Universitat Autònoma de Barcelona

2020/2021

Aplicacions de la Teoria de Codis

Codi: 105074
Crèdits: 6

Titulació	Tipus	Curs	Semestre
2502441 Enginyeria Informàtica	OT	4	1

La metodologia docent i l'avaluació proposades a la guia poden experimentar alguna modificació en funció de les restriccions a la presencialitat que imposin les autoritats sanitàries.

Professor/a de contacte

Nom: Mercè Villanueva Gay

Correu electrònic: Merce.Villanueva@uab.cat

Utilització d'idiomes a l'assignatura

Llengua vehicular majoritària: anglès (eng)

Grup íntegre en anglès: Sí

Grup íntegre en català: No

Grup íntegre en espanyol: No

Equip docent

Joaquim Borges Ayats

Cristina Fernández Córdoba

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 les assignatures "Informació i Seguretat" i "Fonaments de Tecnologies de la Informació".

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.

Aquest curs ens permet construir la base per poder desenvolupar el "treball final de grau" (TFG) relacionat amb aquest tema i/o continuar estudis de postgrau relacionats. Contempa la possibilitat d'assumir aquesta assignatura i el TFG simultàniament.

Competències

- Adquirir hàbits de pensament.
- Adquirir hàbits de treball personal.
- Capacitat per a seleccionar, desplegar, integrar i gestionar sistemes d'informació que satisfacin les necessitats de la organització, amb els criteris de cost i qualitat identificats.
- Capacitat per concebre, redactar, organitzar, planificar, desenvolupar i signar projectes en l'àmbit de l'enginyeria informàtica que tinguin per objecte la concepció, el desenvolupament o l'explotació de sistemes, serveis i aplicacions informàtiques.

- Capacitat per dissenyar, desenvolupar, avaluar i assegurar l'accessibilitat, l'ergonomia, la usabilitat i la seguretat dels sistemes, serveis i aplicacions informàtiques, així com de la informació que gestionen.
- Capacitat per dissenyar, desenvolupar, seleccionar i avaluar aplicacions i sistemes informàtics, assegurant-ne la fiabilitat, la seguretat i la qualitat, d'acord amb els principis ètics i la legislació i la normativa vigents.

Resultats d'aprenentatge

1. Desenvolupar la capacitat d'anàlisi, síntesi i prospectiva.
2. Dissenyar les solucions informàtiques que permetin integrar a un sistema distribuït les necessitats d'accessibilitat i seguretat.
3. Dissenyar, desenvolupar, seleccionar i avaluar aplicacions, assegurant la seva fiabilitat i seguretat.
4. Dissenyar, desenvolupar, seleccionar i avaluar sistemes informàtics, assegurant la seva fiabilitat, seguretat i qualitat.
5. Identificar els principals atacs que pot rebre un sistema informàtic, així com els possibles mètodes de protecció, detecció i aplicació de polítiques de seguretat que permetin evitar el dany al sistema o minimitzar la seva repercussió.
6. Incorporar sistemes distribuits de tractament de la informació a una organització per a incrementar la capacitat operativa.
7. Treballar de manera autònoma.

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, el pràcticum i una breu xerrada pública sobre un tema específic aprovat prèviament. 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:

Activitats formatives

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
Classes teóriques i pràctiques	38	1,52	1, 2, 3, 4, 5, 6, 7
Pràctiques	12	0,48	1, 2, 3, 4, 5, 6, 7
Tipus: Supervisades			
Supervisió de la presentació oral	6	0,24	1, 7
Supervisió de pràctiques	6	0,24	1, 7
Tutories i consultes	6	0,24	1, 7
Tipus: Autònomes			
Preparació d'exercicis i pràctiques	35	1,4	1, 2, 3, 4, 5, 6, 7
Preparació de la presentació oral	40	1,6	1, 2, 3, 4, 5, 6, 7

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. Presentació oral. Es tracta d'una tasca individual. Consisteix a fer 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 que els altres estudiants hauran de respondre. També haurà de corregir i puntuar les respostes. 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 ésla 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, 7
Assistència i participació activa	10	0	0	1, 2, 3, 4, 5, 6, 7
Presentació oral	40	1	0,04	1, 2, 3, 4, 5, 6, 7
Resolució d'exercicis	25	3	0,12	1, 2, 3, 4, 5, 6, 7

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.