Guía docente
270170 - CCQ - Computación y Criptografía Cuánticas

Última modificación: 11/07/2025

Unidad responsable: Facultad de Informática de Barcelona
Unidad que imparte: 748 - FIS - Departamento de Física.

Titulación: GRADO EN INGENIERÍA INFORMÁTICA (Plan 2010). (Asignatura optativa).

Curso: 2025 **Créditos ECTS:** 6.0 **Idiomas:** Catalán

PROFESORADO

Profesorado responsable: ROSENDO REY ORIOL

Otros: Primer quadrimestre:
LLUIS AMETLLER CONGOST - 10

CAPACIDADES PREVIAS

1. Conocimientos: Física y Matemáticas a nivell de Fase Inicial.

2. Capacidades: Capacidad de aprendizaje, de resolución de problemas, de búsqueda de información, de abstracción y de uso del lenguaje matemático.

COMPETENCIAS DE LA TITULACIÓN A LAS QUE CONTRIBUYE LA ASIGNATURA

Específicas:
CCO1.1. Evaluar la complejidad computacional de un problema, conocer estrategias algorítmicas que puedan conducir a su resolución, y recomendar, desarrollar e implementar la que garantice el mejor rendimiento de acuerdo con los requisitos establecidos.
CT1.1A. Demostrar conocimiento y comprensión de los conceptos fundamentales de la programación y de la estructura básica de un computador. CEFB4. Conocimiento de los fundamentos del uso y programación de los computadores, los sistemas operativos, las bases de datos y, en general, los programas informáticos con aplicación en ingeniería.
CT1.1B. Interpretar, seleccionar y valorar conceptos, teorías, usos y desarrollos tecnológicos relacionados con la informática y su aplicación a partir de los fundamentos matemáticos, estadísticos y físicos necesarios. CEFB2. Capacidad para comprender y dominar los fundamentos físicos y tecnológicos de la informática: electromagnetismo, ondas, teoría de circuitos, electrónica y fotónica y su aplicación para la resolución de problemas propios de la ingeniería.
CT1.2A. Demostrar conocimiento y comprensión de los conceptos fundamentales de la programación y de la estructura básica de un computador. CEFB5. Conocimiento de la estructura, funcionamiento e interconexión de los sistemas informáticos, así como los fundamentos de su programación.
CT1.2B. Interpretar, seleccionar y valorar conceptos, teorías, usos y desarrollos tecnológicos relacionados con la informática y su aplicación a partir de los fundamentos matemáticos, estadísticos y físicos necesarios. CEFB3. Capacidad para comprender y dominar los conceptos básicos de matemática discreta, lógica, algorítmica y complejidad computacional, y su aplicación para el tratamiento automático de la información por medio de sistemas computacionales y su aplicación para la resolución de problemas propios de la ingeniería.
CT1.2C. Interpretar, seleccionar y valorar conceptos, teorías, usos y desarrollos tecnológicos relacionados con la informática y su aplicación a partir de los fundamentos matemáticos, estadísticos y físicos necesarios. CEFB1: Capacidad para la resolución de los problemas matemáticos que puedan plantarse en la ingeniería. Aptitud para aplicar los conocimientos sobre: algebra, cálculo diferencial e integral i métodos numéricos; estadística y optimización.

Genéricas:
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

METODOLOGÍAS DOCENTES

Los contenidos teóricos se trabajarán en clases de teoría seguidas de sesiones de clases de problemas, o bien en clases mixtas de teoría / problemas.

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

1.El alumno ha de ser capaz de describir el comportamiento de las partículas del microcosmos.
2.El alumno ha de ser capaz de enumerar los postulados de la Física Cuántica y aplicarlos en casos concretos.
3.El alumno ha de ser capaz de completar operaciones básicas con bits cuánticos.
4.El alumno debe ser capaz de extraer las probabilidades de hacer medidas en Física Cuántica a partir de un estado superposición
5.El alumno ha de ser capaz de distinguir entre estados separables y estados entrelazados.
6.El alumno debe ser capaz de aplicar los estados entrelazados en teleportación y codificación densa.
7.El alumno debe ser capaz de describir la lógica de algunos algoritmos cuánticos de encriptación: Protocolos BB84 y B92.
8.El alumno debe ser capaz de hacer simulaciones de los protocolos BB84 y B92.
9.El alumno debe ser capaz de describir la lógica de algoritmos cuánticos de interés académico: Deutsch, su generalización Deutsch-Jozsa y Vazirani.
10.El alumno debe ser capaz de implementar el Algoritmo de Grover de búsqueda de un elemento dentro de una base de datos no estructurada.
11.El alumno debe ser capaz de implementar el algoritmo clásico de encriptación RSA.
12.El alumno debe ser capaz de implementar todos los ingredientes básicos del algoritmo de factorización de Shor.

