

Guia docent

270170 - CCQ - Computació i Criptografia Quàntiques

Última modificació: 10/02/2025

Unitat responsable: Facultat d'Informàtica de Barcelona

Unitat que imparteix: 748 - FIS - Departament de Física.

Titulació: GRAU EN ENGINYERIA INFORMÀTICA (Pla 2010). (Assignatura optativa).

Curs: 2024

Crèdits ECTS: 6.0

Idiomes: Català

PROFESSORAT

Professorat responsable: ROSENDO REY ORIOL

Altres: Primer quadrimestre:
LLUIS AMETLLER CONGOST - 10

Segon quadrimestre:
ROSENDO REY ORIOL - 10

CAPACITATS PRÈVIES

1. Coneixements: Física i Matemàtiques de nivell Fase Inicial.

2. Capacitats: Capacitat d'aprenentatge, de resolució de problemes, de cerca d'informació, d'abstracció i d'ús del llenguatge matemàtic.

COMPETÈNCIES DE LA TITULACIÓ A LES QUALS CONTRIBUEIX L'ASSIGNATURA

Específiques:

CCO1.1. Avaluar la complexitat computacional d'un problema, conèixer estratègies algorísmiques que puguin dur a la seva resolució, i recomanar, desenvolupar i implementar la que garanteixi el millor rendiment d'acord amb els requisits establerts.

CT1.1A. Demostrar coneixement i comprensió dels conceptes fonamentals de la programació i de l'estructura bàsica d'un computador.

CEFB4. Coneixement dels fonaments de l'ús i de la programació dels computadors, dels sistemes operatius, de les bases de dades i, en general, dels programes informàtics amb aplicació a l'enginyeria.

CT1.1B. Demostrar coneixement i comprensió dels conceptes fonamentals de la programació i de l'estructura bàsica d'un computador.

CEFB5. Coneixement de l'estructura, funcionament i interconnexió dels sistemes informàtics, i dels fonaments de la seva programació.

CT1.2A. Interpretar, seleccionar i valorar conceptes, teories, usos i desenvolupaments tecnològics relacionats amb la informàtica i la seva aplicació a partir dels fonaments matemàtics, estadístics i físics necessaris. CEFB1: capacitat per a resoldre els problemes matemàtics que es plantegin en la enginyeria. Aptitud per a aplicar els coneixements sobre: àlgebra, càlcul diferencial i integral i mètodes numèrics; estadística i optimització.

CT1.2B. Interpretar, seleccionar i valorar conceptes, teories, usos i desenvolupaments tecnològics relacionats amb la informàtica i la seva aplicació a partir dels fonaments matemàtics, estadístics i físics necessaris. CEFB2. Capacitat per a comprendre i dominar els fonaments físics i tecnològics de la informàtica: electromagnetisme, ones, teoria de circuits, electrònica i fotònica i la seva aplicació per a la resolució de problemes propis de l'enginyeria.

CT1.2C. Interpretar, seleccionar i valorar conceptes, teories, usos i desenvolupaments tecnològics relacionats amb la informàtica i la seva aplicació a partir dels fonaments matemàtics, estadístics i físics necessaris. CEFB3. Capacitat per a comprendre i dominar els conceptes bàsics de matemàtica discreta, lògica, algorísmica i complexitat computacional, i la seva aplicació per al tractament automàtic de la informació mitjançant sistemes computacionals i la seva aplicació per a la resolució de problemes propis de l'enginyeria.

Genèriques:

G9. Capacitat de raonament crític, lògic i matemàtic. Capacitat de resoldre problemes en la seva àrea d'estudi. Capacitat d'abstracció: capacitat de crear i utilitzar models que reflecteixin situacions reals. Capacitat de dissenyar i realitzar experiments senzills, i analitzar-ne i interpretar-ne els resultats. Capacitat d'anàlisi, de síntesi i d'avaluació.

METODOLOGIES DOCENTS

Els continguts teòrics es treballaran en classes de teoria seguides de sessions de classes de problemes, o bé en classes mixtes de teoria/problemes.

