Two hours

Question ONE is COMPULSORY

UNIVERSITY OF MANCHESTER  
SCHOOL OF COMPUTER SCIENCE

Verified Development

Date: Tuesday 14th January 2014
Time: 14:00 - 16:00

Please answer Question ONE  
and one other Question from the remaining TWO Questions available.

This is a CLOSED book examination

The use of electronic calculators is NOT permitted
1. **COMPULSORY**

   a) Briefly describe two advantages and two disadvantages of using model based development methods in industrial settings. (4 marks)

   b) Let \( X \) and \( Y \) be generic *Perfect* types. Let \( A \) be of type \( \text{map of}(X \rightarrow Y) \). Write down the definition of the \texttt{append} method that adds a pair \( a:\text{pair of}(X,Y) \) to \( A \). (4 marks)

   c) Write down the *Contract Refinement Proof Obligations*, and briefly describe what they mean in words. (4 marks)

   d) In the diagram below, the upper level is an abstract system and the lower level is a concrete system which is intended to be a contract refinement of it using the retrieve relation indicated by the dashed vertical lines. Write down the ways in which contract refinement fails. (4 marks)

   ![Diagram](image)

   e) In *Perfect*, suppose you have an integer variable \( z \). Assuming you also have a schema \texttt{!double} that doubles \( z \), write a *Perfect* property that says that \( z \) modulo 4 is 0 if you apply \texttt{!double} to \( z \) twice. Why can you not do the same when \( \text{twice/4} \) is replaced by \( a/2^a \) where \( a \) is a natural number valued variable? (4 marks)
2. A simple supermarket automated checkout system utilises a resource that maps a barcode to the expected weight and price of the relevant item. Once checking out starts, items are scanned one by one, and as they are bagged, the increase in bag weight is checked against the expected increment. The system can report an “Unexpected item” at any time, which requires a member of staff to clear the problem. Write a Perfect class to model this situation as simply as possible. There should be sensible invariants relating the checkout state to the current bag. There should be class members as below.

Data structures:  

Invariants:  

a) Add an item to the barcode inventory.  

b) Start checking out.  

c) Scan an item.  

d) Place an item in the bag.  

e) Unexpected item.  

f) Unexpected item clearance.  

g) Pay and finish.  

You can make reasonable simplifying assumptions, but any such assumptions must be clearly stated. Minor errors of Perfect syntax in your answer will not be penalised excessively, provided the intended meaning is clear.
3. Write a model of an ATM (automated teller machine) system with the following features. You insert your card. You enter your PIN (personal identification number). Your PIN is encrypted (using a loosely specified encryption function) and then checked against a database of encrypted PINs held by the bank. If your PIN checks, you can make a withdrawal (changing the account balance held by the bank), or change your PIN (changing the account’s encrypted PIN held by the bank). If you enter the wrong PIN, the card is rejected. Use different classes for the bank and the ATM. Your model should include the following.

Data structures: (3 marks)

Use of different classes for ATM and bank: (3 marks)

a) Enter card. (2 marks)

b) Enter PIN. (2 marks)

c) Reject bad PIN. (2 marks)

d) With good PIN, offer withdrawal or PIN change. (2 marks)

e) Withdraw cash. (3 marks)

e) Change PIN. (3 marks)

You can make reasonable simplifying assumptions, but any such assumptions must be clearly stated. Minor errors of Perfect syntax in your answer will not be penalised excessively, provided the intended meaning is clear.

END OF EXAMINATION