



EXAMINATIONS – 2014
END-OF-YEAR

SWEN 224
Formal Foundations
of Programming

Time Allowed: THREE HOURS

Instructions: Open Book

You may answer all 5 questions but **only the best 4 answers** will count to your final mark

All questions are of equal value

No Calculators permitted

Question	Topic	Marks	Achieved
1.	Assertions	45	<input type="checkbox"/>
2.	Verifying Programs	45	<input type="checkbox"/>
3.	Finite Languages	45	<input type="checkbox"/>
4.	Regular Languages	45	<input type="checkbox"/>
5.	Processes	45	<input type="checkbox"/>
Total of best 4 questions		180	

Question 1. Assertions

[45 marks]

Let A be an array of integers indexed from 0 to $|A| - 1$ and B be an array of integers indexed from 0 to $|B| - 1$. Let x, y and z be integers.

(a) Consider the following assertion:

$$x < y \wedge x = z$$

(i) [1 mark] State in words what the assertion means.

For each of the following, say whether the above assertion is true or false:

(ii) [1 mark] $x = 2, y = 3, z = 3$

(iii) [1 mark] $x = 3, y = 3, z = 3$

(iv) [1 mark] $x = 2, y = 3, z = 2$

(b) Consider the following assertion:

$$\forall j \bullet 0 \leq j < |A| \rightarrow A[j] > 10$$

(i) [2 marks] State in words what the above assertion means.

For each of the following arrays, say whether the above assertion is true or false:

(ii) [1 mark] $A = [100, 50, 10]$

(iii) [1 mark] $A = []$

(c) Consider the following assertion

$$\left(\exists j \bullet 1 \leq j < |A| \rightarrow A[j-1] = A[j]\right) \wedge \left(\forall i \bullet 0 \leq i < |A| \rightarrow A[i] > i\right)$$

(i) [4 marks] State in words what the above assertion means.

For each of the following arrays, say whether the above assertion is true or false.

(ii) [1 mark] $A = [1, 3, 3, 5]$

(iii) [1 mark] $A = [1, 2, 3, 3, 7]$

(iv) [1 mark] $A = []$

(v) [1 mark] $A = [10, 10, 3]$

(d) Write a First Order Logic Predicate formalising each of the following statements:

(i) [3 marks] x is less than y and greater than z .

(ii) [4 marks] A contains at least one element greater than d .

(iii) [4 marks] If A contains 0 then no element is greater than 10.

(iv) [4 marks] If the two arrays A and B share a common element then these elements are one of the first three elements of each array.

(v) [4 marks] No element in A is in B .

(e) Program contracts.

(i) [5 marks] Write a formal contract, a pre-condition (the requirements the parameters must satisfy) and post-condition (the condition the returned values must satisfy) , for the following program specification.

The program must take three arrays, A , B and C , containing the lengths, widths and heights respectively of a sequence of boxes (cuboids). So $A[i]$, $B[i]$ and $C[i]$ are the length, width and height of box i (the i th box). The program outputs an array, V , containing the volume of the box. Note the volume is defined by $volume = length \times width \times height$.



(ii) [5 marks] Write a formal contract, a pre-condition and post-condition, for the following program specification.

The program inputs, P , an array of pairs. When i is an index of P then the first element of pair $P[i]$ is written as $first(P[i])$ and is a student name. The second element of $P[i]$ is written as $second(P[i])$ and is the integer grade for the student. The program outputs:

1. SB - the set of student names for students that have grade "B", that is their numeric grade is greater than or equal to 70 and less than 75.
2. CB - the number of students that have grade "B".

Question 2. Verifying Programs

[45 marks]

Each question has a program and a post-condition. Use Hoare Logic to compute the missing conditions, simplifying your answers where appropriate.

Variables $x, y, z, w \dots$ are integers and A is an array of integers.

(a) [5 marks] What are the conditions: **P**, **P1** and **P2**?

<p>P _____</p> <p style="text-align: center;">$y := 5x;$</p> <p>P1 _____</p> <p style="text-align: center;">$y := y + 3x;$</p> <p>P2 _____</p> <p style="text-align: center;">$x := y + 4;$</p> <p>Q $\{x \times y < 44\}$</p>

(b) [5 marks] What are the conditions: **P**, **P1**, **P2** and **P3**?

