COM3412: Logic and Computation

Solutions to Exercise on Peano Arithmetic

2nd March 2009

1. Addition is associative: $\forall x \forall y \forall z(x + (y + z) = (x + y) + z)$.

   - **Base Case** ($z = 0$)

     $$\begin{array}{rcll} x + (y + 0) & = & x + y & \text{(A1, } x/y\text{)} \\ & = & (x + y) + 0 & \text{(A1, } x/x + y\text{)} \end{array}$$

   - **Induction Step** (from $z = a$ to $z = sa$)
     From Induction Hypothesis $x + (y + a) = (x + y) + a$ we derive $x + (y + sa) = (x + y)$.

     $$\begin{array}{rcll} x + (y + sa) & = & x + s(y + a) & \text{(A2, } x/y, y/a\text{)} \\ & = & s(x + (y + a)) & \text{(A2, } x/x, y/y + a\text{)} \\ & = & s((x + y) + a) & \text{(IH)} \\ & = & (x + y) + sa & \text{(A2, } x/x + y, y/a\text{)} \end{array}$$

2. Cancellation by subtraction: $\forall x \forall y \forall z(x + z = y + z \rightarrow x = y)$.

   - **Base Case** ($z = 0$)

     $$x + 0 = y + 0 \quad \rightarrow \quad x = y \quad \text{(A1 twice, } x/x \text{ and } x/y\text{)}$$

   - **Induction Step** (from $z = a$ to $z = sa$)
     From Induction Hypothesis $x + a = y + a \rightarrow x = y$ we derive $x + sa = y + sa \rightarrow x = y$.

     $$\begin{array}{rcll} x + sa = y + sa & \rightarrow & s(x + a) = s(y + a) & \text{(A2 twice, } x/x \text{ and } x/y\text{)} \\ & \rightarrow & x + a = y + a & \text{(S2, } x/x + a, x/y + a\text{)} \\ & \rightarrow & x = y & \text{(from induction hypothesis)} \end{array}$$

3. Pre-multiplication by zero: $\forall x(0 * x = 0)$.
   Solution currently unavailable.

4. Pre-multiplication by a successor: $\forall x \forall y(sx * y = (x * y) + y)$.
   Solution currently unavailable.

5. Multiplication is commutative: $\forall x \forall y(x * y = y * x)$.
   Solution currently unavailable.

6. Multiplication is distributive over addition: $\forall x \forall y \forall z(x * (y + z) = (x * y) + (x * z))$.

   - **Base Case** ($z = 0$)

     $$\begin{array}{rcll} x * (y + 0) & = & x * y & \text{(A1, } x/0\text{)} \\ & = & x * y + 0 & \text{(A1, } x/x * y\text{)} \\ & = & x * y + x * 0 & \text{(M1, } x/x\text{)} \end{array}$$

- **Induction Step** (from $z = a$ to $z = sa$)
From Induction Hypothesis $x*(y+a) = x*y+x*a$ we derive $x*(y+sa) = x*y+x*sa$.

$$\begin{aligned} x*(y+sa) &= x*s(y+a) && \text{(A2, } x/y, y/a) \\ &= x*(y+a)+x && \text{(M2, } x/x, y/y+a) \\ &= (x*y+x*a)+x && \text{(IH)} \\ &= x*y+(x*a+x) && \text{(Question 1 above)} \\ &= x*y+x*sa && \text{(M2, } x/x, y/a) \end{aligned}$$

7. Multiplication is associative: $\forall x \forall y \forall z(x*(y*z) = (x*y)*z)$.

- **Base Case** ($z = 0$)

$$\begin{aligned} x*(y*0) &= x*0 && \text{(M1, } x/y) \\ &= 0 && \text{(M1, } x/x) \\ &= (x*y)*0 && \text{(M1, } x/x*y) \end{aligned}$$

- **Induction Step** (from $z = a$ to $z = sa$)
From Induction Hypothesis $x*(y*a) = (x*y)*a$ we derive $x*(y*sa) = (x*y)*sa$.

$$\begin{aligned} x*(y*sa) &= x*((y*a)+y) && \text{(M2, } x/y, y/a) \\ &= (x*(y*a))+(x*y) && \text{(From q.6, } x/x, y/(y*a), z/y) \\ &= ((x*y)*a)+(x*y) && \text{(From Induction Hypothesis)} \\ &= (x*y)*sa && \text{(M2, } x/(x*y), y/a) \end{aligned}$$

8. Divisors of zero: $\forall x \forall y(x*y = 0 \rightarrow x = 0 \vee y = 0)$.

- **Base Case** ($y = 0$)

$x*0 = 0 \quad \rightarrow \quad x = 0 \vee 0 = 0$ (True since $0 = 0$ — which is an instance of the identity axiom $\forall x(x = x)$.)

