1. Administrative remarks

Quantum information, computation, algorithms

András Molnár / Norbert Schuch

1.1. Lecture information:

- 6 credits, lecture 2x 90 min/week.
- Prof. Schuch takes over around 25/11
- There is no mandatory presence
- Oral exam at the end of semester. 2-3 dates.
- Prerequisites: quantum physics knowledge is not assumed, but you need a solid understanding and practice in linear algebra.

1.2 Exercise classes

- 4 credits, 1x 90 min/week.
- Recommended to acquire practice
- 2 groups: Andras Molnar on Wednesday
  Andreas Klingler on Tuesday

- Format: exercises are solved by students.
- Mandatory attendance
- Present the solution of (#exercises/#students) exercises. First-come-fist serve.
  ⚠ Early exercises are easier
  ⚠ #exercises ≈ #students
- Available on Moodle, course website.

1.3 Literature

- Lecture notes at prof. Norbert Schuch's webpage. (per chapter) and on Moodle (per lecture)
- Past lecture notes on the website
- John Preskill: Quantum comp. lecture notes
- Nielsen & Chuang: Quantum info and comp.

2. Introduction

2.1. Quantum physics/mechanics

- Small objects (eg. atoms, electrons) behave differently than macroscopic objects.
- Important for understanding certain materials:
  - semi-conductors (silicon, ...)
  - superconductors (large magnets, e.g. MRI)

  Usual modeling: material: nuclei fixed position (crystal), electrons move. You see the quantumness in "strange" behavior of the material.
- In this course we'll learn abstact description of discrete systems
  - → energy levels in an atom
  - → photon polarization
  - → magnetic degree of freedom of electrons, atoms
  - → current in a closed superconducting circuit

We will learn the framework used to describe these systems, not the concrete physical details.

2.2. Quantum Computation

In (classical) computers information is stored and processed as discrete (binary) data. Physically, it's either small magnets or voltage in transistors.

In quantum computers information is stored and processed in binary quantum systems = qubits.

Eg.: energy levels of atoms, current in superconductors, magnetic degree of freedom of ions, polarization of photons.

Challenging task: you need to engineer and control many such individual constituents. Problem: ability to control ≅ ability of environment to influence the system ⇒ noise.

2.3. Quantum algorithms

As the principle of information storage is fundamentally different, one has to adapt the algorithms.

Good news: as Nature is inherently quantum, one expects that quantum computers are better suited for describing (certain) phenomena observed in Nature.

E.g: creating new drugs, fertilizers, simulating building blocks of the universe.

Bad news: it is hard to device algorithms solving "classical" problems. We will learn essential building blocks + Shor's factorization algorithm.

2.4. Quantum information

Factoring algorithm actually has huge impact: current security protocols rely on the assumption that factoring (i.e., decomposing a number into the product of primes such as $15 = 5 \times 3$) is difficult: factorization of large numbers take a lot of time.

If you have a q. computer, this is no longer true: Shor's algorithm runs fast.

When encoding secrets, one has to be aware that these protocols will be crackable in the future.

Luckily quantum mechanics also gives us tools to encript messages in a way that security is not based on assumptions but it is provable.

For this, you need to transfer quantum information (e.g. polarization of photons). As communication is inherently noisy, one treats them slightly differently: we will learn a "probabilistic" version of quantum theory.