EE2336 02 Discrete Mathematics Midterm II

May 18 2005

(1) Note that there are two pages in total.
(2) Please remember to write down your name and ID.

True or False (30pts)

1. A problem that is solvable using an algorithm with polynomial worst-case complexity is called tractable. That is, an algorithm with complexity of $O(2^n)$ is tractable.
2. Problems for which a solution can be checked in polynomial time are said to belong to the class **NP**. Tractable problems are said to belong to class **P**. And it's known that $\mathbf{NP} \subseteq \mathbf{P}$.
3. The set of positive integers that are divisible by 3 is countable, but the set of positive integers that are not divisible by 3 is uncountable.
4. Let $a = bq + r$, where a, b, q, and r are integers, then $\gcd(a, b) = \gcd(q, r)$.
5. The generalized pigeonhole principle is that if N objects are placed into k boxes, then there is at least one box containing at least $\lceil N/k \rceil$ objects.
6. The number of r-permutations of a set of n objects with repetition allowed is $n!$.
7. Let E and F be two probability events. If $p(E \cap F) = p(E)p(F)$, we can conclude that E and F are independent.
8. If S is the sample space and the probability of the event E is $p(E)$, the probability of its complementary event is $p(S - E)$.
9. The function $(n^3 + n^2 \log n)(\log n + 25) + 2(14 \log n + 11)(n^3 + 6)$ is $O(n^4)$.
10. For two matrices **A** and **B**, if **AB** and **BA** are both defined, **A** and **B** are square matrices of the same size. And we can conclude that $\mathbf{AB} \neq \mathbf{BA}$.

Answer the Question

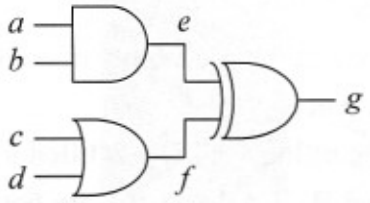
1. (5pts) List the following commonly used complexity in a descending order: $O(c^n)$, $O(n)$, $O(\log n)$, $O(n^c)$, $O(n!)$, $O(1)$, $O(n \log n)$, where c is a constant and $c > 1$.
2. (5pts) Let $\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$. Find $(\mathbf{A} \times \mathbf{B}) \times (\mathbf{A} \times \mathbf{B})^t$.
3. (8pts) (a) Using pseudocode to give an iterative algorithm to compute $b^n \bmod m$, where b, n and m are large integers. What is the complexity? You have to explain the complexity. (b) Give a recursive algorithm with the same complexity to do the same job. Also you have to explain its complexity.
4. (7pts) The RSA encryption can be done by $C = M^e \bmod n$, where C is the ciphertext; $n = pq$, p and q are large primes; M is the plaintext; e is the encryption

key, and $\gcd(e, (p-1)(q-1)) = 1$. Prove the RSA decryption with the decryption key d, where $de \equiv 1 \bmod (p-1)(q-1)$.

Hint:

Fermat's Little Theorem: if p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$. And for every integer a we have $a^p \equiv a \pmod{p}$.

5. (7pts) Prove that $8|(n-1)(n+1)$ whenever n is an odd positive integer by mathematical induction.
6. (9pts) Show that if six integers are selected from the first 10 positive integers, there must be at least one pair of these integers with the sum 11.
7. (9pts) How many solutions are there to the inequality $y_1 + y_2 + y_3 \le 12$, where y_1, y_2, and y_3 are nonnegative integers?
8. (20pts) For a modern CMOS electrical circuit, signal transition is the major contribution to the power consumption. To estimate the power consumption without any information of the input vectors, probability technique can be applied.
   (a) (7pts) For the following gate-level circuit, derive the signal probability of the primary output g (i.e., $p(g=1)$ and $p(g=0)$), assuming that signal probability of all the inputs is equally likely (i.e., $p(a=1) = p(b=1) = p(c=1) = p(d=1) = 1/2$). All the signals are independent to others.



   (b) (8pts) The signal transition count can be measured by counting the change from 0 to 1, or from 1 to 0. For example, a sequence (001) has one transition, while (010) has two, and (000) has none. If we check a 3-bit output sequence, given the probability of g. And assume that each bit is generated randomly and independently to others. What is the expected value of the transition count of the 3-bit sequence at g?
   (c) (5pts) What is the variance of the transition count of the 3-bit sequence at g?

$E(X^2) - E(X)^2$

Good luck and happy examining!