Universitat Autònoma de Barcelona

2022/2023

Aplicaciones de la Teoría de Codigos

Código: 105074
Créditos ECTS: 6

Titulación	Tipo	Curso	Semestre
2502441 Ingeniería Informática	OT	4	1

Contacto

Nombre: Mercè Villanueva Gay
Correo electrónico: merce.villanueva@uab.cat

Uso de idiomas

Lengua vehicular mayoritaria: catalán (cat)
Algún grupo íntegramente en inglés: No
Algún grupo íntegramente en catalán: Sí
Algún grupo íntegramente en español: No

Equipo docente

Joaquim Borges Ayats
Cristina Fernandez Cordoba

Prerequisitos

No hay requisitos previos. Sin embargo, los estudiantes deben tener un buen nivel matemático y estar familiarizados con los conceptos de álgebra fundamental, o haber aprobado las asignaturas "Información y Seguridad" y "Fundamentos de Tecnologías de la Información".

Objetivos y contextualización

El curso se centra en la teoría de la codificación y sus aplicaciones en el mundo real. La teoría de la codificación es el estudio de métodos para la transmisión eficiente y precisa de información de un lugar a otro. Se ocupa del problema de detectar y corregir los errores de transmisión causados por el ruido en el canal. En sistemas de almacenamiento distribuido, la teoría de códigos ofrece también soluciones, para mejorar la tolerancia a fallos en los discos duros, que son mucho más eficientes que las basadas en la replicación.

Este curso nos permite construir la base para poder desarrollar el "trabajo final de grado" (TFG) relacionado con este tema y/o continuar estudios de posgrado relacionados. Contempla la posibilidad de asumir esta asignatura y el TFG simultáneamente.

Competencias

- Adquirir hábitos de pensamiento.
- Adquirir hábitos de trabajo personal.
- Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar proyectos en el ámbito de la ingeniería en informática que tengan por objeto la concepción, el desarrollo o la explotación de sistemas, servicios y aplicaciones informáticas.
- Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.

- Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.
- Capacidad para seleccionar, desplegar, integrar y gestionar sistemas de información que satisfagan las necesidades de la organización, con los criterios de coste y calidad identificados.

Resultados de aprendizaje

1. Desarrollar la capacidad de análisis, síntesis y prospectiva.
2. Diseñar las soluciones informáticas que permitan integrar en un sistema distribuido las necesidades de accesibilidad y seguridad.
3. Diseñar, desarrollar, seleccionar y evaluar aplicaciones asegurando su fiabilidad y seguridad.
4. Diseñar, desarrollar, seleccionar y evaluar sistemas informáticos, asegurando su fiabilidad, seguridad y calidad.
5. Identificar los principales ataques que puede recibir un sistema informático, así como los posibles métodos de protección, detección y aplicación de políticas de seguridad que permitan evitar el daño al sistema o minimizar su repercusión.
6. Incorporar sistemas distribuidos de tratamiento de la información en una organización para incrementar la capacidad operativa.
7. Trabajar de forma autónoma.

Contenido

1. Polinomios y cuerpos finitos.
   - 1.1. El anillo de enteros Z y los anellos Z/p.
   - 1.2. El anillo de polinomios Z/p.
   - 1.3. Cuerpos finitos GF(p^n)
1. Códigos lineales sobre cuerpos finitos.
   - 2.1. Introducción a la teoría de códigos.
   - 2.2. Matriz generadora y códigos equivalentes.
   - 2.3. Códigos ortogonales y descodificación via síndrome.
   - 2.4. Códigos de Hamming.
1.

Códigos
cíclicos sobre cuerpos finitos.

3.1.
Introducción a los códigos
cíclicos.

3.2.
Polinomio y matriz generadora.

3.3.
Polinomio y matriz de control.

3.4.
Codificación y descodificación.

1.
Códigos
algebraicos. Códigos BCH y RS.

4.1.
Introducción y definiciones generales

4.2.
Codificación con un código algebraico

4.3.
Decodificación con un código algebraico.

4.4.
Códigos BCH y RS.

4.5.
Corrección de errores y borrones.

1.
Applicaciones
de los códigos correctores de errores.

5.1.
Códigos correctores de errores al QR, Blu-ray,
DVD.

5.2.
Códigos
correctores de errores en las transmisiones de
información.

5.3.
Códigos correctores de errores aplicados al almacenaje distribuido.

5.4.
Criptografía basada en códigos correctores de errores.

5.5.
Códigos correctores de errores aplicados a *watermarking* y *steganograph*y.

5.6.
Códigos correctores de errores utilitzados en computación cuántica.

Metodología

La metodología aplicada al trabajo del estudiante combinará les classes magistrals, la resolución de ejemplos, la práctica y una breve charla pública sobre un tema específico previamente aprobado. Durante las sesiones, se introducirán diferentes conceptos y se propondrá que los alumnos resuelvan los ejercicios.
Las propuestas prácticas se guiarán y se validarán respondiendo algunas preguntas. El Campus Virtual se utilizará para la comunicación entre profesores y estudiantes (material, actualizaciones, anuncios, etc.).

Se realizarán diferentes actividades durante el curso:

Nota: se reservarán 15 minutos de una clase dentro del calendario establecido por el centro o por la titulación para que el alumnado rellene las encuestas de evaluación de la actuación del profesorado y de evaluación de la asignatura o módulo.

