Advanced complexity analysis

Textbook: Chapter 10

Approximation Algorithms

- Even if a problem is NP-hard, we can find approximate solutions $\in P$

Probabilistic Algorithms

Def: *BPP* is the class of languages which are recognized by probabilistic polynomial-time Turing machines with an error probability of $\frac{1}{3}$ (or equivalently any other constant c where $0 < c < \frac{1}{2}$).

Def: *RP* is the class of languages *recognized* by probabilistic polynomial-time Turing machines where any strings in the language are accepted with a probability $\geq \frac{1}{2}$ and any strings not in the language are rejected with a probability of 1.

- No false positives, fewer than 50% false negatives

Alternation and Alternating Turing Machines

- A nondeterministic Turing Machine accepts if *any* of its branches do
  - This is not the only way!
- We could also specify that *all* branches must
- We could even alternate between *all* and *any*

Def: An **alternating Turing Machine (ATM)** is a nondeterministic Turing machine where every non-terminal state (not accepting or rejecting) is either **universal** or **existential**. A *universal* node in the nondeterministic execution tree accepts if **all** of its nondeterministic branches do. An *existential* node, on the other hand, accepts if **any** sub-branches do.

- Time and space complexity are defined as in nondeterministic Turing machines
- This allows us to do "short-circuit" boolean logic in special nondeterministic cases

The Polynomial Time Hierarchy

Interactive Proof Systems

Uniform Boolean Circuits

P-Completeness

Def: A language B is P-complete if both

1. $B \in P$
2. For every language A, if $A \in P$ then A is log-space reducible to B

Cryptography

Public-Key Cryptosystems

One-Way Functions

Trapdoor Functions

Next up: Final presentations

- Everyone should do a final presentation and/or project
- Each person will have a full class period to present
- Try to think up a “cool” topic not covered in class (or go deeper into something that was covered)