OBJECTIUS D'APRENTATGE DE L'ASSIGNATURA

- 1.L'alumne ha de ser capaç de descriure el comportament de les partícules del microcosmos.
- 2.L'alumne ha de ser capaç d'enumerar els postulats de la Física Quàntica i aplicar-los en casos concrets.
- 3.L'alumne ha de ser capaç de completar operacions bàsiques amb bits quàntics.
- 4.L'alumne ha de ser capaç d'extreure les probabilitats de fer mesures en Física Quàntica a partir d'un estat superposició.
- 5.L'alumne ha de ser capaç de distingir entre estats separables i estats entrellaçats.
- 6.L'alumne ha de ser capaç d'aplicar els estats entrellaçats en teleportació i codificació densa,
- 7.L'alumne ha de ser capaç de descriure la lògica d'alguns algorismes quàntics d'encryptació: Protocols BB84 i B92,.
- 8.L'alumne ha de ser capaç de fer simulacions dels protocols BB84 i B92.
- 9.L'alumne ha de ser capaç de descriure la lògica d'algorismes quàntics d'interès acadèmic: Deutsch, la seva generalització Deutsch-Jozsa i Vazirani.
- 10.L'alumne ha de ser capaç d'implementar l'Algorisme de Grover de busca d'un element dins una base de dades no estructurada..
- 11.L'alumne ha de ser capaç d'implementar l'algorisme clàssic d'encryptació RSA.
- 12.L'alumne ha de ser capaç d'implementar tots els ingredients bàsics de l'algorisme de factorització de Shor.

HORES TOTALES DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores activitats dirigides	6,0	4.00
Hores aprenentatge autònom	84,0	56.00
Hores grup gran	30,0	20.00
Hores grup mitjà	30,0	20.00

Dedicació total: 150 h

CONTINGUTS

Tema 1: Física Quàntica.

Descripció:

Breu introducció a la Física Quàntica i la seva importància en el món del microcosmos.

Es fa èmfasi en la motivació històrica i s'incideix especialment en la dualitat ona-partícula.

S'introdueixen els postulats de la Física Quàntica, fent èmfasi especial en l'equació de Schrödinger i en el caràcter probabilístic de la mesura.

Es resol l'equació de Schrödinger per un potencial unidimensional d'un pou infinit. L'exemple conté tots els ingredients bàsics per entendre els estats estacionaris i la superposició d'estats, que tindran un paper preeminent per la descripció dels bits quàntics.

Tema 2: Qubits.

Descripció:

Sistemes de dos estats: bits quàntics (qubits).

S'introdueixen les operacions bàsiques a través de bras i kets, els brackets com a productes escalars, les superposicions d'estats base.

Tema 3: Criptografia Quàntica.

Descripció:

S'exposen els principis bàsics de la Criptografia Quàntica. S'analitzen en detall protocols que usen l'entrellaçament com el d'Eckert, i d'altres basats en el postulat de mesura com són BB84 i B92.

Tema 4: Lògica Quàntica. Portes i algorismes quàntics senzills.

Descripció:

Es descriu:

- a) L'evolució temporal dels qubits en termes d'operadors unitaris i la seva connexió amb les portes lògiques quàntiques.
- b) El conjunt mínim de portes lògiques quàntiques que permet realitzar qualsevol computació en sistemes d'un nombre arbitrari de qubits.
- c) Els diagrames de portes, com a diagrames de flux de la computació.
- d) L'evaluació de funcions quàntiques, implementades amb operadors unitaris.
- e) Algorismes quàntics senzills d'interès acadèmic: Deutsch, Deutsch-Jozsa i Vazirani.

Tema 5: Algorisme de Grover de busca d'elements en una base de dades no estructurada.

Descripció:

S'estudia en detall l'algorisme de busca d'un element en una base de dades no estructurada, conegut com algorisme de Grover, capaç de localitzar-lo amb una eficiència que escala com arrel quadrada de N , essent N el nombre total d'elements de la base de dades.

Tema 6: Algorisme de factorització de Shor.

Descripció:

A partir de les bases de l'algorisme clàssic d'encryptació RSA, s'introdueix l'algorisme quàntic de factorització de Shor.

S'en dona una descripció detallada distingint-ne aquelles parts de l'algorisme purament clàssiques, que requereixen conceptes de teoria de nombres, aritmètica modular i fraccions contínues, de la part quàntica, que utilitza el principi de superposició i la transformada de Fourier quàntica, per extreure el període d'una funció periòdica, a partir del qual es poden deduir els factors del nombre a factoritzar.

ACTIVITATS

Exposició i sumari del contingut de tot el curs.

Descripció:

S'exposa amb transparències tot el contingut del curs, essent doncs una introducció i sumari a la vegada.

Objectius específics:

1, 2, 3

Competències relacionades:

G9. Capacitat de raonament crític, lògic i matemàtic. Capacitat de resoldre problemes en la seva àrea d'estudi. Capacitat d'abstracció: capacitat de crear i utilitzar models que reflecteixin situacions reals. Capacitat de dissenyar i realitzar experiments senzills, i analitzar-ne i interpretar-ne els resultats. Capacitat d'anàlisi, de síntesi i d'avaluació.

