

Recap

Questions?

Algorithms

- Polynomial Time
 - Stable Marriage
 - Approximation for Vertex Cover (x 2)
 - Maximal Matching
 - Linear Programming relaxation
 - Set Cover
 - Greedy
 - Learning Disjunctions with Bounded Number of Mistakes
- Did not Cover
 - A LOT
 - Not just P and not P
 - Many algorithmic techniques developed

Incomputable Functions

- Different levels of infinity
 - “Cardinality” via existence of bijections
- Halting Problem, Hello Problem, Kolmogorov Complexity

NP-completeness

- “Short Proofs”
- Horde of Problems
 - 3-SAT
 - 3-coloring
 - Traveling Salesman Problem
 - Vertex Cover
 - Clique
 - Independent Set
 - Hamiltonian Cycle
 - Graph partition
 - Conductance

Dealing with NP-completeness

- Average Case Complexity
 - Some instances may have short proofs
- Approximation
 - Can approximate certain problems
 - Others resistant to approximation
- Reductions

Dealing with NP-completeness

- Average Case Complexity
 - Some instances may have short proofs
- Approximation
 - Can approximate certain problems
 - Others resistant to approximation
- Exponential Time Algorithms
- Reductions
- Did not talk about
 - Barriers to Progress

Reductions

- Use Hard Problem to show another problem is hard
 - Reduce from hard problem
- Use Easy Problem to show another problem is easy
 - Reduce to easy problem
- NP-completeness
- Undecidable
- Dealing with NP-completeness
- Show Cryptographic security

Learning

- Learning is
 - Prediction
 - Compression
 - Memorization??
- Classification
 - With error/ without error
 - Used Linear Threshold Functions to Learn Disjunctions with Winnow [Multiplicative Updates]
- Online-Optimization
 - Experts

Experts Algorithms

- Approximate Linear Programming
- Hard-core Sets
- Boosting Learning Algorithms

Randomness

- Kolmogorov Complexity
 - Define “random” string is incompressible (unlearnable)
- Showed that “random graphs” have no large cliques or independent sets
 - Stated that we do not know how to construct these without randomness “Finding hay in a haystack”
- Randomness Used in algorithms
 - Small change of incorrect answer.
 - We don’t think it is necessary, but cannot get rid of it
 - Polynomial Identity Testing
- Randomness in Protocols
 - Provably need it to efficiently check equality

Communication Complexity

- Rectangular Method for Lower Bounds
 - Set Intersection
 - Equality
- Upper bounds
 - Trivial algorithm
 - Fingerprints for checking equality

Cryptography

- “Sealed Envelops”
 - Coin flipping
 - Commitment
 - encryption
- Zero Knowledge Proofs

Methodology

- Borrowed from mathematics
- Proof based
- Model computation mathematically
 - Ideal computers

What we did not cover

- Well, lots.
- Did not talk at all about data structures
- Did not talk much about optimizing algorithm run times

Computational/Algorithmic Lens

- Look at our world through the lens of computation
- Biology
 - Evolution (as a form of learning)
 - Sexual reproduction
- Social Sciences
 - 6 degrees of separation with navigation
 - Information Agregation
- Economics
 - Efficiently finding equilibria
- Physics
 - Quantum Mechanics
 - Phase Transitions