Universität Tübingen
Ángela Capel Cuevas

Seminar on Quantum Information Theory

Preliminary meeting: 18. July 2022, 10:00 C4H33

Prerequisites:

- Mathematical Analysis, Linear Algebra and Probability Theory.
- No prior knowledge on Quantum Physics is assumed.

Target audience:

- Originally intended for master students from the Master Program in Mathematical Physics.
- But also open to any student from any other master or bachelor program in the Mathematics Department.

Aim of the course:

The main aim of this seminar is to provide a formal (and mathematically rigorous) introduction to quantum computing. All the topics discussed will be presented in mathematical formalism, and some applications for these results will be addressed. We will therefore choose the bibliography individually for each topic to fulfil our expectations.

More specifically, some of the possible sub-aims for this seminar are as follows:

- Learn some of the most basic notions on Quantum Information Theory oriented towards Quantum Computation.
- Understand how quantum information is transmitted via quantum channels and construct some basic quantum circuits.
- Learn the main differences between quantum and classical computing, as well as between quantum algorithms and classical algorithms.
- Get familiar with some of the first quantum algorithms and quantum cryptographic protocols.
- Understand some quantum attacks to classical cryptographic protocols.
- Learn about some different complexity classes and Turing machines.
- Discuss state-of-the-art of quantum computing and possible applications in other fields.

Some specific topics:

Here I list some possible topics for the talks in the seminar. However, the specific topics will be chosen jointly with the students attending the seminar, depending on their particular interest as well as their individual background. Some possible suggestions, however, are:

- First sessions to learn about qubits, quantum mechanics, quantum circuits and some basic protocols such as teleportation.
- Quantum algorithms: Deutsch-Jozsa, Simon, Grover, Shor, etc.
- Quantum attacks.
- Quantum cryptography (BB84, e.g).
- Overview on quantum post-cryptography and NIST competition.
- Quantum error correction.
- Turing machines and undecidability of some properties?
- Overview on complexity classes and relation between them. MIP*=RE?
- Applications to other fields: Quantum money, quantum machine learning, atomic clocks, quantum sensors, quantum gravity, etc.