Module Title: Formal Specifications of Software Systems
Level: Five
Time Allowed: Two hours

Instructions to students:
- Enter your student number **not** your name on all answer books.
- Answer **three** questions: the **one compulsory** question from **Section A** and **two** questions from **Section B**.
- Where a question has more than one part the division of marks is stated.
- Unless explicitly required, there is no need to consider failure of preconditions in Z schemas which specify operations.
- Any symbolic expressions written by candidates should be accompanied by appropriate explanatory annotation in **plain English** otherwise marks may be withheld.

---

<table>
<thead>
<tr>
<th>No. of Pages</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Questions</td>
<td>5</td>
</tr>
</tbody>
</table>
Answer the **one compulsory** question.

**Question 1**

Provide answers to the following as succinctly as possible:

**a.** If \( A = \{ a, b, c, d \} \), \( B = \{ b, d, f, h \} \) and \( C = \{ b, f, h \} \) write down the sets:

i. \( A \cup B \cup C \)  
ii. \( A \cap B \cap C \)  
iii. \( A \setminus (B \cap C) \)

**b.** Enumerate the following sets:

i. \( \{ n : \mathbb{N} \| n < 4 \cdot 3n \} \)  
ii. \( \{ n : \mathbb{N} \| n \leq 5 \} \cap \{ 1, 2, 3, 4 \} \cap \{ n : \mathbb{N} \| n = 4 \} \)

**c.** Given the declarations:

\( x, y, z : \mathbb{N}; a : \text{PERSON}; b : \text{BOOK}; \)  
\( \text{on\_loan} : \text{P BOOK}; \text{novelists} : \text{P PERSON} \)

Say whether the following notations are **well-formed**:

i. \( x > y \)  
ii. \( x \in \text{on\_loan} \)  
iii. \( a \in \text{on\_loan} \)  
iv. \( a \in \text{novelists} \)  
v. \( \text{on\_loan} \subseteq \text{novelists} \)  
vi. \( \text{on\_loan} \subseteq \text{Book} \)  
vii. \( \{ \text{on\_loan}, \text{novelists} \} \)  
viii. \( \{ a, b \} \)  
ix. \( \#x + y \)  
x. \( \#\text{on\_loan} = y \)

**d.** If \( A = \{ a, b \} \), \( B = \{ b, c \} \) and \( C = \{ a, b, c \} \) write out:

i. \( A \times B \)  
ii. \( \mathcal{P} \ C \)  
iii. \( \mathcal{P} \ A \)  
iv. \( A \times C \)
e. Given the relations \( X = \{(1, 4), (2, 8), (3, 12)\} \) and \( Y = \{(4, 1), (8, 1), (12, 1)\} \) evaluate:

i. \( X \bowtie Y \) \hspace{2cm} (2 marks)
ii. \( X \bowtie Y \bowtie Y^{-1} \) \hspace{2cm} (2 marks)
iii. \( Y \bowtie X \) \hspace{2cm} (2 marks)
iv. \( X^{-1} \bowtie Y^{-1} \) \hspace{2cm} (2 marks)

f. If \( S = \{1, 2\} \) and \( R = \{(1, 1), (1, 5), (1, 10), (10, 11)\} \), find:

i. \( \{1\} \triangleleft R \) \hspace{2cm} (2 marks)
ii. \( \text{ran}\{S \triangleleft R\} \) \hspace{2cm} (2 marks)
iii. \( R^{-\downarrow} \) \hspace{2cm} (2 marks)
iv. \( R \{\{S\}\} \) \hspace{2cm} (2 marks)

g. Create a truth table to evaluate the following:

\[
P \text{ XOR } Q \iff (P \lor Q) \land \neg (P \land Q)
\]

(6 marks)

Total: 50 marks
Section B

Answer two out of four questions.

