UNIVERSITY OF
BIRMINGHAM

School of Computer Science

Postgraduate Papers

Main Summer Examinations 2020

Contents

5 credits

26942 Advanced Topics in Functional Programming (Extended)

(a) Add a predicate instead of the question mark so that the function *hd* which returns the head of a list can be safely implemented. Informally, the predicate should state the property that *the list is not empty*. Implement the function so that it type-checks in Agda.

$$hd : \{A : Set\} \to (xs : List\ A) \to ? \to A$$

[10 marks]

(b) Add a predicate instead of the question mark so that the function *nth* which returns the *n*-th element of a list (the head is at position 0) can be safely implemented. Informally, the predicate should state the property that *the length of the list xs is greater than n*. Implement the function so that it type-checks in Agda.

$$nth : \{A : Set\} \to (n : \mathbb{N}) \to (xs : List\ A) \to ? \to A$$

[10 marks]

(c) Add a predicate instead of the question mark so that the function *map2* which maps a function *f* over two lists can be safely implemented. Informally, the predicate should state the property that *the lists have the same length*. Implement the function so that it type-checks in Agda.

$$\begin{aligned} map_2 : \{A\ B\ C : Set\} &\to (f : A \to B \to C) \\ &\to (xs : List\ A) \to (ys : List\ B) \to ? \to List\ C \end{aligned}$$

[10 marks]

(d) Add a predicate instead of the question mark so that the function *strip* which removes the prefix *xs* from a function *ys* can be safely implemented. Informally, the predicate should state the property that *xs is a prefix of ys*. Implement the function so that it type-checks in Agda. **Hint:** You need to define *prefix* as a relation.

$$strip : \{A : Set\} \to (xs : List\ A) \to (ys : List\ A) \to ? \to List\ A$$

[10 marks]

6 credits

15255 Compilers and Languages (Extended)

(a) *Type Inference* **[20 marks]**

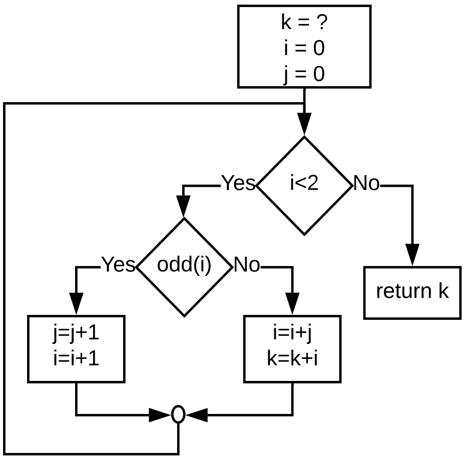
(i) Using the Hindley-Milner method derive the type of the following term in a programming language that has function types: $(\lambda f.\lambda x.f(f\ x))(\lambda y.y)$. Your solution must include the type derivation tree of the term, annotated with equations, the step-by-step solution of the system of equation using unification, the final inferred type and of variables f, x, y.

(ii) How would your answer change if the term was : $(\lambda f.\lambda x.f(f\ x))\ inc$, where inc is a function of type $inc : Integer \to Integer$.

(iii) Simple types are used in programming languages to prevent runtime crashes due to mismatches between functions and arguments (e.g. $(\lambda x.x+x)(\lambda x.x))$. Is a simple type system *complete*? This means, is it impossible to have a program which does not have a correct type but it would execute without any runtime problems?

(b) *Optimisations.* Consider the program below and its CFG. **[20 marks]**

```
i = 0
j = 0
while i < 2
    if odd(i) then
        j = j + 1
        i = i + 1
    else
        i = i + j
        k = k + i
return k
```



Note: For your convenience the diagram can be found at `https://www.lucidchart.com/invitations/accept/ccdd24de-f7bf-4f69-a343-95b67e102e76`.

(i) Perform constant folding and constant propagation on the CFG.

(ii) Put the resulting graph in single static assignment form.

Note: To create the answers you may use any software tool, or draw the diagrams on paper then photograph or scan. The answer must be embedded into a self-contained PDF; do not submit links!

8 credits

20008 Cryptography

(a) Consider the ith round of a Feistel network, used for example in the DES block cipher. It operates on a word (L_{i-1}, R_{i-1}), a round key K_i, and uses a Feistel function F. Write down formulas for L_i and R_i, in terms of L_{i-1}, R_{i-1}, F and K_i. **[6 marks]**

(b) Assume a two-round Feistel block cipher with an 8 bit key and a 16 bit block size. We write 8 bit words as a decimal number (from 0 to 255). The encryption key is $K = 80$. The round subkey derivation is defined as $K_i = (3 \times i) + K \pmod{256}$, where $1 \leq i \leq 2$. The Feistel function is $F(K_i, R_{i-1}) = 2 \times (K_i + R_{i-1}) \pmod{256}$. Encrypt the message $(L_0, R_0) = (40, 60)$. (Notation: as usual, + and × are addition and multiplication respectively.) **[7 marks]**

(c) A bank proposes to use 3DES in CBC mode to encrypt a set transactions. The transactions will be encrypted individually. Each transaction is specified in a data block consisting of 100 bits. The result of encrypting the 100 bits with 3DES in CBC mode is then transmitted. How many bits is needed to transmit each transaction? Justify your answer. (You can use the fact that the DES block size is 64 bits.) **[7 marks]**

(d) Let us explore the possibility of constructing secure hash functions using asymmetric key cryptography building blocks. Concretely we are going to use the RSA function as a candidate building block. Let's recall that the RSA function $F_{(N,e)} : \mathbf{Z}_N^\star \to \mathbf{Z}_N^\star$ on public key $PK = (N, e)$ is defined as $F_{(N,e)}(x) := x^e \bmod N$. Our candidate hash function $H : \mathbf{Z}_N^\star \to \mathbf{Z}_N^\star$ is defined as $H(m) := F_{(N,e)}(m)$ and only works on inputs of small and fixed size.

Is there any restriction on the choice of e given the modulus N? Is it possible to define the inverse of function of $F_{(N,e)}$? Justify your answers. **[6 marks]**

(e) Argue whether H is one-way and under which computational assumption. **[7 marks]**

(f) Argue whether H is collision-resistant and if yes, whether this property depends on any computational assumption. **[7 marks]**

23856 Evaluation Methods and Statistics (Online paper) 8 credits

You have been asked to design an experiment to investigate the effects of texting while driving a car.

(a) Would you conduct this experiment in a driving simulator or driving a car on public roads? In your answer, pay particular attention to ethical concerns, confounding variables, and ecological validity. **[12 marks]**

(b) Provide ONE Independent Variable for this experiment, and define Control and Experiment levels. Would you use a within- or between-subjects design? **[4 marks]**

(c) Provide ONE Dependent variable for this experiment, and explain how it can be measured. **[4 marks]**

You collect the following data from 20 participants in a repeated measures study.

Control	**Experimental**
0.7	0.9
1.2	1.5
0.8	0.8
0.5	0.7
0.9	1.2
0.8	0.8
0.4	0.9
0.6	1.6
0.9	1.2
1.2	0.9
0.8	1.3
0.9	0.8
0.7	1.2
1	0.9
0.7	1.2
0.7	1.6
1.3	1.4
1.1	1.5
0.8	1
1	1.6

(d) Apply a Shapiro-Wilk test on the full set of data. Explain why this result suggests that you can apply a parametric statistical test to the data and what the value of p means. **[5 marks]**

(e) Apply an appropriate test for the t-statistic on the data in the table. Assuming 95% confidence, what can you say about the result? **[9 marks]**

(f) Using an appropriate test for Cohen's d, comment on the effect size of the result calculated in (e). **[6 marks]**

8 credits

21923 Fundamentals: Databases

(a) This question relates to the Pagila database, the schema of which is avalable at https://canvas.bham.ac.uk/courses/38421/pages/pagila-schema. Ensure that your queries are well formatted.

(i) Write an SQL statement to find the city each customer is from. The result of your query should consist of two columns: The first consisting of each customer's "first_name" and the second column, the associated city. [5 marks]

(ii) Convert the SQL statement from the previous part of this question to a Relational Algebra expression. [5 marks]

(iii) Draw an expression tree for the Relational Algebra expression in the previous part of this question. [5 marks]

[15 marks]

(b) Draw an Entity Relationship Diagram (ERD) based on the Instance Diagram in Figure 1 below. Be sure to clearly show the cardinalities. **[10 marks]**

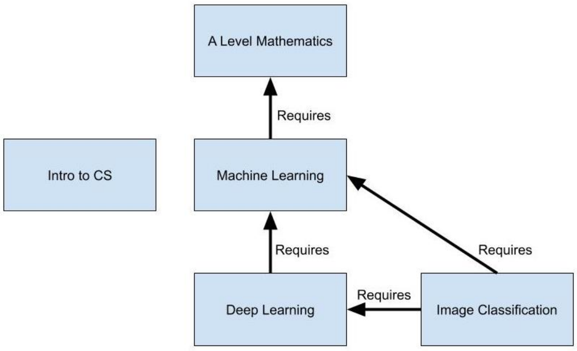


Figure 1: Instance Diagram of Modules and their prerequisites.