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTADO

Tipo	Horas	Porcentaje
Horas grupo mediano	30,0	20.00
Horas actividades dirigidas	6,0	4.00
Horas grupo grande	30,0	20.00
Horas aprendizaje autónomo	84,0	56.00

Dedicación total: 150 h

CONTENIDOS

Tema 1: Física Cuántica.

Descripción:
Breve introducción a la Física Cuántica y su importancia en el mundo del microcosmos.
Se hace énfasis en la motivación histórica y se incide especialmente en la dualidad onda-partícula.
Se introducen los postulados de la Física Cuántica, haciendo especial énfasis en la ecuación de Schrödinger y en el carácter probabilístico de la medida.
Se resuelve la ecuación de Schrödinger para un potencial unidimensional de un pozo infinito. El ejemplo contiene todos los ingredientes básicos para entender los estados estacionarios y la superposición de estados,
que tendrán un papel preeminente para la descripción de los bits cuánticos.

Tema 2: Qubits.

Descripción:
Sistemas de dos estados: bits cuánticos (qubits).
Se introducen las operaciones básicas a través de bras y kets, los brackets como productos escalares, las superposiciones de estados base.

Tema 3: Criptografía Cuántica.

Descripción:
Se exponen los principios básicos de la Criptografía Cuántica. Protocolos que usan el entrelazamiento, como el de Eckert y otros, basados en el postulado de medida como son BB84 y B92, son analizados en detalle.

Tema 4: Lógica Cuántica. Puertas y algoritmos cuánticos sencillos.

Descripción:
Se describe:
a) Se describe la evolución temporal de los qubits en términos de operadores unitarios y su conexión con las puertas lógicas cuánticas.
b) El conjunto mínimo de puertas lógicas cuánticas que permite realizar cualquier computación en sistemas de un número arbitrario de qubits.
c) Los diagramas de puertas, como diagramas de flujo de la computación.
d) La evaluación de funciones cuánticas, implementadas con operadores unitarios.
e) Algoritmos cuánticos sencillos de interés académico: Deutsch, Deutsch-Jozsa y Vazirani.

Tema 5: Algoritmo de Grover de búsqueda de elementos en una base de datos no estructurada.

Descripción:
Se estudia con detalle el algoritmo de búsqueda de un elemento en una base de datos no estructurada, conocido como algoritmo de Grover, capaz de localizarlo con una eficiencia que escala como
raíz cuadrada de N, siendo N el número total de elementos de la base de datos.

Tema 6: Algoritmo de factorización de Shor.

Descripción:
A partir de las bases del algoritmo clásico de encriptación RSA, se introduce el algoritmo cuántico de factorización de Shor.
Se da una descripción detallada distinguiendo aquellas partes del algoritmo puramente clásicas, que requieren conceptos de teoría de números, aritmética modular y fracciones continuas, de la parte cuántica, que utiliza el principio de superposición y la transformada de Fourier cuántica , para extraer el periodo de una función periódica, a partir del cual se pueden deducir los factores del número a factorizar.

ACTIVIDADES

Exposición y sumario del contenido de todo el curso.

Descripción:
Se expone con transparencias todo el contenido del curso, siendo pues una introducción y sumario a la vez.

Objetivos específicos:
1, 2, 3

Competencias relacionadas:
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 6h
Aprendizaje autónomo: 4h
Grupo grande/Teoría: 2h

Tema 1: Física Cuántica.

Descripción:
Desarrollo del tema de Física Cuántica.

Objetivos específicos:
1, 2

Competencias relacionadas:
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 24h
Aprendizaje autónomo: 12h
Grupo grande/Teoría: 6h
Grupo mediano/Prácticas: 6h

Control de resolución de problemas asociados al tema 1.