Question 2

A college offers many courses. A number of different tutors are responsible for teaching on each course and each of these tutors will teach on two or more courses. A student, who is registered with the college, may be enrolled on only one course at any one time and each course has a limited capacity (i.e. for each course there is a maximum number of permitted student enrolments), which is determined at the time that the course is added to the college portfolio. Tutors are assigned to teach on a course and students can be enrolled for a course only after the course has been added to the portfolio. No course can be removed from the portfolio if it has tutors assigned to it, nor if students are enrolled for it.

Suppose we declare the following:

[TUTOR] the set of all tutors that might ever be employed by the college;
[COURSE] the set of all courses that might ever be offered by the college;
[STUDENT] the set of all students that might ever register at the college;

with the following derived sets to model the system:

taught_by which describes the connection between courses and the tutors teaching on them;
has_enrolled which describes the connection between courses and the students enrolled on them;
course_limit which describes the connection between courses and their corresponding permitted maximum enrolments;
known_students the set of all students currently registered with the college;
tutors the set of tutors employed to teach on the college courses;
portfolio the set of courses currently offered by the college.

If College is the state schema created to specify the essential properties of the system described above, a draft version of College is illustrated over the page:

Question 2 continues overleaf
a. Draw a diagram to illustrate how the six sets defined in the declaration part of the College state schema are related.  

(4 marks)

b. Explain, in plain English, the meaning of each of the five lines in the predicate part of the above state schema, College.  

(5 marks)

c. Why are has_enrolled and course_limit partial functions rather than total functions?  

(2 marks)

d. The College schema given above does not provide a complete specification of the system properties as outlined on page 4. In particular, the following constraints are not currently specified:

i. No student can be enrolled for more than one course
ii. No course can exceed its prescribed maximum enrolment
iii. Every tutor must teach on at least two courses

Using suitable quantifiers, or otherwise, represent each of these three constraints symbolically.  

(9 marks)

e. Devise a Z schema Remove_Course which specifies the operation to delete a course, c?, from the college portfolio of courses. Include reasonable preconditions; but do not consider violation of any of these preconditions.  

(5 marks)

Total: 25 marks
Question 3

Certain medicines may be given to patients diagnosed as suffering from particular illnesses. Suppose we attempt to model this system using the following given sets:

- [PATIENT] : all people who might ever be patients
- [ILLNESS] : all illnesses from which people may suffer
- [MEDICINE] : all medicines that might be used to treat illnesses

Since

- patients may suffer from more than a single illness;
- many patients can suffer from the same illness;
- a particular illness may be treated with different medicines; and,
- a particular medicine can be used to treat many illnesses,

it seems likely that the following sets of ordered pairs could prove useful as a basis for modelling:

- complaints : PATIENT \(\leftrightarrow\) ILLNESS
- treatments : ILLNESS \(\leftrightarrow\) MEDICINE

a. By referring to the simple system modelled above:

i. state what sort of mathematical structure has been used to model the two sets complaints and treatments.

(1 mark)

ii. draw a suitably labelled diagram which includes representations of the sets PATIENT, ILLNESS, MEDICINE, complaints and treatments.

(3 marks)

b. If medications : PATIENT \(\leftrightarrow\) MEDICINE is a set of ordered pairs matching patients with the medicines that they are taking, use relational composition to write down a symbolic expression showing how the set medications can be derived from the two sets complaints and treatments.

(3 marks)

c. If our model needs to incorporate extra information to show that particular medicines should not be prescribed to treat certain illnesses, we might declare:

\[ \text{not_permitted} : \text{ILLNESS} \leftrightarrow \text{MEDICINE} \]

where \((i, m) \in \text{not_permitted}\) only when illness \(i\) should not be treated with medicine \(m\).

