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) $\neg q \rightarrow \neg p \vdash p \rightarrow q$

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

2. (20 %) Consider an alternative to the Coq formalization of group theory done earlier in one of our homework assignments. Here the existence of an inverse (both left and right inverse) for every element is axiomatized via a function that takes an element and gives the inverse of the element. Your task is to reprove the two lemmas stating the left and the right elimination rules and also prove two additional lemmas concerning commutativity. Please write down the proof scripts on the exam paper and also email the corresponding self-contained .v file to the instructor.

```
Section Group.

Variable G : Set.
Variable op : G -> G -> G.
Infix "o" := op (at level 35, right associativity).
Variable e : G.
Variable inv : G -> G.
Notation "a -" := (inv a) (at level 25, left associativity).

Axiom assoc : forall a b c : G, a o (b o c) = (a o b) o c.
Axiom unit_l : forall a : G, e o a = a.
Axiom unit_r : forall a : G, a o e = a.
Axiom inv_l : forall a : G, a- o a = e.
Axiom inv_r : forall a : G, a o a- = e.
```

```
Lemma elim_l :
  forall a b c, c o a =  c o b -> a = b.

Lemma elim_r :
  forall a b c, a o c = b o c -> a = b.

Lemma comm_aabb :
  (forall a b : G, a o b = b o a) ->
  forall a b : G, a o a o b o b = a o b o a o b.

Lemma aabb_comm :
  (forall a b : G, a o a o b o b = a o b o a o b) ->
  forall a b : G, a o b = b o a.

End Group.
```

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. (20 %) The following simple C function finds a largest entry in an array of integers. Annotate the code to show its behavior (including particularly a suitable function contract) and prove correctness of your annotation using Frama-C. Please write down the annotations on the exam paper and also email the corresponding self-contained .c file to the instructor.

```
int max(int* a, int n)
{ int m, i;

  m = 0;
  for (i=1; i<n; i++)
    if (a[i] > a[m])
      m = i;
  return m;
}
```

5. (10 %) Can the formation rules for proof outlines produce something like the following? Why or why not? Please explain.

$$\ldots S_1;\ \{P_1\}\ \{P_2\}\ \{P_3\}\ S_2; \ldots$$

6. (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.

$$\{acc = 0\}$$

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

$$\{acc = 2\}$$