270170 - CCQ - Quantum Computing and Cryptography

Coordinating unit: 270 - FIB - Barcelona School of Informatics
Teaching unit: 748 - FIS - Department of Physics
Academic year: 2019
Degree: BACHELOR'S DEGREE IN INFORMATICS ENGINEERING (Syllabus 2010). (Teaching unit Optional)
ECTS credits: 6
Teaching languages: Catalan

Teaching staff

Coordinator: - Lluis Ametller Congost (lluis.ametller@upc.edu)

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

<table>
<thead>
<tr>
<th>Total learning time: 150h</th>
<th>Hours large group:</th>
<th>30h</th>
<th>20.00%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours medium group:</td>
<td>30h</td>
<td>20.00%</td>
<td></td>
</tr>
<tr>
<td>Hours small group:</td>
<td>0h</td>
<td>0.00%</td>
<td></td>
</tr>
<tr>
<td>Guided activities:</td>
<td>6h</td>
<td>4.00%</td>
<td></td>
</tr>
<tr>
<td>Self study:</td>
<td>84h</td>
<td>56.00%</td>
<td></td>
</tr>
</tbody>
</table>
# Content

## Topic 1: Quantum Physics.

**Degree competences to which the content contributes:**

**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.

**Degree competences to which the content contributes:**

**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.

**Degree competences to which the content contributes:**

**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.


**Degree competences to which the content contributes:**

**Description:**
- A description is given of:
  - a) The temporal evolution of the qubits is given in terms of unitary 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.**

**Degree competences to which the content contributes:**

**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.**

**Degree competences to which the content contributes:**

**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.
### Planning of activities

<table>
<thead>
<tr>
<th>Description</th>
<th>Hours</th>
<th>Theory classes</th>
<th>Practical classes</th>
<th>Laboratory classes</th>
<th>Guided activities</th>
<th>Self study</th>
</tr>
</thead>
</table>
| **Introduction and summary of the content of the course.**  
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 | | 6h | | | | 4h |
| **Item 1: Quantum Physics.**  
Development of the Quantum Physics subject.  
**Specific objectives:**  
1, 2 | | 24h | 6h | 5h | 0h | 12h |
| **Control of solving problems related to item 1.**  
It is a control about solving problems in class by students.  
**Specific objectives:**  
1, 2 | | 7h | | | 1h | 6h |
| **Item 2: Qubits** | | 15h | 4h | 4h | 0h | 6h | 1h |

**Description:**  
Development of the contents of the topic 2.
### Specific objectives:

3, 4, 5, 6

### Control of problem solving about single qubits and systems of qubits.

<table>
<thead>
<tr>
<th>Hours</th>
<th>9h</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guided activities</td>
<td>1h</td>
</tr>
<tr>
<td>Self study</td>
<td>8h</td>
</tr>
</tbody>
</table>

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

**Specific objectives:**
3, 5

### Item 3: Quantum Chryptography

<table>
<thead>
<tr>
<th>Hours</th>
<th>11h</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theory classes</td>
<td>3h</td>
</tr>
<tr>
<td>Practical classes</td>
<td>4h</td>
</tr>
<tr>
<td>Laboratory classes</td>
<td>0h</td>
</tr>
<tr>
<td>Guided activities</td>
<td>0h</td>
</tr>
<tr>
<td>Self study</td>
<td>4h</td>
</tr>
</tbody>
</table>

**Description:**
Development of the contents of topic 3.

**Specific objectives:**
7, 8

### Solving problems of Quantum Cryptography's control.

<table>
<thead>
<tr>
<th>Hours</th>
<th>1h</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guided activities</td>
<td>1h</td>
</tr>
<tr>
<td>Self study</td>
<td>0h</td>
</tr>
</tbody>
</table>

**Description:**
Control of problem solving about Quantum Cryptography.

**Specific objectives:**
7

### Item 4: Quantum Gates and simple Quantum Algorithms.

<table>
<thead>
<tr>
<th>Hours</th>
<th>20h</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theory classes</td>
<td>5h</td>
</tr>
<tr>
<td>Practical classes</td>
<td>4h</td>
</tr>
<tr>
<td>Laboratory classes</td>
<td>0h</td>
</tr>
<tr>
<td>Guided activities</td>
<td>1h</td>
</tr>
<tr>
<td>Self study</td>
<td>10h</td>
</tr>
</tbody>
</table>

**Description:**
Development of the contents of topic 4.
### Specific objectives:
- 9

### Control of solving problems related to simple quantum algorithms.

**Hours:** 7h  
Guided activities: 1h  
Self study: 6h

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

### Item 5: Grover's algorithm.

**Hours:** 15h  
Theory classes: 4h  
Practical classes: 2h  
Laboratory classes: 0h  
Guided activities: 1h  
Self study: 8h

**Description:**  
Development of the topic 5.

### Item 6: Shor's factorization algorithm.

**Hours:** 29h  
Theory classes: 6h  
Practical classes: 5h  
Laboratory classes: 0h  
Guided activities: 2h  
Self study: 16h

**Description:**  
Development of the topic 6.

### Specific objectives:
- 10
- 11, 12

### Control of solving problems related to items 5 and 6.

**Hours:** 12h  
Guided activities: 2h  
Self study: 10h

**Description:**  
It is a control about solving problems in class by students.
The grade of the technical skills of the course is calculated from 2 sources:
- Arithmetic mean of 4 or 5 exams that are performed during the year (C)
- Arithmetic mean of exercises to do at home (E)

The grade of the continuous assessment (CA) is: \[ AC = 0.8 + 0.2 \times C \times E \]

There will be a final exam for those students who have not passed the continuous assessment, or want to improve the grade.

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

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

**Bibliography**

**Basic:**