Sample questions on the Formal Methods part

Sample: Book-Work style questions

- Name and explain *one* reason why software systems are fundamentally different from mathematical axiom systems.

  [2 marks]

Samples: Working with semantics

- Prove that the + operator of regular expressions is associative, i.e., it holds that

  $$((A + B) + C) = (A + (B + C))$$

  for all regular expressions A, B, D over the same alphabet $\mathcal{A}$.

  Reminder: the denotational semantics of the + operator is defined as follows:

  $[\![(\varphi + \psi)]\!] \triangleq [\![\varphi]\!] \cup [\![\psi]\!]$.

  That is, $(\varphi + \psi)$ denotes the union of the denotations of φ and ψ.

  [2 marks]

- Give the operational semantics of `ATM4`:

```
ATM4 = Display.ready -> CardSlot.cardI
     -> KeyPad.pinE -> Display.menu
     ->  ( (Buttons.checkBalance -> Display.accountBalance
            -> CardSlot.cardO -> ATM4)
          []
            (Buttons.withdrawCash -> CardSlot.cardO
             -> CashSlot.cashO -> ATM4)
          )
```

  You might find the following firing rules to be useful:

  To this end, you might want to consider the following firing rules:

  Action Prefix:

$$\frac{}{(a \to P) \xrightarrow{a} P}$$

Equation:

$$\frac{}{PN \xrightarrow{\tau} P} \text{ if there is an equation } PN = P$$

External Choice:

$$\frac{P \xrightarrow{a} P'}{P \,\Box\, Q \xrightarrow{a} P'} \; a \neq \tau \qquad \frac{Q \xrightarrow{a} Q'}{P \,\Box\, Q \xrightarrow{a} Q'} \; a \neq \tau$$

An internal event leaves the choice unresolved:

$$\frac{P \xrightarrow{\tau} P'}{P \,\Box\, Q \xrightarrow{\tau} P' \,\Box\, Q} \qquad \frac{Q \xrightarrow{\tau} Q'}{P \,\Box\, Q \xrightarrow{\tau} P \,\Box\, Q'}$$

[4 marks]

Sample Question: Simple modelling in CSP

- Consider the following narrative:

  There is a rectangular 3x4 game board, i.e., there are 12 positions where a piece can be on the board. Initially, the piece is in position (0,0). The piece can move up, down, left, right - but only as long it remains on the game board.

  Write a CSP process capturing all possible moves that a piece can make, when initially placed in position (0,0).

[4 marks]

Sample Question: Explaining security protocols

- Consider the Needham-Schroeder protocol:

$$\begin{aligned}&(1)\ A \rightarrow B : \{N_A, A\}_{pk_B}\\ &(2)\ B \rightarrow A : \{N_A, N_B\}_{pk_A}\\ &(3)\ A \rightarrow B : \{N_B\}_{pk_B}\end{aligned}$$

  Explain each of its steps. Pay particular attention to the question which knowledge each participant has after each of the three steps of the protocol, and how this knowledge is justified by the rules of encryption and decryption and the original key distribution.

  [3 marks]

Challenging Question

There will be a challenging question, for which it is not possible to provide a sample: the challenging question will ask you to perform some 'new', non-mechanical task, where you shall apply your knowledge gained during formal methods unit.