<p>P _____</p>	
<p>P1 _____</p> <p style="text-align: center;">$x := x - 1;$</p> <p>Q $\{10 > x + y\}$</p>	<p>P2 _____</p> <p style="text-align: center;">$y := -y;$</p> <p>P3 _____</p> <p style="text-align: center;">$x := 5$</p> <p>Q $\{10 > x + y\}$</p>
<p>If $0 \leq x$ then $x := x - 1;$ else $y := -y; x := 5;$ fi</p> <p>Q $\{10 > x + y\}$</p>	

(c) [5 marks] What are the conditions: **P**, **P1**, **P2** and **P3**, and the statement **S1**?

P _____	<p>P1 _____</p> <p style="margin-left: 20px;">$y := y + 1;$</p> <p>P2 _____</p> <p style="margin-left: 20px;">$x := 3 - y;$</p> <p>Q $\{x < 10\}$</p>	<p>P3 _____</p> <p>S1 _____</p> <p>Q $\{x < 10\}$</p>
<p>If $(x > 3)$ then $y := x + 1; x := 3 - y;$ fi</p> <p>Q $\{x < 10\}$</p>		

(d) [5 marks] What are the conditions: **P**, **P1**, **P2** and **P3**?

P _____	<p style="margin-left: 20px;">$w := x;$</p>
P1 _____	<p style="margin-left: 20px;">$x := 8;$</p>
P2 _____	<p style="margin-left: 20px;">$A[x] := 8;$</p>
P3 _____	<p style="margin-left: 20px;">$z := A[w];$</p>
Q $\{z > 10\}$	

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.

(e) For a while program with guard **B** and code in the body of the loop **S**:

```
while B do { S }
```

(i) [3 marks] **state the three loop conditions** using the loop invariant **L**, the pre-condition **P** and post-condition **Q**.

Consider the following program:

```
int i := 0;
int x := 0;
while (i < z) then {
  x := x + 3;
  i := i + 1;
}
```

(ii) [4 marks] Given the program above, the program pre-condition **Pre** = $\{0 < z \wedge 3z \leq 16\}$ and the program post-condition **Q** = $\{x \leq 16\}$.

Define **L** - the loop invariant and **P** - the loop pre-condition.

(iii) [6 marks] Prove your loop invariant, pre-condition and post-condition satisfies the **three loop conditions** (see subquestion (i) above).



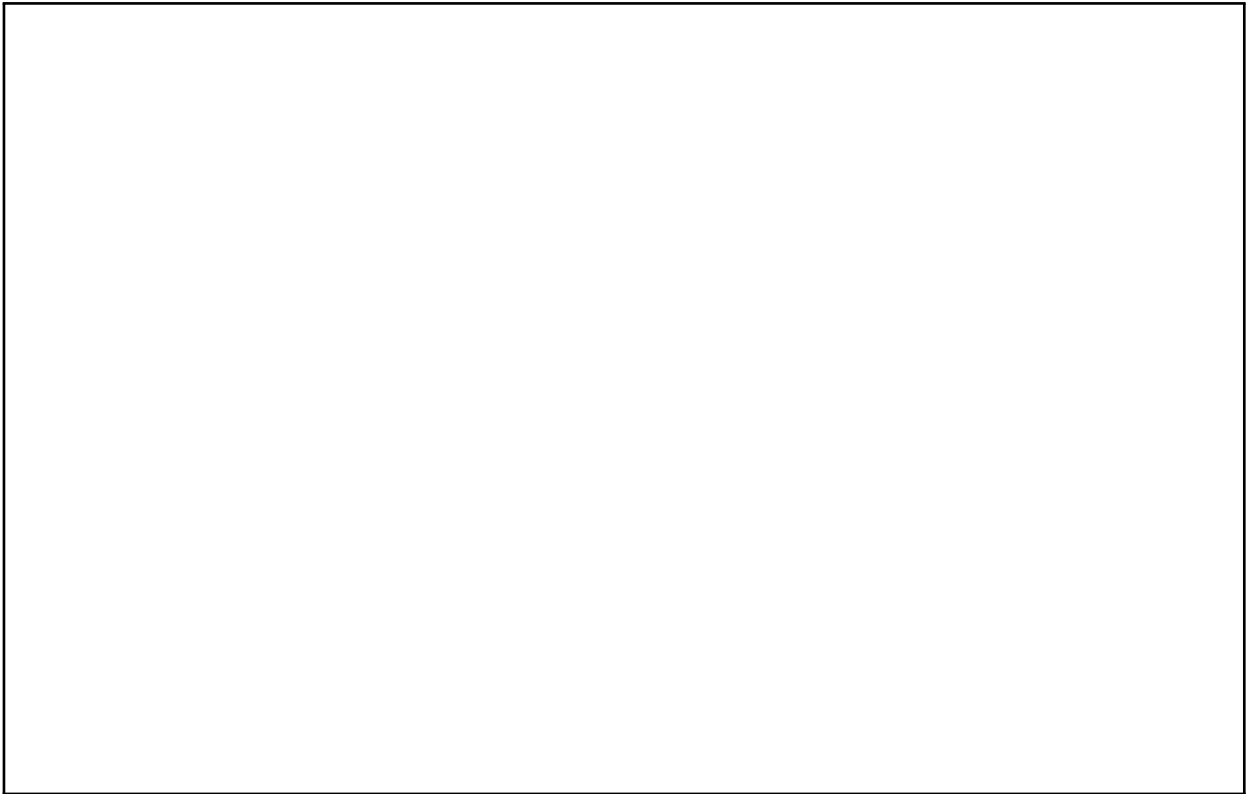
(f) The program below takes two arrays A and B of the same size containing the height and width of rectangles. Rectangle i having height $A[i]$ and width $B[i]$. The program computes a the sum of the areas of the rectangles. The area of a rectangle is *height* \times *width* (in the program the area of rectangle i is $A[i] * B[i]$).

```
int i := 0;
int a := 0;
while i < |A| then {
    i := i + 1;
    a := a + (A[i] * B[i]);
}
```

