

NO NOTES, BOOKS, ELECTRONIC DEVICES, OR INTERPERSONAL COMMUNICATION ALLOWED. Submit each solution on a separate sheet of paper.

## Problems

LO7. Answer the following.

- (a) Provide the dynamic-programming recurrence for computing the distance  $D(u, v)$ , from a vertex  $u$  to a vertex  $v$  in a directed acyclic graph (DAG)  $G = (V, E, c)$ , where  $c(x, y)$  gives the cost of edge  $e = (x, y)$ , for each  $e \in E$ . Hint: step *backward* from  $v$ , rather than forward from  $u$ .
- (b) Draw the vertices of the following DAG  $G$  in a linear left-to-right manner so that the vertices are topologically sorted, meaning, if  $(u, v)$  is an edge of  $G$ , then  $u$  appears to the left of  $v$ . The vertices of  $G$  are a-h, while the weighted edges of  $G$  are

$$(a, b, 2), (a, e, 5), (a, f, 5), (b, c, 5), (b, g, 2), (c, d, 1), (c, g, 4), (c, h, 5), (d, h, 5), (e, b, 1), (e, f, 3), \\ (f, b, 5), (f, c, 2), (f, g, 1), (g, d, 2), (g, h, 3).$$

- (c) Starting from left to right in topological order, use the recurrence to compute

$$d(a, a), \dots, d(a, h).$$

LO8. Do/answer the following.

- (a) Draw the implication graph  $G_{\mathcal{C}}$  associated with the 2SAT instance

$$\mathcal{C} = \{(\bar{x}_1, x_2), (\bar{x}_1, \bar{x}_3), (x_1, x_4), (x_2, x_4), (\bar{x}_2, \bar{x}_4), (\bar{x}_2, \bar{x}_5), (\bar{x}_3, \bar{x}_4)\}.$$

- (b) Apply the improved 2SAT algorithm to obtain a satisfying assignment for  $\mathcal{C}$ . When deciding on the next reachability set  $R_l$  to compute, follow the literal order  $l = x_1, \bar{x}_1, \dots, x_5, \bar{x}_5$ . For each consistent reachability set encountered, provide the partial assignment  $\alpha_{R_l}$  associated with  $R_l$  and draw the reduced implication graph before continuing to the next reachability set. Note: do *not* compute the reachability set for a literal that has already been assigned a truth value. Provide a final assignment  $\alpha$  and verify that it satisfies all the clauses.
- (c) Suppose 2SAT instance  $\mathcal{C}$  is satisfiable and uses 336 variables and 615 clauses. Using the original 2SAT algorithm, what is the *least* number of queries to a Reachability oracle that needs to be made in order to establish  $\mathcal{C}$ 's satisfiability. In other words, if we make fewer than this number of queries then it is possible that the 2SAT instance  $\mathcal{C}$  may be unsatisfiable. Explain.

LO9. Answer the following.

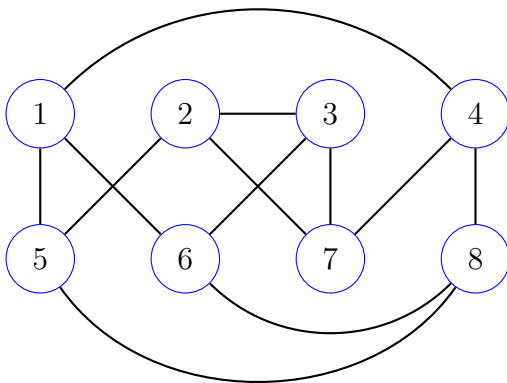
- (a) Provide the definition of what it means to be a mapping reduction from decision problem  $A$  to decision problem  $B$ .
- (b) For the mapping reduction  $f : \text{Subset Sum} \rightarrow \text{Set Partition}$ , determine  $f(S, t)$  for **Subset Sum** instance  $(S = \{12, 15, 17, 24, 26, 27\}, t = 70)$ . Show work.
- (c) Verify that both  $(S, t)$  and  $f(S, t)$  are either both positive instances or both negative instances of their respective decision problems. If both are positive, then provide valid certificates for each. Otherwise, explain why neither has a valid certificate.

LO10. An instance of the **Quadratic Residue (QR)** decision problem is a triple  $(a, c, m)$  of positive integers, where  $a, c \leq m$ , and the problem is to decide if there is an  $1 \leq x \leq c$  for which  $x^2 \equiv a \pmod{m}$ .

- (a) For a given instance  $(a, c, m)$  of **QR** describe a certificate in relation to  $(a, c, m)$ .
- (b) Provide a semi-formal verifier algorithm that takes as input i) an instance  $(a, c, m)$ , and ii) a certificate for  $(a, c, m)$  as defined in part a, and decides if the certificate is valid for  $(a, c, m)$ .
- (c) Suppose  $m$  is a  $b$ -bit number, explain why  $b$  is a more appropriate size parameter than  $m$ .
- (d) Use the  $b$  size parameter to describe the running time of your verifier from part b. Hint: make reference to the complexity of certain arithmetic algorithms.

LO11. Recall the mapping reduction  $f : \text{HC} \rightarrow \text{TSP}$  from **Hamilton Cycle** to **Traveling Salesperson** described in lecture.

- (a) Given the **HC** instance  $G$  shown below, draw  $f(G)$  and indicate its  $k$  value.



- (b) By providing valid certificates for each, verify that both  $G$  and  $f(G)$  are positive instances of their respective decision problems. Show work and explain.