Suggested Solutions for Homework Assignment #2

We assume the binding powers of the logical connectives and the entailment symbol decrease in this order: $\neg$, $\{\forall, \exists\}$, $\{\wedge, \vee\}$, $\rightarrow$, $\leftrightarrow$, $\vdash$. Note that $\rightarrow$ associates to the right, i.e., $p \rightarrow q \rightarrow r$ should be parsed as $p \rightarrow (q \rightarrow r)$.

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 $\mathit{isGCD}(m, n, \textbf{originalEuclid}(m, n))$ 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 $\mathit{divides}(a, b)$, 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 $\mathit{isGCD}(x, y, z)$ be

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

   where $\mathit{divides}(a, b)$ 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) $\forall x(P(x) \rightarrow Q(x)) \vdash \exists x P(x) \rightarrow \exists x Q(x)$

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

   $$\dfrac{\dfrac{\dfrac{}{\forall x(P(x) \rightarrow Q(x)), \exists x P(x) \vdash \exists x P(x)}\,(Hyp) \quad \dfrac{\alpha}{\forall x(P(x) \rightarrow Q(x)), P(y) \vdash \exists x Q(x)}\,(\exists I)}{\forall x(P(x) \rightarrow Q(x)), \exists x P(x) \vdash \exists x Q(x)}\,(\exists E)}{\forall x(P(x) \rightarrow Q(x)) \vdash \exists x P(x) \rightarrow \exists x Q(x)}\,(\rightarrow I)$$

   α :

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

   □

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

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

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

□

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.

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

   □

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

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

   Alternatively (without the axiom of *Symmetry* or *Transitivity*),

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

   □

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

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

Alternatively (without the axiom of *Symmetry* or *Transitivity*),

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

□

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:

   $M \vdash \forall a \forall b \forall c((b \cdot a = c \cdot a) \to b = c)$,

   which states the right cancellation property.

   (Hint: a typical proof in algebra books is the following: $b = b \cdot e = b \cdot (a \cdot a^{-1}) = (b \cdot a) \cdot a^{-1} = (c \cdot a) \cdot a^{-1} = c \cdot (a \cdot a^{-1}) = c \cdot e = c$.)

   Solution.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\alpha \qquad \beta}{M, y \cdot x = z \cdot x \vdash y = (y \cdot x) \cdot x^{-1}}\,(= Transitivity) \qquad \dfrac{\gamma \qquad \delta}{M, y \cdot x = z \cdot x \vdash (y \cdot x) \cdot x^{-1} = z}\,(= Transitivity)}{M, y \cdot x = z \cdot x \vdash y = z}\,(= Transitivity)}{M \vdash (y \cdot x = z \cdot x) \to y = z}\,(\to I)}{M \vdash \forall c((y \cdot x = c \cdot x) \to y = c)}\,(\forall I)}{M \vdash \forall b \forall c((b \cdot x = c \cdot x) \to b = c)}\,(\forall I)}{M \vdash \forall a \forall b \forall c((b \cdot a = c \cdot a) \to b = c)}\,(\forall I)$$

α :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{M, y \cdot x = z \cdot x \vdash \forall a(a \cdot e = a \wedge e \cdot a = a)}\,(Hyp)}{M, y \cdot x = z \cdot x \vdash y \cdot e = y \wedge e \cdot y = y}\,(\forall E)}{M, y \cdot x = z \cdot x \vdash y \cdot e = y}\,(\wedge E_1) \qquad \dfrac{\varepsilon \qquad \zeta}{M, y \cdot x = z \cdot x \vdash y \cdot e = y \cdot (x \cdot x^{-1})}\,(= E)}{M, y \cdot x = z \cdot x \vdash y = y \cdot e}\,(= Symmetry)}{M, y \cdot x = z \cdot x \vdash y = y \cdot (x \cdot x^{-1})}\,(= Transitivity)$$

β :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{M, y \cdot x = z \cdot x \vdash \forall a \forall b \forall c (a \cdot (b \cdot c) = (a \cdot b) \cdot c)}\,(Hyp)}{M, y \cdot x = z \cdot x \vdash \forall b \forall c (y \cdot (b \cdot c) = (y \cdot b) \cdot c)}\,(\forall E)}{M, y \cdot x = z \cdot x \vdash \forall c (y \cdot (x \cdot c) = (y \cdot x) \cdot c)}\,(\forall E)}{M, y \cdot x = z \cdot x \vdash y \cdot (x \cdot x^{-1}) = (y \cdot x) \cdot x^{-1}}\,(\forall E)$$

γ :

$$\dfrac{\dfrac{\gamma_1 \qquad \gamma_2}{M, y \cdot x = z \cdot x \vdash (y \cdot x) \cdot x^{-1} = (z \cdot x) \cdot x^{-1}}\,(= E) \qquad \dfrac{\dfrac{\text{similar to } \beta}{M, y \cdot x = z \cdot x \vdash z \cdot (x \cdot x^{-1}) = (z \cdot x) \cdot x^{-1}}}{M, y \cdot x = z \cdot x \vdash (z \cdot x) \cdot x^{-1} = z \cdot (x \cdot x^{-1})}\,(= \textit{Symmetry})}{M, y \cdot x = z \cdot x \vdash (y \cdot x) \cdot x^{-1} = z \cdot (x \cdot x^{-1})}\,(= \textit{Transitivity})$$

δ :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{M, y \cdot x = z \cdot x \vdash \forall a (a \cdot a^{-1} = e \wedge a^{-1} \cdot a = e)}\,(Hyp)}{M, y \cdot x = z \cdot x \vdash x \cdot x^{-1} = e \wedge x^{-1} \cdot x = e}\,(\forall E)}{M, y \cdot x = z \cdot x \vdash x \cdot x^{-1} = e}\,(\wedge E_1)}{M, y \cdot x = z \cdot x \vdash e = x \cdot x^{-1}}\,(= \textit{Symmetry}) \qquad \dfrac{\text{similar to the left branch of } \alpha}{M, y \cdot x = z \cdot x \vdash z \cdot e = z}}{M, y \cdot x = z \cdot x \vdash z \cdot (x \cdot x^{-1}) = z}\,(= E)$$

γ_1 :

$$\dfrac{}{M, y \cdot x = z \cdot x \vdash y \cdot x = z \cdot x}\,(Hyp)$$

γ_2 :

$$\dfrac{}{M, y \cdot x = z \cdot x \vdash (y \cdot x) \cdot x^{-1} = (y \cdot x) \cdot x^{-1}}\,(= I)$$

□