6.045 Final Topics

Spring 2012

Final date: Tuesday, May 22, 2012

This is a brief review of the topics that you should be prepared for on the 6.045 final that were not included on the midterm (you are still responsible for the material on the midterm, so please see the midterm topics review sheet for that contents). Most of this material is unfortunately not covered in Sipser, so you will need to refer primarily to the lecture notes. As before, this list (as well as the midterm topics list) is not exhaustive. It is just meant as a basic rundown of some of the material covered in the class). Please review the lecture notes and psets as they may contain material not explicitly mentioned here.

NP

- What a polynomial-time Turing reduction is, what a polynomial-time mapping reduction is, what the difference between the two is, and why they need to be polynomial for proof of NP-hardness.
- What NP-hardness means, what NP-completeness means, what the difference between the two is, and how to prove that a language is NP-hard or NP-complete.
- What the Cook-Levin Theorem is and the basic intuition for how it works (you don’t need to memorize or be able to reproduce the proof or anything).
- Some examples of famous NP complete problems (SAT/CIRCUIT-SAT, 3SAT, 3COLORING, CLIQUE, etc.)
- Analysis of the NP class vis-à-vis the P-vs-NP problem:
  - What a relativizing proof is and the relevance for the P-vs-NP problem
  - Why we think prime factoring is not NP-complete

Space complexity

- What PSPACE is and where it fits in relationship to other complexity classes.
- The intuition for why PSPACE=NPSPACE.
Probabilistic computing

- The axioms and basic results of probability (union bound, linearity of expected value, Markov’s inequality, the Chernoff bound)
- The definitions of the probabilistic complexity classes we covered (RP, coRP, ZPP, BPP), some examples of problems in each, and how they relate to other complexity classes, particularly P, NP, coNP, and PSPACE (both conjectured and proven).
- What amplification is, how it’s used, and why it works.

Cryptography

- The one-time-pad cryptosystem
- Definition of one-way functions, trapdoor one-way functions, pseudorandom number generators, cryptographic pseudorandom number generators, what they’re used for, and their relationship to each other.
- The Diffie-Hellman key exchange
- The RSA cryptosystem, including applications in authentication and the dating protocol
- Zero-knowledge proofs and protocols (understand the examples we gave you and how to apply other topics, such as RSA and NP-completeness, to make them work)

Quantum computing

- Definitions and manipulation of qubits, entanglement, unitary transformations, etc.
- The BQP class and its relationship to other complexity classes (particularly NP, BPP, and PSPACE)
- The significance and application of Shor’s algorithm