_y^C|\mathrm{GHZ}\rangle = +1 \tag{35}$$

$$\langle \mathrm{GHZ}|\sigma_y^A \otimes \sigma_x^B \otimes \sigma_y^C|\mathrm{GHZ}\rangle = +1 \tag{36}$$

$$\langle \mathrm{GHZ}|\sigma_y^A \otimes \sigma_y^B \otimes \sigma_x^C|\mathrm{GHZ}\rangle = +1 \tag{37}$$

When one observer measures X and two measure Y, the product is always $+1$

Quantum Predictions

XYY calculation

$$\sigma_x \otimes \sigma_y \otimes \sigma_y |\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(\sigma_x|0\rangle \otimes \sigma_y|0\rangle \otimes \sigma_y|0\rangle - \sigma_x|1\rangle \otimes \sigma_y|1\rangle \otimes \sigma_y|1\rangle) \tag{38}$$

$$= \frac{1}{\sqrt{2}}(|1\rangle \otimes i|1\rangle \otimes i|1\rangle - |0\rangle \otimes (-i)|0\rangle \otimes (-i)|0\rangle) \tag{39}$$

$$= \frac{1}{\sqrt{2}}(i^2|111\rangle - (-i)^2|000\rangle) \tag{40}$$

$$= \frac{1}{\sqrt{2}}(-|111\rangle - |000\rangle) \tag{41}$$

Quantum Predictions

Inner product

$$\langle \mathrm{GHZ}|\sigma_x \otimes \sigma_y \otimes \sigma_y|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(\langle 000| - \langle 111|) \cdot \frac{1}{\sqrt{2}}(-|111\rangle - |000\rangle) \tag{42}$$

$$= \frac{1}{2}(-\langle 000|000\rangle - \langle 000|111\rangle + \langle 111|000\rangle + \langle 111|1 \tag{43}$$

$$= \frac{1}{2}(-1 - 0 + 0 + 1) = \frac{1}{2}(0) = 0 \tag{44}$$

Quantum Predictions

For the GHZ state $|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$:

XXX case

$$\langle \mathrm{GHZ}|\sigma_x \otimes \sigma_x \otimes \sigma_x|\mathrm{GHZ}\rangle = -1$$

XYY, YXY, YYX cases

Let's use $\sigma_x^{(j)}$ to denote σ_x applied to the jth particle:

$$\langle \mathrm{GHZ}|\sigma_x^{(1)} \otimes \sigma_y^{(2)} \otimes \sigma_y^{(3)}|\mathrm{GHZ}\rangle = +1 \quad (45)$$

$$\langle \mathrm{GHZ}|\sigma_y^{(1)} \otimes \sigma_x^{(2)} \otimes \sigma_y^{(3)}|\mathrm{GHZ}\rangle = +1 \quad (46)$$

$$\langle \mathrm{GHZ}|\sigma_y^{(1)} \otimes \sigma_y^{(2)} \otimes \sigma_x^{(3)}|\mathrm{GHZ}\rangle = +1 \quad (47)$$

These correct quantum predictions will be used in developing the GHZ paradox.

Local Realism Assumptions

Realism

Physical systems have definite properties prior to and independent of measurement

Locality

No influence can travel faster than light; the outcome of a measurement cannot be affected by actions at a spatially separated location

In the GHZ context

- Each particle has predetermined values for both X and Y measurements
- Denote: $X_j = \pm 1$ is the value for particle j measured in X-basis
- Denote: $Y_j = \pm 1$ is the value for particle j measured in Y-basis

Local Realist Predictions: Step 1

From quantum mechanics, we know:

$$X_1 X_2 X_3 = -1 \quad \text{(XXX case)} \tag{48}$$
$$X_1 Y_2 Y_3 = +1 \quad \text{(XYY case)} \tag{49}$$
$$Y_1 X_2 Y_3 = +1 \quad \text{(YXY case)} \tag{50}$$
$$Y_1 Y_2 X_3 = +1 \quad \text{(YYX case)} \tag{51}$$

