

Teoria de la codificació

Codi	Tipus	Curs/Semestre	Crèdits
20374	Optativa Semestral	4 / 1	5

Objectius

Competències específiques

Coneixements

1. Conèixer el concepte de comunicació digital vs. analògica. Teorema de Nyquist. Modulació del senyal.
2. Aprofundir en els conceptes de la Teoria de la Informació. Entropia.
3. Aprofundir en el coneixement dels cossos finits i dels espais vectorials de dimensió finita sobre un cos finit.
4. Conèixer el concepte de font i de canal i els teoremes de Shannon.
5. Conèixer el llenguatge de programació simbòlica MAGMA.
6. Conèixer el concepte de codi corrector d'errors. Codis bloc. Paràmetres associats. Capacitat correctora.
7. Conèixer la representació matricial d'un codi lineal. Codificació. Descodificació via taula estàndard i via síndrome.
8. Conèixer alguns codis lineals específics. Codis de Hamming. Codis de Reed-Muller. Mètodes de correcció corresponents.
9. Conèixer els codis cíclics.
10. Conèixer els codis BCH i de Reed-Solomon. Codificació habitual i descodificació pel procediment de Berlekamp-Massey.
11. Conèixer les aplicacions habituals dels codis Reed-Solomon (CDs, DVDs, TDT, etc.).
12. Conèixer el concepte de codi convolucional. Algorisme de Viterbi.
13. Conèixer el concepte de codificació Turbo. Codis TPC.
14. Conèixer el concepte de codificació LDPC o altres
15. Codificacions properes a la fita de Shannon.

Habilitats

1. Saber calcular les relacions entre els paràmetres perquè una comunicació digital sigui possible.
2. Saber calcular entropies, entropies condicionades i informacions mútues de variables aleatòries.
3. Saber utilitzar el llenguatge MAGMA per a la manipulació via software de cossos finits i polinomis sobre cossos finits.
4. Saber calcular els paràmetres habituals de codis bloc senzills.
5. Saber calcular la matriu de control a partir de la matriu generadora d'un codi lineal i viceversa.

6. Saber descodificar (corregint errors) via taula estàndard i via síndrome.
7. Saber descodificar (corregint errors i/o esborralls) codis de Hamming binaris i sobre cossos finits en general.
8. Saber codificar codis cíclics.
9. Saber relacionar les matrius generadora i de control d'un codi cíclic amb els polinomis generador i de control.
10. Saber utilitzar el llenguatge MAGMA per a la construcció i manipulació de diferents tipus de codis.
11. Saber construir codis BCH i utilitzar-los per a la correcció d'errors i/o esborralls.
12. Saber construir codis Reed-Solomon i utilitzar-los per a la correcció d'errors i/o esborralls.
13. Saber implementar un conjunt de funcions en MAGMA que simulin una transmissió d'informació a través d'un canal utilitzant uns determinats codis i unes determinades tècniques.
14. Saber calcular els paràmetres d'un codi convolucional a partir de la seva expressió polinòmica i viceversa.
15. Saber construir codificadors convolucionals.
16. Dissenyar els descodificadors en la versió general i/o sistemàtica.

Competències genèriques

1. Capacitat de resoldre problemes genèrics aplicant els mètodes de la ciència i l'enginyeria.
2. Capacitat de decidir la utilització d'un cert sistema de correcció d'errors a l'hora de resoldre un problema de comunicacions.

Capacitats prèvies

1. Coneixements de Teoria de la Informació;
2. coneixements del càlcul de probabilitats i del càlcul logarítmic;
3. coneixements sobre l'implementació electrònica (usant un LFSR) de la divisió llarga de polinomis;
4. coneixements d'aritmètica modular;
5. coneixements sobre cossos finits (ha de saber construir-los i fer les operacions habituals en ells),
6. coneixements d'àlgebra lineal (conceptes de dependència i independència lineal, base i dimensió, operacions de suma i producte de matrius, càlcul d'inverses, càlcul de determinants).

Continguts

Introducció	
--------------------	--

Conceptes fonamentals de la teoria del senyal. Canals físics (BSC, Gaussià, Markov,...). Entropia i propietats. Informació mútua. Capacitat d'un canal. Teoremes fonamentals de Shannon. Límit a les comunicacions digitals.

