PRIFYSGOL CYMRU; UNIVERSITY OF WALES

DEGREE EXAMINATIONS JANUARY 2002

SWANSEA

Computer Science

CS 232 Algorithms and Complexity

Attempt 2 questions out of 3

Time allowed: 2 hours

Students are permitted to use the dictionaries provided by the University through the invigilators

CS 232
ALGORITHMS AND COMPLEXITY

(Attempt 2 questions out of 3)

Question 1

(a) Consider Euclid's algorithm EUCLID(a, b) and its extended form EXTENDED-EUCLID(a, b).

(i) Indicate the main stages in a run of EUCLID$(60, 13)$.

(ii) Go through the main stages and give the intermediate results produced in a run of EXTENDED-EUCLID$(60, 13)$. Explain how the result can be used to find a solution x in the range $0 \leqslant x < 60$ to the modular equation $13x \equiv 1 \pmod{60}$.

(iii) Explain why the number of recursive calls in a run of EUCLID(a, b) is linear in the lengths of the binary representations of the arguments.

[9 marks]

(b) Consider modular exponentiation $(a, b, n) \mapsto a^b \bmod n$.

(i) Give two reasons why the following naive algorithm for modular exponentiation is not feasible.

NAIVE-MOD-EXP(a, b, n)

```
1 d := 1
2 FOR i = 1, ..., b  DO   d := da  OD
3 d := d mod n
4 output d
```

(ii) Give pseudocode for the feasible algorithm based on repeated squaring, which works with the binary representation $\langle b \rangle_2 = b_{k-1} \ldots b_0$ of b, MODULAR-EXPONENTIATION(a, b, n).

(iii) Compute $7^{63} \bmod 9$ following MODULAR-EXPONENTIATION$(7, 63, 9)$; carefully list the relevant intermediate results.

[9 marks]

(c) Consider the RSA cryptosystem.

(i) What is the advantage of a public key system, like RSA, over a traditional symmetric key system?

(ii) Explain RSA in the example where Alice selects primes $p = 7$, $q = 11$ with $e = 13$ for her public key $(n, e) = (77, 13)$. Find a matching secret key for Alice, and specify the encryption and decryption transformations for this key pair.

(iii) Why would a feasible factorisation algorithm compromise RSA?

[7 marks]

Question 2

(a) Consider the graph G with vertex set $\{\mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d}, \mathrm{e}, \mathrm{f}\}$ depicted below. Illustrate the operation of breadth-first-search $\mathrm{BFS}(G, \mathrm{a})$ and depth-first-search $\mathrm{DFS}(G)$ on this graph, in the adjacency list representation based on the alphabetical enumeration of vertices.

(i) give this adjacency list representation for G.

(ii) list the vertices in order of discovery in $\mathrm{BFS}(G, \mathrm{a})$ and the final assignments to the auxiliary functions d and π; draw the BFS-tree.

(iii) list the vertices in order of discovery in $\mathrm{DFS}(G)$, indicate the parenthesis structure of nested DFS-VISIT-calls, and the final assignments to the auxiliary functions t_1, t_2 and π; draw the DFS-forest.

[10 marks]

(b) Explain how the size of the adjacency list representation of a graph (V, E) is linear in $|V| + |E|$ and sketch the argument that BFS runs in time linear in this size.

[6 marks]

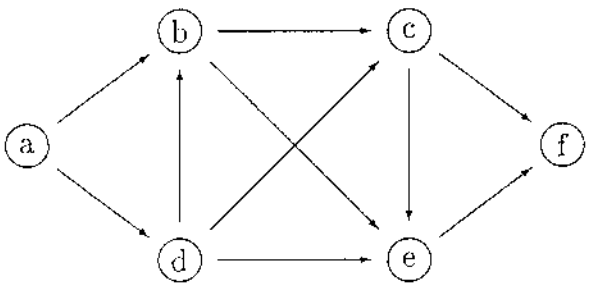
(c) Consider the weighted version G, ω of G depicted below, as a flow network with source **a** and sink **f**, with the boldface weights regarded as capacities.

(i) Let f be the flow that channels 6 units along the path **a**–**d**–**b**–**c**–**e**–**f**. Find the residual network G_f, ω_f associated with this flow. Which path from source to sink in G_f, ω_f affords the greatest augmentation step? Indicate the resulting flow. Is it maximal?

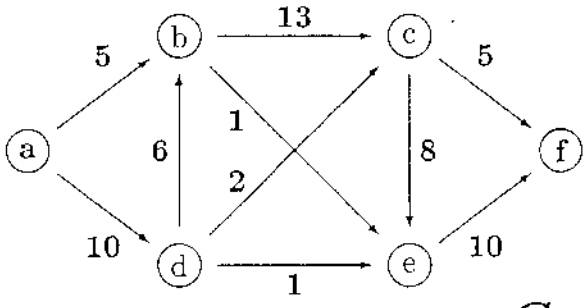
(ii) State the Max-Flow-Min-Cut theorem, with the definition of a cut and its capacity.

(iii) Apply the Max-Flow-Min-Cut theorem to the example in order to show that the maximal total flow from **a** to **f** cannot be more than 14. Find a flow realising a total flow of 14.

[9 marks]



G



G, ω

Question 3

(a) Consider the weighted undirected graph G, ω depicted below, with boldface edge weights. Briefly explain Kruskal's greedy strategy for finding a minimal spanning tree, and apply it to this sample input. List the edges in the order in which you select them, draw the resulting minimal spanning tree and determine its total weight. **[7 marks]**

(b) Give the definition of the complexity class NP in terms of polynomial verification. Apply this characterisation to argue that the following decision problems are in NP, clearly distinguishing the instances, the certificates and the verification problems involved:

(i) 3-COLOURABILITY

(ii) SPANNING-TREE:
given a weighted undirected graph G, ω together with a number $k \in \mathbb{N}$, decide whether G, ω has a spanning tree of total weight less than k.

[8 marks]

(c) Give the definition of NP-completeness, and discuss the role of NP-complete problems in the P versus NP issue.

[5 marks]

(d) Which of the following problems are NP-complete, which known to be in P?

(i) 2-COLOURABILITY

(ii) 3-CNF-SATISFIABILITY

(iii) DNF-SATISFIABILITY

What is the status of the SPANNING-TREE decision problem considered in part (b) (ii)?

[5 marks]

G, ω