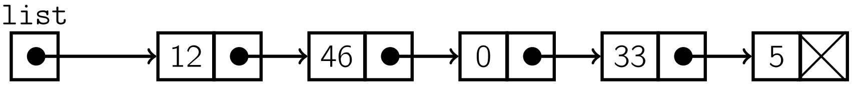
(c) Consider the relation R(A, B, C, D, E) and the functional dependencies $E \rightarrow D$ and $EB \rightarrow C$. Notice how R is in BCNF violation for these functional dependencies. Decompose the relation R using the BCNF algorithm **starting with the functional dependency** $E \rightarrow D$ and list the final set of relations. Be sure to clearly show all working. **[15 marks]**

8 credits

21921 Fundamentals: Data Structures

(a) In answering this question, treat the memory as a large integer array `Mem`. The expression `allocMemory(m)` allocates a block of `m` locations and returns its address. The instruction `freeMemory(n,m)` frees a block of `m` locations starting from `n`.

A linked list of numbers is stored with its head pointer at location `list`. For example:



A null pointer is represented by a location storing the constant END.

Write a program that deletes the first even number, if there is one, and throws an exception otherwise. **[8 marks]**

(b) Trace selection sort on the following example: $[5, 2, 7, 1, 4, 3]$. **[8 marks]**

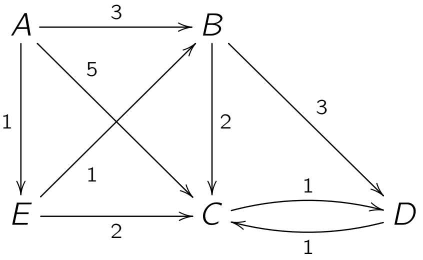
(c) Suppose we modify merge sort so that a portion of size $\leqslant 10$ is treated using selection sort. Show that the complexity is the same as that of unmodified merge sort. (You may make any reasonable assumption about n, and you may use the fact that merging is done in linear time.) **[8 marks]**

(d) A hash table with 5 slots, numbered from zero, employs double hashing, skipping rightwards. A key is a 5-digit number. The primary hash of a key is (2nd digit + 4th digit) mod 5. The secondary hash is (5th digit mod 4) + 1. Initially the hash table is empty, and then the following instructions are executed. For deletion, tombstones are used.

Insert 57131; Insert 28192; Insert 82375; Insert 80051; Delete 82375; Insert 65213.

What are the contents of the slots at the end of these instructions? **[8 marks]**

(e) Use Dijkstra's algorithm to compute the shortest path from A to all other nodes in the following graph.



[8 marks]

8 credits

21933 Fundamentals: Introduction to Computer Science

(a) In this question, numbers are represented using a binary system which uses 8-bits and negative numbers are represented using 2's complement. The first bit is used as the sign bit. Perform the following arithmetic operations. Clearly show all working. Your solution must be provided in the same system.

(i) 0001 1110 – 1110 1100

(ii) 0001 0011 – 0001 0110

[10 marks]

(b) Assume that you have access to a "magical" function *fastMaxSwap(inputArray, startIndex, endIndex)* which finds the maximum value between the indices "startIndex" and "endIndex" in an array "inputArray", and additionally swaps this element with that at "startIndex", all in constant time. Using this function, write a method (in Java or in Pseudocode) to sort an unsorted array "A" in descending order. Your method must take "A" and the length of the array "n" as parameters and return a sorted array. Your method must do this in $O(n)$ time and you are allowed to modify the original array "A". **[15 marks]**

(c) The Lazy Caterer's Sequence describes the maximum number of pieces of a pizza that can be made with a given number of straight cuts. For example, one cut can only result in two pieces, however, two cuts can result in four pieces and three cuts in seven pieces. The maximum number of pieces p that can be created with a given number of cuts n, where $n \geq 0$, is given by Equation 1:

$$p = \frac{n^2 + n + 2}{2} \tag{1}$$

Write a program in iJVM to calculate p for some given input n. Your program must print the value of p when n is greater than or equal to zero and print -1 otherwise.

NOTES:

- In addition to writing the program, ensure that you provide adequate comments to describe the working of your program.
- You might find the iJVM statements listed at https://canvas.bham.ac.uk/courses/38424/files/8231168?module_item_id=1370298 useful for this task.
- Assume that you also have access to a single iJVM statement "PRT" that will pop and print the top value on the iJVM stack.

[15 marks]

8 credits

20233 Intelligent Data Analysis (Extended)

(a) **Text Retrieval:** A corpus consists of just six short texts. After text pre-processing, stop word removal and stemming these texts are $D_1, D_2, D_3, D_4, D_5, D_6$, given by:

D_1: *priority health educate system*
D_3: *child parent educate child child home*
D_5: *health system educate system uk need*
D_2: *uk health educate minister*
D_4: *home school challenge parent*
D_6: *health system priority*

(i) Calculate the Inverse Document Frequency for each word in the vocabulary. Order the vocabulary alphabetically as follows: *challenge, child, educate, health, home, need, parent, priority, school, system, uk.* **[8 marks]**

(ii) Let *Q* be the query *hospital health system*. Calculate the TFI-IDF similarities between *Q* and the documents D_1, D_2, D_3, D_4, D_5 and D_6. **[10 marks]**

(b) **k-means clustering:** Recall that if $u = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$ and $v = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$ then the d_∞ distance $d_\infty(u, v)$ between u and v is given by $d_\infty(u, v) = \max(|u_1 - v_1|, |u_2 - v_2|)$.

Let $\{x_1, x_2, x_3, x_4, x_5\}$ be a set of data points and $\{c_1, c_2\}$ a set of centroids, where:

$$x_1 = \begin{bmatrix} 4 \\ 2 \end{bmatrix}, \; x_2 = \begin{bmatrix} -1 \\ 2 \end{bmatrix}, \; x_3 = \begin{bmatrix} -2 \\ 1 \end{bmatrix}, \; x_4 = \begin{bmatrix} 3 \\ 1 \end{bmatrix}, \; x_5 = \begin{bmatrix} -2 \\ 2 \end{bmatrix}, \; c_1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, c_2 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

(i) Calculate the new values $\{\bar{c}_1, \bar{c}_2\}$ of $\{c_1, c_2\}$ after one iteration of k-means clustering. Use the d_∞ distance measure and show your calculations. **[8 marks]**

(c) **Self-Organizing Map (SOM):** The SOM update rule for a set of centroids $\{c^1, \cdots, c^K\}$ in a topographic map, given the data point x is

$$c^j_{new} = c^j_{old} + h[i(x); j] \times \eta \times (x - c^j_{old}) \tag{1}$$

where $i(x)$ is the index of the closest centroid to x, $\eta = 0.5$, $h[j, k] = e^{\frac{-(j-k)^2}{\sigma}}$ and $\sigma = 10$. Suppose that centroids c_1, c_2, c_3 and data point x are given by

$$c_1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \; c_2 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \; c_3 = \begin{bmatrix} 3 \\ 2 \end{bmatrix} \text{ and } x = \begin{bmatrix} 4 \\ 2 \end{bmatrix}$$

(i) Calculate the new values of c_1, c_2 and c_3 after one application of the SOM update rule with data point x. Use the d_∞ distance measure and show all of your calculations. **[8 marks]**

(ii) What form does the SOM update rule (equation (1)) take as $\sigma \to 0$? **[6 marks]**

8 credits

15267 Intelligent Robotics (Extended)

(a) You are developing software for a mobile robot searching for a robotics book in an office with three rooms. The location of the robot and the book are not known with certainty. The robot's move from a room to another succeeds with probability 0.85. The robot's can move to any particular room, test if it is in a particular room, test if the robotics book is in each room, and confirm the book's presence in a room. The robot's field of view is limited to the room it is in. If the book exists in the room the robot is exploring, it is found 90% of the time; if the book is not in a room, it is still found 15% of the time.