Aritmètica

Cossos finits i algorismes bàsics. Polinomis irreductibles. Construcció i propietats dels cossos finits. Operativa i resolució d'alguns problemes en cossos finits. Algorisme de les divisions successives. Teorema de Dirichlet.

Codis lineals

Introducció als codis lineals. Matriu generadora i matriu de control. Paràmetres i fites. Descodificació via la Taula estàndard. Síndrome i descodificació via Síndrome. Codis de Hamming. Codis de Reed-Muller.

Codis cíclics

Definició i introducció algebraica al tema. Polinomis a coeficients en un cos finit. Anells i ideals en anells de polinomis sobre cossos finits. Polinomi generador i polinomi de control. Codificació d'un codi cíclic. Cossos finits, codis cíclics i la factorització de x^{n-1} sobre $GF(q)$.

Codis BCH i de Reed-Solomon

Introducció. La distància mínima prevista en un codi cíclic. Codis BCH. Codis Reed-Solomon. Equació clau i el teorema de Dirichlet. Correcció d'errors en un codi algebraic. Correcció d'esborralls en un codi algebraic. Tècniques d'interleaving i concatenació de codis. Correcció d'errors i esborralls en els CD i DVD.

Codis convolucional

Introducció. Paràmetres fonamentals. Codis sistemàtics, no-catastròfics i minimal. Descripció matricial d'un codi convolucional. Descripció com a diagrama d'estats d'un codi convolucional. Descripció com a codi reticle. Codis de Winer-Ash. Disseny del codificador i del descodificador. Descodificació dels codis convolucional. Algorisme de Viterbi.

Tècniques recents.

Introducció. Turbo-codis. Codis turbo-producte. Codis turbo-convolucional. Codis LDPC. Codis *rateless*.

Metodologia docent

L'assignatura es dona combinant les classes de teoria, les classes de problemes i les sessions de laboratori. Així els conceptes teòrics s'introdueixen a les classes de teoria; a les classes de problemes es tracten exhaustivament aquests conceptes tot experimentant amb exemples simples concrets; finalment, a la classe de laboratori es pot treballar amb exemples més complexos i verificar/utilitzar els resultats que s'han anat deduint durant el curs.

Cada dues sessions de teoria es lliurarà a l'estudiant un exercici per desenvolupar fora de l'aula i

retornar-lo al professor per a la seva correcció i comentaris. Resoldre aquests exercicis no és obligatori però es tindran en compte en l'avaluació final de l'assignatura.

L'eina de treball a les classes de laboratori és *Magma*. Els exercicis es realitzen per parelles. Hi ha sis sessions de laboratori:

la primera sessió és d'introducció a *Magma*; la segona sessió és de maneig de cossos finits i polinomis; la tercera sessió és de tractament de codis lineals; la quarta sessió és de codis cíclics i la cinquena sessió és sobre codis algebraics.

Les sessions segona, tercera, quarta i cinquena es comencen a classe i es lliuren al principi de la sessió següent.

Al final de tot hi haurà una sisena sessió on es tracten tots els continguts del curs i es desenvolupa completament durant l'horari de laboratori.

Avaluació

1a convocatòria (febrer/juny)		2a convocatòria (juliol/setembre)
Avaluació en grups	Avaluació individual	
No hi ha avaluació continuada.	L'examen final és obligatori per a tothom.	L'examen de segona convocatòria és obert a tothom.

Bibliografia bàsica

Mc.Williams-Sloane: The Theory of Error-Correcting Codes. North-Holland Publishing Company. Amsterdam-N.Y.-Oxford. (1978-1996).

Rifà J., Huguet, L.: Comunicación Digital. Masson Ed. (1991).

Bibliografia complementària

Hill, R.: First Course in Coding Theory. Clarendon Press. Oxford. (1986).

McEliece, R.J.: The Theory of Information and Coding. Addison-Wesley Publishing Company. (1977).

McEliece, R.J.: Finite Fields for Computer Scientists and Engineers. Kluwer Academic Publishers. (1987).

Poli A., Huguet L.: Codes Correcteurs. Masson. Paris (1988).

Enllaços

[Pàgina mantinguda per Robert Morelos-Zaragoza.](#)

<http://fly.isti.cnr.it/software/codes.html>