Final

Note

This is an open-book exam. You may consult any books, papers, or notes, but discussion with other students or seeking outside help is strictly forbidden.

Problems

1. (10 %) Prove, using *Natural Deduction* (in the sequent form), the validity of the following sequents.

   (a) $\vdash (A \to (B \wedge C)) \to ((A \to B) \wedge (A \to C))$

   (b) $\vdash (A \wedge (B \vee C)) \to ((A \wedge B) \vee (A \wedge C))$

2. (10 %) Prove, using Coq, the validity of the following sequents. Write down the proof scripts that you used to complete the proofs.

   (a) $\vdash (A \to (B \wedge C)) \to ((A \to B) \wedge (A \to C))$

   (b) $\vdash (A \wedge (B \vee C)) \to ((A \wedge B) \vee (A \wedge C))$

3. (20 %) A first-order theory for *groups* contains the following three axioms:

   - $\forall a \forall b \forall c (a \cdot (b \cdot c) = (a \cdot b) \cdot c)$. (Associativity)
   - $\forall a ((a \cdot e = a) \wedge (e \cdot a = a))$. (Identity)
   - $\forall a ((a \cdot a^{-1} = e) \wedge (a^{-1} \cdot a = e))$. (Inverse)

   Here $\cdot$ is the binary operation, e is a constant, called the identity, and $(\cdot)^{-1}$ is the inverse function which gives the inverse of an element. Let M denote the set of the three axioms. Prove, using *Natural Deduction* plus the derived rules in HW#2, the validity of the following sequents:

   (a) $M \vdash \forall a ((a^{-1})^{-1} = a)$.

   (b) $M \vdash \forall a \forall b ((a \cdot b)^{-1} = b^{-1} \cdot a^{-1})$.

4. The following program segment sorts an array A with n elements, indexed from 1 through n.

   S1: $i := 1$;
   S2: **while** $i < n$ **do**
   S3: $\quad j := i + 1$;
   S4: $\quad$ **while** $j \leq n$ **do**

```
S5:             if A[i] > A[j] then
S6:                 A[i], A[j] := A[j], A[i];
S7:             j := j + 1;
            od
S8:         i := i + 1;
        od
```

(a) (5 %) Give a pair of pre and post-conditions to describe as precisely as possible what the program segment achieves. You should assume only a simple assertion language with constants (1, etc.), basic arithmetic operations ($+, -$) and equality and inequality relations ($=, <, \cdots$). So, that means you will have to define the relations that would be convenient for writing the needed assertions.

(b) (15 %) Annotate the program segment into a proof outline that clearly shows the correctness of the program (according to the pre and post-conditions).

5. The following is a program for finding a sink in a directed graph of n nodes; a sink is a node with indegree $n-1$ and outdegree 0. The graph is represented by a two-dimensional boolean matrix M; $M[i,j] = true$ if and only if there is an edge from node i to node j (where $1 \leq i, j \leq n$).

```
S1:  i := 1;
S2:  j := 2;
S3:  next := 3;
S4:  while next ≤ n + 1 do
S5:      if M[i, j] then i := next
S6:      else j := next;
S7:      next := next + 1;
     od
S8:  if i = n + 1 then candidate := j
S9:  else candidate := i;
S10: wrong := false;
S11: k := 1;
S12: M[candidate, candidate] := false;
S13: while ¬wrong ∧ k ≤ n do
S14:     if M[candidate, k] then wrong := true;
S15:     if ¬M[k, candidate] then
S16:         if candidate ≠ k then wrong := true;
S17:     k := k + 1;
     od
```

(a) (5 %) Give a pair of pre and post-conditions to describe as precisely as possible what the program segment achieves. You should assume only a simple (typed) assertion language with boolean constants ($\{false, true\}$), integer constants (1, etc.), basic arithmetic operations $(+, -)$ and equality and inequality relations $(=, <, \cdots)$. So, that means you will have to define the relations that would be convenient for writing the needed assertions.

(b) (15 %) Annotate the program segment into a proof outline that clearly shows the correctness of the program (according to the pre and post-conditions).

6. (20 %) Refinement is one of the most fundamental concepts in formal software development.

   (a) Explain the concept of refinement in words (without logical notations).

   (b) How is refinement formulated in Z or B (choose one of them)? Be sure to relate the formulation to the preceding verbal description.

   Please try to be brief, but to the point.