

## Spring 2005 Theory Comprehensive Exam

Answer any 6 out of 8 questions; answering additional questions will earn extra credit but is not necessary to pass.

If you run out of time, the idea of the proof is much more important (and will earn more partial credit) than mathematical formalism.

1. Suppose I have a graph  $G = (V, E)$ . Recall that an *independent set* is a subset  $S \subset V$  which does not contain any neighboring pairs of vertices.

Now suppose that I have access to a friendly oracle, who is happy to answer yes-or-no questions of the form “does  $G = (V, E)$  have an independent set of size  $k$  or greater?” for any  $G$  and  $k$ . Show that, by asking this oracle a polynomial number of such questions, I can find the largest independent set  $S$  of my graph  $G$ .

2. Suppose I have a graph  $G = (V, E)$ , where each vertex is given a weight  $w(v)$ . MAXIMUM-WEIGHT INDEPENDENT SET then asks for the independent set with the largest total weight. Show that MAXIMUM-WEIGHT INDEPENDENT SET is in P in the special case where  $G$  is a tree.

3. Suppose a Turing machine has a read-only tape and a work tape. Furthermore, the head on the read-only tape is restricted so that, at each step, it can stay put or move to the right; it cannot move back to the left.

On the read-only tape we give the machine an input string of parentheses of length  $n$ . We want it the machine to output “yes” if this string is properly nested and “no” if it is not. For instance,  $((()))$  is properly nested but  $(())$  is not.

Show that this Turing machine needs  $\Omega(\log n)$  space on its work tape to perform this task. Specifically, show that if it uses  $o(\log n)$  space, then there is at least one string for which the machine gives the wrong output.

4. The GRAPH 3-COLORING problem asks whether the vertices of a graph  $G = (V, E)$  can be colored with three colors {red, green, blue} such that no two vertices of the same color are connected by an edge.

EQUAL 3-COLORING is a variant of GRAPH 3-COLORING, in which we assume that  $|V|$  is a multiple of 3, and we ask whether it is possible to color the graph so that exactly  $|V|/3$  vertices are colored with each of the three colors. Using the fact that GRAPH 3-COLORING is NP-complete, prove that EQUAL 3-COLORING is NP-complete.

5. Given a Boolean formula  $\phi$  on  $n$  variables, let  $\phi(\ell = \mathbf{true})$  be the formula on  $n - 1$  variables we get if we set the literal  $\ell$  to  $\mathbf{true}$  everywhere (which means setting the variable in  $\ell$   $\mathbf{true}$  or  $\mathbf{false}$  depending on whether or not  $\ell$  is negated).

Suppose a 3-SAT formula  $\phi$  contains a clause  $c = (\ell_1 \vee \ell_2 \vee \ell_3)$ . At least one of these literals must be true. If  $\phi$  is satisfiable, then, it follows that at least one of these three formulas must be satisfiable:

$$\begin{aligned} &\phi(\ell_1 = \mathbf{true}) \\ &\phi(\ell_1 = \mathbf{false}, \ell_2 = \mathbf{true}) \\ &\phi(\ell_1 = \mathbf{false}, \ell_2 = \mathbf{false}, \ell_3 = \mathbf{true}) \end{aligned}$$

Now consider the following algorithm for 3-SAT.

```
SAT( $\phi$ ) {
  If  $\phi$  contains 3-variable clauses {
    Choose a 3-variable clause  $c = (\ell_1 \vee \ell_2 \vee \ell_3)$ 
    If SAT( $\phi(\ell_1 = \mathbf{true})$ ) return "yes"
    Else if SAT( $\phi(\ell_1 = \mathbf{false}, \ell_2 = \mathbf{true})$ ) return "yes"
    Else if SAT( $\phi(\ell_1 = \mathbf{false}, \ell_2 = \mathbf{false}, \ell_3 = \mathbf{true})$ ) return "yes"
    Else return "no"
  }
  Else  $\phi$  is a 2-SAT formula; solve in polynomial time and return the result.
}
```

Let  $T(n)$  be the total running time of this algorithm on formulas with  $n$  variables. Write down a recurrence for the worst-case running time of  $T(n)$ , and show that  $f(n) = O(a^n)$  for some  $a < 2$ .

6. A standard approach to cryptography is to define a function  $f(M, K)$  where  $M$  is the "plaintext" (unencrypted) message we wish to send, and  $K$  is a secret key. The idea is that even if an eavesdropper obtains a copy of the encoded message  $f(M, K)$ , he or she cannot decrypt it and obtain the plaintext  $M$  without knowing the secret key  $K$ .

Discuss to what extent the following statement is true, and justify your answer: "If  $P = NP$ , then there is no such thing as secure cryptography."

7. An ant is crawling on the corners of a hexagon. At each time step, he stays put, moves one step clockwise, or moves two steps clockwise, each with probability  $1/3$  (he never moves counterclockwise). Write down the  $6 \times 6$  transition matrix for this process and find its eigenvectors and eigenvalues.
8. Let  $\mathbf{x} = [x_1 \ x_2 \ \dots \ x_N]^T$  be an eigenvector of a stochastic matrix  $\mathbf{P}$  with eigenvalue  $\lambda$ , i.e.,  $\mathbf{P}\mathbf{x} = \lambda\mathbf{x}$ . Prove that if  $\lambda \neq 1$ , then  $\sum_{i=1}^N x_i = 0$ .