Xi'an Jiaotong-LiverpoolUniversity 西交利物浦大學

PAPER CODE	EXAMINER	DEPARTMENT	TEL
CSE204		Computer Science and Software Engineering	

2nd SEMESTER 2019/20 FINAL EXAMINATIONS

Undergraduate – Year 3

COMPLEXITY OF ALGORITHMS

TIME ALLOWED: 2 Hours

INSTRUCTIONS TO CANDIDATES

1、 **Total marks available are 100. This accounts for 60% of the final mark.**

2、 **Answer all questions.**

3、 **The full marks for each question are indicated in round brackets at the end of the question.**

4、 **The answer should be written in English in the answer booklet. Answer sheets (with labeled pages and question numbers) should be scaned/snapshotted then convert to single Word/PDF file for submission.**

5、 **Relevant and clear steps should be included in the answers.**

6、 **Students must download/print the question paper, answer the questions, scan/snapshot their answers for submission within the 2-hour exam.**

Notes:

- To obtain full marks for each question, relevant and clear steps should be included in the answers.
- Partial marks may be awarded depending on the degree of completeness and clarity.

Question 1: Algorithm Analysis [30 marks]

a) Consider the following code fragment.

```
g(n){
    if n>0 do
        g(n-1)
        for j=n to 2*n do
            output Bingo
    }
```

Let $T(n)$ denote the number of times `Bingo' is printed as a function of n.

i. Express $T(n)$ as a summation.

[5 marks]

ii. Simplify the summation and give the running time using Big-Oh notation.

[7 marks]

iii. Rewrite the function $g(n)$ to a non-recursive version (using **pseudo-code**) and justify the disadvantage of recursive algorithms with one or two sentences.

[6 marks]

b) Given an AVL tree of height h, we wish to find out the element with a key k.

i. Complete the following function *findE* (using **pseudo-code**), which stops after finding the element with a key k of the given AVL tree.

[8 marks]

ii. Compute the time complexity of *findE* function by using Big-Oh notation.

[4 marks]

(Hint: *T.Left* and *T.Right* denote the left and right subtrees, respectively. T.element and T.key denote the element and key of the root of T. T.isExternal(key) denote whether a key is belonging to an external note.)

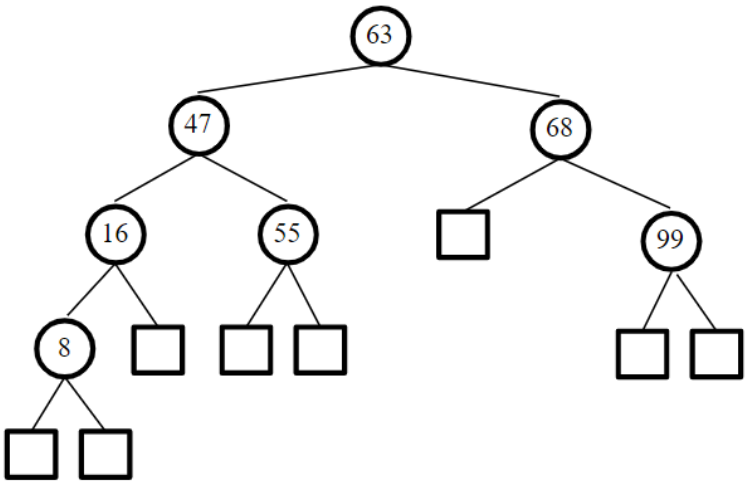
```
findE (T, k)
Input: an AVL tree T and an integer k
Output: the element with the key k.
1_____
2 _____
3_____
…
```

Question 2: Binary Search Trees and Heap [15marks]

a) Convert an array [8, 19, 56, 88, 13, 5, 3, 33, 66, 40] into a maximum heap H. Draw the initial array and the percolation steps of creating the maximum heap.

[5 marks]

b) Use the following graph for this problem.



i. Draw the AVL tree resulting from the insertion of an item with a key 32 into the given binary tree.

[4 marks]

ii. Draw the AVL tree from i. (with the key 32 inserted) after the elements 99 removed. What is the running time of a removal operation in an AVL tree (using Big-Oh notation)?

[6 marks]

Question 3: Efficient Algorithms and Graph [15marks]

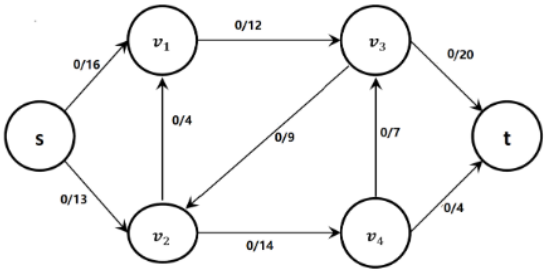
a) Let set S = {a, b, c, d, e} denote a set of objects with weights and benefits as given in the table below.

