Introducción a la Teoría de Códigos

M.A.García, L. Martínez, T.Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

Guía Docente

Mayo de 2017

Contenido

Descripción del curso

Con este curso, queremos proporcionar una base que sirva de introducción a la Teoría de Códigos, poniendo especial énfasis en los aspectos algebraicos de la misma.

El material que comprende este curso es autocontenido. Es por ello que, aparte de los temas que tratan sobre códigos y que cubren un temario básico clásico, hemos considerado oportuno introducir un primer tema que repasa de forma rápida las nociones básicas de espacios vectoriales que se necesitarán en el desarrollo del curso y añadir un anexo final en el que recopilan las definiciones y construcciones sencillas de algunas estructuras algebraicas, en especial la de cuerpo finito, que será herramienta imprescindible en el estudio de los códigos lineales que planteamos. En definitiva, tratamos de presentar el material teórico práctico necesario para que el lector realice una primera aproximación a esta rama del Álgebra, la Teoría de Códigos, que se ha desarrollado de forma muy rápida en la segunda mitad del siglo XX y sea capaz de comprender lo que aquí se expone sin necesidad de consultar constantemente otras fuentes bibliográficas.

En el desarrollo de los temas seleccionados abarcaremos tanto el aspecto teórico, mediante el enunciado, justificación y realización de ejemplos de los resultados básicos más interesantes de la Teoría de Códigos, como el práctico gracias a la resolución de ejercicios y problemas relativos a la materia explicada. Asimismo, el lector podrá examinar su dominio y comprensión de la materia explicada mediante la realización de los ejercicios y problemas propuestos y las pruebas de autoevaluación proporcionadas.

Hemos organizado el material expuesto en cuatro temas y un anexo. Como ya se ha indicado, el primer tema repasa de forma rápida las nociones fundamentales sobre espacios vectoriales que se van a necesitar en los temas posteriores. El lector que se encuentre familiarizado con este tema, puede prescindir de una lectura profunda del mismo y bastará con que se fije en la notación que se introduce y que será empleada a lo largo del resto de los capítulos. El segundo tema trata de situarnos en el problema de codificación y de darnos una visión global de lo que trata esta teoría. En el tercer tema se entra ya en materia más especifica: se hace un estudio básico de los códigos lineales que culmina con la construcción de una de las familias clásicas de códigos lineales: los códigos de Hamming. Finalmente, en el tema 4 se profundiza en un tipo especial de códigos: los códigos cíclicos, mostrando la relación existente entre éstos y los ideales del anillo cociente de . Como ejemplo más sobresaliente de los códigos cíclicos estudiamos los conocidos códigos BCH, que se caracterizan por poder saber a priori cuantos errores al menos podemos asegurar que van a corregir.

Además, para aquellos lectores que tengan un dominio limitado de los cuerpos finitos hemos incorporado un anexo en el que se trabaja con esta estructura algebraica. De esta forma, conseguimos que un lector con unos conocimientos mínimos sobre Álgebra Lineal y soltura en el manejo de los cuerpos finitos disponga del material suficiente para familiarizarse con las nociones básicas de la Teoría de Códigos Lineales y encuentre a lo largo de los diferentes capítulos una exposición clara y rigurosa desde el punto de vista formal de la misma.

A la hora de redactar cada uno de los temas de este proyecto, seguiremos el esquema siguiente: en el apartado de material teórico incluimos las definiciones y enunciados de las propiedades más relevantes de forma que el lector pueda hacerse una idea global del mismo. Asimismo, en esta parte teórica se muestran diversos ejemplos desarrollados que ayudan a consolidar lo aprendido en ese tema. Para asegurar la comprensión de lo expuesto, en la parte práctica se resolverán algunos ejercicios seleccionados de entre los que se proponen y se plantearán diversas pruebas de autoevaluación. Obviamente, cada lector, en función de sus necesidades, tendrá la oportunidad de completar el material que ofrecemos con alguna de las lecturas recomendadas que inciden más en las demostraciones de los resultados recogidos en la parte teórica.

