Suggested Solutions for Homework Assignment #2

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.

   Solution. Let $isGCD(x, y, z)$ be

   $$z > 0 \wedge divides(z, x) \wedge divides(z, y) \wedge \forall w(divides(w, x) \wedge divides(w, y) \rightarrow divides(w, z)),$$

   where $divides(a, b)$ denotes that a divides b, formally $\exists q(b = a \times q)$.

   □

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

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

   Solution. Assume w does not occur free either in $P(x)$ or in $Q(x)$.

   $$\dfrac{\dfrac{\dfrac{\alpha \qquad \dfrac{\dfrac{}{\forall x(P(x) \rightarrow Q(x)), \forall xP(x) \vdash \forall xP(x)}\,(Hyp)}{\forall x(P(x) \rightarrow Q(x)), \forall xP(x) \vdash P(w)}\,(\forall E)}{\forall x(P(x) \rightarrow Q(x)), \forall xP(x) \vdash Q(w)}\,(\rightarrow E)}{\forall x(P(x) \rightarrow Q(x)), \forall xP(x) \vdash \forall xQ(x)}\,(\forall I)}{\forall x(P(x) \rightarrow Q(x)) \vdash \forall xP(x) \rightarrow \forall xQ(x)}\,(\rightarrow I)$$

   α :

   $$\dfrac{\dfrac{}{\forall x(P(x) \rightarrow Q(x)), \forall xP(x) \vdash \forall x(P(x) \rightarrow Q(x))}\,(Hyp)}{\forall x(P(x) \rightarrow Q(x)), \forall xP(x) \vdash P(w) \rightarrow Q(w)}\,(\forall E)$$

   □

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

   Solution. Assume both w and z do not occur free in $P(x, y)$.

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\exists x\forall y P(x,y) \vdash \exists x\forall y P(x,y)}\,(Hyp) \qquad \dfrac{\dfrac{\dfrac{}{\exists x\forall y P(x,y), \forall y P(z,y) \vdash \forall y P(z,y)}\,(Hyp)}{\exists x\forall y P(x,y), \forall y P(z,y) \vdash P(z,w)}\,(\forall E)}{\exists x\forall y P(x,y), \forall y P(z,y) \vdash \exists x P(x,w)}\,(\exists I)}{\exists x\forall y P(x,y) \vdash \exists x P(x,w)}\,(\exists E)}{\exists x\forall y P(x,y) \vdash \forall y\exists x P(x,y)}\,(\forall I)}{\vdash \exists x\forall y P(x,y) \to \forall y\exists x P(x,y)}\,(\to I)
$$

□

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)
   Solution.

$$
\dfrac{\dfrac{}{t_2 = t_1 \vdash t_2 = t_1}\,(Hyp) \qquad \dfrac{}{t_2 = t_1 \vdash t_2 = t_2}\,(= I)}{t_2 = t_1 \vdash t_1 = t_2}\,(= E)
$$

□

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

$$
\dfrac{\dfrac{}{t_1 = t_2, t_2 = t_3 \vdash t_2 = t_3}\,(Hyp) \qquad \dfrac{}{t_1 = t_2, t_2 = t_3 \vdash t_1 = t_2}\,(Hyp)}{t_1 = t_2, t_2 = t_3 \vdash t_1 = t_3}\,(= E)
$$

□

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

   (a) $\dfrac{\Gamma \vdash t_2 = t_1}{\Gamma \vdash t_1 = t_2}\,(= Symmetry)$
   Solution.

$$
\dfrac{\dfrac{\dfrac{}{\Gamma, t_2 = t_1 \vdash t_1 = t_2}\,(Axiom(Symmetry))}{\Gamma \vdash t_2 = t_1 \to t_1 = t_2}\,(\to I) \qquad \Gamma \vdash t_2 = t_1}{\Gamma \vdash t_1 = t_2}\,(\to E)
$$

□

   (b) $\dfrac{\Gamma \vdash t_1 = t_2 \qquad \Gamma \vdash t_2 = t_3}{\Gamma \vdash t_1 = t_3}\,(= Transitivity)$
   Solution.