(i) What mathematical formulation is suitable and why? **[2 marks]**

(ii) Specify and describe the components of the chosen mathematical formulation for the task of estimating the location of the robot and the location of the book, using the *Cassandra* format. Specify any related probability functions for at least one sensing action related to the robot, one sensing action related to the book, one movement action, and one terminal action. **[14 marks]**

(iii) State key challenges in using the chosen mathematical formulation for complex robotics problems. Describe some potential solution to these challenges. **[4 marks]**

(b) You are writing software for a robot navigating from any cell to the goal in a 3×3 grid. Grid cells are numbered from "0" in the top left, scanning each row from left to right, until the bottom right. Cells "0", "2", and "7" are danger zones and cell "5" is the goal. The robot can move up, down, left, right, or stay in place. Any attempt to move out of the grid, or to stay in place, causes no change. All other move actions succeed with probability 0.85, and the robot's location is known after executing an action. Executing a movement action incurs a cost, reaching the goal is a good outcome, and entering a danger zone is a very bad outcome.

(i) Choose a suitable mathematical formulation for the task and justify the choice. Describe components of this formulation in the *Cassandra* format, including probabilistic functions (e.g., state transition) for at least two actions that change the state and one action that does not change the state. **[14 marks]**

(ii) Describe the formulation of the task as a reinforcement learning problem, and state the differences with the formulation used in the previous question. **[2 marks]**

(iii) Also, describe the differences in formulation if the robot's location is not known with certainty after executing an action. **[4 marks]**

8 credits

32235 LM Advanced Aspects of Nature-Inspired Search and Optimisation

(a) An explorer found a treasure chest in which there are n valuable items, each with a weight w_i and a value v_i, where $i = 1, \cdots, n$. However, the explorer only has one backpack with a maximum weight capacity W. He needs to decide which items to put into the backpack so that total value is as large as possible.

(i) Formulate the decision making problem as a constrained optimisation problem. **[6 marks]**

(ii) Design an evolutionary algorithm for solving the constrained optimisation problem, justifying all your design decisions.

a) Describe a suitable chromosome representation of an individual. **[2 marks]**

b) Based on your choice of representation, design evolutionary operators. Use examples to show how they work. **[4 marks]**

c) Design a selection scheme. **[2 marks]**

d) We will use a method called the feasibility rule to handle constraints. Explain what is the feasibility rule. Discuss its main drawback and how to address this drawback. **[6 marks]**

(b) (i) How does single-objective optimisation differ from multi-objective optimisation? **[8 marks]**

(ii) The figure below shows the values of 9 search points according to objective function f_1 and objective function f_2. Which solutions are non-dominated

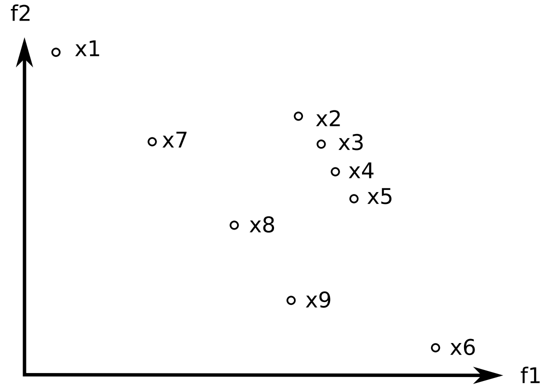
a) if f_1 should be minimised and f_2 should be minimised?

b) if f_1 should be minimised and f_2 should be maximised?

c) if f_1 should be maximised and f_2 should be maximised?

[6 marks]

(iii) Assume that both objectives are to be maximised, but you can only select four search points. Which four search points would you select? Justify your answer. **[6 marks]**



8 credits

30017 LM Advanced Cryptography

Recall the discrete logarithm problem, computational Diffie-Hellman problem and decisional Diffie-Hellman problem for a cyclic group G and generator g. In this question we will consider "implementation errors" in the use of ElGamal encryption scheme.

(a) Show that the decisional Diffie-Hellman problem is easy when the group order is even. (Hint: if the order is $n = 2m$, consider the possible values of $(g^x)^m$.) **[12 marks]**

(b) Consider the pseudo-code to generate a group G and a generator g to be used for ElGamal encryption given in Figures 1 and 2, using finite fields and elliptic curves respectively. Show that the resulting ElGamal encryption implementations are insecure in the IND-CPA sense. **[12 marks]**

```
(i) Choose a random prime $p$ with 2000 bits
(ii) Let $K := \mathbf{F}_p$ be the finite field with $p$ elements
(iii) Let $G := K^*$ be the multiplicative group of $K$
(iv) Let $g$ be a generator in $G$
```

Figure 1: Parameter generation algorithm for ElGamal over finite fields

```
(i) Choose a random prime $p$ with 256 bits
(ii) Let $K := \mathbf{F}_p$ be the finite field with $p$ elements
(iii) Let $a, b$ be random elements in $K$
(iv) Let $E$ be the elliptic curve defined by the equation $y^2 = x^3 + ax + b$
(v) Let $P$ be a random point over $E$
(vi) Let $g := P$ and let $G$ be the cyclic group generated by $P$
```

Figure 2: Parameter generation algorithm for ElGamal over elliptic curves

(c) Give a scenario where an IND-CPA attack like the one developed in Part (b) is a serious threat. (Hint: consider an e-voting scenario.) **[8 marks]**

(d) Can the issues in the parameter generation routines in Figures 1 and 2 be used to accelerate key recovery attacks and decryption of arbitrary ElGamal ciphertexts? Justify your answer. **[8 marks]**

8 credits

25020 LM Advanced Human-Computer Interation

You are asked to lead a design project for Acme Interactive Ltd. to create a new interactive feedback tool for use in lecture theatres. They are undecided on what form this should take, but want at least two options, one of which is to be an app-based approach that runs on a smartphone, and one which takes a different form not on a phone - for example, based around Internet of Things technologies.

They are used to using a conventional user-centered design (UCD) approach, but you favour the double-diamond model.

(a) Describe the benefits of the double diamond model. **[2 marks]**

(b) Describe in detail how you can map the different elements of the user-centered model into the different parts of the double diamond approach. **[6 marks]**

They ask you to prepare a proposal for them, in which they want you to provide examples of how the double diamond process would work in practice. You therefore decide to apply the double diamond design approach to ideate and refine solutions for their project, to demonstrate both your creativity and mastery of the approaches. You therefore must come up with (at least) two possible solutions (one an app-based approach, one that is not an app) as a result of applying the techniques.

(c) For each stage in the double diamond process, select the most appropriate activity for this client's project and justify it. (2 marks per stage) **[8 marks]**

(d) Again for each stage, give a detailed explanation of your chosen activity applied to the scenario, including the outputs you would expect, so that the client can see how the process shapes the evolution of the product. You should simulate any data that you would expect to collect if you were to actually win the contract, though your data must be reasonable and appropriate. At the end you should give a clear description of your two options, and compare and contrast them in a table format.

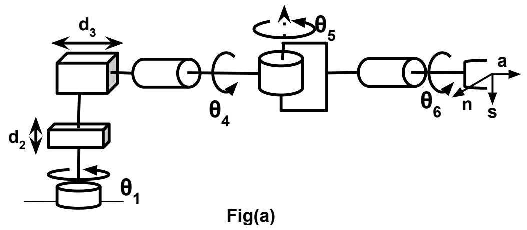
(6 marks per stage.) **[24 marks]**

16 credits

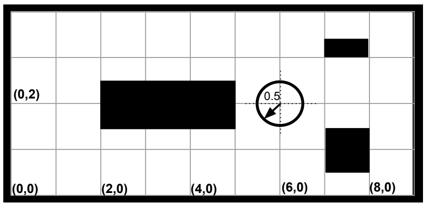
25021 LM Advanced Robotics

(a) For the robot manipulator in Fig(a): (i) Assign and draw proper frames for each link and the base. (ii) Derive the table of Denavit-Hartenberg (DH) parameters. **[12 marks]**

(b) A disk-shaped robot of radius $0.5m$, equipped with a manipulator, operates in a warehouse whose 2-D map is in Fig(b) with obstacles shaded black. You are to design a planner based on a motion model for multiple tasks. (i) Which sampling-based motion planner would you choose and why? (ii) Under which key assumption will your chosen method *not* work? (iii) Provide a detailed example of the result of this motion planner in the form of a graph. Explain its nodes and edges and how they are obtained. **[8 marks]**

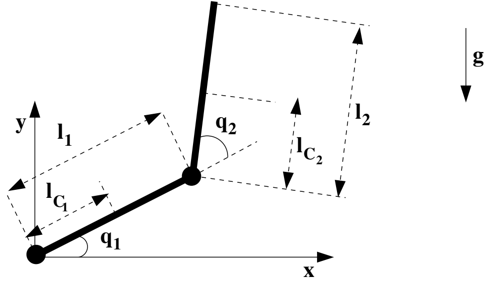


Fig(a)



Fig(b)

(c) Derive the equations of motion for the planar robot arm (below) after including a spring (stiffness k_1) from $(d, 0)$ to COM of link-1, and a spring (stiffness k_2) from $(0, 0)$ to COM of link-2. Describe changes introduced by the addition of springs. Describe the changes if the arm had a hypothetical third rotational link. **[10 marks]**



(d) Describe the choice of control space (task, joint) and controller (e.g., force, impedance, hybrid) for the following tasks with proper reasoning and equations (as appropriate). Assume that pose and velocity of the robot's joints are known.