Finalmente, señalamos que los contenidos de este curso los hemos elaborados de forma específica para este proyecto OCW. Nos hemos basado en nuestra experiencia y en el material original propio que usamos para impartir la primera de las partes de la asignatura *Códigos y Criptografía,* optativa del 4º curso del Grado en Matemáticas de la UPV/EHU. Consideremos que la materia aquí expuesta es de interés no sólo para estudiantes del Grado en Matemáticas que deseen ampliar sus conocimientos sobre el tema, sino también para estudiantes de diversas ingenierías (Ingeniería Informática, Ingeniería Electrónica, Ingeniería de Telecomunicaciones,…) que precisen una aproximación matemática rigurosa a esta teoría.

Objetivo del curso

El objetivo principal de este curso es que el lector conozca las bases teóricas y las aplicaciones principales de la Teoría de Códigos, haciendo especial incidencia en el aspecto algebraico de la misma. Para ello, realizaremos una exposición rigurosa desde el punto de vista matemático de los contenidos del curso que se completará con ejemplos desarrollados.

Competencias

Las competencias que se trabajarán en este curso son las siguientes:

CM01 - Entender la idea de la codificación y saber diferenciar entre la detección y corrección de errores.
CM02 - Saber calcular la distancia mínima de un código lineal y relacionar esta distancia mínima con el número de errores que puede corregir ese código.
CM03 – Ser capaz de determinar, si es que existe, la matriz generadora estándar de un código lineal y su matriz de control.
CM04 – Saber calcular el código dual de un código lineal, la dimensión del código dual y relacionar este código con la matriz de control
CM05 – Determinar mediante técnicas diferentes la distancia mínima de un código lineal (por ejemplo, relacionarla con el peso mínimo ó con el número de columnas linealmente dependientes de la matriz de control del código lineal)
CM06 - Saber utilizar el método de corrección por síndromes.
CM07 - Saber utilizar el método de corrección por líderes.
CM09 – Saber construir códigos cíclicos de una longitud y dimensión determinadas.
CM10 – Saber calcular el polinomio generador y el de control de un código cíclico y construir a partir de ellos una matriz generadora y una matriz de control de un código cíclico
CM11 - Conocer algunos códigos importantes (códigos de Hamming, códigos BCH) y sus propiedades.

Prerrequisitos

Como ya hemos indicado, el material expuesto es autocontenido y en él se pueden encontrar todas los conceptos necesarios para la comprensión de los contenidos expuestos. No obstante, presuponemos que el lector está familiarizado con los conceptos básicos del Álgebra Lineal como espacios vectoriales, bases, aplicaciones lineales,… que se repasan en el primero de los temas propuestos y cuenta con la destreza mínima necesaria para realizar los cálculos que se presentan, en especial, que tiene soltura al trabajar en cuerpos finitos.

Programa del curso

Detallamos a continuación los temas y sus correspondientes apartados que componen el curso:

Tema 1: PRELIMINARES SOBRE ÁLGEBRA LINEAL
1.1 Espacios vectoriales: definiciones básicas
1.2 Subespacio vectorial
1.3 Base y dimensión de un espacio vectorial
1.4 Coordenadas de un vector

Tema 2: NOCIONES BÁSICAS DE LA TEORÍA DE CÓDIGOS
2.1 Introducción: El problema de la codificación
2.2 Códigos detectores y correctores de errores
2.3 Distancia de Hamming
2.4 Códigos perfectos
2.5 Códigos equivalentes

Tema 3: CÓDIGOS LINEALES
3.1 Definición y primeras propiedades
3.2 Matriz generadora de un código lineal
3.3 Matriz de control de un código lineal. Código dual de un código lineal
3.4 Codificación y decodificación para códigos lineales
3.5 Ejemplo de códigos lineales: Códigos de Hamming

