NP-Complete Problems

Why Consider Complexity?

- Encryption algorithms that are complex, should be hard for analysts to attack.
- In particular, problems for which the number of possible solutions is large, should be essentially infeasible to solve using brute force attacks with computer assistance.

Problem 1: Satisfiability

- Determine whether any given logical formula is satisfiable, that is, whether there is a way of assigning the values TRUE and FALSE to the variables so that the result of the formula is TRUE.

Example of Problem 1

- Consider Boolean variables A,B, and C and their complements A', B', and C'.
- The following formula is satisfiable:
  - A AND (B OR C) AND (C' OR A')
- The following formula is not satisfiable:
  - A AND (B OR C) AND (C' OR A') AND (B')

Problem 2: Knapsack

- Given a set of nonnegative integers and a target, is there a subset of the integers whose sum equals the target?

Example of Problem 2

- Let S = {4,7,1,12,10} and let the target sum be T.
  - For T = 17, we have a solution: 4 + 1 + 12 =17.
  - For T = 25, there is no solution.

Problem 3: Clique

- Given a graph G and integer n, is there a subset of n vertices such that every vertex in the subset shares an edge with every other vertex in the subset (this is called a clique.)

Characteristics of NP-Complete Problems

- The three problems have similar characteristics:
  - Each is solvable, using enumeration.
  - Suppose there are 2^n cases to consider--then the total time to check all possibilities is proportional to 2^n.
  - Problems are from different disciplines, hence apparently unrelated.
  - If we could guess perfectly, we could solve the problem in relatively little time--ie, the time to verify a solution is bounded.

The Classes of P and NP

- Let **P** be the collection of all problems for which there is a solution that runs in time bounded by a polynomial function of the size of the problem.
- Let **NP** be the set of all problems that can be solved in time bounded by a polynomial function of the size of the problem, assuming the ability to guess perfectly.

Relationship of the Classes

- There is a class EXP, which consists of problems for which a deterministic solution exists in exponential time, c^n for some constant n.
- $P \subseteq NP \subseteq EXP$

The Meaning of NP-Completeness

- The satisfiability problem is NP-Complete, meaning that it can represent the entire class NP.
- If there is a deterministic, polynomial time algorithm for the satisfiability problem, then there is a determinisitc, polynomial time algorithm for every problem in NP.
- But no polynomial time solutions have been found (yet.)

NP-Completeness and Cryptography

- Encryption based on an NP-complete problem would be difficult for an attacker to solve.
- However, if n is small, then 2^n tries may not take long, especially with improvement in hardware speed and parallelism.

Other Hard Problems

- Number theory problems , although not NP-complete, can computationally very-time consuming.
- In particular, computation in Galois fields and factoring large numbers, have been used in encryption algorithms.