$$
\dfrac{\dfrac{\alpha \qquad \Gamma \vdash t_1 = t_2}{\Gamma \vdash t_2 = t_3 \to t_1 = t_3}\,(\to E) \qquad \Gamma \vdash t_2 = t_3}{\Gamma \vdash t_1 = t_3}\,(\to E)
$$

   α :

$$
\dfrac{\dfrac{\dfrac{}{\Gamma, t_1 = t_2, t_2 = t_3 \vdash t_1 = t_3}\,(Axiom(Transitivity))}{\Gamma, t_1 = t_2 \vdash t_2 = t_3 \to t_1 = t_3}\,(\to I)}{\Gamma \vdash t_1 = t_2 \to (t_2 = t_3 \to t_1 = t_3)}\,(\to I)
$$

$\square$

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:

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

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

   Solution. We use N to denote $x \cdot y = e \wedge y \cdot x = e \wedge x \cdot z = e \wedge z \cdot x = e$, i.e., the assumption in the target formula with the universally quantified variables replaced by fresh free variables.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\alpha \quad \beta}{M, N \vdash y = y \cdot (x \cdot z)}\,(= \textit{Transitivity}) \qquad \dfrac{\gamma \quad \delta}{M, N \vdash y \cdot (x \cdot z) = z}\,(= \textit{Transitivity})}{M, N \vdash y = z}\,(= \textit{Transitivity})}{M \vdash (x \cdot y = e \wedge y \cdot x = e \wedge x \cdot z = e \wedge z \cdot x = e) \rightarrow y = z}\,(\rightarrow I)}{M \vdash \forall c ((x \cdot y = e \wedge y \cdot x = e \wedge x \cdot c = e \wedge c \cdot x = e) \rightarrow y = c)}\,(\forall I)}{M \vdash \forall b \forall c ((x \cdot b = e \wedge b \cdot x = e \wedge x \cdot c = e \wedge c \cdot x = e) \rightarrow b = c)}\,(\forall I)}{M \vdash \forall a \forall b \forall c ((a \cdot b = e \wedge b \cdot a = e \wedge a \cdot c = e \wedge c \cdot a = e) \rightarrow b = c)}\,(\forall I)$$

α :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{M, N \vdash \forall a (a \cdot e = a \wedge e \cdot a = a)}\,(\textit{Hyp})}{M, N \vdash y \cdot e = y \wedge e \cdot y = y}\,(\forall E)}{M, N \vdash y \cdot e = y}\,(\wedge E_1)}{M, N \vdash y = y \cdot e}\,(= \textit{Symmetry})$$

β :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{M, N \vdash x \cdot y = e \wedge (y \cdot x = e \wedge (x \cdot z = e \wedge z \cdot x = e))}\,(\textit{Hyp})}{M, N \vdash y \cdot x = e \wedge (x \cdot z = e \wedge z \cdot x = e)}\,(\wedge E_2)}{M, N \vdash x \cdot z = e \wedge z \cdot x = e}\,(\wedge E_2)}{M, N \vdash x \cdot z = e}\,(\wedge E_1) \qquad \dfrac{}{M, N \vdash y \cdot (x \cdot z) = y \cdot (x \cdot z)}\,(= I)}{M, N \vdash y \cdot e = y \cdot (x \cdot z)}\,(= E)$$

$\gamma:$

$$\dfrac{\dfrac{\dfrac{\overline{M, N \vdash \forall a \forall b \forall c (a \cdot (b \cdot c) = (a \cdot b) \cdot c)}\ (Hyp)}{M, N \vdash \forall b \forall c (y \cdot (b \cdot c) = (y \cdot b) \cdot c)}\ (\forall E)}{M, N \vdash \forall c (y \cdot (x \cdot c) = (y \cdot x) \cdot c)}\ (\forall E)}{M, N \vdash y \cdot (x \cdot z) = (y \cdot x) \cdot z}\ (\forall E)$$

$\delta:$

$$\dfrac{\dfrac{\text{similar to } \beta}{M, N \vdash (y \cdot x) \cdot z = e \cdot z} \quad \dfrac{\text{similar to } \alpha}{M, N \vdash e \cdot z = z}}{M, N \vdash (y \cdot x) \cdot z = z}\ (= \mathit{Transitivity})$$

□