Final

Note

This is an open-book exam. You may consult any book, paper, note, or on-line resource, but discussion with others (in person or via a network) is strictly forbidden.

Problems

1. (20 %) Prove, using *Natural Deduction* (in the sequent form), the validity of the following sequents.

   (a) $\vdash A \vee \neg A$

   (b) $\neg\exists x(\neg A(x)) \vdash \forall x A(x)$

2. (20 %) Consider the Coq formalization of group theory done earlier in one of our homework assignments. Prove the following two additional lemmas that concern commutativity. Please write down the proof scripts and also email the corresponding self-contained .v file to the instructor.

```
Definition comm := forall a b : G, a o b = b o a.

Lemma aa :
  (forall a : G, a o a = e) -> comm.

Lemma aabb :
  comm <-> forall a b : G, a o a o b o b = a o b o a o b.
```

3. (30 %) 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
S6:          i := next
         else
S7:          j := next;
```

```
S8:       next := next + 1;
          od
S9:   if i = n + 1 then
S10:      candidate := j
          else
S11:      candidate := i;
S12:  wrong := false;
S13:  k := 1;
S14:  M[candidate, candidate] := false;
S15:  while ¬wrong ∧ k ≤ n do
S16:      if M[candidate, k] then
S17:          wrong := true;
S18:      if ¬M[k, candidate] then
S19:          if candidate ≠ k then
S20:              wrong := true;
S21:      k := k + 1;
          od
```

Annotate the program segment into a standard proof outline that clearly shows the partial correctness of the program. 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.

4. (10 %) Prove this equivalence: $wlp(S_1; S_2, q) \leftrightarrow wlp(S_1, wlp(S_2, q))$.

5. (20 %) Prove the partial correctness of the following program using the Owicki-Gries method. Variables T, s_0, and s_1 are of the same type.

$$
\begin{array}{l}
\{true\} \\
acc := 0; \\
\left[\begin{array}{lcl}
T := 0; & & T := 1; \\
\textbf{await } T \neq 0; & & \textbf{await } T \neq 1; \\
s_0 := acc; & \| & s_1 := acc; \\
acc := s_0 + 1; & & acc := s_1 + 1; \\
T := 0; & & T := 1;
\end{array}\right] \\
\{acc = 2\}
\end{array}
$$