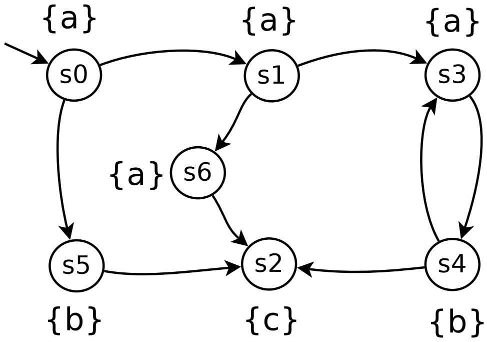
(i) A manipulator's end-effector has to follow a predefined pattern while immersed in a liquid. Consider three situations: 1) viscosity of liquid is fixed and known; 2) viscosity is changing continuously; and 3) mathematical model (f) of changing viscosity is known. **[5 marks]**

(ii) A manipulator's end-effector has to polish a car's hood (with constant friction) along a desired trajectory, while remaining normal to the surface and maintaining constant normal force. Consider: 1) perfect vision and force-torque (FT) sensors; 2) perfect FT sensor; and 3) noisy FT sensor. **[5 marks]**

8 credits

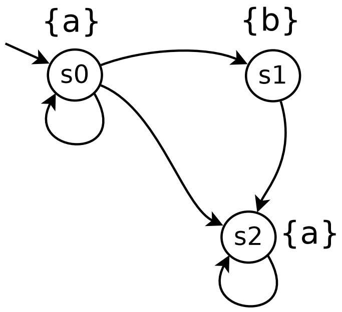
28206 LM Computer-Aided Verification (extended)

(a) Illustrate the application of the CTL model checking algorithm to determine whether the LTS below satisfies the CTL formula $\phi = \exists((a \wedge \neg b) \bigcup c) \wedge \exists \bigcirc \neg \exists \bigcirc c$ **[10 marks]**



(b) An LTL formula ψ is said to be equivalent to a CTL formula ϕ if both formulas are satisfied by the same LTSs. Provide a detailed explanation of why the LTL formula $\Diamond\Box a$ is not equivalent to the CTL formula $\forall\Diamond\forall\Box a$, where a is an atomic proposition. Your explanation should include two distinct counterexamples (2 LTSs). Are your counterexamples also counterexamples for the equivalence of $\Box\Diamond a$ and $\forall\Box\forall\Diamond a$? Justify your answer. **[10 marks]**

(c) Let $\psi_1 = \Box(a \vee b)$ and $\psi_2 = \Box\Diamond a$. Illustrate the LTL model checking algorithm for both ψ_1 and ψ_2 on the following LTS:



[10 marks]

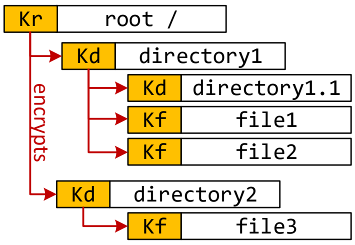
(d) Explain how one checks that the language accepted by an NBA is non-empty. Describe the time complexity of the procedure you just explained. Explain how LTL model checking relates to this non-emptiness problem. Compare the time complexity of that non-emptiness problem with the time complexity of LTL model checking. Explain what the main scalability issue of model checking is due to. **[10 marks]**

10 credits

28214 LM Designing Secure Systems

(a) A file-based encryption scheme is set up as follows:

Files in the system have keys Kf associated to them which are used to encrypt their contents and meta-data. Similarly, directories are associated with keys Kd which are used to encrypt the keys Kf belonging to the files inside the directory, and keys Kd belonging to subdirectories, as shown in the figure to the right. Finally, all the 1st level keys Kd are encrypted with the root key Kr.



(i) What is the easiest way of re-encrypting the filesystem and why? **[6 marks]**

(ii) Give a valid function that can be used to protect the whole filesystem using a password. Explain explain its inputs and outputs and their purpose in the function. **[7 marks]**

(iii) Using a TEE, and without decrypting any directories, propose a way that allows files in `directory1` to be accessible without a password, and for files in `directory2` to be accessible only after a password was used. **[7 marks]**

(b) (i) What are the smallest changes that you can make to the Needham Schroeder Public Key Protocol protocol to give its users forward secrecy? Write the improved version of the protocol in Alice and Bob notation, describe how the protocol works, what guarantees it gives you, and why it gives you forward secrecy. **[6 marks]**

(ii) Now assume we have Alice, Bob and Charlie, all of which know each other's public keys. How can the Needham Schroeder Public Key Protocol be extended to authenticate Alice, Bob and Charlie to each other? If the protocol finishes then each participant must be able to conclude that the other two did take part in the protocol even if one of the participants deviates from the protocol and acts maliciously. Describe how your protocol works, state all of the security goals, and how your protocol achieves them. **[8 marks]**

(iii) For the TLS protocol, what would be the effect on the confidentiality and authentication properties of removing the client nonce N_C from this protocol, what would it allow an attacker to do? **[3 marks]**

(iv) For the TLS protocol, what would be the effect on the confidentiality and authentication properties of removing the server nonce N_S from this protocol, what would it allow an attacker to do? **[3 marks]**

16 credits

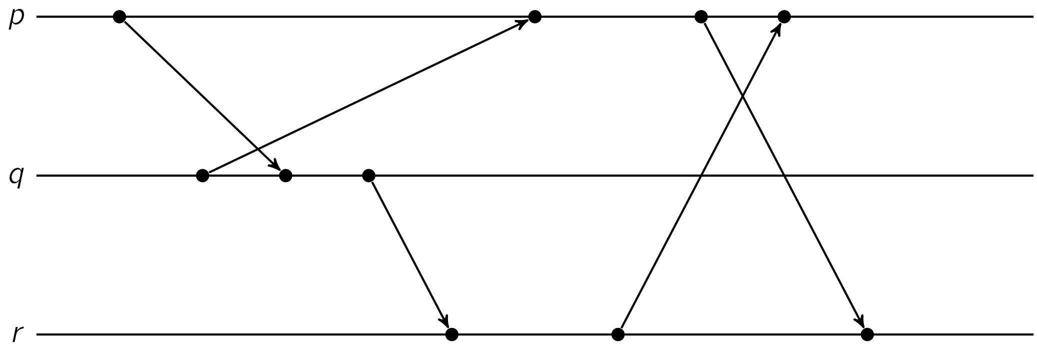
32230 LM Distributed and Parallel Computing (EXTENDED)

(a) What are the advantages of the concept of **Linearizabilty** over that of **Sequential Consistency** in reasoning about concurrent object-oriented systems? In your answer, include an example history of a First-In-First-Out (FIFO) queue which is sequentially consistent but not linearizable and explain why it is sequentially consistent but not linearizable. **[10 marks]**

(b) In the context of a CUDA kernel function, explain the two problems of non-coalesced global memory accesses and shared memory bank conflicts. Give examples of typical scenarios and/or code that has these problems and how they should be modified to fix them. **[10 marks]**

(c) Explain what a bitonic sequence is and then explain the idea behind how a bank of comparators can be used as a step in bitonic sort. How many pair-wise comparators would you need to sort an array of 4 inputs? Draw a diagram of the arrangment. **[10 marks]**

(d) (i) Consider the following space-time diagram of a distributed execution on 3 processes:



If the events and messages shown are the only only ones in the system, say what the values of both a Lamport and a Vector clock would be for the **final** events in each of the processes *p*, *q* and *r*.

(ii) Explain why the Chandy-Lamport global snapshot algorithm fails on a non-FIFO network.

[10 marks]

30016 LM Forensics and Malware Analysis

(a) You disassemble the following code (left) and a function called within that code (right):

```
c1:xor  EBX, EBX
  ;load effective address to EBX       f1:weird_fun         ;function name
c2:lea  EBX, loc_4005EA                 f2: push EAX         ;save EAX to stack
c3:call weird_fun                       f3: mov EAX, EBX     ;copy EBX to EAX
c4:lret_400600:leave                    f4: mov [ESP+4], EAX ;place EBX on stack
c5:            retn                     f5: pop EAX          ;restore EAX
c6:loc_4005EA: call do_bad_stuff        f6: ret              ;return
c7:            lea  EBX, lret_400600
c8:            call weird_fun
```

(i) Assuming all the lines in the code above are executed, give the execution sequence starting from c1. **[6 marks]**

(ii) What code obfuscation technique is used in the code above? Assuming that the stack is used to indicate the return address from a function, explain what the code in *weird_fun* function does. **[7 marks]**

(iii) Can the code in the *weird_fun* function be shortened/optimised? If yes please write the new code, clearly indicating the lines you replace. **[7 marks]**

(b) The UK police seized a Windows 7 computer of a suspected criminal who is absconding.