From the last three equations

$$X_1 = Y_2 Y_3 \tag{52}$$
$$X_2 = Y_1 Y_3 \tag{53}$$
$$X_3 = Y_1 Y_2 \tag{54}$$

Local Realist Predictions: Step 2

Substituting these expressions into the first equation:

$$X_1 X_2 X_3 = -1 \tag{55}$$
$$(Y_2 Y_3)(Y_1 Y_3)(Y_1 Y_2) = -1 \tag{56}$$
$$Y_1^2 Y_2^2 Y_3^2 = -1 \tag{57}$$

But we know that $Y_j^2 = 1$ (since $Y_j = \pm 1$), so:

$$1 \cdot 1 \cdot 1 = -1 \tag{58}$$
$$1 = -1 \tag{59}$$

Contradiction!

Local realism leads to the logical contradiction $1 = -1$

The GHZ Paradox: Summary

Quantum mechanics predicts:

- XXX: The product of results is always -1
- XYY, YXY, YYX: The product of results is always +1

Local realism analysis:

- If we assume each particle has predetermined values for X and Y measurements
- Then we can derive relationships between these values based on quantum predictions
- These relationships lead to a contradiction: $1 = -1$

Conclusion

Local realism is incompatible with quantum mechanics in a direct, non-statistical way

Experimental Tests

- Pan et al. (2000): First experimental realization using photon polarization
- Leibfried et al. (2005): Implementation with trapped ions
- Erven et al. (2014): Three-photon GHZ states transmitted over separate optical fibers
- Results consistently confirm quantum predictions and rule out local realism

Challenges

- Creating high-fidelity GHZ states
- Ensuring high detection efficiency
- Achieving space-like separation of measurements

Implications of GHZ Paradox

Conceptual significance

- Stronger than Bell's inequality: direct contradiction rather than statistical violation
- "All or nothing"test of quantum mechanics vs. local realism
- Minimal interpretation requires abandoning either:
  - Realism: Properties don't exist until measured
  - Locality: Instantaneous influence exists between particles
  - Or both

Practical applications

- Quantum computing: GHZ states as resources
- Quantum communication: Multi-party protocols
- Quantum error correction: GHZ-like codes

Comparison with Other "No-Go"Theorems

EPR Paradox

- Challenge to completeness
- Two entangled particles
- No direct contradiction

Bell's Theorem

- Statistical violation
- Two entangled particles
- Requires multiple measurements

GHZ Paradox

- Direct contradiction
- Three entangled particles
- Single-shot experiment

Progression

GHZ represents the culmination of a progression toward increasingly clear demonstrations of quantum non-locality

Conclusions

- The Mermin-GHZ paradox provides the clearest demonstration of quantum non-locality
- Key contribution: Shows direct logical contradiction between local realism and quantum mechanics
- Doesn't depend on statistical analysis like Bell's inequality
- Experimental results consistently confirm quantum predictions
- Forces us to abandon deeply held classical intuitions about the nature of reality
- Fundamental implications for our understanding of quantum mechanics and physical reality

References

- Greenberger, D. M., Horne, M. A., & Zeilinger, A. (1989). Going beyond Bell's theorem. In Bell's theorem, quantum theory and conceptions of the universe (pp. 69-72). Springer.
- Mermin, N. D. (1990). Quantum mysteries revisited. American Journal of Physics, 58(8), 731-734.
- Mermin, N. D. (1990). Simple unified form for the major no-hidden-variables theorems. Physical Review Letters, 65(27), 3373.
- Pan, J. W., Bouwmeester, D., Daniell, M., Weinfurter, H., & Zeilinger, A. (2000). Experimental test of quantum nonlocality in three-photon Greenberger–Horne–Zeilinger entanglement. Nature, 403(6769), 515-519.

