Final

Note

This is an open-book exam. Problems 2 and 4 require electronic submission. Please pack all files for the two problems in one single .zip file and email it to the instructor (`tsay@ntu.edu.tw`). 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) $p \rightarrow q \vdash \neg q \rightarrow \neg p$

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

2. (20 %) Prove the following two lemmas using Coq. (Hint: for constructing the proofs, most needed lemmas may be found in the `ZArith.BinInt` library.)

```
Require Import ZArith.

Open Scope Z_scope.

Lemma div_minus_l: forall a b c: Z, (b > c) -> (a | (b - c)) ->
                   (a | c) -> (a | b).
Lemma div_minus_r: forall a b c: Z, (a | b) -> (a | c) ->
                   (b > c) -> (a | (b - c)).
```

3. (10 %) Why the law of Distributivity of Disjunction, namely $wp(S, Q_1) \vee wp(S, Q_2) \equiv wp(S, Q_1 \vee Q_2)$, works only for deterministic S but not nondeterministic S? Please explain by an example.

4. (30 %) The following C function implements a simplified variant of the Euclid's algorithm that computes the GCD of two positive integers. Annotate the code to show its behavior (including particularly a suitable function contract) and prove correctness of your annotation using Frama-C.

ACSL predicate lemma

```
int myEuclid(int m, int n) {
  int x,y,tmp;
```

```
  x = m;
  y = n;
  while (x != y) {
    if (x < y) {
      tmp = x;
      x = y;
      y = tmp;
    }
    x = x - y;
  }
  return x;
}
```

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.

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