(i) Assume that the suspect created an encrypted container using a disk-encryption tool called ToyCrypt. You want to see the contents of the container. Would memory forensics be useful if the suspect had hibernated the computer after dismounting the encrypted container? Briefly explain your answer. **[3 marks]**

(ii) From now on, assume that the computer was fully powered-off. You are aware that ToyCrypt derives a 16-byte AES encryption key from a given 5-digit password by applying only one round of SHA256. However, the 5-digit password is not available. Describe the steps that you will follow to see the contents of the encrypted container? Briefly explain your answer. **[5 marks]**

(iii) You believe that the suspect had sent and received messages over Skype as Skype is present in the seized computer. However, you do not have the login credentials of the suspect. Describe how you could see the Skype messages. **[4 marks]**

(iv) After having discussions with the family members of the suspect, the UK police think that the suspect had been receiving online training to perform harmful activities from some unknown website(s) for about one year. Describe way(s) to get the list of websites that the suspect had visited in the past one year. Briefly explain your answers. **[8 marks]**

5 credits

28217 LM Hardware and Embedded Systems Security

(a) You are given an implementation of AES. The developer has provided two alternative implementations for the `xtime` function used in `MixColumns`:

```
uint8_t xtime_variant_1(uint8_t x) {
   uint8_t r = x << 1;
   if(x & 0x80) {
      r = r ^ 0x1B;
   }
   return r;
}

uint8_t xtime_variant_2(uint8_t x) {
   return ( (x << 1) ^ ( ( (x >> 7) & 0x1) * 0x1B ) );
}
```

Explain why variant 1 and variant 2 are equivalent in terms of the implemented functionality. **[5 marks]**

(b) For each variant in task (a), indicate if it would make the whole AES implementation vulnerable to i) a timing side-channel attack and ii) a Simple Power Analysis (SPA) attack with a small number of traces. Explain your answer in your own words and mention if you made any specific assumptions. **[15 marks]**

(c) Someone proposes to use variant 2 from task (a) and claims that this choice would also prevent Differential Power Analysis (DPA). Is this true? Explain your answer. **[5 marks]**

(d) You design a smartcard that computes an RSA signature $y = x^d \bmod n$. The public exponent is short with $e = 2^{16} - 1$. The signed value x is computed from the actual (attacker-controlled) input x' through a padding scheme as $x = f(x', r)$, where r is a random number that changes with every invocation. The smartcard outputs the signature y and the random value r. The padding function $f()$ is also publicly known. Someone argues that because the padding is randomised, Simple Power Analysis (SPA) of the exponentiation algorithm cannot recover the private exponent d. Is this true? Explain your answer. **[10 marks]**

(e) Assume that the signature in (d) is computed using the Chinese Remainder Theorem (CRT) optimization. To protect against fault injection, someone proposes to run the signature algorithm from (d) twice (on x after the padding has been applied) and compare the results before outputting it. Under which circumstances is this an *effective* countermeasure? Is there a more *efficient* way of achieving a similar level of protection? **[5 marks]**

10 credits

30512 LM Human Computer Interaction Theory and Practice

You are asked to lead a design project for Acme Interactive Ltd. to create a new interactive feedback tool for use in lecture theatres. They are undecided on what form this should take, but want at least two options, one of which is to be an app-based approach that runs on a smartphone, and one which takes a different form not on a phone - for example, based around Internet of Things technologies.

They are used to using a conventional user-centered design (UCD) approach, but you favour the double-diamond model.

(a) Describe the benefits of the double diamond model. **[2 marks]**

(b) Describe in detail how you can map the different elements of the user-centered model into the different parts of the double diamond approach. **[6 marks]**

They ask you to prepare a proposal for them, in which they want you to provide examples of how the double diamond process would work in practice. You therefore decide to apply the double diamond design approach to ideate and refine solutions for their project, to demonstrate both your creativity and mastery of the approaches. You therefore must come up with (at least) two possible solutions (one an app-based approach, one that is not an app) as a result of applying the techniques.

(c) For each stage in the double diamond process, select the most appropriate activity for this client's project and justify it. (2 marks per stage) **[8 marks]**

(d) Again for each stage, give a detailed explanation of your chosen activity applied to the scenario, including the outputs you would expect, so that the client can see how the process shapes the evolution of the product. You should simulate any data that you would expect to collect if you were to actually win the contract, though your data must be reasonable and appropriate. At the end you should give a clear description of your two options, and compare and contrast them in a table format.

(6 marks per stage.) **[24 marks]**

14 credits

25689 LM Mobile & Ubiquitous Computing (Extended)

You have been put in charge of implementing an Android app that will help support a huge festival after the COVID-19 vaccine has been successfully rolled-out. The organisers expect 200,000 people per day to attend. There will be dozens of stages and hundreds of stalls crammed into the venue. Users of the app will be able to add friends to a list that lets them keep track of where their friends are. The app also provides festival-specific navigation to help people find their way. The app lets festival-goers see the last five places other festival goers within 10m of them have visited. To preserve privacy with this functionality, festival goers who are not friends see made-up names and a randomly-generated avatar.

(a) Android has three built-in location providers: `NETWORK_PROVIDER`, `PASSIVE_PROVIDER` and `GPS_PROVIDER`. Describe one advantage and one limitation of each of these providers. Which of these providers would be most suitable for obtaining location in this app, given the features described? Justify your answer. **[10 marks]**.

(b) Explain how absolute, symbolic and relative representations of location could be used to best effect in this app. **[10 marks]**

(c) Describe one 'seam' that could appear in this system. How could you could *represent* this 'seam' most effectively to users in this context? Explain your reasoning. **[10 marks]**

(d) Describe two privacy concerns that people could have about this app. Describe possible mitigations for each concern, explaining why the mitigations would help. **[10 marks]**

8 credits

29637 LM Network Security (Extended)

The first part of this question is about *rogue access points*. This refers to the idea that an attacker who controls a wireless access point, and can persuade users to connect their devices to it, is able to read, modify, inject and delete packets between the user and the systems they are accessing.

(a) Explain how a rogue access point can be used to capture traffic. **[4 marks]**

(b) In reality, there have been very documented actual cases where user data has been compromised. Why do you think this might be? Explain how standard features in web browsers work to reduce the risk of an attacker who controls the network being able to access user data. **[8 marks]**

(c) There are new technologies which reduce the impact of rogue access points. One of these is Host Strict Transport Security (HSTS), and another is the increasing use of Virtual Private Networks (VPNs). Explain how these technologies reduce the risks from a rogue access point. **[6 marks]**

(d) Users often ask how they can improve their security. Assume you are the operator of a bank website which has deployed HSTS. Write a short note for users explaining how to get the best protection from this new facility. **[4 marks]**

For the remainder of the question, assume you are the newly-appointed security lead for a company which offers financial services to private individuals. Your website has been developed over many years by a large number of different people and sub-contractors. Your website allows customers to conduct high-value transactions. The website stores all of the customer data in an SQL database.

(e) Your management are concerned that they have no clear idea of the security of the website, and are worried that an audit by regulators could be difficult. Write a memo for your CEO which explains the measures you could put in place to improve the security of the website, **without** needing to analyse or re-engineer the website code itself. **[10 marks]**

(f) Your management are also worried about the security of data which is transmitted from your website to a backup facility a hundred kilometres away. Describe how you would secure data transfer over the Internet, between two data centres. You should consider both access to the machines that are sending and receiving data, and also the security of the data in transit. **[8 marks]**

16 credits

26950 LM Networks (Extended)

(a) In order to be useful, it is essential that networks offer useful applications. HTTP, over TCP, is by far the most used protocol in the application layer, and it is used to convey a wide variety of services, APIs and products.

The failure of HTTP servers has substantial impact on users and therefore it is important to serve content from multiple systems.

Describe three mechanisms that could be used to serve identical content from multiple servers. You should consider the geographic limitations of each solution, and the effect it has on complex services involving databases. **[12 marks]**

(b) When planning a service which is offered world-wide, some users of an HTTP service will inevitably be far away, both in terms of distance and in terms of network hops, from the servers. HTTP sessions tend to consist of the transfer of large numbers of relatively small objects.

Explain three problems for the performance of HTTP over TCP that are caused as the delay in a network increases, and explain two mechanisms that have been added to TCP or HTTP in order to improve performance. Explain which of the problems you have listed are solved by these mechanisms. Justify your answer. **[12 marks]**

(c) Many core Internet protocols, including SNMP and DNS, were originally delivered over UDP. Increasingly TCP is seen as a better alternative, and newer protocols usually use TCP or another, similar, reliable transport service.