The Problem of Secure Key Distribution

- Cryptography relies on secure keys shared between parties
- Classical key distribution has no unconditional security
- Quantum mechanics offers a solution: using quantum states to distribute keys
- Core advantage: measurement disturbs quantum systems
- Any eavesdropping attempt can be detected

Two Approaches to QKD

BB84 (Bennett & Brassard, 1984)

- Uses quantum uncertainty principle
- Non-commuting observables
- Based on single-qubit states
- No entanglement required

E91 (Ekert, 1991)

- Uses quantum entanglement
- Security linked to Bell's inequality
- Based on EPR pairs
- Employs concepts from Bell's theorem

BB84: Basic Principles

Key idea

Use two non-commuting bases to encode information:

- Z-basis (rectilinear): $\{|0\rangle, |1\rangle\}$
- X-basis (diagonal): $\{|+\rangle, |-\rangle\}$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Encoding

Bit value	Z-basis	X-basis
0	$\|0\rangle$	$\|+\rangle$
1	$\|1\rangle$	$\|-\rangle$

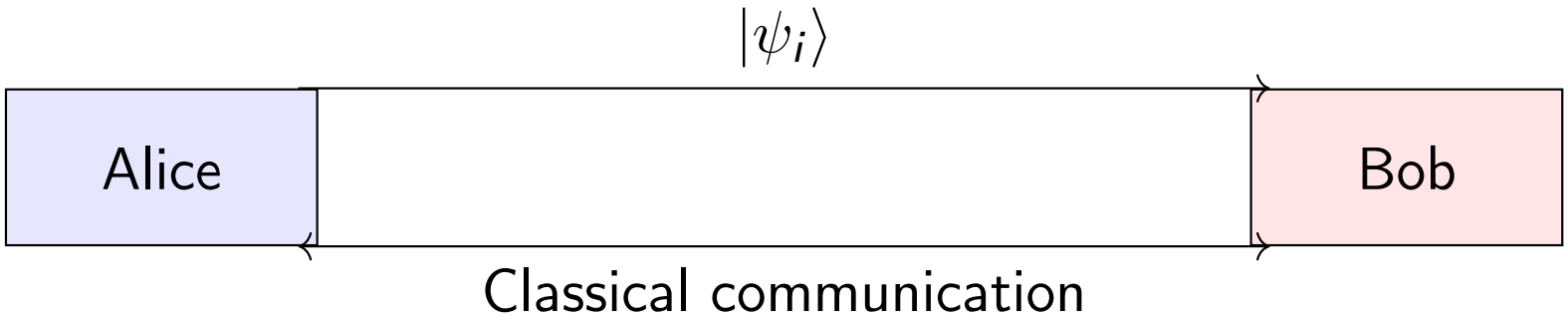
BB84: Protocol Steps

1. **Quantum transmission:**
   - Alice generates random bits $a_i \in \{0, 1\}$
   - Alice generates random bases $\alpha_i \in \{Z, X\}$
   - Alice prepares states $|\psi_i\rangle$ encoding a_i in basis α_i
   - Alice sends $|\psi_i\rangle$ to Bob
2. **Quantum measurement:**
   - Bob generates random bases $\beta_i \in \{Z, X\}$
   - Bob measures each received qubit in basis β_i
   - Bob records measurement results $b_i \in \{0, 1\}$

BB84: Post-processing

3. **Basis reconciliation:**
   - Alice and Bob publicly announce their bases (α_i, β_i)
   - They keep only the bits where $\alpha_i = \beta_i$ (same basis)
   - This forms the sifted key
4. **Error estimation:**
   - Alice and Bob sacrifice a subset of the sifted key
   - They publicly compare these bits to estimate error rate e
   - If $e > e_{threshold}$, they abort the protocol
5. **Information reconciliation and privacy amplification:**
   - Correct remaining errors (e.g., using error-correcting codes)
   - Reduce Eve's potential knowledge (e.g., using hash functions)
   - Results in the final secure key