Question 3 continues overleaf
i. If \( \text{banned\_medications} : \text{PATIENT} \rightarrow \text{MEDICINE} \) shows those medicines patients must not take, write a symbolic expression to derive the set \( \text{banned\_medications} \) from sets defined above. 

\[ \text{(2 marks)} \]

ii. Write down a symbolic expression for the set containing pairs of medicines which may “clash”, in the sense that the first medicine of the pair may be used to treat a particular illness while the second is forbidden for that illness.

\[ \text{(2 marks)} \]

iii. Write down a symbolic expression for the set containing pairs of illnesses such that the first illness in the pair may be treated by some medicine while the second in the pair should not be treated by the same medicine.

\[ \text{(2 marks)} \]

d. If at least one of the medicines \( m_1, m_2, m_3 \) is being taken by the patients in a particular set, write down a symbolic expression for that set using:

i. relational image 

\[ \text{(3 marks)} \]

ii. domain restriction

\[ \text{(3 marks)} \]

iii. range restriction

\[ \text{(3 marks)} \]

e. Create a symbolic expression which gives the set of medicines appropriate for illnesses \( i_1, i_2, i_3, \text{ or } i_4 \) if the medicines must also be suitable for patients \( p_1, p_2 \) and \( p_3 \).

\[ \text{(3 marks)} \]

Total: 25 marks
Question 4

As a software engineer working in a small to medium software house you have been asked to evaluate the potential of using formal methods within some or all of your companies’ software development projects. Opinion is mixed but your provisional research suggests that formal methods could potentially benefit some of the software systems your company currently develop.

Write a short report, for the managing director of your company, to include the following essential information:

a. The characteristics of any software development where the deployment of formal methods would be appropriate. Ensure you include details of at least two successful projects that have utilised formal methods.  
   (5 marks)

b. Outline some of the myths about formal methods providing, where possible, examples to justify your findings.  
   (5 marks)

c. Discuss the potential impact of using formal methods on project cost, speed and development life cycle.  
   (5 marks)

d. Identify the types of project where formal methods would be inappropriate and provide justification for your conclusions.  
   (5 marks)

e. Outline the potential negative aspects of introducing formal methods for your organisation with respect to issues such as training, case tool procurement and availability of subject experts.  
   (5 marks)

Where appropriate reference suitable example software projects where formal methods have been deployed and any academic papers that you have studied to support your recommendations.

Total: 25 marks
Question 5

As a formal specification expert you have been asked to formally specify PASCAL’s file processing operations using standard Z-notation. The following essential information regarding the filing system has already been collated:

- In PASCAL, a file is a *sequential* structure of any type of elements.
- A file can be in one of two modes, *inspection* mode, or *generation* mode.

  - *Inspection* mode is:
    - initiated by a *Reset* operation,
    - and permits *Read* operations on a file,
    - and has associated BOOLEAN *end_of_file*.

  - *Generation* mode is:
    - initiated by a *Rewrite* operation, and
    - permits *Write (append)* operations on a file.

To accommodate the above information, the following partial specification has been completed in Z-notation:

[X] -- any type of data permitted by PASCAL language

FILEMODE ::= inspection \| generation

The state schema for file system being modelled by:

\[
\text{PASCAL\_File}[X] \begin{array}{l}
\text{file : seq } X \\
\text{still\_to\_read : seq } X \\
\text{mode : FILEMODE} \\
\exists \text{already\_read : seq } X \cdot \\
\quad \text{already\_read} \sim \text{still\_to\_read} = \text{file}
\end{array}
\]

Note that *end_of_file* will be *true* when *still_to_read* = \(\langle \rangle\).
Using the partially specified Pascal File system on page 9, construct schemas for the following operations. Ensure that you include suitable English annotation for each of your mathematical statements.

a. A “Reset” operation that changes the mode to inspection, with the whole file still to be read and the content of the file being unchanged. (5 marks)

b. A “Read” operation that has the pre-conditions:
   - the mode must be inspection
   - the part of the file still to be read must not be empty

   And the post-conditions that ensure:
   - neither mode nor file are changed
   - any value returned is taken from the front of the file section still to be read

   (8 marks)

c. A “Rewrite” operation that makes the file empty. (4 marks)

d. A “Write” operation that ensure the mode is in generation throughout the process and allows the new data to be added to the end of the file. (8 marks)

Total: 25 marks