Dedicació: 6h

Aprenentatge autònom: 4h

Grup gran/Teoria: 2h

Tema 1: Física Quàntica.

Descripció:

Desenvolupament del tema de Física Quàntica.

Objectius específics:

1, 2

Competències relacionades:

G9. Capacitat de raonament crític, lògic i matemàtic. Capacitat de resoldre problemes en la seva àrea d'estudi. Capacitat d'abstracció: capacitat de crear i utilitzar models que reflecteixin situacions reals. Capacitat de dissenyar i realitzar experiments senzills, i analitzar-ne i interpretar-ne els resultats. Capacitat d'anàlisi, de síntesi i d'avaluació.

Dedicació: 24h

Aprenentatge autònom: 12h

Grup gran/Teoria: 6h

Grup mitjà/Pràctiques: 6h

Control de resolució de problemes associats al tema 1.

Descripció:

És un control on es proposen problemes per resoldre a classe per part dels estudiants.

Objectius específics:

1, 2

Competències relacionades:

G9. Capacitat de raonament crític, lògic i matemàtic. Capacitat de resoldre problemes en la seva àrea d'estudi. Capacitat d'abstracció: capacitat de crear i utilitzar models que reflecteixin situacions reals. Capacitat de dissenyar i realitzar experiments senzills, i analitzar-ne i interpretar-ne els resultats. Capacitat d'anàlisi, de síntesi i d'avaluació.

Dedicació: 7h

Aprenentatge autònom: 6h

Activitats dirigides: 1h

Tema 2: Qubits

Descripció:

Es desenvolupen els continguts del tema 2.

Objectius específics:

3, 4, 5, 6

Competències relacionades:

G9. Capacitat de raonament crític, lògic i matemàtic. Capacitat de resoldre problemes en la seva àrea d'estudi. Capacitat d'abstracció: capacitat de crear i utilitzar models que reflecteixin situacions reals. Capacitat de dissenyar i realitzar experiments senzills, i analitzar-ne i interpretar-ne els resultats. Capacitat d'anàlisi, de síntesi i d'avaluació.

Dedicació: 14h

Aprenentatge autònom: 6h

Grup gran/Teoria: 4h

Grup mitjà/Pràctiques: 4h

Tema 3: Criptografia Quàntica

Descripció:

Es desenvolupa el tema 3.

Objectius específics:

7, 8

Competències relacionades:

G9. Capacitat de raonament crític, lògic i matemàtic. Capacitat de resoldre problemes en la seva àrea d'estudi. Capacitat d'abstracció: capacitat de crear i utilitzar models que reflecteixin situacions reals. Capacitat de dissenyar i realitzar experiments senzills, i analitzar-ne i interpretar-ne els resultats. Capacitat d'anàlisi, de síntesi i d'avaluació.

Dedicació: 11h

Aprenentatge autònom: 4h

Grup gran/Teoria: 3h

Grup mitjà/Pràctiques: 4h

Control de resolució problemes de qubits i Criptografia Quàntica.

Descripció:

És un control on es proposen problemes per resoldre a classe per part dels estudiants.

Objectius específics:

7

Competències relacionades:

G9. Capacitat de raonament crític, lògic i matemàtic. Capacitat de resoldre problemes en la seva àrea d'estudi. Capacitat d'abstracció: capacitat de crear i utilitzar models que reflecteixin situacions reals. Capacitat de dissenyar i realitzar experiments senzills, i analitzar-ne i interpretar-ne els resultats. Capacitat d'anàlisi, de síntesi i d'avaluació.

Dedicació: 9h

Aprenentatge autònom: 8h

Activitats dirigides: 1h

Tema 4: Portes Quàntiques i Algorismes quàntics senzills.

Descripció:

Es desenvolupen els continguts del tema 4.

Objectius específics:

9

Competències relacionades:

G9. Capacitat de raonament crític, lògic i matemàtic. Capacitat de resoldre problemes en la seva àrea d'estudi. Capacitat d'abstracció: capacitat de crear i utilitzar models que reflecteixin situacions reals. Capacitat de dissenyar i realitzar experiments senzills, i analitzar-ne i interpretar-ne els resultats. Capacitat d'anàlisi, de síntesi i d'avaluació.