BB84: Protocol Diagram



Random bits a_i
Random bases α_i
Encodes a_i in α_i

Random bases β_i
Measures in β_i
Gets results b_i

BB84: Mathematical Analysis

When bases match ($\alpha_i = \beta_i$)

- If $\alpha_i = \beta_i = Z$ and $a_i = 0$: Bob measures $|0\rangle \rightarrow b_i = 0$
- If $\alpha_i = \beta_i = Z$ and $a_i = 1$: Bob measures $|1\rangle \rightarrow b_i = 1$
- If $\alpha_i = \beta_i = X$ and $a_i = 0$: Bob measures $|+\rangle \rightarrow b_i = 0$
- If $\alpha_i = \beta_i = X$ and $a_i = 1$: Bob measures $|-\rangle \rightarrow b_i = 1$

Result: $b_i = a_i$ with probability 1 (in ideal case with no noise)

When bases don't match ($\alpha_i \neq \beta_i$)

- If $\alpha_i = Z, \beta_i = X$ and $a_i = 0$: Bob measures $|0\rangle$ in X-basis
- If $\alpha_i = X, \beta_i = Z$ and $a_i = 0$: Bob measures $|+\rangle$ in Z-basis

Result: $b_i = a_i$ with probability 0.5 (random result)

BB84: Security Analysis

Effect of measurement on non-matching basis

For example, measuring $|0\rangle$ in the X-basis:

$$|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle \tag{60}$$

$$P(+) = P(-) = \frac{1}{2} \tag{61}$$

Then if measured back in the Z-basis:

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{62}$$

$$P(0) = P(1) = \frac{1}{2} \tag{63}$$

Original information is lost!

BB84: Intercept-Resend Attack

Eve's strategy

- Eve intercepts each qubit from Alice
- Eve measures in a randomly chosen basis $\gamma_i \in \{Z, X\}$
- Eve resends to Bob a new qubit prepared in the state she measured

Error analysis

- When $\gamma_i \neq \alpha_i$: Eve gets random result, introduces 50% error
- When $\gamma_i = \alpha_i$: Eve gets correct result, introduces 0% error
- On average, Eve introduces 25% error rate in the sifted key

Conclusion

Any eavesdropping attempt introduces detectable errors!

E91: Using Entanglement

Key idea

- Use entangled EPR pairs: $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$
- Security based on violation of Bell's inequality
- Perfect correlations in same measurement basis
- No predetermined values (quantum vs. classical)

Connection to Bell's theorem

- Uses the same CHSH inequality: $|S| \leq 2$ for local hidden variables
- Quantum mechanics predicts: $|S| = 2\sqrt{2}$
- Violation ensures no local hidden variable description possible
- This guarantees no eavesdropping

E91: Measurement Settings

Alice's settings:

- $\vec{a}_1 = (0, 0, 1)$ (z-axis)
- $\vec{a}_2 = (1, 0, 0)$ (x-axis)
- $\vec{a}_3 = \frac{1}{\sqrt{2}}(1, 0, 1)$ (45° in x-z plane)

Bob's settings:

- $\vec{b}_1 = \frac{1}{\sqrt{2}}(1, 0, 1)$ (45° in x-z plane)
- $\vec{b}_2 = (1, 0, 0)$ (x-axis)
- $\vec{b}_3 = \frac{1}{\sqrt{2}}(1, 0, -1)$ (135° in x-z plane)

- Key generation: Settings $(\vec{a}_2, \vec{b}_2)$ and $(\vec{a}_3 \frac{1}{\sqrt{2}}, \vec{b}_1)$ correspond to orthogonal bases
- Security check: Settings $(\vec{a}_1, \vec{b}_1)$, $(\vec{a}_1, \vec{b}_3)$, $(\vec{a}_2, \vec{b}_1)$, and $(\vec{a}_2, \vec{b}_3)$ are used to test Bell's inequality

