C95
(9)

UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE CIENCIAS EXACTAS Y NATURALES

1. DEPARTAMENTO: Computación.
2. CUATRIMESTRE: Segundo de 1995.
3. ASIGNATURA: CIRCUITOS BOOLEANOS Y ARITMÉTICOS
4. CARRERA: Licenciatura en Ciencias de la Computación
5. CARÁCTER DE LA MATERIA: Optativa.
6. NUMERO DE CÓDIGO DE CARRERA: 18
7. NUMERO DE CÓDIGO DE MATERIA: C608
8. PUNTAJE: 4 puntos planes 82 y 87; 3 plan 93.
9. PLAN DE ESTUDIOS AÑO: 82. 87 y 93.
10. DURACIÓN DE LA MATERIA: Cuatrimestral
11. HORAS DE CLASE SEMANAL:

    a)TEÓRICAS 6 HS. c)PROBLEMAS
    b)LABORATORIO HS. d)SEMINARIOS

12. CARGA HORARIA TOTAL: 6 HS.
13. ASIGNATURAS CORRELATIVAS: Algoritmos y estructuras de datos III y teoría de lenguajes (planes 82 y 93)teoría de lenguajes y matemática discreta(plan 87).
14. FORMA DE EVALUACIÓN: Examen Final
15. PROGRAMA Y BIBLIOGRAFÍA: Adjuntas a esta hoja

FECHA: 15/10/95

J.H.
Firma del Profesor

Firma del Director

J. HEINTZ
Aclaración de la Firma

LIC. ROBERTO BEVILACQUA
DIRECTOR ADJUNTO INTERINO
DEPARTAMENTO DE COMPUTACION
Sello Aclaratorio

APROBADO POR RESOLUCION CD. Nº 269/96

CIRCUITOS BOOLEANOS Y ARITMÉTICOS

Materia optativa

Profesor: Joos Heintz

Carga horaria: 8 horas semanales

Correlativas: Una materia de estructura de datos. Nociones de teoría de lenguajes y álgebra lineal

Este es un curso introductorio a la teoría de complejidad *no uniforme* mediante los modelos de circuito booleano (midiendo la complejidad bit) y de circuito aritmético (midiendo la cantidad de operaciones aritméticas). La atención estará centrada en las medidas de tiempo (secuencial y paralelo) y de espacio (de memoria de trabajo). Se estudiarán asimismo máquinas de Turing (uniformes y no uniformes), las cuales intervienen en la formulación de las condiciones de uniformidad necesarias para relacionar tiempo paralelo y espacio.

El curso tratará de dar un panorama representativo de los distintos métodos actuales de demostración de *cotas inferiores* de complejidad para ciertas funciones que son fundamentales en un amplio espectro de aplicaciones de la informática a otros campos.

Una parte importante del curso estará dedicada a la presentación del punto de vista de la complejidad estructural, que trata de obtener un cierto ordenamiento entre las distintas clases de complejidad.

La noción de circuito aritmético trata de modelizar aspectos de la informática cercanos al comportamiento *real* de la máquina, en particular del hardware. Complejidad en este sentido mide tiempo de computación, interpretación, ejecución y ocupación de memoria central. Por otra parte, la complejidad estructural transmite conocimientos útiles para la selección de la algorítmica adecuada en el desarrollo del software.

LIC. ROBERTO BEVILACQUA
DIRECTOR ASOCIADO INTERINO
DEPARTAMENTO DE COMPUTACION

Programa del curso

Repaso de funciones booleanas y de sus subclases canónicas (por ejemplo 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. Algebra 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 Nečiporuk, Krapčenko, 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). Paralelización 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 P–expresibles, 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, Weispfeming–Davenport–Heintz). Relación con la geometría diofántica y la complejidad bit.

Referencias

Libros

[1] J. Balcázar, J. Díaz, J. Gabarró: Structural Complexity I. EATCS Monographs on Theoretical Computer Science **11** Springer (1988).

[2] J. Balcázar, J. Díaz, 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, 5th 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, Algorithms and Complexity, Ch. 2, 8, 11, 12, 14, 17. North-Holland, Amsterdam (1990).