Komplexitätstheorie 2004
Überblick

14. Februar 2005

1 NP-Vollständigkeit

Literatur: Garey/Johnson, Schöning, Papadimitriou, Immerman, Aho/Hopcroft/Ullman

- Polynomielle Algorithmen
- Invarianzthese, polynomielle Turingmaschinen
- Definition von **NP** durch deterministische polynomielle Überprüfung
- Reduktionen als polynomielles Preprocessing, Vollständigkeitsbegriff.
- Problemdefinitionen: CircuitSat, Sat, 3Sat, CnfSat, HornSat, Clique, VertexCover, IndependentSet, 3Coloring, Max2Sat, HamiltonPath, HamiltonCircle, Knapsack, SubsetSum, Tsp, Minesweeper, etc.
- Satz: **P** hat uniforme Schaltkreise polynomieller Größe.
- Satz von Cook/Levin: Beweis der **NP**-Vollständigkeit von CircuitSat aus Uniformitätssatz.
- **NP**-Vollständigkeitsbeweise:
  - Sat Varianten (CircuitSat auf 3Sat sh. Schöning)
  - Clique, VertexCover, IndependentSet (sh. zB. Schöning)
  - 3Sat auf 3Coloring (Immerman)
  - HamiltonPath, HamiltonCircle und Tsp (Schöning)
  - Max2Sat (Papadimitriou)
- Reduktionen auf Sat, CircuitSat, und IntegerProgramming

2 Strukturelle Komplexität

Literatur: vorwiegend Papadimitriou

- Berechnungsprobleme als formale Sprachen
- Turing-Maschinenmodelle: deterministisch, nichtdeterministisch, Orakel, Mehrbandmaschinen, Maschinen fr kleine Platzklassen.
- Nichtdeterministische Algorithmen, Guess & Check
- Time-constructible/Space-constructible
- Hierarchiestze
- Gap Theorem
- **DTIME**, **NTIME**, **DSPACE**, **NSPACE**
- **L**, **NL**, **P**, **NP**, **PSPACE**, **NPSPACE**, **EXP** etc.
- Polynomielle Reduktionen als Prä-Ordnung, Vollständigkeitsbegriff fr allgemeine Komplexitätsklassen.
- Co-Klassen, Abschluss deterministischer Klassen unter Komplement
- Natürliche Inklusionsbeziehungen zwischen Zeit und Platz durch Simulationen
- Orakel, polynomielle Hierarchie
- Konfigurationsgraph
- Satz von Savitch
- Logspace-Reduktionen: Definition, Transitivität, Mächtigkeit.
- Reachability ist **NL**-vollstndig (generischer Beweis).
- Satz von Immerman/Szelepzsceny: **NL** = **coNL**: Inductive Counting; nichtdeterministische Platzklassen sind unter Komplement abgeschlossen.
- Monotone CircuitEval Evaluation ist P-vollständig (aus Uniformitätssatz)
- QSat, Geography: **PSPACE**-Vollständigkeit
- Reduktionen: many-one (Karp), Turing (Cook), truth-table, logtime
- Abschluss unter Reduktionen
- Alternierende Turingmaschinen
- **AP** = **PSPACE** (mittels QBF)
- **AL** = **P** (mittels CircuitEval)

3 Deskriptive Komplexität

- First Order Logic ist in LOGSPACE.
- Komplexität von Queries: Datenkomplexität, Ausdruckskomplexität
- 0/1 Laws (ohne Beweis)
- Komplexität von DATALOG.
- Satz von Fagin

4 Kryptographie

- Geschichtlicher Überblick
  - Steganographie
  - monoalphabetische und polyalphabetische Chiffren
  - Kerckhoffs' Maxime
  - Enigma
- "unconditional security" (Shannon)
- Computationale Sicherheit
  - Semantische Sicherheit
  - Ununterscheidbarkeit
- Probabilistische Algorithmen, Klassen **BPP**, **RP**, **co–RP**, **ZPP**
- Primzahltest
  - Satz von Pratt
  - PRIMES $\in$ **co–RP**
  - PRIMES $\in$ **P** (ohne Beweis)
- Public-Key Kryptographie
  - Inverse Funktionen polynomiell berechenbarer Funktionen
  - One-way functions
  - Hard-core predicates
  - Trapdoor-one-way functions
  - RSA
  - ElGamal, diskreter Logarithmus
  - RSA-OAEP
- Zufallszahlengeneratoren
  - Next Bit Tests
  - Konstruktion von Pseudozufallszahlengeneratoren durch Hard-core predicates

5 Effiziente Approximationsalgorithmen & Härte der Approximation

- Interaktive Protokolle
  - Definitionen der Klassen **IP** und **AM**
  - Beispiele: NON GRAPHISOMORPHISM, 3COLORING (zero knowledge)
  - Klassenrelationen: **BPP** $\subseteq$ **IP**, **NP** $\subseteq$ **IP**, **AM** $\subseteq$ **IP**
  - Beweis durch Simulation: **IP** $\subseteq$ **PSPACE**
  - Shamir's Theorem: **PSPACE** $\subseteq$ **AM**, damit **AM** $=$ **IP** $=$ **PSPACE** (ohne Beweis, Erwähnung der Arithmetisierung)
- Optimierungsprobleme
  - Definition derselben
  - Definition der Klasse **NPO**
  - Verhältnis von Entscheidungsproblem und Optimierungsproblem
  - Beispiele: VERTEXCOVER, MAXSAT, KNAPSACK
  - Definition des Performance Ratio (Johnson)
  - Definition von Approximationsproblemen
  - Approximationsalgorithmen mit konstanten Performance Ratio:
    - MAXSAT
    - VERTEXCOVER
  - Definition der Klasse **APX**
  - TSP $\in$ **APX** $\Leftrightarrow$ **P** $=$ **NP**
  - Approximation Schemes
    - die Klassen **PTAS** und **FPTAS**
    - Beispiel: KNAPSACK $\in$ **FPTAS**
    - polynomielle gebundene Probleme, die Klasse **NPO-PB**.
    - Satz: Wenn ein **NP**-hartes Problem in **NPO-PB** in **FPTAS** liegt, dann **P** $=$ **NP**.
  - **PCP** Theorem
    - Definition der Klasse **PCP**$(r(n), q(n))$
    - Härte von Approximationsproblemen: Beispiel MAX3SAT
  - Klassenzusammenhierarchie: **FPTAS** $\subseteq$ **PTAS** $\subseteq$ **APX** $\subseteq$ **NPO**
  - obige Hierarchie ist strikt genau dann und nur wenn **P** $\neq$ **NP**

Prüfung
ca. 20-30 Minuten
Persönliche Terminvereinbarung