E91: Protocol Steps

1. **Quantum distribution:**
   - A source generates entangled pairs in state $|\Phi^-\rangle$
   - One particle from each pair is sent to Alice, one to Bob
2. **Quantum measurement:**
   - Alice randomly chooses setting $\vec{a}_i \in \{\vec{a}_1, \vec{a}_2, \vec{a}_3\}$
   - Bob randomly chooses setting $\vec{b}_j \in \{\vec{b}_1, \vec{b}_2, \vec{b}_3\}$
   - They measure spin/polarization along their chosen directions
   - They record results: $A(\vec{a}_i) = \pm 1$, $B(\vec{b}_j) = \pm 1$

E91: Protocol Steps (continued)

3. **Basis reconciliation:**
   - Alice and Bob publicly announce their measurement settings $\vec{a}_i, \vec{b}_j$ (not results)
   - They partition measurements into two groups:
     - Key generation: when $\vec{a}_i \cdot \vec{b}_j = 0$ (orthogonal settings)
     - Security check: when $\vec{a}_i \cdot \vec{b}_j \neq 0$ (non-orthogonal settings)
4. **Security verification:**
   - Using security check measurements, compute the CHSH parameter:

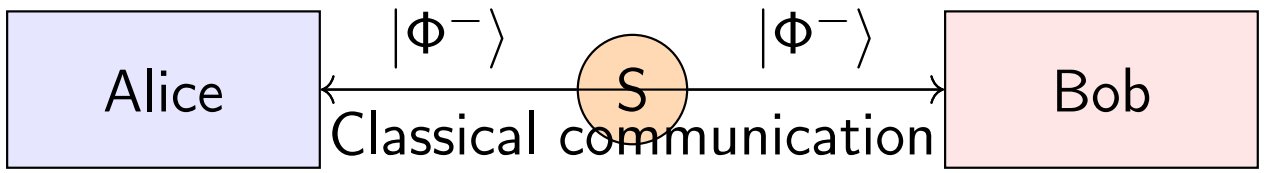
$$S = E(\vec{a}_1, \vec{b}_1) - E(\vec{a}_1, \vec{b}_3) + E(\vec{a}_2, \vec{b}_1) + E(\vec{a}_2, \vec{b}_3) \tag{64}$$

   - If $|S| < 2\sqrt{2} - \epsilon$, abort the protocol

E91: Protocol Steps (final)

5. **Key generation:**
   - From remaining measurements (orthogonal settings), Alice and Bob derive their key
   - Alice: $A(\vec{a}_1) = -1 \mapsto 0$, $A(\vec{a}_1) = +1 \mapsto 1$
   - Bob: $B(\vec{b}_2) = +1 \mapsto 0$, $B(\vec{b}_2) = -1 \mapsto 1$
   - Similarly for $A(\vec{a}_2)$ and $B(\vec{b}_1)$
6. **Error correction and privacy amplification:**
   - Same as in BB84
   - Correct remaining errors (information reconciliation)
   - Reduce Eve's potential knowledge (privacy amplification)

E91: Protocol Diagram



Settings $\vec{a}_i$
Results $A(\vec{a}_i) = \pm 1$

Settings $\vec{b}_j$
Results $B(\vec{b}_j) = \pm 1$

E91: Mathematical Analysis

Correlation function for the singlet state

For the state $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$:

$$E(\vec{a}, \vec{b}) = -\vec{a} \cdot \vec{b} = -\cos\theta_{ab} \tag{65}$$

where θ_{ab} is the angle between directions $\vec{a}$ and $\vec{b}$.