Descripción:
Es un control en el que se proponen problemas para resolver en clase por parte de los estudiantes.

Objetivos específicos:
1, 2

Competencias relacionadas:
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 7h
Aprendizaje autónomo: 6h
Actividades dirigidas: 1h

Tema 2: Qubits

Descripción:
Se desarrollan los contenidos del tema 2.

Objetivos específicos:
3, 4, 5, 6

Competencias relacionadas:
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 14h
Aprendizaje autónomo: 6h
Grupo grande/Teoría: 4h
Grupo mediano/Prácticas: 4h

Tema 3: Criptografía Cuántica.

Descripción:
Se desarrollan los contenidos del tema 3.

Objetivos específicos:
7, 8

Competencias relacionadas:
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 11h
Aprendizaje autónomo: 4h
Grupo grande/Teoría: 3h
Grupo mediano/Prácticas: 4h

Control de resolución problemas de qubits y Criptografía Cuántica.

Descripción:
Es un control en el que se proponen problemas para resolver en clase por parte de los estudiantes.

Objetivos específicos:
7

Competencias relacionadas:
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 9h
Aprendizaje autónomo: 8h
Actividades dirigidas: 1h

Tema 4: Puertas Cuánticas y Algoritmos cuánticos sencillos.

Descripción:
Se desarrollan los contenidos del tema 4.

Objetivos específicos:
9

Competencias relacionadas:
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 20h
Aprendizaje autónomo: 10h
Grupo grande/Teoría: 5h
Grupo mediano/Prácticas: 5h

Control de resolución problemas de algoritmos cuánticos sencillos y puertas cuánticas.

Descripción:
Es un control de resolución de problemas por parte de los estudiantes, realizado en horas de clase.

Objetivos específicos:
9

Competencias relacionadas:
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 7h
Aprendizaje autónomo: 6h
Actividades dirigidas: 1h

Tema 5: Algoritmo de Grover.

Descripción:
Desarrollo del tema 5.

Objetivos específicos:
10

Competencias relacionadas:
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 12h
Aprendizaje autónomo: 8h
Grupo grande/Teoría: 2h
Grupo mediano/Prácticas: 2h

Tema 6: Algoritmo de factorització de Shor.

Descripción:
Desarrollo del tema 6.

Objetivos específicos:
11, 12

Competencias relacionadas:
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 27h
Aprendizaje autónomo: 16h
Grupo grande/Teoría: 6h
Grupo mediano/Prácticas: 5h

Control de resolución de problemas de los algoritmos de Grover y de Shor.

Descripción:
Es un control en el que se proponen problemas para resolver en clase por parte de los estudiantes.

Objetivos específicos:
10, 11, 12

Competencias relacionadas:
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 11h
Aprendizaje autónomo: 10h
Actividades dirigidas: 1h

Examen final

Descripción:
Prueba final para los estudiantes que deseen mejorar notas o aquellos que no han superado la evaluación continuada

Objetivos específicos:
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

Competencias relacionadas:
G9. RAZONAMIENTO: Capacidad de razonamiento crítico, lógico y matemático. Capacidad para resolver problemas dentro de su área de estudio. Capacidad de abstracción: capacidad de crear y utilizar modelos que reflejen situaciones reales. Capacidad de diseñar y realizar experimentos sencillos, y analizar e interpretar sus resultados. Capacidad de análisis, síntesis y evaluación.

Dedicación: 2h
Actividades dirigidas: 2h

SISTEMA DE CALIFICACIÓN

La nota de las competencias técnicas de la asignatura se calculará a partir de 2 notas:

- Media aritmética de 4 controles que se realizarán durante el curso (C)
- Media aritmética de ejercicios propuestos para hacer en casa (E)

La nota de la evaluación contínua (AC) será: AC = 0.8 * C + 0.2 * E

Se hará un examen final (con nota F) para aquellos alumnos que no hayan aprobado la evaluación contínua, o quieran mejorar nota.

La nota final será la máxima entre AC i F.

La nota de la competencia transversal G9.1 resultará de los controles que dan lugar a la evaluación contínua, con calificaciones: A (excelente), B (óptimo), C (suficiente), D (no superado).

BIBLIOGRAFÍA

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