

NUEVO MODELO DE PROGRAMA A REGIR A PARTIR
DEL 1ER. CUATRIMESTRE DE 1994

FACULTAD DE CIENCIAS EXACTAS Y NATURALES

UNIVERSIDAD DE BUENOS AIRES

1. DEPARTAMENTO/INSTITUTO DE MATEMATICA
2. CARRERA de: a) Licenciatura en
Orientación
b) Doctorado y/o Post-grado en Doctorado
c) Profesorado en
d) Cursos Técnicos en Meteorología
e) Cursos de Idiomas
3. 1er. Cuatrimestre/2do. Cuatrimestre 2do Cuat. Año 1995
4. N° DE CODIGO DE CARRERA 53
5. MATERIA **CIRCUITOS BOOLEANOS Y ARITMETICOS**
6. N° DE CODIGO
7. PUNTAJE PROPUESTO (en caso de tratarse de materias optativas para la Licenciatura o de Doctorado y/o Post-Grado) 3 ptos
8. PLAN DE ESTUDIOS Año 1982
9. CARACTER DE LA MATERIA (Obligatoria u optativa) Optativa
10. DURACION (anual, cuatrimestral, bimestral u otra) Cuatrimestral
11. HORAS DE CLASES SEMANALES
 a) Teóricas 3 hs d) Seminarios hs
 b) Problemas 5 hs e) Teórico-Problemas hs
 c) Laboratorio hs f) Teórico-Práctico hs
 g) Totales Horas 8

12. CARGA HORARIA TOTAL 8
FORMA DE EVALUACION Examen final
13. ASIGNATURAS CORRELATIVAS ---
.....
14. PROGRAMA ANALITICO (adjuntarlo) Se adjunta
15. BIBLIOGRAFIA (indicar título del libro, autor, editorial y año de publicación; adjuntar luego del programa)

Fecha 2do. Cuatrimestre 1995

Firma Profesor

Aclaración de firma Dr. Joos HEINTZ

Firma del Director

Sello aclaratorio

Nota: Para la validez de la información presentada se solicita que todas las páginas estén inicialadas y firmadas al final por el Sr. Director del Departamento/Instituto/Carrera o Responsable debidamente selladas y fechadas.

Otra: Se recuerda que los objetivos y los contenidos mínimos están incluídos en el Plan de Estudios respectivo y sólo son modificables por Resolución del Consejo Superior de la Universidad de Buenos Aires.

CIRCUITOS BOOLEANOS Y ARITMETICOS

Repaso de funciones booleanas y de sus subclases canónicas (por ej. funciones monótonas), bases funcionales, formas normales y reescritura. Noción de circuito booleano y su representación como grafo de cálculo (DAGs y árboles). La noción de branching program. Circuitos con bounded y unbounded fan-in. Medidas temporales de complejidad: tamaño y profundidad de circuitos, longitud de fórmula. Las clases NC y AC. Medidas de espacio en circuitos mediante pebble games y registros. Branching programs y espacio. El problema del trade-off entre espacio y tiempo secuencial. Complejidad genérica: los teoremas de Shannon - Lupanov. Técnicas de minimización de circuitos. Prime implicants. Circuitos eficientes para funciones especiales: adición, multiplicación (métodos de Karatsuba - Ofman y Schönhage - Strassen), funciones simétricas. Álgebra lineal y complejidad bit. Cotas inferiores para funciones particulares: cotas inferiores lineales para bases completas, cotas inferiores exponenciales para la complejidad monótona (método de aproximación de Andreev - Kazborov). Cotas inferiores para longitud de fórmula: métodos de Neciporuk, Krapcenko, Specker - Hodes, etc.. Máquinas de Turing con advice. uniformidad, familias de circuitos uniformes y relación entre tiempo paralelo y espacio. Problemas P-completos. Algoritmos probabilísticos, la complejidad bit de algunos problemas típicos de teoría de números y de criptografía. Codificación de números y complejidad de Kolmogorov. La jerarquía aritmética. Definición y origen de la noción de circuito y red aritméticos. Circuitos aritméticos (= straight line program = slp) como estructura de datos en cálculo simbólico y numérico. El Teorema de Heintz - Schnorr. Simplificación de slp's (Vermeidung von Divisionen, teorema de Baur - Strassen - Morgenstern, álgebra lineal por slp's). Parallelización de slp's. Método de Berkowitz - Mulmuley. Cotas inferiores genéricas para polinomios (teoremas de Pan, Belaga y Paterson - Stockmeyer). Cotas inferiores para polinomios específicos: métodos de Strassen, Heintz - Morgenstern - Sieveking y Ben - Or. Complejidad estructural de circuitos aritméticos: familias

Alf

P -expresables, P -computables y P -definibles. La clase $P^{\#}$ y la conjetura de Valiant. $P^{\#}$ -hardness de la geometría algorítmica. Complejidad intrínseca de la eliminación de cuantificadores sobre los complejos y los reales (teoremas de Fischer-Rabin, Weispfennig - Davenport - Heintz). Relación con la geometría diofántica y la complejidad bit.

REFERENCIAS

Libros

- [1] J. Balcázar, J. Diaz, J. Gabarró: Structural Complexity I. EATCS Monographs on Theoretical computer Science 11 Springer (1988).
- [2] J. Balcázar, J. Diaz, J. Gabarró: Structural Complexity II. EATCS Monographs on Theoretical Computer Science 22 Springer (1990).
- [3] I. Wegener: The complexity of boolean functions. Wiley - Teubner Series in Computer Science (1987).

Surveys

- [4] J. von zur Gathen: Feasible arithmetic computations, J. of Symbolic Comput. 4 (1987) 87-100.
- [5] J. von zur Gathen: Parallel arithmetic computations:a survey, proc. 13-th. Conf. MFCS, Springer LN Comput. Sci 233 (1986) 93-112.
- [6] J. Heintz: On the computational complexity of polynomials and bilinear mappings. A survey, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 5 th Intern. Conf. AAECC-5, menorca 1987, L. Huguet and A. Poli, eds., Springer LN Comput. Sci. 356 (1989) 269-300
- [7] J. Heintz, j. Morgenstern: On the intrinsic complexity of elimination theory. journal of Complexity 9 (1993) 471-498.
- [8] J. Van Leeuwen, ed.: Handbook of Theoretical Computer Science, Vol. A, Algoritms and Complexity, Ch. 2,8,11,12,14,17. North - Holland, Amsterdam (1990).

2do Cuatrienestre 1995.

Firma del Profesor:

Aclaración de Firma: Dr. Joos HEINTZ.