Perfect anticorrelations when $\vec{a} = \vec{b}$

$$E(\vec{a}, \vec{a}) = -1 \tag{66}$$

Meaning: when measured in the same direction, results are always opposite

No correlation when $\vec{a} \perp \vec{b}$

E91: Security Analysis

Computing the CHSH parameter

With our optimal measurement settings:

$$\vec{a}_1 \cdot \vec{b}_1 = \frac{1}{\sqrt{2}} \Rightarrow E(\vec{a}_1, \vec{b}_1) = -\frac{1}{\sqrt{2}} \tag{68}$$

$$\vec{a}_1 \cdot \vec{b}_3 = -\frac{1}{\sqrt{2}} \Rightarrow E(\vec{a}_1, \vec{b}_3) = \frac{1}{\sqrt{2}} \tag{69}$$

$$\vec{a}_2 \cdot \vec{b}_1 = \frac{1}{\sqrt{2}} \Rightarrow E(\vec{a}_2, \vec{b}_1) = -\frac{1}{\sqrt{2}} \tag{70}$$

$$\vec{a}_2 \cdot \vec{b}_3 = \frac{1}{\sqrt{2}} \Rightarrow E(\vec{a}_2, \vec{b}_3) = -\frac{1}{\sqrt{2}} \tag{71}$$

Therefore:

$$S = E(\vec{a}_1, \vec{b}_1) - E(\vec{a}_1, \vec{b}_3) + E(\vec{a}_2, \vec{b}_1) + E(\vec{a}_2, \vec{b}_3) \tag{72}$$

$$= -\frac{1}{\sqrt{2}} - \left(\frac{1}{\sqrt{2}}\right) + \left(-\frac{1}{\sqrt{2}}\right) + \left(-\frac{1}{\sqrt{2}}\right) \tag{73}$$

$$= -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} \tag{74}$$

E91: Security via Bell's Theorem

No-cloning theorem

- Eve cannot clone unknown quantum states
- She must interact with the system to gain information
- Any interaction disturbs the entanglement

Bell inequality as security check

- If Eve measures or disturbs the system
- The entanglement is degraded
- The CHSH parameter $|S|$ decreases from $2\sqrt{2}$
- Alice and Bob can detect this change

Conclusion

- Any eavesdropping reduces the violation of Bell's inequality
- Security directly linked to fundamental quantum properties

BB84 vs. E91: Similarities and Differences

Similarities

- Both use quantum properties for security
- Both detect eavesdropping through errors
- Both require quantum + classical channels
- Same post-processing procedures

Differences

- BB84: prepared states
- E91: entangled states
- BB84: uncertainty principle
- E91: Bell's inequality
- Different hardware requirements

Notation Mapping Between Bell's Theorem and QKD

Bell's Theorem	**BB84**	**E91**
Settings a, a'	Alice's bases α_i	Alice's settings $\vec{a}_i$
Settings b, b'	Bob's bases β_i	Bob's settings $\vec{b}_j$
Results $A(a) = \pm 1$	Alice's bits $a_i \in \{0, 1\}$	Alice's results $A(\vec{a}_i) = \pm 1$
Results $B(b) = \pm 1$	Bob's bits $b_i \in \{0, 1\}$	Bob's results $B(\vec{b}_j) = \pm 1$
Correlation $E(a, b)$	Error rate e	Correlation $E(\vec{a}_i, \vec{b}_j)$
CHSH parameter S	Not used	CHSH parameter S

Practical Implementations

- **BB84:**
  - Polarization encoding in photons
  - Phase encoding in interferometers
  - Time-bin encoding
  - Implemented over 100+ km of optical fiber
  - Commercial systems available
- **E91:**
  - Requires entangled photon sources
  - Spontaneous parametric down-conversion
  - More sensitive to noise and loss
  - More complex to implement
  - Less mature technology

Recent Developments

- **Device-independent QKD**
  - Based on Bell's theorem (like E91)
  - No assumptions about devices needed
  - Maximum security, but low key rates
- **Measurement-device-independent QKD**
  - Based on entanglement swapping
  - Untrusted measurement devices
  - Balance between security and performance
- **Twin-field QKD**
  - Extends range beyond direct transmission limits
  - Based on single-photon interference at a middle station
  - Breakthrough for long-distance QKD

Conclusion

- Both BB84 and E91 provide unconditional security based on quantum physics
- BB84 is simpler and more practical for near-term applications (related to no-cloning)
- E91 has deep connection to fundamental physics via Bell's theorem
- Both protocols have inspired many variants and extensions
- QKD is approaching widespread deployment for securing communications
- The field continues to evolve with innovations that improve security, distance, and key rates