Actividades

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
Clases teóricas y pràcticas	38	1,52	1, 2, 3, 4, 5, 6, 7
Prácticas	12	0,48	1, 2, 3, 4, 5, 6, 7
Tipo: Supervisadas			
Supervisión de prácticas	6	0,24	1, 7
Supervisión del trabajo y presentación oral o Tutorías para el examen	6	0,24	1, 7
Tutorias y consultas	5	0,2	1, 7
Tipo: Autónomas			
Preparación de ejercicios y prácticas	35	1,4	1, 2, 3, 4, 5, 6, 7

Preparación de la presentación oral y/o examen	40	1,6	1, 2, 3, 4, 5, 6, 7

Evaluación

Las fechas para la avaluación continuada se publicarán en el Campus Virtual. Si se produce algún cambio de programación en las fechas, éste será comunicado a los estudiantes a través del Campus Virtual (CV), puesto que se entiende que el CV es el mecanismo habitual de comunicación entre el profesorado y los estudiantes.

La evaluación final tendrá en cuenta el portafolio entregado por los estudiantes, la asistencia y participación en clase, y las breves presentaciones orales, de la siguiente manera:

1. Asistencia y participación activa. Al menos el 80% de las clases deben ser atendidas. Las ausencias pueden ser compensadas con una tarea adicional acordada con el profesorado. Nota: 10%.
2. Resoluciones de ejercicios. Esta es una tarea individual. Como parte de la evaluación continua, se deben resolver ejercicios cortos. Algunos serán obligatorios, otros serán opcionales. Nota: 25%.
3. Actividades prácticas Dependiendo del número de estudiantes, será una tarea individual o en grupos de dos personas. Estas actividades prácticas se realizarán utilizando ordenadores. Nota: 25%.
4. Trabajo escrito y presentación oral, y/o examen final, según el número de estudiantes y su perfil. Esta es una tarea individual. Consiste en realizar un examen o bien un trabajo escrito y presentación oral sobre un tema específico. La elección del tema será discutida y acordada en la clase, seleccionando temas de una lista provista por el profesorado o por los propios estudiantes. Además, el estudiante que presenta la charla propondrá un ejercicio o cuestionario que los otros estudiantes deberán responder. Por otro lado, los otros estudiantes en la audiencia deben hacer preguntas (al menos una para cada charla) durante las presentaciones. Unalista preliminar de temas provisionales son los que se describen en el capítulo 5. Nota: 40%.

Sin perjuicio de otras medidas disciplinarias oportunas y de acuerdo con la normativa académica vigente, las irregularidades cometidas por un estudiante que puedan conducir a una variación de la calificación se calificarán con un cero (0). Las actividades de evaluación calificadas de esta forma y por este procedimiento no serán recuperables. Si es necesario superar cualquiera de estas actividades de evaluación para superar la materia, este curso se suspenderá directamente, sin oportunidad de recuperar en el mismo curso. Las irregularidades contempladas incluyen, entre otras:

- la copia parcial o total de cualquier actividad de evaluación;
- permitir a otros copiar;
- presentar un trabajo en grupo que no haya sido realizado enteramente por los miembros del grupo;
- presentar cualquier material preparado por otra persona como si fuera propio, incluso si estos materiales son traducciones o adaptaciones, incluyendo trabajos que no son originales o exclusivos del estudiante.

Para superar la asignatura se requiere una puntuación de como mínimo 5 puntos. Si un estudiante ha participado en más del 50% de los ejercicios y prácticas, o ha realizado la presentación oral, ya no puede ser considerado como "no evaluable". No habrá ningún tratamiento especial para los estudiantes repetidores. Se otorgará la calificación "matrícula de honor" a todos aquellos estudiantes que tienen un excelente y entren dentro del porcentaje de la normativa para las mejores notas.

Es importante tener en cuenta que no se permitirán actividades de evaluación para ningún estudiante en una fecha u hora diferente a la establecida, a menos que sea por causas justificadas debidamente informadas antes de la actividad y con el consentimiento previo del profesor. En todos los demás casos, si una actividad no se ha llevado a cabo, no se puede volver a evaluar.

En el caso de resoluciones de ejercicio y actividades prácticas, se puede solicitar una revisión después de la fecha de la actividad, lo que permite a los estudiantes revisar la actividad con el profesor. En este contexto, los estudiantes pueden discutir la calificación de la actividad otorgada por los profesores responsables de la asignatura. Si los estudiantes no participan en esta revisión, no habrá más oportunidades disponibles.

Normativa de evaluación de la UAB, aprobada por el Consejo de administración de la Universidad Autónoma de BARCELONA (30/09/2010): http://webs2002.uab.es/afers_academics/info_ac/0041.htm

Actividades de evaluación

Título	Peso	Horas	ECTS	Resultados de aprendizaje
Actividades prácticas	25	3	0,12	1, 2, 3, 4, 5, 6, 7
Asistencia y participación activa	10	0	0	1, 2, 3, 4, 5, 6, 7
Resolución de ejercicios	25	3	0,12	1, 2, 3, 4, 5, 6, 7
Trabajo escrito y presentación oral y/o examen	40	2	0,08	1, 2, 3, 4, 5, 6, 7

Bibliografía

- 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.

Software

Las actividades prácticas se realizarán utilizando SageMath. https://www.sagemath.org/

SageMath es un sistema de software matemático de código abierto con licencia GPL.
Se basa en muchos paquetes de código abierto existentes: NumPy, SciPy, matplotlib, Sympy, Maxima, GAP, FLINT, R y muchos más.
Se accede a su potencia combinada a través de un lenguaje común basado en Python o directamente a través de interfaces.
Desde la versión 9.0 lanzada en enero de 2020, SageMath está usando Python 3.