Course guide
270170 - CCQ - Quantum Computing and Cryptography

Last modified: 30/01/2024

Unit in charge:	Barcelona School of Informatics
Teaching unit:	748 - FIS - Department of Physics.
Degree:	BACHELOR'S DEGREE IN INFORMATICS ENGINEERING (Syllabus 2010). (Optional subject).

Academic year: 2023 **ECTS Credits:** 6.0 **Languages:** Catalan

LECTURER

Coordinating lecturer:	ROSENDO REY ORIOL
Others:	Primer quadrimestre: LLUIS AMETLLER CONGOST - 10 Segon quadrimestre: ROSENDO REY ORIOL - 10

PRIOR SKILLS

1. Knowledge of Physics and Mathematics at the Initial Phase level.

2. Abilities: Ability to learn, problem solving, information search, abstraction and use of mathematical language.

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:
CCO1.1. To evaluate the computational complexity of a problem, know the algorithmic strategies which can solve it and recommend, develop and implement the solution which guarantees the best performance according to the established requirements.
CT1.1A. To demonstrate knowledge and comprehension about the fundamentals of computer usage and programming, about operating systems, databases and, in general, about computer programs applicable to the engineering.
CT1.1B. To demonstrate knowledge and comprehension about the fundamentals of computer usage and programming. Knowledge about the structure, operation and interconnection of computer systems, and about the fundamentals of its programming.
CT1.2A. To interpret, select and value concepts, theories, uses and technological developments related to computer science and its application derived from the needed fundamentals of mathematics, statistics and physics. Capacity to solve the mathematical problems presented in engineering. Talent to apply the knowledge about: algebra, differential and integral calculus and numeric methods; statistics and optimization.
CT1.2B. To interpret, select and value concepts, theories, uses and technological developments related to computer science and its application derived from the needed fundamentals of mathematics, statistics and physics. Capacity to understand and dominate the physical and technological fundamentals of computer science: electromagnetism, waves, circuit theory, electronics and photonics and its application to solve engineering problems.
CT1.2C. To use properly theories, procedures and tools in the professional development of the informatics engineering in all its fields (specification, design, implementation, deployment and products evaluation) demonstrating the comprehension of the adopted compromises in the design decisions.

Generical:
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.

TEACHING METHODOLOGY

The theoretical content is worked out in theory classes followed by sessions of classes of problems, or in mixed theory/problem classes.

LEARNING OBJECTIVES OF THE SUBJECT

1.The student should be able to describe the behavior of micro particles.
2.The student should be able to list the postulates of quantum physics and apply them in specific cases.
3.The student should be able to work with quantum bits.
4.Students must be able to extract the probabilities of making measurements in Quantum Physics from a superposition state.
5.The student should be able to distinguish between separable states and entangled states.
6.Students must be able to apply entangled states in teleporting and dense coding.
7.Students must be able to describe the logic of some quantum encryption algorithms: BB84 and B92 protocols.
8.Students must be able to do simulations of the protocols BB84 and B92.
9.Students must be able to describe the logic of quantum algorithms of academic interest: Deutsch, Deutsch-Jozsa generalizations and Vazirani.
10.The student should be able to implement the algorithm of Grover search for an item within an unstructured database.
11.Students must be able to implement the classic encryption algorithm RSA.
12.Students must be able to implement all the basic ingredients of Shor's factoring algorithm.

STUDY LOAD

Type	Hours	Percentage
Hours large group	30,0	20.00
Guided activities	6,0	4.00
Hours medium group	30,0	20.00
Self study	84,0	56.00

Total learning time: 150 h

CONTENTS

Topic 1: Quantum Physics.

Description:
Brief introduction to quantum physics and its importance in the microcosm world.
The historical motivation is given and deepens especially in the wave-particle duality.
The postulates of quantum physics are introduced, with special emphasis on the Schrödinger equation and the probabilistic nature of the measure.
The solution to the Schrödinger equation for a potential well of infinite-dimensional is presented. The example contains all the basic ingredients for understanding the stationary states and also the superposition of states, which will have a prominent role for the description of quantum bits.

Topic 2: Qubits.

Description:
Systems of two states: quantum bits (qubits).
The basic operations through Kets and bras are introduced, the brackets as scalar products, superpositions of base's states.

Topic 3: Quantum cryptography.

Description:
The basic principles of quantum cryptography are outlined. Protocols that use entanglement, such as Eckert's one and others, based on the measure's postulate such as BB84 and B92,
are given detailed attention.

Topic 4: Quantum Logic. Gates and simple quantum algorithms.