Explain why UDP was initially preferred for services like SNMP and DNS. Explain the benefits and problems of migrating these services to use TCP, with particular reference to networks which have a high delay. Under what circumstances would UDP still be preferred? **[8 marks]**

(d) Two major applications on the Internet today are video conferencing and the streaming of pre-recorded video content. Each of these applications has a different sensitivity to network conditions, including *latency*, *reliability* and *available bandwidth*. Explain the different requirements of video conferences and film streaming, and how they are affected by each of these aspects of network performance. Given a network which has poor reliability, describe the different techniques you would consider to give users the best video conferencing experience and the best film streaming experience. **[8 marks]**

16 credits

32212 LM Neural Computation (Extended)

Q1. We have observed n data points $\left\{(\mathbf{x}^{(1)}, y^{(1)}), \ldots, (\mathbf{x}^{(n)}, y^{(n)})\right\}$, where for each $i \in \{1, \ldots, n\}$, $\mathbf{x}^{(i)} \in \mathbb{R}^m$ represents the i-th observed "input vector" (feature vector), and $y^{(i)} \in \mathbb{R}$ represents the i-th observed "output" value. We need to predict the output value, given a new input vector.

(a) Is the problem above an unsupervised learning problem? **[2 marks]**

(b) To predict output values from new input vectors, we define a machine learning model of the form $f_{\mathrm{w}}(\mathbf{x}) = \mathbf{w} \cdot \mathbf{x} + N$, where $\mathbf{w} = (w_1, \ldots, w_m) \in \mathbb{R}^m$ are the model parameters, and N is a random variable sampled from some fixed distribution. To train this model, we use a mean square error (MSE) loss function combined with an L_2-regularisation term with parameter $\alpha > 0$:

$$J(\mathbf{w}) := \frac{1}{n} \sum_{j=1}^{n} \left(\mathbf{w} \cdot \mathbf{x}^{(j)} - y^{(j)}\right)^2 + \alpha \|\mathbf{w}\|_2. \tag{1}$$

What assumption can you make about the random variable N which justifies the use of the mean square error term in the loss function J? **[4 marks]**

(c) Compute ∇J with respect to the model parameters $\mathbf{w}$, and explain how this quantity can be used to set the model parameters. **[8 marks]**

(d) We use gradient descent to optimise the loss function J in Eq. (1) with respect to the model parameters $\mathbf{w}$. Assume that after some iterations of the gradient descent algorithm, the model parameters $\mathbf{w}$ satisfy for some small $\delta > 0$

$$y^{(j)} - \mathbf{w} \cdot \mathbf{x}^{(j)} = \begin{cases} \delta & \text{if } j = 1, \textit{and} \\ 0 & \text{if } j \neq 1. \end{cases}$$

We now make one more step of the gradient descent algorithm. For what values of α will the model parameter w_1 increase? (Assume that $x_i^{(1)} > 0$ and $w_i > 0$.) **[6 marks]**

Q2. (a) Explain why "dropout" is used in neural computation. **[5 marks]**

(b) In which of the following phases is "dropout" used? Justify your answer.

i. during training of the neural network

ii. during testing of the neural network

iii. when using the neural network in an application, such as for medical diagnosis

[5 marks]

(c) During lectures, we described dropout where all activation units in the network shared the same dropout rate. How could the dropout activation units be redefined so that each unit has its own, possibly unique, dropout rate? **[10 marks]**

14 credits

25024 LM Robot Vision

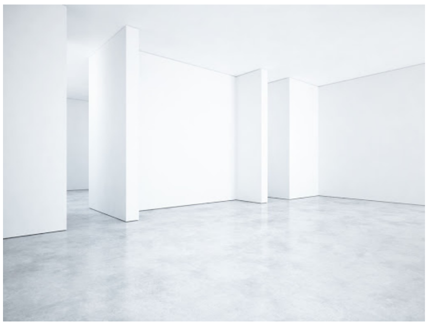
(a) i) Describe what is "Kernel separability" with an $m \times n$ kernel, and ii) explain why it is important for image filtering (applying $m \times n$ kernel) with detailed analysis. iii) Perform the kernel separation on the Sobel kernel:

-1	0	1
-2	0	2
-1	0	1

[8 marks]

(b) You visit the University of Birmingham campus and take a photo of Old Joe (Joseph Chamberlain Memorial Clock Tower) which is 110m high (denoted as Y). You use a camera with a focal length (f_m) of 15mm to take a picture of Old Joe. The actual size of the camera CCD (h_{CCD}) is 6.4mm, and the number of vertical pixels is 640 pixels (h_{img}). In the picture taken in focused, Old Joe was 550 pixels high (y_{img}). At this time, how many meters (Z) are you from the Old Joe (clock tower)? Show your working. **[8 marks]**

(c) Imagine a mobile robot exploring the inside of a new building with all walls, ceiling and floor painted white (as shown below). What problems can the robot face if it uses binocular 3D cameras in this environment? Please suggest another camera type to use in this environment, and describe how it works and why it is appropriate for this environment. **[8 marks]**



(d) What is end-to-end deep learning? When is using end-to-end deep learning a good choice, and when is it not? **[8 marks]**

(e) Given that a convolution neural network has two convolution layers (the first convolution layer is composed of ten 5x5x3 convolution filters with stride 3 and no pooling layers, and the second convolution layer is composed of twenty 3x3x10 convolution filters with stride 1) and an input image size of 65x65x3, (i) what is the total number of parameters in this network? and (ii) what is the dimension of the output after the convolutions? Show your working. **[8 marks]**

8 credits

28213 LM Secure System Management

You are the newly arrived Chief Security Officer for a small financial technology company which offers regulated financial services to customers. The company employs young, well-qualified developers who are chosen for their ability in innovate and produce exciting and compelling products.

There are active debates within its developer community about Bring Your Own Device (BYOD) policies. Many of the developers prefer to use their own machines, and the development manager is happy to save the cost and complexity of buying and managing laptops for developers, particularly for temporary and part-time developers. You believe that BYOD is already happening without any policy or management, and you wish to bring this risk under control.

Write a report for the Head of Development, which will be copied to the CEO, which summarises the issues. It should describe the advantages of having a BYOD policy to give clear rules on what can or cannot be used, and recommend what that policy should be. Remember, complete prohibition is also a policy. It should also include:

- discussion of at least three *risks* which arise from people using their own devices; **[10 marks]**
- discussion of at least three *controls* which can mitigate some or all of these risks; **[10 marks]**
- a residual risk statement for BYOD with an explanation of why the controls do not control all of the risk, what would have to be done in order to close the gap, and the difficulties or costs which currently make that impractical; **[10 marks]**
- an assessment of the balance of risk and benefit, which includes a recommendation on whether the organisation should accept the risk of BYOD with appropriate controls or make a firm prohibition. **[10 marks]**

As background, you have been told that although developers should not use live data to do testing, in practice they do. You have also been told that as this is a "Dev Ops" environment, developers often have access to operational systems.

You should aim to write for no more than one hour, producing perhaps 1500 (one thousand, five hundred) words. This is not a hard limit, but answers longer than this are likely to lack the required focus and concision.

14 credits

26956(b) Software Workshop (MSc) Spring Term

Submit your answers to the sub-questions as separate files in a single **zip** file. Your answers should be written as Java or PDF files as appropriate.

(a) **Testing**

Consider a method for finding the *unique* elements among two lists that are sorted in strictly ascending order. That is, the output list will contain exactly those elements that appear in one of the input lists but not the other. The output list will be sorted in strictly ascending order. Input **a** does not contain duplicates, and neither does input **b**.

```
static List<Integer> unique(List<Integer> a, List<Integer> b)
```

Decide 10 independent test cases for the **a**, **b** combinations, and in a table, state for each test case (i) what property of the method you are trying to test, (ii) the inputs, and (iii) the expected result or effect. You may write lists using the square bracket notation, e.g., [1, 2, 3]. Try to make your test cases small. Make sure that the "boundary cases" are tested. **[10 marks]**

(b) **Recursion**

Using recursion, write an efficient implementation of the method **unique** specified in part (a). You may use the **List** class from Term 2. **[8 marks]**

(c) **Collections**

You are asked to design and implement a solution for a lecturer for managing team projects for their class. A **Student** class is already available, which stores, for each student, the ID number, last name and first name. It has a **toString** method and implements the **Comparable** interface for comparing students by their last name-first name combination. The class also has a field for storing the *team name* for each student, which is a string unique to the team.

You need to define a class **Teams** in which the information pertaining to each team can be stored. It should store at a minimum the students who are members of the team. It should be extensible so that, in future, other information can be added such as the team supervisor, meeting schedules, marks etc. Frequent operations include updating information about individual teams, and tabulating all teams in an alphabetical order.

