Códigos binarios

Trimestre 21-I
Profesor: José Noé Gutiérrez H.
Correo: ngh@xanum.uam.mx
Asesorías: viernes de 14:00 a 14:40 horas o previa cita

TEMARIO

1. Detección y corrección de errores (a) Justificación del estudio de los códigos (b) Canales de comunicación, (c) Decodificación por máxima verosimilitud, (d) Distancia de Hamming, (e) Decodificación por distancia mínima.
2. Códigos lineales (a) Definición de Código Lineal. Matrices generadoras, (b) Códigos duales y matrices verificadoras de paridad, (c) Peso y distancia de Hamming, (d) Equivalencia de códigos, (e) Decodificación por síntoma, (f) Códigos de barras,
3. Cotas para códigos (a) Cota de Hamming y códigos perfectos, (b) Códigos de Hamming, (c) Código de Golay, (d) Cota de Singleton y códigos MDS. (e) Identidad de MacWilliams.
4. Introducción a los campos finitos (a) Definición de campo, (b) Anillo de polinomios y polinomios mínimos, (c) Construcción y aritmética de los campos finitos.
5. Códigos polinomiales (a) Códigos de Reed-Muller, Definición, sus parámetros y decodificación. (b) Códigos de Reed-Solomon. Definición, sus parámetros y decodificación.
6. Polinomios mínimos (a) Cálculo de polinomios mínimos, (b) factorización de $x^n - 1$.
7. Códigos cíclicos (a) Descripción polinomial de los códigos cíclicos y sus duales, (b) Codificación y decodificación de códigos cíclicos.
8. Códigos MDS Distintas caracterizaciones de los códigos MDS.

Evaluación del curso

El 70% de la calificación se asignará al resultado de tres exámenes parciales, o bien al de un global. Quienes tengan dos exámenes parciales aprobados tendrán derecho a presentar recuperación de un parcial. Las tareas tendrán un valor de 30% de la calificación final. Los ejercicios de las tareas pueden responderse con ayuda de la computadora, por ejemplo utilizando Sage, Maxima, Mathematica o GAP-GUAVA.

Las tareas pueden realizarse en equipo, sin límite de integrantes por equipo. Los equipos pueden cambiar en cualquier momento. Las tareas entregadas después de la fecha de señalada se penalizarán con 1 punto por cada día natural de retraso.

Los exámenes se aplicarán los días jueves *22 de abril*, jueves *20 de mayo* y martes *8 de junio*. El examen final se aplicará el día martes 15 de junio.

Durante el curso colocaré material relevante al mismo en la página: https://sites.google.com/site/cdematem/

Escala de calificaciones

Una calificación en el intervalo:

[0, 6) corresponde a **NA**	[7.4, 8.8) corresponde a **B**
[6, 7.4) corresponde a **S**	[8.8, 10] corresponde a **MB**

Bibliografía (*: libro de texto)

1. Hamming, R.W. Error detecting and error correcting codes. Key Papers in the development of Coding Theory. E.R. Berlekamp (Editor). IEEE Press, 1974.
2. Hankerson, D.R. et al., *Coding Theory and Cryptography. The Essentials*, 2nd Ed. CRD Press. 2000. (*)
3. Hill, R. *A first course in Coding Theor*y. Oxford University Press. 1994.
4. Justesen, J., Høholdt, T. *A Course In Error-Correcting Codes*, 2nd Ed. European Mathematical Society, 2017. (*)
5. Ling, S., Xing, C. *Coding Theory. A first course*. Cambridge Univ. Press, 2004.
6. McEliece, R.J. *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Pub., 1987.
7. Pellikaan R., Wu, X.-W., Bulygin, S., Jurrius, R. *Codes, Cryptology and Curves with Computer Algebra*. Cambridge Univ. Press, 2018.
8. Pless, V. *Introduction to the Theory of Error-Correcting Codes*. 3rd edition. Wiley, 1998. (*)
9. Roman, S. *Coding and Information Theory*. Springer-Verlag (GTM), 1992. (*)

Notas de códigos en español:
http://delta.cs.cinvestav.mx/~gmorales/TeoriaDeCodigos/
http://www.famaf.unc.edu.ar/series/pdf/pdfCMat/CMat35-3.pdf