Description:
A description is given of:
a) The temporal evolution of the qubits is given in terms of unitary operators operators and their connection with quantum logic gates.
b) The minimal set of quantum logic gates that allows any computation performed on any system implying an arbitrary number of qubits.
c) Quantum gate diagrams, as a flowchart of the computation.
d) The evaluation of quantum functions, implemented by unitary operators.
e) Simple quantum algorithms of academic interest are worked out:
Deutsch, Deutsch-Jozsa and Vazirani.

Topic 5: Grover algorithm about finding elements of an unstructured database.

Description:
The algorithm to find an item in an unstructured database, known as Grover's algorithm, which is able to locate it with an efficiency that scales as
square root of N, N being the total number of items in the database.

Topic 6: Shor's factoring algorithm.

Description:
From the foundations of the classical RSA encryption's algorithm, the Shor's quantum factoring algorithm is introduced.
A detailed description is given, distinguishing those parts of the purely classical algorithm, requiring concepts of number theory, modular arithmetic and continuous fractions, from the quantum part, which uses the principle of superposition and quantum Fourier transform to extract the period of a periodic function, from which one can deduce the factors of the number to be factorized.

ACTIVITIES

Introduction and summary of the content of the course.

Description:
Slides with all the course's contents are displayed and commented, thus being an introduction and summary at the same time.

Specific objectives:
1, 2, 3

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.

Full-or-part-time: 6h
Theory classes: 2h
Self study: 4h

Item 1: Quantum Physics.

Description:
Development of the Quantum Physics subject.

Specific objectives:
1, 2

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.

Full-or-part-time: 24h
Theory classes: 6h
Practical classes: 6h
Self study: 12h

Control of solving problems related to item 1.

Description:
It is a control about solving problems in class by students.

Specific objectives:
1, 2

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.

Full-or-part-time: 7h
Guided activities: 1h
Self study: 6h

Item 2: Qubits

Description:
Development of the contents of the topic 2.

Specific objectives:
3, 4, 5, 6

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.

Full-or-part-time: 14h
Theory classes: 4h
Practical classes: 4h
Self study: 6h

Item 3: Quantum Chryptography

Description:
Development of the contents of topic 3.

Specific objectives:
7, 8

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.

Full-or-part-time: 11h
Theory classes: 3h
Practical classes: 4h
Self study: 4h

Solving problems of qubits and Quantum Cryptography's control.

Description:
Test where the students need to solve a series of problems

Specific objectives:
7

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.

Full-or-part-time: 9h
Guided activities: 1h
Self study: 8h

Item 4: Quantum Gates and simple Quantum Algorithms.

Description:
Development of the contents of topic 4.

Specific objectives:
9

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.

Full-or-part-time: 20h
Theory classes: 5h
Practical classes: 5h
Self study: 10h

Control of solving problems related to simple quantum algorithms.

Description:
It is a control about solving problems in class by students.

Specific objectives:
9

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.

Full-or-part-time: 7h
Guided activities: 1h
Self study: 6h

Item 5: Grover's algorithm.

Description:
Development of the topic 5.

Specific objectives:
10

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.

Full-or-part-time: 12h
Theory classes: 2h
Practical classes: 2h
Self study: 8h

Item 6: Shor's factorization algorithm.

Description:
Development of the topic 6.

Specific objectives:
11, 12

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.

Full-or-part-time: 27h
Theory classes: 6h
Practical classes: 5h
Self study: 16h

Control of solving problems related to items 5 and 6.

Description:
It is a control about solving problems in class by students.

Specific objectives:
10, 11, 12

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.

Full-or-part-time: 11h
Guided activities: 1h
Self study: 10h

Final exam

Description:
Final test for those students who aim for a better grade or those that have failed the continued evaluation

Specific objectives:
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.

Full-or-part-time: 2h
Guided activities: 2h

GRADING SYSTEM

The technical skills grade results from 2 contributions:

- Arithmetic mean of 4 exams that are performed during the year (C)
- Arithmetic mean of exercises to do at home (E)

The continuous assessment (AC) grade is computed as: AC = 0.8 + 0.2 * C * E

There will be a final exam (with grade F) for those students who have not passed the continuous assessment, or wish to improve their AC grade.

The final grade will be the maximum between AC and F.

The grade of the transversal competence G9.1 will be determined from the exams of the continuous assessment, with grades: A (excellent), B (best), C (adequate), D (not completed).

BIBLIOGRAPHY

Basic:
- French, A. P; Taylor, Edwin F. Introducción a la física cuántica. Reverté, 1982. ISBN 8429141677.