MA-53J Tópicos en Matemáticas Discretas II

(Semestre Otoño 2000)

Requisitos
Optimización Combinatorial (MA 37A), o Fundamentos de Ciencias de la Computación (CC 30B), o autorización del profesor. (Es recomendable cierta familiaridad con técnicas de análisis de algoritmos, teoría de la complejidad computacional, y madurez matemática.)

Unidades: 10 UD.

Objetivos
Estudiar y discutir las nociones fundamentales de las matemáticas discretas y sus aplicaciones.

Programa

I. Complejidad de Kolmogorov

- Introducción, historia, y preliminares matemáticos
- Complejidad algorítmica.
  - Complejidad plana: el teorema de invarianza, imposibilidad de comprimir, complejidad de Kolmogorov vista como una función de enteros.
  - Complejidad prefijo: el teorema de invarianza, imposibilidad de comprimir, complejidad de Kolmogorov prefijo vista como una función de enteros.
- Razonamiento inductivo.
  - Introducción.
  - Teoría de predicciones de Solomonoff.
- Física, información y calculabilidad.
  - Cálculos reversibles.

II. Reticulados y sus Aplicaciones

- Introducción a la teoría de reticulados.
- Problemas algorítmicos de la teoría de reticulados.
  - Problemas computacionalmente difíciles.
  - Algoritmo de reducción de base de Gauss.
  - Algoritmo de Lenstra-Lenstra-Lovasz (LLL).
- Aplicaciones.
  - Programación lineal entera en dimensión fija.
  - Factorización de polinomios.

– Aplicaciones a la criptografía.

Números Aleatorios: Teoría y Práctica

- La generación de números aleatorios.
- Tests estadísticos.
- Test teóricos.
- Otros tipos de objetos aleatorios.
- Que es una sucesión aleatoria.

Bibliografía

1. An introduction to Kolmogorov complexity and its applications. Li y Vitanyi, Graduate Texts in Computer Science, Springer, 1993.
2. Structural Complexity I y II, Balcazar, Diaz y Gabarro. Springer Verlag, 1988.
3. An introduction to probability theory and its applications, Feller, Wiley, 1968.
4. The art of Computer Programming, Knuth, volumen 2, Ch. 3, segunda edición, 1981.
5. Modern cryptography, probabilistic proofs and pseudo-randomness, Goldreich, Algorithms and Combinatorics, volumen 17, Springer, 1999.
6. A course in computational algebraic number theory, Cohen, Graduate Texts in Mathematics, volumen 138, Springer, 1993.
7. An algorithmic theory of numbers, graphs and convexity, Lovász, Regional Conference Series in Applied Mathematics, volumen 50, SIAM, 1986.
8. Lattices and their application to cryptography, Dwork, Lecture Notes, Standford University, spring quarter, 1998.
9. Algebra and computation, Sudan, Lecture Notes, Massachusetts Institute of Technology, fall semester, 1998.