- **Induction Step** (from $y = a$ to $y = sa$)

$$\begin{aligned} x*sa = 0 &\rightarrow (x*a)+x = 0 && \text{(M1, } x/x, y/a) \\ &\rightarrow x = 0 && \text{(Since if } x = sb\text{, say, } (x*a)+x = s((x*a)+b) \neq 0) \\ &\rightarrow x = 0 \vee sa = 0 && \text{(By } \vee\text{-introduction)} \end{aligned}$$

Note that we didn't need to use the induction hypothesis! This is the exception rather than the rule.

9. Cancellation by division: $\forall x \forall y \forall z(x*sz = y*sz \rightarrow x = y)$.
This one is tricky, and merits a somewhat different style of answer. We'll do the induction with respect to x. But the predicate we substitute for Φ in $\mathbf{Ind}$ has to contain a quantifier (in all previous cases we used arbitrary constants for the other variables, but this doesn't seem to work here). Thus the instance of $\mathbf{Ind}$ we are using is

(**1**)
$$\begin{aligned} &\forall y(0*sz = y*sz \rightarrow 0 = y) \wedge \\ &\forall x(\forall y(x*sz = y*sz \rightarrow x = y) \rightarrow \forall y(sx*sz = y*sz \rightarrow sx = y)) \rightarrow \\ &\quad \forall x \forall y(x*sz = y*sz \rightarrow x = y) \end{aligned}$$

The base case is now readily proved:

$$\begin{aligned} 0*sz = y*sz &\rightarrow 0 = y*sz && \text{(Question 3 above)} \\ &\rightarrow 0 = y \vee 0 = sz && \text{(Question 8 above)} \\ &\rightarrow 0 = y && (\mathbf{S1}) \end{aligned}$$

All-introduction on this gives

$$(\mathbf{2}) \qquad \forall y(0 * sz = y * sz \to 0 = y).$$

For the induction step we assume

$$(\mathbf{IH}) \qquad \forall y(a * sz = y * sz \to a = y).$$

We now have

$$\begin{array}{rcll} sa * sz = y * sz & \to & (a * sz) + sz = y * sz & \text{(Question 4 above)} \\ & \to & s((a * sz) + z) = y * sz & (\mathbf{A2}) \\ & \to & y * sz \neq 0 & (\mathbf{S1}) \\ & \to & y \neq 0 & \text{(Question 3 above)} \end{array}$$

If $y \neq 0$ then $y = sd$ for some d; starting again, we have

$$\begin{array}{rcll} sa * sz = y * sz & \to & sa * sz = sd * sz & \text{(As shown above)} \\ & \to & (a * sz) + sz = (d * sz) + sz & \text{(Question 4 above, twice)} \\ & \to & a * sz = d * sz & \text{(Question 2 above)} \\ & \to & a = d & (\mathbf{IH}) \\ & \to & sa = sd & \text{(Identity rules)} \\ & \to & sa = y & \text{(Since } y = sd\text{)} \end{array}$$

By All-intro we now have

$$\forall y(sa * sz = y * sz \to sa = y),$$

and since this is derived from $\mathbf{IH}$, If-intro allows us to assert

$$\forall y(a * sz = y * sz \to a = y) \to \forall y(sa * sz = y * sz \to sa = y).$$

By All-intro this gives

$$(\mathbf{3}) \qquad \forall x(\forall y(x * sz = y * sz \to x = y) \to \forall y(sx * sz = y * sz \to sx = y))$$

which is the full induction step. $\mathbf{1}, \mathbf{2}, \mathbf{3}$ now give us

$$\forall x \forall y(x * sz = y * sz \to x = y)$$

which by All-intro gives

$$\forall z \forall x \forall y(x * sz = y * sz \to x = y).$$

All that remains is to reorder the quantifiers (actually, this is not a totally trivial step, it needs to be proved using All-intro and All-elim that this is allowed—but we'll take that as read).

I told you this one was harder!