Overview

First half of 20th century: QM provides extremely successful machinery for predicting properties of microscopic and cond.-mat. systems. "Shut up and calculate" phase.

Later: increased focus on conceptual implications of QM.

Examples:

- QM makes probabilistic predictions. Attempts to find more fundamental deterministic theory lead nowhere. (Later essentially proved impossible by Bell).
- QM seems to predict faster-than-light effects over arbitrary distances! Major issue!
- Uncertainty and complementarity: The better we know some properties of a system, the less we know about others. A limitation of QM? Of measurement schemes? (Later shown to be fundamental!)
- When simulating many-body quantum systems on class. comp., adding one particle seems to double memory and time complexity!

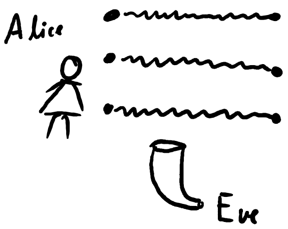
1940s - 1990s: Discussed as "metaphysical" problems

Since mid-1990s: Massive change of perspective. Use concepts from information theory and computer science to give precise and quantifiable versions of these philosophical and vague problems. That's quantum info theory.

Ongoing: Turn these into useful *quantum technology*.

Ex.: (I) 1940s: Certain quantum states show "spooky action at a distance" (Einstein).

1990s: Given n copies of such states, what is number k of secret key bits that two distant parties can generate from it, with probability of compromise $\leq p$?



Rigorous. Quantitative. Clear. At the same time: Neither succeeds nor even attempts to "explain 'what really happens'".

2017: China launches experimental quantum key distribution satellite.

(II) Old perspective: QM source of computational difficulties for computer physics.

1990s: Turn this around: Which *classical* problems could a computer relying on QM solve fundamentally better than any classical machine (beyond simulating itself)?

Turns out: A "quantum computer" using few thousand perfect "qubits" could solve all number-theo puzzles underlying the crypto used on Internet.

Turns out: A "quantum computer" using few thousand perfect "qubits" could solve all number-theo puzzles underlying the crypto used on Internet.

Computer science is subfield of physics, not just math.

This course

Three parts:

Ⓘ <u>(Re-) introduction</u> of <u>QM</u> from more "structured" p.o.v. ("no analysis, just linear algebra")

- finite-dim. many-body systems, density matrices, partial trace, entanglement, unitary gates and circuits, Bell inequalities, no cloning and uncertainties in QM <u>and</u> <u>beyond</u>.

Ⓘⓘ <u>Information and Communication</u>

- info theory: entropy, capacities, coding for classical and quantum systems.
- quantum key distribution.

Ⓘⓘⓘ <u>Computation</u>

- Grover's algorithm
- Classical public key crypto (Diffie-Hellman)

- Shor's algorithm

(- Quantum complexity / physical implementations)