

Theory Comprehensive Exam
Department of Computer Science
Yale University
May 18, 2000

For this exam you may take as known facts that 3-SAT, Vertex Cover, Clique, Hamiltonian Circuit, Bin-packing and Subset-sum are all NP-Complete problems. You may also assume access to a source of random bits.

1. (20 pts) You are given a word w of length n (over some constant-sized alphabet), a set of m words x_1, x_2, \dots, x_m of length at most n each, and an integer k . The problem is to determine if there is some sequence i_1, i_2, \dots, i_k of indices (not necessarily distinct) such that w can be written by concatenating $x_{i_1}, x_{i_2}, \dots, x_{i_k}$. (In other words, if w can be broken up into exactly k words from the list.)

Give a polynomial-time algorithm that determines if such a sequence exists, or show that this problem is NP-complete.

2. (20 pts) Ben and Jerry need to exchange secret information (Gigabytes of it) over an open¹ but authenticated² channel. At the present time, they share no secret information. Explain how they can solve this problem without using an alternative communication channel. Be thorough in your explanation e.g. if you write "Ben generates a prime number", give the size of the number and explain the method by which it is found.

¹"open" means anybody can listen in.

²"authenticated" messages cannot be altered by a third party.

Do any four of the following problems. Please do not do all five.

- (15 pts) Calculate $10^{(5^{3^4})}$ modulo 77. Explain your method. Do not use a calculator.
- (15 pts) Design a deterministic finite automaton that accepts a binary string w if and only if w contains the pattern 1101 or ends with 00.
- (15 pts) The entries of an $n \times n$ matrix M are integers such that $M[i, j+1] \geq M[i, j]$ and $M[i+1, j] \geq M[i, j]$. The problem is to find out whether or not the matrix contains an entry with the number 10. You may ask to see any entry in the matrix. The "complexity" of the problem is the number of matrix entries you need to look at. Give the best upper and lower bounds you can for this problem.
- (15 pts) Consider rolling 5 (six sided) dice. Event "TRIPLE" is defined as "three or more dice show the same number". Event "TWO PAIRS" is defined as "two distinct numbers appear at least twice". What is the probability that either or both of these events occur?
- (15 pts) The "wheel subgraph problem" is defined as follows. given a graph G and a number k , decide if G contains a subgraph consisting of a wheel with k spokes (see picture below).

Give a polynomial-time algorithm that determines if G contains such a subgraph, or show that this problem is NP-complete.