(i) [2 marks] Clearly, the post condition of the program is the post condition of the while loop. From the specification of the program define Q - the post-condition of the while loop,

(ii) [4 marks] Define L - the loop invariant and P - the pre-condition to the loop.

(iii) [6 marks] Prove your loop invariant, pre-condition and post-condition satisfy the three loop conditions for the given program.



SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.

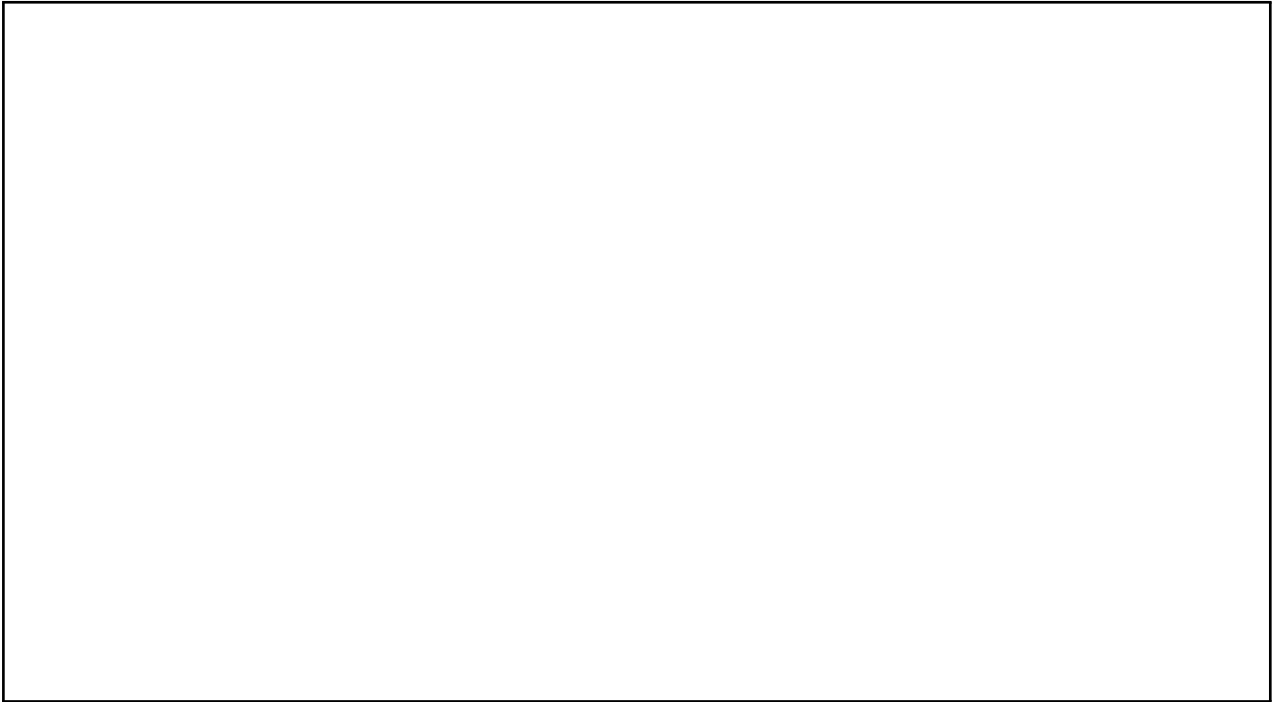
SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.

