Universitat Autònoma de Barcelona

2022/2023

Mètodes Avançats de la Teoria de la Informació i de la Codificació

Codi: 104371
Crèdits: 6

Titulació	Tipus	Curs	Semestre
2503758 Enginyeria de Dades	OT	4	1

Professor/a de contacte

Nom: Mercè Villanueva Gay

Correu electrònic: merce.villanueva@uab.cat

Utilització d'idiomes a l'assignatura

Llengua vehicular majoritària: català (cat)

Grup íntegre en anglès: No

Grup íntegre en català: Sí

Grup íntegre en espanyol: No

Equip docent

Joaquim Borges Ayats

Cristina Fernandez Cordoba

Prerequisits

No hi ha requisits previs. Tanmateix, els estudiants han de tenir un bon nivell matemàtic i estar familiaritzats amb els conceptes d'àlgebra fonamental, o haver superat l'assignatura "Teoria de la Informació i de la Codificació".

Objectius

El curs està enfocat a la teoria de codis i les seves aplicacions al món real. La teoria de codificació és l'estudi de mètodes per a una transmissió eficaç i precisa d'informació d'un lloc a un altre. Tracta el problema de detectar i corregir els errors de transmissió causats pel soroll al canal. En sistemes d'emmagatzematge distribuit, la teoria de codis ofereix també solucions, per millorar la tolerància a fallades en els discs durs, que són molt més eficients que les basades en la replicació.

Competències

- Concebre, dissenyar i implementar sistemes d'emmagatzematge de dades de forma eficient i segura.
- Generar propostes innovadores i competitives en l'activitat professional i en la investigació.
- Que els estudiants hagin desenvolupat aquelles habilitats d'aprenentatge necessàries per emprendre estudis posteriors amb un alt grau d'autonomia.
- Que els estudiants tinguin la capacitat de reunir i interpretar dades rellevants (normalment dins de la seva àrea d'estudi) per emetre judicis que incloguin una reflexió sobre temes destacats d'índole social, científica o ètica.
- Treballar cooperativament, en entorns complexos o incerts i amb recursos limitats, en un context multidisciplinari, assumint i respectant el rol dels diferents membres de l'equip.

Resultats d'aprenentatge

1. Dissenyar sistemes que protegeixin la privadesa de les dades personals clíniques en l'àmbit de ciències de la salut
2. Estudiar les adaptacions que es fan als algoritmes d'anàlisi i consulta de dades perquè preservin la privadesa de les dades d'entrada, dels models apresos o de les sortides dels models utilitzats en l'àmbit de la intel·ligència empresarial.
3. Generar propostes innovadores i competitives en l'activitat professional i en la investigació.
4. Que els estudiants hagin desenvolupat aquelles habilitats d'aprenentatge necessàries per emprendre estudis posteriors amb un alt grau d'autonomia.
5. Que els estudiants tinguin la capacitat de reunir i interpretar dades rellevants (normalment dins de la seva àrea d'estudi) per emetre judicis que incloguin una reflexió sobre temes destacats d'índole social, científica o ètica.
6. Treballar cooperativament, en entorns complexos o incerts i amb recursos limitats, en un context multidisciplinari, assumint i respectant el rol dels diferents membres de l'equip.

