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 $\vdash A \vee \neg A$. Try to find a proof as short as possible.

2. (20 %) Prove, using *Natural Deduction* (in the sequent form), the validity of the following sequents. You may assume $\vdash A \vee \neg A$ if it makes the proof shorter and simpler.

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

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

3. (20 %) The following program segment finds the maximum element of an array A with n elements.

   S1: $i := 0$;
   S2: $max := A[i]$;
   S3: **while** $i < n - 1$ **do**
   S4: $i := i + 1$;
   S5: **if** $max < A[i]$ **then**
   S6: $max := A[i]$;
   od

   (a) 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 $(0, 1)$, 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) Annotate the program segment into a proof outline that clearly shows the total correctness of the program (according to the pre and post-conditions).

4. (20 %) Prove the partial correctness of the following program using the Owicki-Gries method.

$\{true\}$
$acc := 0;$
$Q_0, Q_1 := false, false;$

$$
\left[\begin{array}{ll}
Q_0 := true; & Q_1 := true; \\
t_0 := T_0; & t_1 := T_1; \\
T_1 := t_0; & T_0 := \overline{t_1}; \\
\textbf{if } Q_1 \textbf{ then} & \textbf{if } Q_0 \textbf{ then} \\
\quad \textbf{await } T_0 \neq t_0 & \quad \textbf{await } T_1 \neq t_1 \\
\textbf{fi}; & \| \quad \textbf{fi}; \\
s_0 := acc; & s_1 := acc; \\
acc := s_0 + 1; & acc := s_1 + 1; \\
Q_0 := false; & Q_1 := false; \\
t_0 := T_0; & t_1 := T_1; \\
T_1 := t_0 & T_0 := \overline{t_1}
\end{array}\right]
$$

$\{acc = 2\}$

5. (30 %) Solve the following problems for fair transition systems, which we have studied as a model for concurrent reactive systems. You may consider only justice, and ignore compassion, constraints.

   (a) Give a suitable formal definition for *open* fair transition systems, or fair transition modules, where the set of variables is partitioned into *in* and *out* variables. A system reads from, but does not write on, its *in* variables. The environment of an open system reads from, but does not write on, the *out* variables of the system. The computation of an open system should take into account the interference from its environment.

   (b) Define a parallel composition operation "$\|$"on two open fair transition systems that follows the interleaving model of concurrency. The parallel composition of two open systems is another open system. Be careful about the condition under which two systems may be composed.

   (c) For two systems S_1 and S_2 that are composable, prove that the set of computations of $S_1 \,\|\, S_2$, namely $Comp(S_1 \,\|\, S_2)$, is the intersection of $Comp(S_1)$ and $Comp(S_2)$. (Note: adjust your definitions in the preceding sub-problems so that this compositional property holds.)