Homework Assignment #2

Due Time/Date

2:20PM Wednesday, September 27, 2023. Late submission will be penalized by 20% for each working day overdue.

How to Submit

Please write or type your answers on A4 (or similar size) paper. Put your completed homework on the instructor's desk before the class starts. For late submissions, please drop them in Yih-Kuen Tsay's mail box on the first floor of Management Building 2. You may discuss the problems with others, but copying answers is strictly forbidden.

Problems

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. (20 points) In HW#0, we have investigated Algorithm **originalEuclid** that computes the greatest common divisor of two input numbers which are assumed to be positive integers. We are now concerned with a precise statement of the correctness requirement on its output. Please write a first-order formula describing the requirement on the output of **originalEuclid**, using the first-order language $\{+, -, \times, 0, 1, <\}$, which includes symbols for the usual arithmetic functions ($+$, $-$, and $\times$), constants (0 and 1), and predicates ($<$ and $\leq$) for integers; "$=$" is implicitly assumed to be a binary predicate. That is, write a defining formula for a predicate, say $isGCD$, such that $isGCD(m, n, \textbf{originalEuclid}(m, n))$ holds if **originalEuclid** is correct, assuming that both m and n are greater than 0.

   Note: you certainly would bring up the notion of "a divides b", perhaps in the form of a predicate $divides(a, b)$, or alternatively $a \mid b$, but this is not directly available in the allowed language and you would need to spell out the defining formula.

2. (20 points) Prove, using *Natural Deduction*, the validity of the following sequents:

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

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

3. (20 points) Prove, using *Natural Deduction* for the first-order logic with equality ($=$), that $=$ is an equivalence relation between terms, i.e., the following are valid sequents, in

addition to the obvious "$\vdash t = t$" (Reflexivity), which follows from the $=$-Introduction rule.

(a) $t_2 = t_1 \vdash t_1 = t_2$ (Symmetry)

(b) $t_1 = t_2, t_2 = t_3 \vdash t_1 = t_3$ (Transitivity)

4. (20 points) Taking the preceding valid sequents as axioms, prove using *Natural Deduction* the following derived rules for equality.

(a) $$\frac{\Gamma \vdash t_2 = t_1}{\Gamma \vdash t_1 = t_2}\ (= \textit{Symmetry})$$

(b) $$\frac{\Gamma \vdash t_1 = t_2 \qquad \Gamma \vdash t_2 = t_3}{\Gamma \vdash t_1 = t_3}\ (= \textit{Transitivity})$$

5. (20 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)
- $\forall a ((a \cdot a^{-1} = e) \wedge (a^{-1} \cdot a = e))$. (Inverse)

Here $\cdot$ is the binary operation, e is a constant, called the identity, and $(\cdot)^{-1}$ is the inverse function which gives the inverse of an element. Let M denote the set of the three axioms subsequently, for brevity.

Prove, using *Natural Deduction* plus the derived rules in the preceding problem, the validity of the following sequent:

$M \vdash \forall a \forall b \forall c (((a \cdot b = e) \wedge (b \cdot a = e) \wedge (a \cdot c = e) \wedge (c \cdot a = e)) \to b = c)$, which says that every element has a unique inverse.

(Hint: a typical proof in algebra books is the following: $b = b \cdot e = b \cdot (a \cdot c) = (b \cdot a) \cdot c = e \cdot c = c$.)