Homework Assignment #3

Due Time/Date

2:20PM Wednesday, October 19, 2022. Late submission will be penalized by 20% for each working day overdue.

How to Submit

Please pack all your answers in one single .v file. Name your .v file according to this pattern: "b097050xx-hw3.v". Upload the file to the NTU COOL site for Software Specification and Verification 2022. You may discuss the problems with others, but copying answers is strictly forbidden.

Problems

All the problems must be solved using Coq. In the problem statements, we assume the binding powers of the logical connectives and the entailment symbol decrease in this order: $\neg$, $\{\forall, \exists\}$, $\{\wedge, \vee\}$, $\rightarrow$, $\leftrightarrow$, $\vdash$.

1. (30 points) Formalize the following sequents and prove their validity:

   (a) $\vdash (p \wedge q \rightarrow r) \rightarrow (p \rightarrow (q \rightarrow r))$

   (b) $p \vee q \rightarrow r \vdash (p \rightarrow r) \wedge (q \rightarrow r)$

2. (30 points) Formalize the following sequents and prove their validity:

   (a) $\vdash \exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y)$

   (b) $\forall x(P(x) \rightarrow Q(x)) \vdash \forall x P(x) \rightarrow \forall x Q(x)$

3. (40 points) A first-order theory for *groups* contains the following three axioms:

   - $\forall a \forall b \forall c(a \cdot (b \cdot c) = (a \cdot b) \cdot c)$. (Associativity)
   - $\forall a((a \cdot e = a) \wedge (e \cdot a = a))$. (Identity)
   - $\forall a(\exists b((a \cdot b = e) \wedge (b \cdot a = e))$. (Inverse)

   Here $\cdot$ is the binary operation and e is a constant, called the identity. Let M denote the set of the three axioms. Formalize the following sequent and prove its validity:

   $M \vdash \forall a \forall b \forall c((a \cdot b = a \cdot c) \rightarrow b = c)$. (Hint: a typical proof in algebra books is the following: $b = e \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c) = (a^{-1} \cdot a) \cdot c = e \cdot c = c$, where $(\cdot)^{-1}$ is the inverse function giving the inverse of an element.)