Tema 4: CÓDIGOS CÍCLICOS
4.1 Definición y construcción de códigos cíclicos
4.2 Polinomio generador y matriz generadora de un código cíclico
4.3 Polinomio de control y matriz de control de un código cíclico. Código dual de un código cíclico
4.4 Codificación y decodificación de un código cíclico
4.5 Ejemplo de códigos cíclicos: Códigos BCH

Anexo: CUERPOS FINITOS
A1. Algunas estructuras algebraicas interesantes
A2. Construcción de cuerpos finitos
A3. Ejemplos de cuerpos finitos

El material teórico está preparado para que el lector pueda descargarse tanto el tema completo como cada uno de los apartados del mismo. Bastará pinchar sobre el título del tema (si se desea el tema completo) ó el título del apartado (si solo se eestá interesado en la información de un apartado concreto) para acceder a la información.

Metodología

Al tratarse de un curso de autoaprendizaje la metodología que recomendamos es la siguiente:

Fase 1. Asimilación teórica: En cada tema el lector debe realizar una lectura reflexiva del material proporcionado hasta asegurarse de la comprensión de todos los puntos tratados en el mismo. Sería conveniente que se consultaran algunas de las lecturas recomendadas para completar nuestro material con demostraciones de los resultados enunciados, otros ejemplos, etc

Fase 2. Adquisición de destreza práctica: Una vez asimilado el contenido de cada tema, se recomienda trabajar los ejemplos expuestos para comprobar que se obtiene lo que allí se indica. Tras ello, es conveniente intentar la realización de los ejercicios resueltos del tema estudiado y comprobar con las soluciones si lo que estamos haciendo coincide con lo expuesto. Finalmente, se recomienda la resolución de los ejercicios propuestos de ese tema, que son similares en cuanto a enunciado y técnicas usadas que los resueltos en el mismo tema.

Obviamente el lector no familiarizado con el manejo de cuerpos finitos y/o espacios vectoriales debe trabajar este aspecto antes de entrar al estudio de los temas 2, 3 y 4.

Finalmente, deseamos destacar que, aunque los temas se han concebido para poder ser trabajados de forma independiente, es conveniente seguir la secuencia de temas indicada en el programa y que el lector se asegura del correcto dominio de los conceptos de un tema antes de pasar a trabajar los contenidos del siguiente.

Cronograma

Presuponiendo un conocimiento de los conceptos básicos del Algebra Lineal, el tiempo recomendable para el estudio de los contenidos de la asignatura es de 10 semanas a razón de un mínimo de 4 horas/semana. Una distribución óptima del tiempo recomendado para la correcta comprensión de los contenidos de este curso es la siguiente:

Estudio del Tema 1 y 2: 4 horas de las cuales 3 se dedican a la comprensión de conceptos y desarrollo teórico y 1 hora al práctico.
Estudio de los Temas 3 y 4: 16 horas/tema de las cuales 7 se dedican al desarrollo teórico y 9 al práctico.

Destacamos que en la distribución temporal anterior no se incluye el tiempo de manejo de los cuerpos finitos. Si el lector no está familiarizado con este tipo de cuerpos, será necesario aumentar el tiempo inicial previsto (10 semanas a razón de 4 horas /semana) en al menos otras dos semanas más para adquirir la destreza mínima necesaria en la realización de operaciones que involucran cuerpos finitos para poder proseguir con éxito el estudio de los códigos lineales y cíclicos. Lo mismo sucederá si el lector no tiene las destrezas mínimas en el manejo de espacios vectoriales: deberá aumentar el tiempo dedicado al tema 1 en, al menos 8 horas más y completar lo que aquí se propone mediante la realización de ejercicios de otros cursos de Álgebra Lineal introductorios que le ayuden a dominar las técnicas básicas empleados en el estudio de los espacios vectoriales.