References

- Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (Vol. 175, p. 8).
- Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661.
- Bell, J. S. (1964). On the Einstein Podolsky Rosen Paradox. Physics, 1(3), 195-200.
- Clauser, J. F., Horne, M. A., Shimony, A., & Holt, R. A. (1969). Proposed experiment to test local hidden-variable theories. Physical Review Letters, 23(15), 880.
- Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. Physical Review Letters, 85(2), 441.

Quantum teleportation

- Transmission of a quantum state using entanglement and a classical communication channel

$$|\psi\rangle \otimes \left|\Phi^+\right\rangle \rightarrow \left|\Phi^+\right\rangle \otimes |\psi\rangle \tag{76}$$

- Does not violate relativity theory (classical channel required)
- Key element in quantum communication and computing
- Experimentally realized over distances exceeding 1400 km (Micius satellite)

Quantum computing

- Utilizes superposition and entanglement
- Parallel information processing
- Shor's algorithm: factorization in polynomial time
- Grover's algorithm: database searching
- Quantum simulations
- Eavesdropping-resistant distributed computing

Quantum-enhanced technologies

- Quantum communication networks
- Quantum radar and imaging
- Quantum atomic clocks with increased precision
- Quantum metrology using entangled states
- Distributed quantum computing
- Quantum Random Number Generators (QRNG) based on non-locality

Comparison of quantum paradoxes

- **Non-locality:** instantaneous "action at a distance"
- **Non-contextuality:** impossibility of assigning objective values to all observables
- **Entanglement:** inseparability of quantum states
- **Steering:** asymmetric control of states at a distance

- Common source: principles of superposition and measurement
- Fundamental challenge to the classical worldview
- Paradoxes become resources in quantum technologies
- From paradoxes to quantum advantage

Open research problems

- Measurement problem and quantum-to-classical transition
- The role of quantum paradoxes in machine learning
- Quantum gravity and the role of entanglement in spacetime structure
- Non-classical correlations in many-body systems
- Role of contextuality in quantum advantage
- Effective detection and quantification of multipartite entanglement
- Decoherence and its role in the emergence of classicality

Quantum paradoxes remain an active area of research!

Questions?

Thank you for your attention!

Questions?

bark@amu.edu.pl

Bibliography – assorted papers from UAM I

Kadlec, J., Bartkiewicz, K., Černoch, A., Lemr, K., & Miranowicz, A. (2024).

Experimental hierarchy of the nonclassicality of single-qubit states via potentials for entanglement, steering, and Bell nonlocality.

Opt. Express, 32, 2333–2346.

Abo, S., Soubusta, J., Jiráková, K., Bartkiewicz, K., Černoch, A., Lemr, K., & Miranowicz, A. (2023).

Experimental hierarchy of two-qubit quantum correlations without state tomography.

Sci. Rep., 13.

Bartkiewicz, K., Tulewicz, P., Roik, J., & Lemr, K. (2023).

Synergic quantum generative machine learning.

Sci. Rep., 13.

Bibliography – assorted papers from UAM II

Jiráková, K., Černoch, A., Lemr, K., Bartkiewicz, K., & Miranowicz, A. (2021).
Experimental hierarchy and optimal robustness of quantum correlations of two-qubit states with controllable white noise.
Phys. Rev. A, 104, 062436.

Jiráková, K., Bartkiewicz, K., Černoch, A., & Lemr, K. (2019).
Experimentally attacking quantum money schemes based on quantum retrieval games.
Sci. Rep., 9.

Maskalaniec, D., & Bartkiewicz, K. (2021).
Hierarchy and robustness of multilevel two-time temporal quantum correlations.
arXiv:2106.02844.

Bartkiewicz, K., Černoch, A., Lemr, K., Miranowicz, A., & Nori, F. (2016).
Experimental temporal quantum steering.
Sci. Rep., 6, 38076.

