

POSSIBILITIES FOR QUANTUM INFORMATION PROCESSING

ŠTĚPÁN HOLUB

ABSTRACT. The tutorial introduces into quantum information science, a quickly developing area of multidisciplinary research. The basic idea of the field is to record the information in physical systems obeying the laws of quantum mechanics, which yields promising possibilities compared to the classical information.

Quantum information science is an intersection of mathematics, physics and informatics. We explain basic ingredients, that contribute to the general picture. Although we mention also some up-to-date experimental results, the focus will be on the theoretical description of a may-be quantum computer and quantum cryptography systems.

(TENTATIVE) CONTENTS

- (1) The differences between classical and quantum physics
 - Mach-Zehnder interferometer
 - Postulates of Quantum Mechanics
- (2) Algorithms and complexity
 - Notion of an algorithm
 - Gates and circuits
 - Reversible computation
- (3) Quantum algorithms
 - Deutsch-Jozsa algorithm
 - Fast Fourier Transform
 - Shor's factoring algorithm
 - Grover's search algorithm
- (4) Quantum cryptography
 - No Cloning Theorem
 - Protocol BB-84