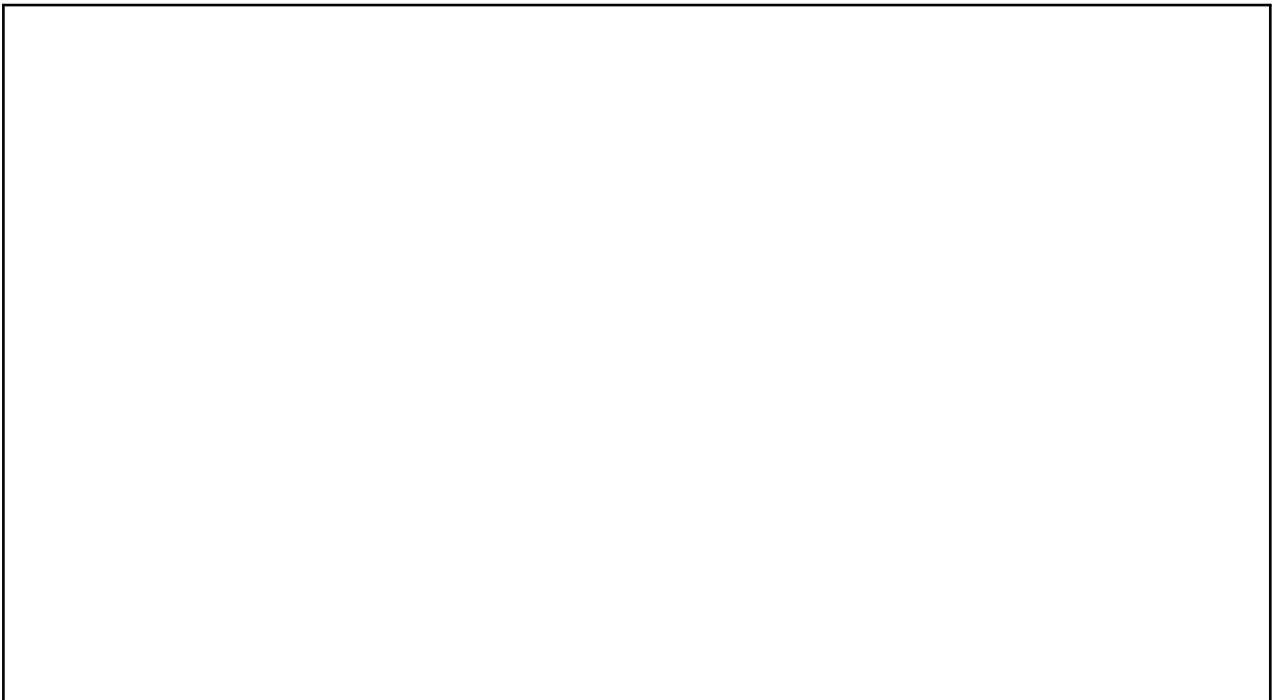
Question 3. Finite Languages

[45 marks]

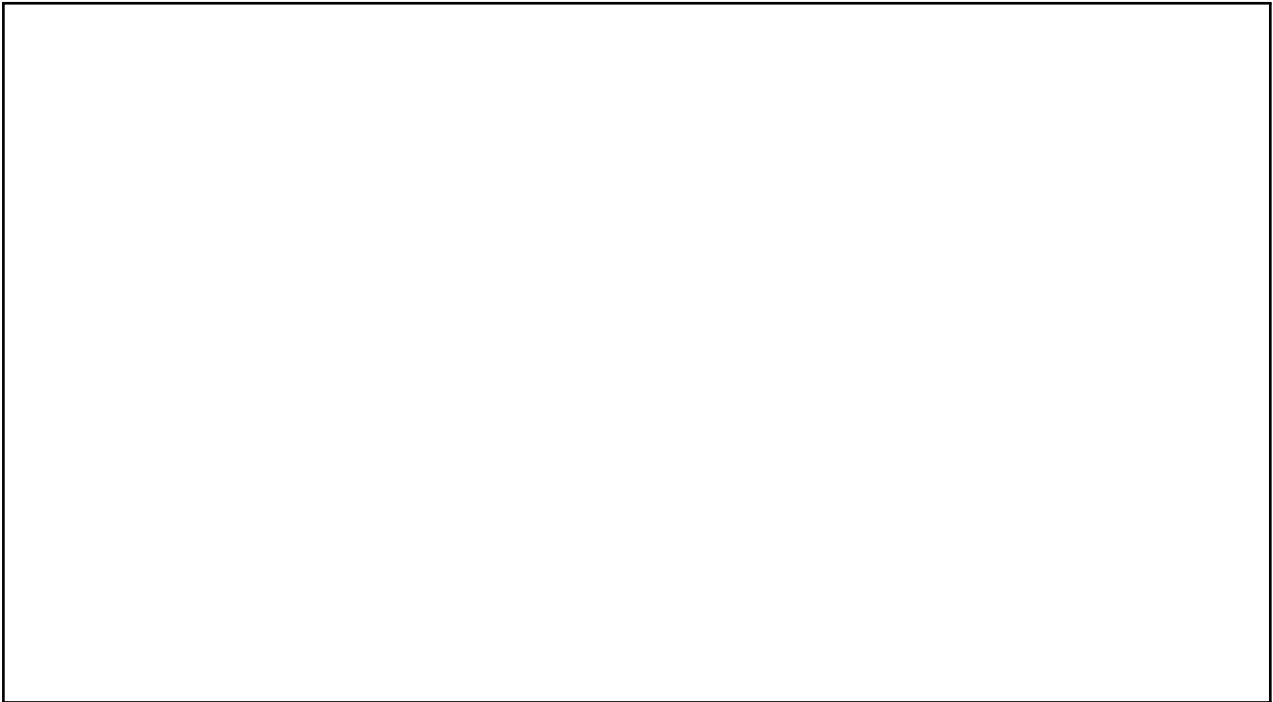
(a) [15 marks] **write down a trie that will recognise all words in the language and only the words in the language** $\{hat, bat, boot, hoot, hot, hatter\}$