Continguts

1. Polinomis i cossos finits.

1.1. L'anell d'enters Z i els anells Z/p.

1.2. L'anell de polinomis Z/p.

1.3. Cossos finits GF(p^n)

1. Codis lineals sobre cossos finits.

2.1. Introducció a la teoria de codis.

2.2. Matriu generadora i codis equivalents.

2.3. Codis ortogonals i descodificació via síndrome.

2.4. Codis de Hamming.

1. Codis cíclics sobre cossos finits.

3.1. Introducció als codis cíclics.

3.2. Polinomi i matriu generadora.

3.3. Polinomi i matriu de control.

3.4. Codificació i descodificació.

1. Codis algebraics. Codis BCH i RS.

4.1. Introducció i definicions generals

4.2. Codificació amb un codi algebraic

4.3. Decodificació amb un codi algebraic.

4.4. Codis BCH i RS.

4.5. Correcció d'errors i esborralls.

1. Applicacions dels codis correctors d'errors.

5.1. Codis correctors d'errors al QR, Blu-ray, DVD.

5.2. Codis correctors d'errors en les transmissions d'informació.

5.3. Codis correctors d'errors aplicats al emmagatzematge distribuit.

5.4. Criptografia basada en codis correctors d'errors.

5.5. Codis correctors d'erros aplicats a *watermarking* i *steganograph*y.

5.6. Codis correctors d'erros utilitzats en computació quàntica.

Metodologia

La metodologia aplicada al treball de l'estudiant combinarà les classes magistrals, la resolució d'exemples i el pràcticum. Durant les sessions s'introduiran diferents conceptes i es proposarà la resolució d'exercicis perquè resolguin els estudiants.
Les propostes del pràcticum seran guiades i es validaran responent a algunes preguntes. El Campus Virtual s'utilitzarà per a la comunicació entre professors i estudiants (material, actualitzacions, anuncis, etc.).

Durant el curs es duran a terme diferents activitats:

Nota: es reservaran 15 minuts d'una classe, dins del calendari establert pel centre/titulació, per a la complementació per part de l'alumnat de les enquestes d'avaluació de l'actuació del professorat i d'avaluació de l'assignatura/mòdul.

Activitats formatives

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
Classes teóriques i pràctiques	38	1,52	1, 2, 3, 4, 5, 6
Pràctiques	12	0,48	1, 2, 3, 4, 5, 6
Tipus: Supervisades			
Supervisió de pràctiques	6	0,24	1, 2, 3, 4, 5, 6
Tutories i consultes	11	0,44	1, 2, 3, 4, 5, 6
Tipus: Autònomes			
Preparació d'exercicis i pràctiques	35	1,4	1, 2, 3, 4, 5, 6
Preparació de la presentació oral i/o examen	40	1,6	1, 2, 3, 4, 5, 6

Avaluació

Les dates per a l'avaluació continuada es publicaran al Campus Virtual (CV). Si es produeix algun canvi de programació en les dates, aquest serà comunicat als estudiants a través del CV, ja que s'entén que el CV és el mecanisme habitual de comunicació entre professorat i estudiants.

L'avaluació final tindrà en compte el portafoli lliurat pels estudiants, l'assistència i participació a classe, i les breus exposicions orals, de la següent manera:

1. Assistència i participació activa. Com a mínim, cal assistir al 80% de les classes. Es poden compensar les absències amb un treball addicional acordat amb el professorat. Nota: 10%

2. Resolucions d'exercici. Es tracta d'una tasca individual. Com a part de l'avaluació contínua, s'han de resoldre exercicis breus. Alguns seran obligatoris, altres seran opcionals. Nota: 25%
3. Activitats pràctiques. Segons el nombre d'estudiants, serà una tasca individual o en grups de dues persones. Aquestes activitats pràctiques es realitzaran mitjançant ordinadors. Nota: 25%.
4. Treball escrit i presentació oral, i/o examen final, segons el nombre d'estudiants i el seu perfil. Es tracta d'una tasca individual. Consisteix a fer un examen o bé un treball escrit i una presentació oral sobre un tema concret. L'elecció del tema es discutirà i acordarà a la classe, seleccionant temes d'una llista proporcionada pel professorat o pels propis estudiants. A més, l'estudiant que presenta la xarrada proposarà un exercici o qüestionari que els altres estudiants hauran de respondre. D'altra banda, els altres estudiants del públic han de fer preguntes (almenys una per a cada xerrada)durant les presentacions. Una llista preliminar de temes provisionals és la descrita al capítol 5. Nota: 40%.

