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. 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) (10 %) $\neg(A \wedge B) \vdash \neg A \vee \neg B$

   (b) (10 %) $\forall x A(x) \vdash \neg \exists x(\neg A(x))$

3. The program segment below computes the greatest common divisor of the two numbers initially stored in variables x and y.

   while $x \neq 0$ and $y \neq 0$ do
       if $x < y$ then $x, y := y, x$ fi;
       $x := x - y$
   od

   (a) (10 %) 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 $(+, -, \times,$ without division) and equality and inequality relations. So, that means you will have to define the relations that would be convenient for writing the needed assertions.

   (b) (10 %) Annotate the program segment into a proof outline that clearly shows the partial correctness of the program (according to the pre and post-conditions).

4. (20 %) Assuming that the leads-to operator in UNITY is defined without the disjunction rule, prove the following derived rule.

$$\frac{p \mapsto q \qquad p' \mapsto q'}{p \vee p' \mapsto q \vee q'}$$

5. (30 %) Prove the partial correctness of the following program using the Owicki-Gries method.

$$
\begin{array}{l}
\{\mathit{true}\} \\
\mathit{acc} := 0; \\
Q_0, Q_1 := \mathit{false}, \mathit{false}; \\
\left[\begin{array}{lcl}
Q_0 := \mathit{true}; & & Q_1 := \mathit{true}; \\
t_0 := T_0; & & t_1 := T_1; \\
T_1 := t_0; & & T_0 := \overline{t_1}; \\
\textbf{if } Q_1 \textbf{ then} & & \textbf{if } Q_0 \textbf{ then} \\
\quad \textbf{await } T_0 \neq t_0 & & \quad \textbf{await } T_1 \neq t_1 \\
\textbf{fi}; & \| & \textbf{fi}; \\
s_0 := \mathit{acc}; & & s_1 := \mathit{acc}; \\
\mathit{acc} := s_0 + 1; & & \mathit{acc} := s_1 + 1; \\
Q_0 := \mathit{false}; & & Q_1 := \mathit{false}; \\
t_0 := T_0; & & t_1 := T_1; \\
T_1 := t_0 & & T_0 := \overline{t_1}
\end{array}\right] \\
\{\mathit{acc} = 2\}
\end{array}
$$