600.363/463 Introduction to Algorithms/Algorithms I November 16, 2009

Handout 13: Homework 7

Instructor: Susan Hohenberger *TA: Ming Chuang*

This assignment is due by the start of lecture on November 23, 2009. Please clearly indicate your collaborators.

1. (30 points) $G = (V, E)$ is a directed graph with edges weighted between 0 and 1, i.e., $0 \leq w(i, j) \leq 1$, for all $(i, j) \in E$.

   (a) Design an $O(V^3)$ algorithm to find the minimum-cost cycle in G. (Assume G contains no self-loops. That is, all cycles contains at least 2 edges.)

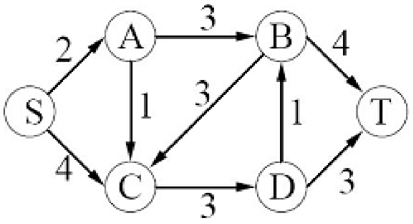
   (b) We say that a directed cycle with c edges is *expensive*, if its sum of the weights of edges is more than $c - 1$. Give an $O(V^3)$ algorithm to decide whether or not G contains an expensive cycle. Argue your algorithm is correct and analyze the running time. (**HINT:** Apply part (a) on a modified input.)

2. (20 points) (CLRS 26.1-7) Let f be a flow in a network, and let α be a real number. The **scalar flow product**, denoted αf, is a function from $V \times V$ to $\mathbf{R}$ defined by

$$(\alpha f)(u, v) = \alpha \cdot f(u, v)$$

   Prove that the flows in a network form a **convex set**. That is, show that if f_1 and f_2 are flows, then so is $\alpha f_1 + (1 - \alpha) f_2$ for all α in the range $0 \leq \alpha \leq 1$.

3. (30 points) Use Ford-Fulkerson algorithm to find the maximum flow. Assume the first two augmenting paths are $S \rightarrow A \rightarrow C \rightarrow D \rightarrow T$, and then $S \rightarrow A \rightarrow B \rightarrow C \rightarrow D \rightarrow T$.



   (a) Draw its *residual network* so far.

   (b) List all possible choices for the next augmenting path.

   (c) What is the value of the maximum flow? Show the minimum cut by drawing a dotted line on the graph.

4. (20 points) Read over the description of the RSA Public-Key Cryptosystem in Section 31.7. Let's consider a toy example with an RSA key set to $p = 13$, $q = 17$, $n = 221$ and $e = 5$. Show your work.

(a) What is the value of $\phi(n)$?

(b) For the above setting of n, we could not have chosen $e = 3$. Explain why.

(c) What value of d should be used in the secret key? We need $de \equiv 1 \bmod \phi(n)$. Show the steps of the EXTENDED-EUCLID algorithm on page 937 of the textbook.

(d) What is the encryption of the message $M = 65$?

(e) What is the decryption of the ciphertext $C = 64$?

(f) This exact version of RSA encryption is not used in practice, because it has a security issue. In fact, *any* deterministic encryption algorithm has a security issue. Explain this.