Item	a	b	c	d	e
Benefit	13	9	8	15	6
Weight	5	5	5	3	1

What is an optimal solution to the fractional Knapsack problem for S assuming that we have a sack that can hold objects with total weight 18?

[3 marks]

b) The figure below describes a flow assignment in a flow network. The notation a/b describes a units of flow in an edge of capacity b.



Execute the Ford-Fulkerson maximum flow algorithm on this network N. What is the value of maximum flow in the network N? Show the flow network that gives this maximum flow and draw the minimum cut.

[5 marks]

c) Let $G = (V, E)$ be a bipartite graph with vertex partition $V = L \cup R$, and let G' be its corresponding flow network. Give a good upper bound on the length of any augmenting path found in G' during the execution of FORD-FULKERSON. Write down the answer and the analysis.

[7 marks]

Question 4: Number Theory and Cryptography [15marks]

a) Evaluate the value of $17^{121} mod 143$ using Eulers theorem.

[3 marks]

b) Consider a cryptosystem wherein $n = 33$ and $e = 7$.

i. Verify that the pair (n, e) is a valid public key for an RSA cryptosystem.

[3 marks]

ii. Calculate the associated private key d.

[4 marks]

iii. Suppose we have a set of blocks encoded with the RSA algorithm and we don't have the private key. Assume $n = p \times q$, e is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with n. Does this help us in any way? Justify yourself with several sentences.

[5 marks]

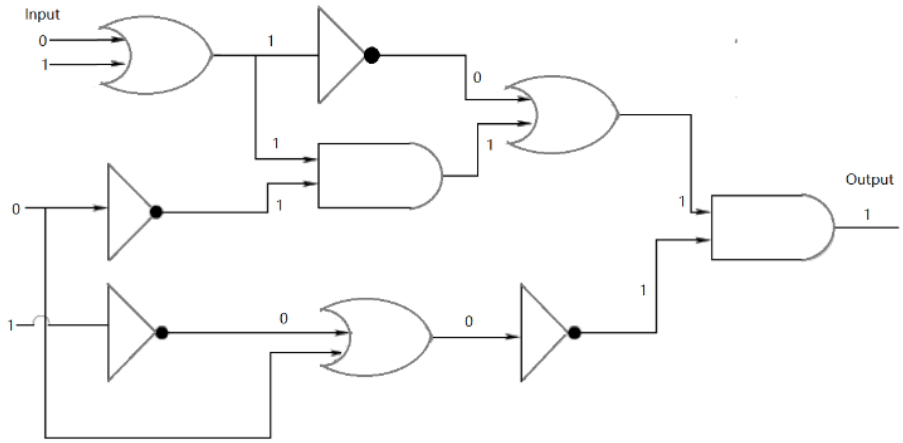
Question 5: NP-Completeness [25marks]

a) Let X be a decision problem. If we prove that X is in the class NP and give a poly-time reduction from X to 3-COLORING, we may conclude that X is NP-complete. Is it true or false? Briefly justify yourself with one or two sentences.

[4 marks]

b) A Boolean circuit is a directed acyclic graph for which each vertex v is labelled by: a literal or a constant 1 or 0 if v does not have an incoming edge, or one of the symbols $\wedge$ or $\vee$ if v has two incoming edges exactly, or $\neg$ if v has a unique incoming edge.

In theoretical computer science, the circuit satisfiability problem (also known as CIRCUIT-SAT, CircuitSAT, CSAT, etc.) is the decision problem of determining whether a given Boolean circuit has an assignment of its inputs that makes the output true.



We wish to show that CIRCUIT-SAT is reducible to the CNF-SAT problem. To this end, a Boolean circuit is associated with a set of clauses using the variables $x_1, \cdots, x_n$ that label the input vertices as well as variables y_v for the outputs of vertices v representing gates of the circuit. For example, the set of clauses satisfying the formula $x = y$ is $U = \{\bar{x} \vee y, x \vee \bar{y}\}$, since the formula $x = y$ is equivalent to $(\bar{x} \vee y) \wedge (x \vee \bar{y})$. This equivalence can be checked using a truth table.

i. Relying on the result from the given an example, give the sets U of clauses using the variables x, y, z in the following cases:

1. the clauses in U are satisfied iff $x = \bar{y}$. **[3 marks]**
2. the clauses in U are satisfied iff $x = y \wedge z$. **[3 marks]**
3. the clauses in U are satisfied iff $x = y \vee z$. **[3 marks]**

ii. State the CNF-SAT problem. **[4 marks]**

iii. Show that CIRCUIT-SAT is reducible to CNF-SAT. **[8 marks]**

END OF EXAM PAPER