18.310 Exam 2

Monday, November 20, 2006

- You have 50 minutes to complete this exam.
- One 8.5" x 11" sheet of notes allowed. No calculators allowed.
- A correct answer does not guarantee full credit and a wrong answer does not guarantee loss of credit. You should concisely indicate your reasoning. The grade on each problem is based on our judgment of your level of understanding as reflected by what you have written.
- For all True/False questions, a very short, clear and concise explanation must be provided. A correct answer with wrong reasoning nets zero points.
- There are 4 problems. Budget your time accordingly.

Problem 1: (25 points)

Let M be a $N \times N$ matrix with entries either "0" or "1". Each row sum and each column sum of M is k. Can M can be written as a sum of k permutation matrices? Show why or why not. (A permutation matrix is a matrix where each entry is a "0" or "1" such that each column contains exactly one "1" and each row contains exactly one "1".)

Problem 2: (50 points - 10 points each problem) True/False plus short Reasoning.

(A) There exists an x such that $x^{200} = 2 \pmod{401}$.
(Note: The number 401 is prime.)

(B) If x is an element in the multiplicative group $(\mathbb{Z}_N^*, \cdot)$, then it is always true that $x^{N-1} \equiv 1 \text{ Mod } N$. (The group $\mathbb{Z}_N^*$ contains all numbers from $1, \ldots, N-1$ that are relatively prime to N).

(C) In RSA coding, M and $N = pq$ are known to the public. The encoder raises the message to the power M Mod N. If M and N are not relatively prime, then the decoder fails.

(D) The binary expansion of a large N is (1101....10101). On our spreadsheet, we raise an arbitrary number x to the $(N-1)^{\text{th}}$ power and get the following,

$$\begin{aligned} x^{(1101....10100)} &= 1 \mod N \\ x^{(1101....1010)} &= 1 \mod N \\ x^{(1101....101)} &= x \mod N \\ x^{(1101....10)} &= 1 \mod N \\ x^{(1101....1)} &= x \mod N \\ \vdots &= \vdots \end{aligned}$$

The number "N" is prime and not a Carmichael number.

(E) In Linear Programming, if the primal problem is feasible, then so is its dual and the optimal values of the objective functions are equal.

Problem 3: (25 points)

For the following LP problem, set-up the first step of the Simplex Algorithm and demonstrate the first pivot step. Write down its dual as well.
Maximize $x_1 + x_2 + x_3$ subject to $x_1, x_2, x_3 \geq 0$ and

$$\begin{aligned} x_1 + 2x_2 + 3x_3 &\leq 5 \\ x_1 - x_2 + x_3 &\leq 1 \\ x_1 + x_2 - x_3 &\leq 2 \end{aligned}$$

Problem 4: (25 points)

Suppose you have been observing the price of a stock for 10 days and would like to buy the stock in the next 15 days. Assume that the stock prices have uniform distribution over the 25 day period. Your goal is to purchase the stock at the lowest or second lowest price. Assume for simplicity that you are forced to buy at exactly noon each day, if at all, at the current price (you see the price once per day). Describe what you would do (what computation you would make) to determine the optimal strategy for accepting either the best or second best alternative (you win if you end up with one of these and lose otherwise). What are possible best strategies with this goal?" (A long answer is NOT required.)