Describe what data structure you would use to store the teams and discuss its efficiency considerations. **[7 marks]**

Define the **Teams** class along with

- a constructor that takes an array of **Student** objects.
- methods to *add* and *delete* students.
- a **print** method that prints all the teams along with their members in the format

  team : member 1, member 2, . . .

  where the teams as well as members appear in sorted order. **[15 marks]**

You will be assessed for the quality of your solution in addition to its correctness.

6 credits

20236 Machine Learning (Extended)

(a) The following table describes a binary classification dataset $\mathcal{D} = \{x_i, y_i, z_i, t_i\}_{i=0}^{7}$ with independent variables x, y, and z; and dependent variable t.

i	x_i	y_i	z_i	t_i
0	0	0	0	0
1	0	0	1	0
2	0	1	0	0
3	0	1	1	1
4	1	0	0	0
5	1	0	1	1
6	1	1	0	1
7	1	1	1	1

The target $t = 1$ when two or more of the independent variables are 1.

(i) Using the principle of maximum information gain to determine the order of the variable splits, construct the full decision tree for this dataset, using data points $i = \{0, 1, 2, 4, 6, 7\}$ as the training set. Test your tree on data points $i = \{3, 5\}$ and explain your result. You do not need to draw the tree.

(ii) Describe three ways which can be used to improve the generalisation performance of decision tree-based classifiers, and discuss whether any of these would improve the result on this example.

[20 marks]

(b) A measurement technique called mass spectrometry is often used to measure the chemical composition of a sample by extracting molecules from the sample, and "weighing" them by measuring how they respond to electromagnetic fields. For each sample, the measurement can be represented by a vector which represents the number of molecules within each of a large number of mass bins.

In one experiment, a researcher measures 10,000 samples using a mass spectrometer that can measure the number of molecules in each of 800,000 mass bins. They wish to separate the samples into groups of similar chemical composition.

(i) Describe how they could do this, highlighting any potential problems they might encounter and how they could solve them.

(ii) The researcher learns that there are twelve distinct groups within the sample and identifies 50 examples from each group. Suggest how you might use this information to improve the result, again highlighting any potential problems you might encounter, and how you would solve them.

[20 marks]

7 credits

27112 MSc Introduction to Artificial Intelligence

(a) Assume that we have N products, each with a weight and a profit. We would like to decide which of these products to load in a lorry, with the objective of maximising the total profit of loaded products. The maximum weight W that the lorry can withstand must not be exceeded. To solve this problem using an optimisation algorithm, we decide to *modify* the objective of the problem to the following function, as a strategy to deal with the maximum weight constraint:

$$maximise \quad \sum_{i=1}^{N} v_i p_i - \sum_{i=1}^{N} v_i w_i \tag{1}$$

where v_i has value 1 (one) if product i is loaded and 0 (zero) if it is not loaded; p_i is the profit of product i; and w_i is the weight of product i.

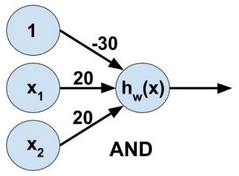
(i) Is this strategy adequate to deal with the constraint? Why?

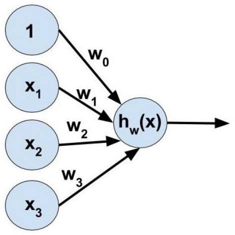
(ii) Give an example of a feasible and an infeasible solution that illustrates your argument, along with their objective values computed using Eq. 1. If your answer to (a)(i) is yes/no, your example should support/refute the proposed strategy to deal with the constraint. Assume that $W = 8$, $N = 3$, $p_1 = 10$, $p_2 = 5$, $p_3 = 20$, $w_1 = 3$, $w_2 = 3$, and $w_3 = 4$.

[20 marks]

(b) (i) List *one* advantage and *two* disadvantages of the KNN algorithm.

(ii) The Neural Network on the left performs the logical operation AND on the inputs x_1 and x_2 using one neuron. The incomplete network on the right is required to perform a given logical operation on three input variables.





The activation function of the above Neural Networks is the Sigmoid function given by the equation $\frac{1}{1+e^{-x}}$. You may assume that $sigmoid(x) \approx 0$ for $x \leq -4$ and $sigmoid(x) \approx 1$ for $x \geq +4$.

For each of the logical operations below, provide values for w_0, w_1, w_2, and w_3 so that the network performs this logical operation on three inputs. Draw a table to illustrate the input and output for each of your nodes that clearly shows why your network performs this operation.

(i) AND (ii) OR

[20 marks]

8 credits

26255 Operating Systems and Networks

(a) Processes are a key concept in operating systems. In this question there are 3 single-threaded processes, P1, P2 and P3, that have all been placed in memory. The total memory size is 256KB. The operating system occupies the first 64KB of memory. The size of P1's address space is 100KB, the size of P2's address space is 42KB and P3's is 50KB. For each of the processes, the code section is placed in the first 2KB of memory allocated to that process. One of P1's instructions is at physical address 107KB. What are the values held in the base and bounds registers for each process? Please show how you came to these answers. **[6 marks]**

(b) In our system, P1 has an execution time of 100ms and arrives at t=0ms, P2 has an execution time of 50ms and arrives at t = 15ms and P3 has an execution time of 30ms and arrives at t = 5ms. Assume that there is no cost associated to context switching or job selection. Calculate the average turnaround time and average response time when a first in, first out scheduler and a shortest job first scheduler are independently used to schedule the processes. Ensure you show your working. If more processes with arbitrary execution and arrival times were to be added following these three processes, explain which, if either, of the scheduling algorithms would be preferable to use in our system. **[8 marks]**

(c) In this sub-question, imagine there is a process that has multiple threads of execution. The threads work on a shared variable x to repeatedly increment its value by a set amount. Explain the potential problem with the threads interacting with x and what you could do to solve this? **[6 marks]**

(d) With reference to the internet protocol suite, explain how networked video conferencing software such as Zoom works. Consider potential choices of protocol that are fundamental to the functionality of such an application in your answer. **[14 marks]**

(e) Alice sends a message to Bob, Carol and David, who all read the message. Bob and Carol reply to Alice, who reads their responses, but David does not, so Alice sends a further message to him. In this scenario, assume that identities are authenticated by digital signatures using public key cryptography. Explain how many keys are actively used in this scenario and give the uses for each of these keys. **[6 marks]**

16 credits

26952 Operating Systems (Extended)

Consider a system for online exams for a university with thousands of students. This system consists of a web server which students can use to download exam papers and upload their answers. After an answer has been submitted, the system runs simple checks (is the student submitting the answer for the correct degree, is this a double submission etc). The submission is only accepted if these checks pass. The answers are also submitted to a plagiarism checker, which takes longer and is memory intensive. The results of the plagiarism checker are not available to the students.

A short response time to requests for downloading exam papers or submitting answers is essential.

(a) Which processes and threads would you use for such a system? For each process and thread, describe its purpose. Keep in mind that the system will be heavily loaded—many students will download the exam papers or submit answers at the same time. If you use threads, would you use user-level or kernel-level threads? Justify your answer. **[10 marks]**

(b) Describe how you would schedule the processes and threads identified in part (a). You should justify your choice of scheduling algorithms used. **[10 marks]**

(c) Describe how you would manage memory in such a system. You should also explain how your memory management strategy ensures a short response time to requests for downloading exam papers or submitting answers. You should also describe any effects your memory management strategy may have on scheduling. **[10 marks]**

(d) Exam papers are stored encrypted on the web server. How can you store the encryption key for the exam papers in a way that even someone with root access cannot access this encryption key? If your solution requires specific hardware, please identify the precise nature of this hardware and explain why this hardware is necessary. **[10 marks]**

7 credits

26954 Principles of Programming Languages (Extended)

Submit your answers in a single zip file, with either text documents or jpg images.

(a) Which of the following purported isomorphisms hold for arbitrary sets A, B and C? Prove your answers. **[8 marks]**

$$\begin{aligned} (A \times B) \to C &\cong (A \to C) \times (B \to C) \\ C \to (A \times B) &\cong (C \to A) \times (C \to B) \end{aligned}$$

(b) What polymorphic functions exist of type $A \to A \to A \times A$, for arbitrary sets A? Explain your answer. For full credit, you need to give a formal argument using relational parametricity showing that these are the only possible functions. **[9 marks]**

(c) Define a Haskell function `prime :: Int -> Bool` which, given a positive integer n, returns a boolean value indicating whether n is a prime number. Define this using standard *higher-order functions*, without using explicit recursion.