Sense perjudici d'altres mesures disciplinàries que s'estimin oportunes, i d'acord amb la normativa acadèmica vigent, les irregularitats comeses per un estudiant que puguin conduir a una variació de la qualificació es qualificaran amb un zero (0). Les activitats d'avaluació qualificades d'aquesta forma i per aquest procediment no seran recuperables. Si és necessari superar qualsevol d'aquestes activitats d'avaluació per a superar la matèria, aquest curs se suspendrà directament, sense oportunitat de recuperar en el mateix curs. Les irregularitats contemplades inclouen, entre d'altres:

- la còpia parcial o total de qualsevol activitat d'avaluació;
- permetre a altres copiar;
- presentar un treball en grup que no hagi estat realitzat enterament pels membres del grup;
- presentar qualsevol material preparat per una altra persona com si fos propi, fins i tot si aquests materials són traduccions o adaptacions, incloent treballs que no són originals o exclusius de l'estudiant;

Per superar l'assignatura es requereix una puntuació de com a mínim 5 punts. Si un estudiant ha participat en més del 50% dels exercicis i pràctiques o ha realitzat la presentació oral ja no pot ser considerat com a "no avaluable". No hi haurà cap tractament especial per als estudiants repetidors. S'atorgarà la qualificació "matrícula d'honor" a tots aquells estudiants que tinguin un excel·lent i entrin dintre del percentatge que la normativa permeti de les millors notes.

És important tenir en compte que no es permetrà activitats d'avaluació per a cap estudiant en una data o hora diferent a l'establerta, tret per causes justificades degudament avisades abans de l'activitat i amb el consentiment previ del professor. En la resta de casos, si no s'ha realitzat una activitat, no es pot tornar a avaluar.

En el cas de resolucions d'exercicis i activitats pràctiques es pot sol·licitar una revisió després de la data de l'activitat, permetent als estudiants revisar l'activitat amb el professor. En aquest context, els estudiants podran discutir la nota sobre l'activitat que concedeixen els professors responsables de l'assignatura. Si els estudiants no participen en aquesta revisió, no hi haurà més possibilitat disponible.

Normativa d'avaluació de la UAB, aprovada pel Consell de Govern de la Universidat Autònoma de Barcelona: http://webs2002.uab.es/afers_academics/info_ac/0041.htm

Activitats d'avaluació

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Activitats pràctiques	25	3	0,12	1, 2, 3, 4, 5, 6
Assistència i participació activa	10	0	0	1, 2, 3, 4, 5, 6
Resolució d'exercicis	25	3	0,12	1, 2, 3, 4, 5, 6
Treball escrit i presentació oral i/o examen	40	2	0,08	1, 2, 3, 4, 5, 6

Bibliografia

- C. H. Bennett, P. Shor, "Quantum Information Theory", IEEE Trans. Inf. Theory, vol. 44, n.6, pp. 2724-2742, 1998.

- D. J. Bernstein, J. Buchmann, E. Dahmen (Eds.), Post-Quantum Cryptography, Springer-Verlag, 2009.
- Thomas M. Cover and Joy A. Thomas (1991). Elements of Information Theory, John Wiley & Sons, Inc.
- K. Gracie and M.-H. Hamon, "Turbo and turbo-like codes: Principles and applications", IEEE Proceedings of in Telecommunications, vol. 95, pp: 1228 - 1254, 2000.
- K. J. Horadam, Hadamard Matrices and Their Applications, Princeton University Press, 2007.
- Robert J. McEliece, The Theory of Information and Coding, Addison-Wesley Publishing Co., 1977.
- J. Rifà and Ll. Huguet, Comunicación Digital, Masson Ed. 1991.
- P. Shor, "Algorithms for Quantum Computation: Discrete Logarithm and Factoring", Proceedings 35-th Annual Symposium on Foundations of Computer Science, pp. 124-134, 1994.
- Mc. Williams-Sloane: The Theory of Error-Correcting Codes. North-Holland Publishing Company. Amsterdam-N.Y.-Oxford. 1978-1996.

Programari

Les activitats pràctiques es realitzaran mitjançant SageMath. https://www.sagemath.org/

SageMath és un sistema de programari de matemàtiques de codi obert gratuït amb llicència GPL. Es basa en molts paquets de codi obert existents: NumPy, SciPy, matplotlib, Sympy, Maxima, GAP, FLINT, R i molts més. S'accedeix a la seva potència combinada mitjançant un llenguatge comú basat en Python o directament mitjançant interfícies. Des de la versió 9.0 publicada el gener del 2020, SageMath utilitza Python 3.