(b) [15 marks] From the Trie construct the **language equations**



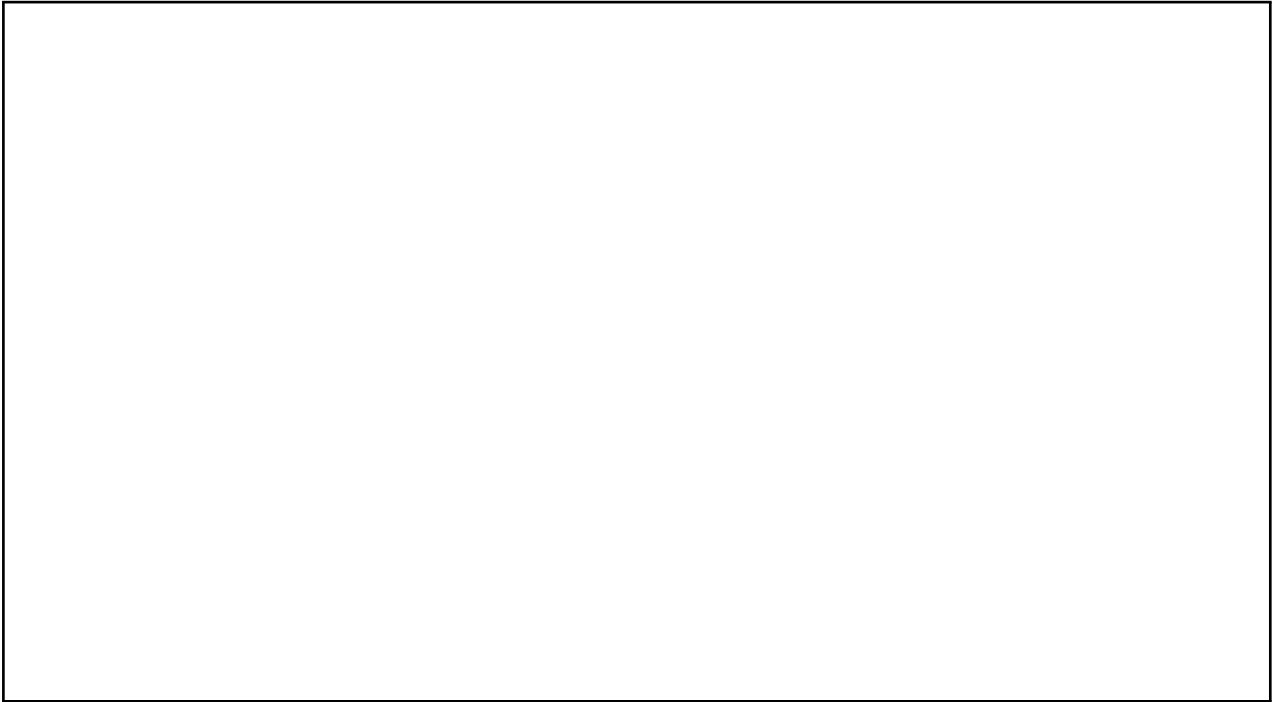
(c) [15 marks] Solve the equations to reconstruct the language

A large, empty rectangular box with a thin black border, intended for the student to write their solution to the problem.

