Quantum Cryptography

IAM 510 Lecture Notes

Prof. Dr. İbrahim Yurdahan Güler

Contents

1 Lecture 1 **3**
- 1.1 Quantum Mechanics . . . 3
- 1.2 LINEAR OPERATORS ON V . . . 7
- 1.3 HOMEWORK . . . 8

2 LECTURE 2 **10**
- 2.1 THE POSTULATES OF QUANTUM MECHANICS . . . 14
- 2.2 HOMEWORK: . . . 16

3 LECTURE 3 **18**
- 3.1 HOWEWORK . . . 23

4 Lecture 4 **25**
- 4.1 Preliminary Study for Quantum Computation . . . 28

5 Lecture 5 **31**
- 5.1 Quantum Computation . . . 31
- 5.2 Quantum Computation . . . 32

6 Lecture 6 **36**

7 Lecture 7 **37**
- 7.1 Quantum Function Evaluation . . . 37
- 7.2 Simple Quantum Algorithms . . . 39

8 Lecture 8 **41**
- 8.1 Quantum Fourier Transformation . . . 41
- 8.2 Quantum Fourier Transformation . . . 42
- 8.3 Quantum Circuit of Discrete Fourier Transform . . . 44

9 Lecture 9 **46**
9.1 46
9.2 Shor's Factorization Algorithm 47

10 Lecture 10 **51**
10.1 Shor's Factorization Algorithm 51
10.2 Classical Case: 51
10.3 Quantum Case: 52
10.4 Polarization of Light 54

11 Lecture 11 **55**
11.1 Quantum Cryptography 55

12 Lecture 12 **59**
12.1 No Cloning Theorem 59
12.2 Quantum Dense Coding 60

13 Lecture 13 **64**
13.1 QUANTUM TELEPORTATION 64
13.2 PROCEDURE 64

14 Lecture 14 **67**
14.1 Physical Realizations 67

Chapter 1

Lecture 1

1.1 Quantum Mechanics

Quantum mechanics is based on classical mechanics. There are basically three approaches for point particle mechanics.

1. Newtonian:
$$\vec{F} = m \cdot \vec{a} = m \cdot \frac{\partial^2 \vec{r}}{\partial t^2} \tag{1.1}$$
This is a second order differential equation in time t.

2. Lagrangian: Motion is described by the function on which is called Lagrangian of the system of particles as,
$$L(q_i, \dot{q}_i, t) = T(q_i, \dot{q}_i) - V \tag{1.2}$$
Here q_i are generalized coordinates, $\dot{q}_i$ are generalized velocities. V is the potential, T is the total kinetic energy of the system in (1.2).

   Equations of motions are called the Euler-Lagrange equations, and they are expressed as:
$$\frac{d}{dt}\left(\frac{\partial L}{\partial \dot{q}_i}\right) - \frac{\partial L}{\partial q_i} = 0, \forall i = 1, ..., n$$
These equations are valid for conservative systems.

3. Hamiltonian: The physical system will be described by the Hamiltonian $H(q_i, p_i, t)$ in the phase .. space as,
$$H(q_i, p_i, t) = T(q_i, \dot{q}_i) + V \tag{1.3}$$