Dedicació: 20h

Aprenentatge autònom: 10h

Grup gran/Teoria: 5h

Grup mitjà/Pràctiques: 5h

Control de resolució de problemes d'algorismes quàntics senzills i portes quàntiques.

Descripció:

És un control de resolució de problemes per part dels estudiants, realitzat en hores de classe.

Objectius específics:

9

Competències relacionades:

G9. Capacitat de raonament crític, lògic i matemàtic. Capacitat de resoldre problemes en la seva àrea d'estudi. Capacitat d'abstracció: capacitat de crear i utilitzar models que reflecteixin situacions reals. Capacitat de dissenyar i realitzar experiments senzills, i analitzar-ne i interpretar-ne els resultats. Capacitat d'anàlisi, de síntesi i d'avaluació.

Dedicació: 7h

Aprenentatge autònom: 6h

Activitats dirigides: 1h

Tema 5: Algorisme de Grover.

Descripció:

Desenvolupament del tema 5.

Objectius específics:

10

Competències relacionades:

G9. Capacitat de raonament crític, lògic i matemàtic. Capacitat de resoldre problemes en la seva àrea d'estudi. Capacitat d'abstracció: capacitat de crear i utilitzar models que reflecteixin situacions reals. Capacitat de dissenyar i realitzar experiments senzills, i analitzar-ne i interpretar-ne els resultats. Capacitat d'anàlisi, de síntesi i d'avaluació.

Dedicació: 12h

Aprenentatge autònom: 8h

Grup gran/Teoria: 2h

Grup mitjà/Pràctiques: 2h

Tema 6: Algorisme de Shor de factorització.

Descripció:

Desenvolupament del tema 6.

Objectius específics:

11, 12

Competències relacionades:

G9. Capacitat de raonament crític, lògic i matemàtic. Capacitat de resoldre problemes en la seva àrea d'estudi. Capacitat d'abstracció: capacitat de crear i utilitzar models que reflecteixin situacions reals. Capacitat de dissenyar i realitzar experiments senzills, i analitzar-ne i interpretar-ne els resultats. Capacitat d'anàlisi, de síntesi i d'avaluació.

Dedicació: 27h

Aprenentatge autònom: 16h

Grup gran/Teoria: 6h

Grup mitjà/Pràctiques: 5h

Control de resolució de problemes dels algorismes de Grover i de Shor.

Descripció:

És un control on es proposen problemes per resoldre a classe per part dels estudiants.

Objectius específics:

10, 11, 12

Competències relacionades:

G9. Capacitat de raonament crític, lògic i matemàtic. Capacitat de resoldre problemes en la seva àrea d'estudi. Capacitat d'abstracció: capacitat de crear i utilitzar models que reflecteixin situacions reals. Capacitat de dissenyar i realitzar experiments senzills, i analitzar-ne i interpretar-ne els resultats. Capacitat d'anàlisi, de síntesi i d'avaluació.

Dedicació: 11h

Aprenentatge autònom: 10h

Activitats dirigides: 1h

Examen final

Descripció:

Prova final pels alumnes que vulguin pujar nota o aquells que no han superat l'avaluació continuada

Objectius específics:

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

Competències relacionades:

G9. Capacitat de raonament crític, lògic i matemàtic. Capacitat de resoldre problemes en la seva àrea d'estudi. Capacitat d'abstracció: capacitat de crear i utilitzar models que reflecteixin situacions reals. Capacitat de dissenyar i realitzar experiments senzills, i analitzar-ne i interpretar-ne els resultats. Capacitat d'anàlisi, de síntesi i d'avaluació.

Dedicació: 2h

Activitats dirigides: 2h

SISTEMA DE QUALIFICACIÓ

La nota de les competències tècniques de l'assignatura es calcularà a partir de 2 notes:

- Mitjana aritmètica de 4 controls que es realitzaran durant el curs (C)
- Mitjana aritmètica d'exercicis proposats per fer a casa (E)

La nota de l'avaluació continuada (AC) serà: $AC = 0.8 \cdot C + 0.2 \cdot E$

Es farà un examen final (amb nota F) per aquells alumnes que no hagin aprovat l'avaluació continuada, o vulguin millorar nota.

La nota final serà el màxim entre AC i F.

La nota de la competència transversal G9.1 serà determinada en els controls que donen lloc a l'avaluació continuada, amb notes: A (excel·lent), B (òptim), C(suficient), D (no superat).

BIBLIOGRAFIA

Bàsica:

- French, A. P; Taylor, Edwin F. Introducció a la física quàntica. Reverté, 1982. ISBN 8429141677.