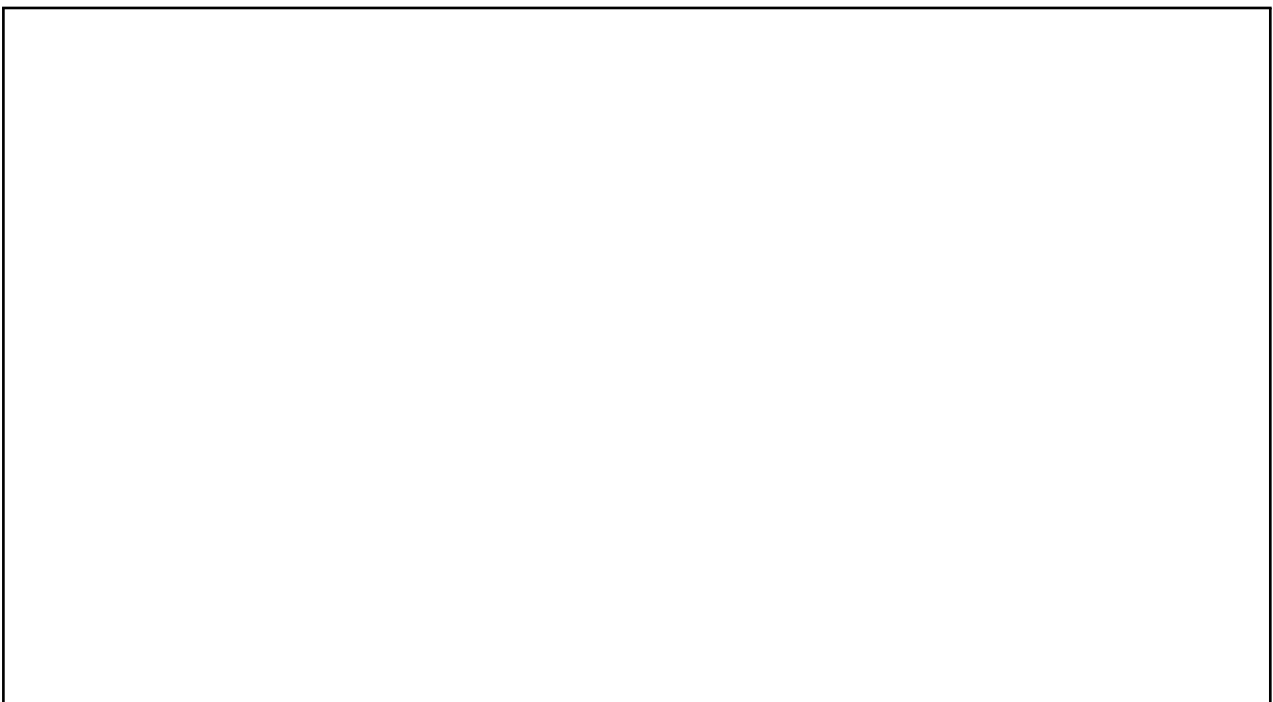
Question 4. Regular Languages

[45 marks]

(a) [10 marks] Construct the Nondeterministic Finite Automata, NFA, from the regular expression $(a|(b.c))^*.e$



(b) [15 marks] Apply the Subset construction to the NFA in the previous question and display the Deterministic Finite Automata, DFA. Each node of the DFA must be labeled with a set of NFA nodes.