Bibliography – assorted papers from UAM III

Bartkiewicz, K., Černoch, A., Lemr, K., Miranowicz, A., & Nori, F. (2016).

Temporal steering and security of quantum key distribution with mutually unbiased bases against individual attacks.

Phys. Rev. A, 93, 062345.

Bartkiewicz, K., Lemr, K., Černoch, A., Soubusta, J., & Miranowicz, A. (2013).

Experimental Eavesdropping Based on Optimal Quantum Cloning.

Phys. Rev. Lett., 110, 173601.

Bibliography – milestones I

Bell, J. S. (1964).
On the Einstein Podolsky Rosen paradox.
Physics Physique Fizika, 1(3), 195–200.

Einstein, A., Podolsky, B., & Rosen, N. (1935).
Can quantum-mechanical description of physical reality be considered complete?
Physical Review, 47(10), 777–780.

Greenberger, D. M., Horne, M. A., & Zeilinger, A. (1989).
Going beyond Bell's theorem.
In *Bell's theorem, quantum theory and conceptions of the universe*, pp. 69–72.

Kochen, S., & Specker, E. P. (1967).
The problem of hidden variables in quantum mechanics.
Journal of Mathematics and Mechanics, 17(1), 59–87.

Bibliography – milestones II

Bohr, N. (1935).
Can quantum-mechanical description of physical reality be considered complete?
Physical Review, 48(8), 696–702.

Schrödinger, E. (1935).
Discussion of probability relations between separated systems.
Mathematical Proceedings of the Cambridge Philosophical Society, 31(4), 555–563.

Aspect, A., Dalibard, J., & Roger, G. (1982).
Experimental test of Bell's inequalities using time-varying analyzers.
Physical Review Letters, 49(25), 1804–1807.

Clauser, J. F., Horne, M. A., Shimony, A., & Holt, R. A. (1969).
Proposed experiment to test local hidden-variable theories.
Physical Review Letters, 23(15), 880–884.

Bibliography – milestones III

Mermin, N. D. (1990).

Quantum mysteries revisited.

American Journal of Physics, 58(8), 731–734.

Bell, J. S. (1966).

On the problem of hidden variables in quantum mechanics.

Reviews of Modern Physics, 38(3), 447–452.

Wiseman, H. M., Jones, S. J., & Doherty, A. C. (2007).

Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox.

Physical Review Letters, 98(14), 140402.

Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., & Wootters, W. K. (1993).

Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels.

Physical Review Letters, 70(13), 1895–1899.

Bibliography – milestones IV

Bennett, C. H., & Brassard, G. (1984).

Quantum cryptography: Public key distribution and coin tossing.

In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179.

Horodecki, R., Horodecki, P., Horodecki, M., & Horodecki, K. (2009).

Quantum entanglement.

Reviews of Modern Physics, 81(2), 865–942.

Cabello, A., Severini, S., & Winter, A. (2014).

Graph-theoretic approach to quantum correlations.

Physical Review Letters, 112(4), 040401.

Peres, A. (1993).

Quantum theory: concepts and methods.

Kluwer Academic Publishers.

Bibliography – milestones V

Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V., & Wehner, S. (2014).

Bell nonlocality.

Reviews of Modern Physics, 86(2), 419–478.

Pan, J. W., Bouwmeester, D., Daniell, M., Weinfurter, H., & Zeilinger, A. (2000).

Experimental test of quantum nonlocality in three-photon Greenberger–Horne–Zeilinger entanglement.

Nature, 403(6769), 515–519.

Reid, M. D. (1989).

Demonstration of the Einstein-Podolsky-Rosen paradox using nondegenerate parametric amplification.

Physical Review A, 40(2), 913–923.

Leggett, A. J. (2003).

Nonlocal hidden-variable theories and quantum mechanics: An incompatibility theorem.

Foundations of Physics, 33(10), 1469–1493.