15-451 Algorithms, Spring 2007

Homework # 6 **due: Mon-Thursday, April 23-26, 2007**

This homework is to be presented orally in groups of three. Wednesday evening or Thursday afternoon (at the latest) signups will be available on Michelle's door, until 5pm. Once they have been posted, a message will be sent to the bulletin board and an announcement will be posted on the website. **You must sign up in groups of three. Unauthorized sign-ups with less than 3 individuals will be struck from the schedule. If you need help finding a group, please let Michelle know. Groups must sign up by Friday 5pm. If your group hasn't signed up by 5pm, we reserve the right to penalize your group's final score**. In addition, regardless of what day you sign up, help from TAs must be sought before the first group is graded. After that, out of fairness to groups that have already presented, the TAs will not answer non-clarification questions (i.e., no hints). Start your homework early!

Problems:

1. [**Approximation and Online Algorithms**]

   (a) Recall the generalized shortest supersequence problem from Homework 5 - given a set of n strings $X = \{x^i = x_1^i x_2^i \dots x_{m_i}^i \mid m_i \geq 1,\ i = 1, \dots, n\}$ over an alphabet Σ, find a supersequence z of X of minimum length. Recall that x^i is not required to occur contiguously in z; only the order of the characters appearing in x^i must be the same as that of their counterparts in z.

   In this problem we assume that $\Sigma = \{0, 1\}$, *i.e.* that all strings in X are binary.

   Consider the following approximation algorithm A: Let $M = \max_i m_i$ be the length of the longest string x^i in X. Output $z = (01)^M$, *i.e.* 01 repeated M times.

   Prove that A is a 2-approximation algorithm for the binary generalized shortest supersequence problem. In particular, show that the output z is a supersequence of X and is at most twice as long as the optimal supersequence of X.

   (b) Consider the following on-line problem. In order to keep up with the current trend, you have decided that you must obtain a Nintendo Wii. You decide to buy the Wii from Crazy Jim's and you know that he is going to offer you a sequence of prices $\{p_1, p_2, p_3, \dots, p_m\}$ all in the range, $\ell \leq p_i \leq h$ for real numbers $h > \ell > 0$. When presented with the option of buying the Wii at price p_i, you already know $p_1, \dots, p_{i-1}$ and have passed on these offers, but you know nothing about $p_{i+1}, \dots, p_m$ except that they are all in the range between ℓ and h. So when Crazy Jim offers you p_i you can either buy the Wii for that price, or pass, in which case you have committed to buying it at a price among $p_{i+1}, \dots, p_m$. (So if you wait until p_m, then you are obligated to buy the Wii at that price, even if it is h.) Your goal is to buy the Wii at the lowest price possible. Here is a deterministic on-line algorithm A for this problem. Accept the first price p_i such that $p_i \leq \sqrt{\ell h}$. (If all $p_i > \sqrt{\ell h}$ then A accepts p_m.) Prove that this algorithm is $\sqrt{r}$ competitive where $r = \frac{h}{\ell}$ is the ratio of the highest to lowest possible price.

2. [**Number Theory**] Let p and q be distinct primes. Let (ℓ, m) be a pair of integers with $0 \le \ell < p$ and $0 \le m < q$.

   (a) Show that for every such pair (ℓ, m) there is at most one integer i with $0 \le i < pq$ such that $i \equiv \ell \bmod p$ and $i \equiv m \bmod q$.

   (b) Let z be $0 \le z < p$ and $z \equiv q^{-1} \bmod p$. Let y be $0 \le y < q$ and $y \equiv p^{-1} \bmod q$. Prove that given (ℓ, m), one can recover an integer i as above (such that $0 \le i < pq$ and $i \equiv \ell \bmod p$ and $i \equiv m \bmod q$) by computing

$$i \equiv (\ell \cdot zq + m \cdot yp) \bmod pq.$$

   You have shown a special case of the well known Chinese Remainder Theorem. It says that given m distinct primes $p_1, \ldots, p_m$ and m integers $a_1, \ldots, a_m$, the system of equations

$$\begin{aligned} x &\equiv a_1 \quad \mathrm{mod} p_1 \\ x &\equiv a_2 \quad \mathrm{mod} p_2 \\ &\cdots \\ x &\equiv a_m \quad \mathrm{mod} p_m \end{aligned}$$

   has a unique solution $0 \le x < \prod_{i=1}^{m} p_i$.

   You may use this (Chinese Remainder Theorem) in problem 3 below.

3. [**Insecure RSA**] Alice and her three friends are all users of the RSA cryptosystem. Her friends have chosen their public keys $(N_i, e_i = 3)$, $i = 1, 2, 3$, where as always, $N_i = p_i q_i$ for randomly chosen n-bit primes p_i, q_i. Alice has a n-bit message M she wants to send securely to each of her friends. She encrypts M using RSA for each of her friends in the normal manner, namely she encrypts and broadcasts $M^3 \bmod N_1$, $M^3 \bmod N_2$, and $M^3 \bmod N_3$. Unfortunately, Malory is listening to Alice's transmissions and intercepts all three encrypted messages. Show that Mallory can efficiently reconstruct M.