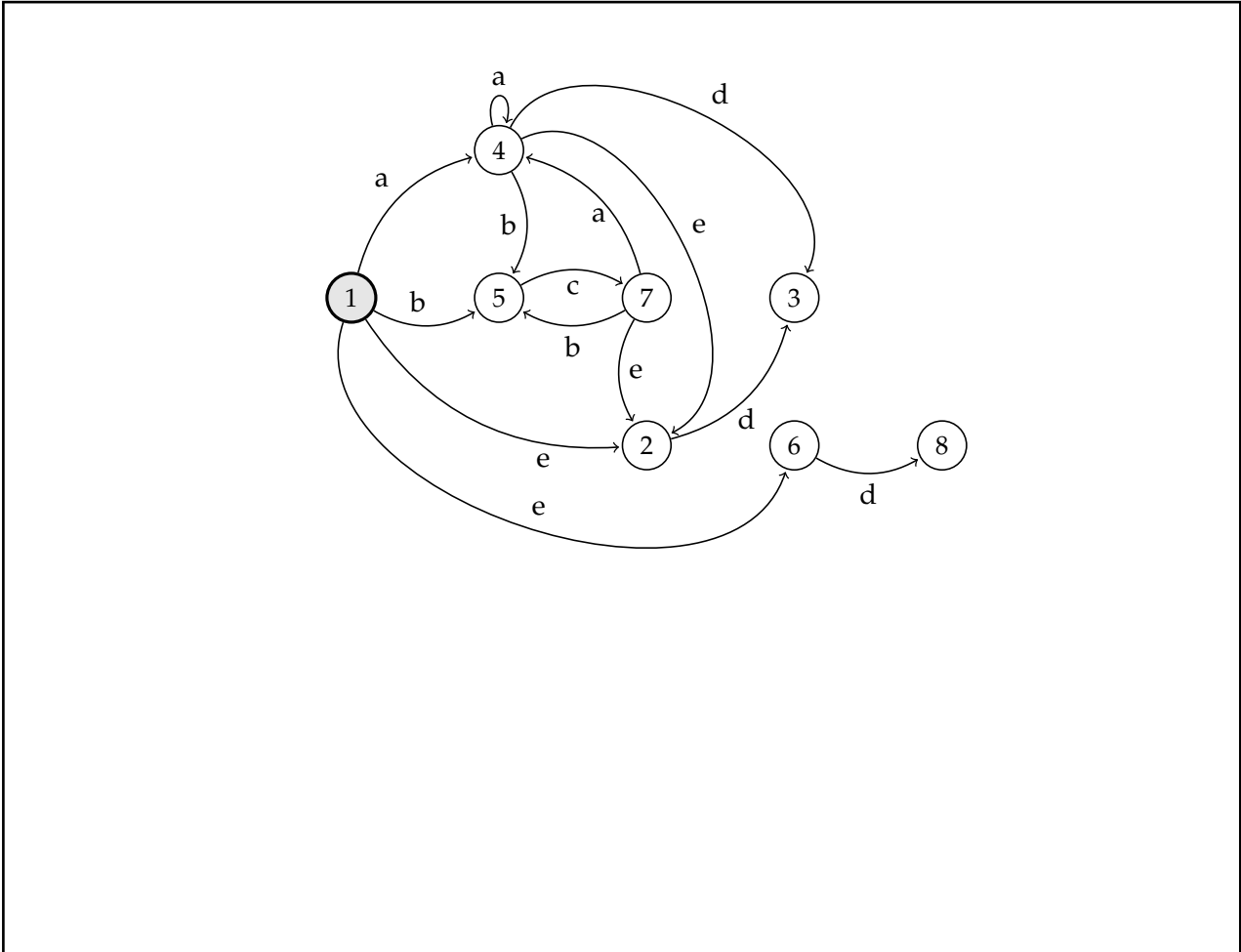
(c) [10 marks] Write down the equations from the DFA

(d) [10 marks] Solve these equations to construct a regular expression. Justifying your steps as you go.

Question 5. Processes

[45 marks]

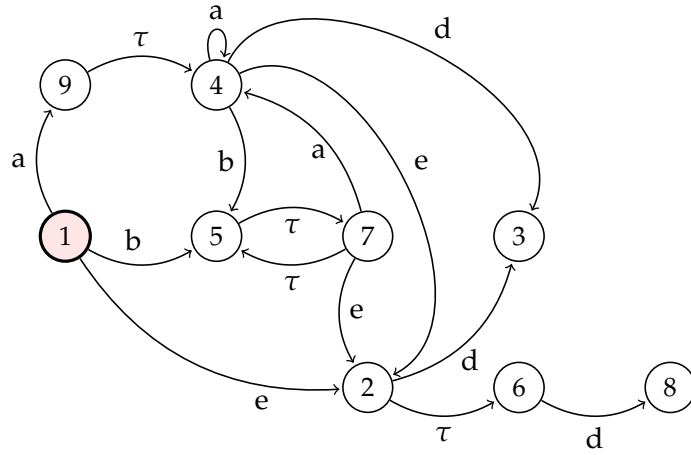
(a) [10 marks] Build a bisimulation Colouring for the given automata



(b) [5 marks] Build an automata from the automata in the previous question by identifying the equivalent nodes



(c) [15 marks] Add observable events and remove the τ events by applying the abstraction function to the given automata.