Recall that an integer range can be expressed in Haskell as `[i..j]`. **[5 marks]**

(d) Consider the following form of a "sequential let construct", in which the variable defined in the first definition (x_1) can be used in the defining term of the second definition (M_2). Both the variables can be used in the body of let (N):

$$\begin{aligned} &\textbf{letseq}\ x_1 = M_1; \\ &\qquad\quad\ x_2 = M_2 \\ &\textbf{in}\ N \end{aligned}$$

Propose a *type rule* for the sequential let construct, and state how it can be *desugared* into the standard let construct. **[8 marks]**

(e) Consider the abstract data type (ADT) `Queue` given in Handout 8 and its correctness proof using logical relations. The front operation is defined as follows:

```
front q = let Q (front, rear) = reform q
          in head front
```

Explain the role of the `reform` operation in this code.

Modify the Queue ADT so that the `reform` operation is not used in `front`. (It can perhaps be done elsewhere.)

Give the *logical relation* between the modified ADT and SimpleQueue ADT, and prove that it is preserved by the `insert` operation. **[10 marks]**

8 credits

20010 Secure Programming

In the context of a global pandemic, a country leader has fallen ill and is temporarily unable to lead his country. The other ministers of his government decide to elect a temporary leader among themselves. As everybody is working remotely, the administration sets up a voting website for the ministers to use. The website serves as an interface to a C program containing the following function.

```
 1  void registerVote() {
 2    // getting the vote from user
 3    char vote [30] ;
 4    printf("Please give your vote for our temporary prime minister\n");
 5    printf("Choose among: Donald Duck, Boris Vian, Angela Jolie\n");
 6    scanf("%s",vote);
 7
 8    // operations to process the vote
 9    ...
10
11    // confirmation to user that their vote has taken place
12    printf("You voted for ");
13    printf(vote);
14    printf(" as temporary prime minister.\n");
15    printf("Thank you for voting!");
16  }
```

(a) Identify two vulnerabilities in the code above. For each vulnerability

(i) Give the vulnerability name and the code line where it occurs.

(ii) Describe how a malicious user could use the vulnerability to crash the program, and explain why the attack works.

(iii) Discuss potential consequences of these vulnerabilities.

[16 marks]

(b) Could static and dynamic analysis tools have detected the above vulnerabilities? Justify your answer. **[7 marks]**

(c) Provide a secure version of the code above. **[10 marks]**

(d) After realizing that some of the ministers may fall ill in turn, the administration decides to maintain a database of available (healthy) government members, and use a *static* SQL command in line 5 to print the list of available members. Could this change lead to further vulnerabilities to the above code? Justify your answer. **[7 marks]**

8 credits

27113 Software Engineering I (Extended)

(a) (i) You work at a software company that follows the more linear ways of working (Plan Driven), but you think projects would benefit from an Agile approach. Briefly, discuss how you can help your company move towards this through a more hybrid solution. **[3 marks]**

(ii) Assume that you are a project manager for developing a high-risk ambulance service software where changes may require at any time. Describe the appropriate development approach that you will choose for that project. Your choice should be properly justified. **[5 marks]**

(b) You are working on a software project where the client (project owner) negotiates for an early software release to meet with some market opportunities. As a software engineer, you anticipate that pushing toward an early release will affect product quality.

(i) If you are in a position that you need to make a trade-off, what quality attributes you might pay less attention to based on the above scenario? (state three quality attributes and justify your answer) **[6 marks]**

(ii) What are the characteristics of the final project that are likely to be affected as a result of your decision above? **[6 marks]**

(c) Consider the following code

```
Start
Do Until B=C
    If Today=Monday
        Set A=2
    Else if Today=Wednesday
        Set A=3
        Set B=C
    End if
    If B<C
         Set B=B+1
    End if
 End loop
 End
```

(i) Draw the Control Flow. **[6 marks]**

(ii) Compute and analyse the Cyclomatic Complexity in the given code. **[6 marks]**

(iii) How many test cases are required to achieve 100% Branch Coverage (Decision Coverage)? Provide a valid example of each test case. **[8 marks]**

5 credits

27114 Software Engineering II (Extended)

Consider an online Food ordering and delivery System (FoodSys), where restaurants can sign up to the service to advertise for their cuisine and accept orders. FoodSys checks each restaurant's application, and may reject the application if deemed to be irrelevant, illegal, or because the restaurant has a poor hygiene rating. The checking takes up to 24 hours. Once the restaurant passes the check and registers successfully, FoodSys will charge £50 for joining the service and a monthly payment of £100. Restaurants can use FoodSys to upload their menu, advertise offers, see analytics and contact the customer (e.g. for order modification). Online users can sign up to FoodSys to browse menus and special offers, make online orders, search for restaurants, rank and review restaurants, and pay for the food. FoodSys can also provide recommendations to the users based on location, preference information, patterns of use etc. Upon ordering and paying, the user will receive a confirmation receipt of his/her order to email and/or mobile phones. All transaction information passed by the system to the credit/debit card consortium is secure and encrypted using 128-bit SSL certificates. Processing of online payments should not exceed 30 seconds. FoodSys is designed to be available 24/7. It can handle up to 1 million online users during off-peak time. Users' and restaurants' profiles are stored and backed up to four distinct database servers to prevent catastrophic failure.

(a) Provide a use case diagram for FoodSys. Identify TEN use cases related to the system and FOUR actors. Make use of both ⟨⟨include⟩⟩ and ⟨⟨extend⟩⟩ stereotypes. Explain any necessary assumptions you make. **[20 marks]**

To draw the diagram, use the online tool "draw.io" (https://app.diagrams.net): a) create new diagram; b) create basic blank diagram; 3) all the shapes for the use case diagram can be found in the "General" section on the left-hand side.

A handwritten diagram or using other software is accepted if you cannot access draw.io. Please ensure the clarity and readability.

(b) The architect has considered two possible candidate architecture styles for modelling the recommendation subsystem to enable automatic restaurant suggestions for online users. One candidate is based on a rule-based style, where suggestions/advertisements are produced based on a set of pre-defined rules. The second candidate is based on an event-driven style, where changes in online user's location, preference information, etc. can trigger suggestions/advertisements in real time. Discuss the scalability, adaptability and performance trade-offs in comparing the two candidate solutions. **[20 marks]**

14 credits

26956(a) Software Workshop (MSc) Autumn Term

Your submission should contain for each sub-question fully working programs in form of **.java** files including **main** methods, submitted in form of a single **zip** file. Ideally your programs run and the programs are of a high quality. But the code will be marked line by line, and anything that contributes substantially towards a correct answer will attract some of the marks. Even with minor syntactic inaccuracies full marks may be obtained. While you may want to use an IDE, you do not have to and it may actually be not a good idea if you do not have a working IDE already installed.

(a) **Computation (conditionals, loops, arrays, exceptions)**
Assume that we need for testing purposes **n** randomly generated values of type **double** in the range between **a** and **b**. Write a corresponding method
public static double[] generateTestValues(int n, double a, double b).
If **a** is greater than **b** or **n** is negative your method should throw an **IllegalArgumentException**. Demonstrate that the code works with four well chosen examples in a **main** method. **[14 marks]**

(b) **Classes, Sub-classes**
An online shop sells items. Each item has a **price** and a **name**. Items are either DVDs or books, for a DVD the **playingTime** is given in addition, for a book the **numberOfPages**. Furthermore any item may be discounted by a **discountPercentage** between 0 (included) and 100 (excluded). Represent the situation by a suitable class structure. Each class should contain a suitable constructor and a **toString** method that presents the information in a suitable human readable form. Make use of inheritance where appropriate. Give suitable examples for the different possibilities of items (DVD versus book, and some items discounted versus some not) in **main** methods.
Important: Justify your design decisions (as Java comments). **[13 marks]**

(c) **Graphics, Graphical User Interfaces**
Two values in a fixed range (such as temperature between -10 and 40, and air pressure between 0.87 hPa and 1.09 hPA, or volume-left and volume-right for two loudspeakers) are to be displayed by two indicators as shown in Figure 1 below. You can assume that the values are already converted to angles between 0 and 90 degrees.

Using only the **Line** and **Polyline** classes write a JavaFX program to produce the corresponding display. Note that angles between **0** and **90** may need to be appropriately converted to angles between **0** and **Math.PI/2**. Note furthermore that a circle segment can be represented by a function **x -> Math.sqrt(1-x*x)**. You may wish to use for your answer the **FunctionGraph.java** example of week 8 in Term 1 (see **wk08.zip** on the Term 1 Canvas page or **https://www.cs.bham.ac.uk/~mmk/FunctionGraph.java**). Your answer must be general and work for any two angles between **0** and **90** degrees.

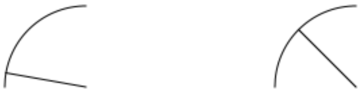


Figure 1: Expected display for angles **10** degrees and **45** degrees. **[13 marks]**