SPARE PAGE FOR EXTRA ANSWERS

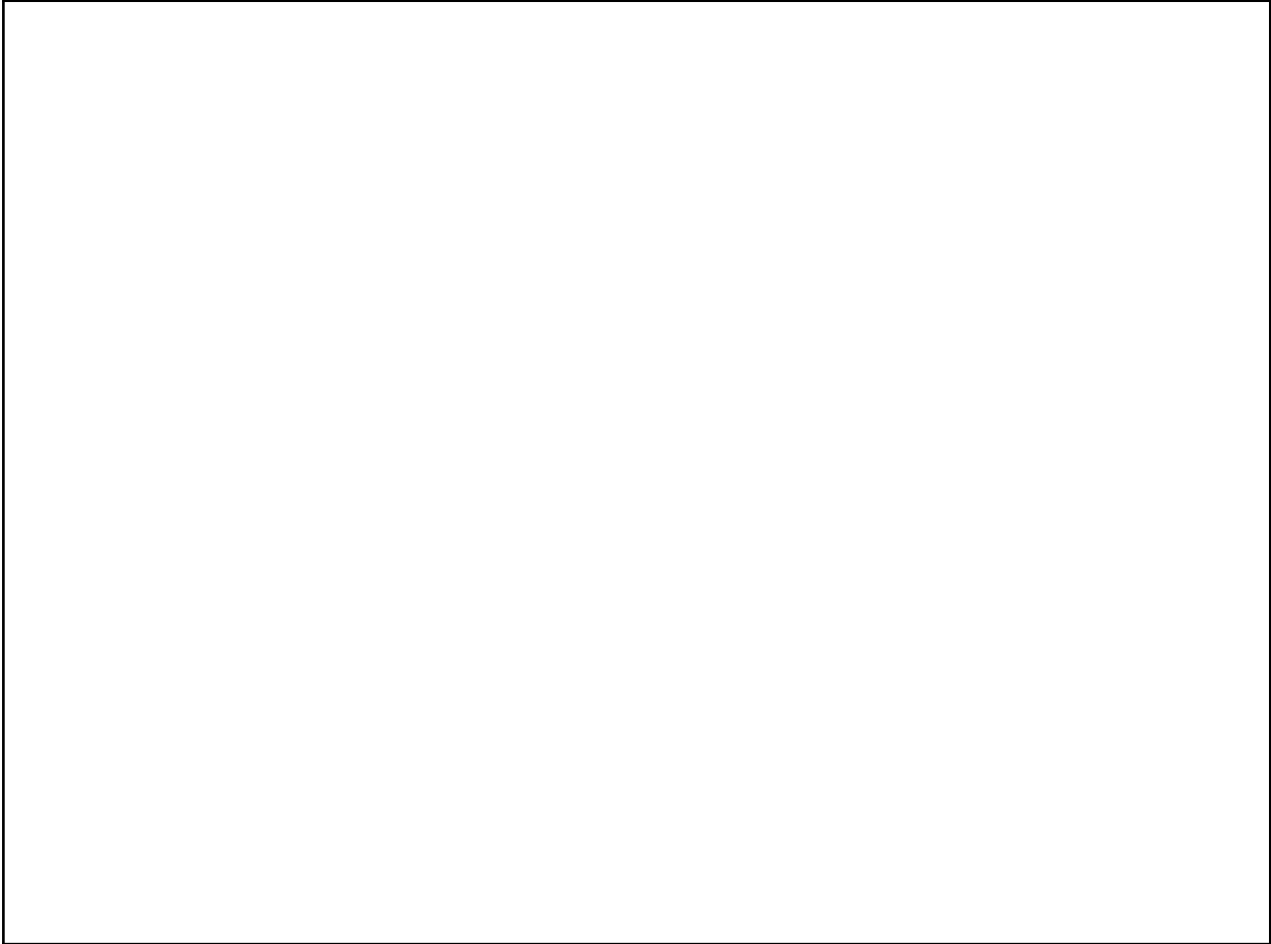
Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.

Build an automata model of a gate controller for a pest proof fence. Name any synchronising events you use *SyncA, SyncB, SyncC, ...*

(d) [7 marks] The gate has a short corridor with two doors **A** and **B**. Build two processes each controlling one of the doors. The controllers can only “talk” to each other, and talk to each other using synchronising events. The controllers must ensure that both doors must not be open at the same time. Use events *OpenA, CloseA, OpenB* and *CloseB*.



(e) [8 marks] Refactor your initial model to add a lock down process that includes events **Lock** and **Unlock**. When the **Lock** event is executed the gates are “locked” i.e. can not open. For safety reasons when the **Lock** event occurs if the last gate open was the **B** gate then the gates continue to function until the **A** gate opens once and only once.



* * * * *