Solutions to Problem Set 3
Advanced Logic
5th October 2022

1. (40%) Suppose that A is a set; R is an *injective* relation on A; and B is a subset of A such that whenever $x \in B$, it is not the case that Rxx. Let C be the closure of B under R. Prove that whenever $x \in C$, it is not the case that Rxx.

> This is proved by induction. The base case is the given fact that whenever $x \in B$ it is not the case that Rxx. So it suffices to prove the induction step: whenever Rxy and it is not the case that Rxx, it is also not the case that Ryy. But this follows from the fact that R is injective, since if Rxy and Ryy we must have $x = y$ and hence Rxx.

2. Prove that the following hold for all $m, n \in \mathbb{N}$

(a) (20%) $$\operatorname{double} n = n + n$$

(b) (10%) $$m + n = n + m$$

(c) (10%) $$\operatorname{double} n = 2 \times n$$

(d) (5%) $$0 \times n = 0$$

(e) (5%) $$(\operatorname{suc} n) \times m = (n \times m) + m$$

(f) (5%) $$n \times m = m \times n$$

(g) (5%) $$\text{If } \operatorname{double} m = \operatorname{double} n, \text{ then } m = n$$

Note: in these proofs you may assume the Axiom of Numbers and the following principles about addition, multiplication, and the 'double' function (which follow from their standard recursive definitions):

(Dz) $$\operatorname{double} 0 = 0$$

(Ds) $$\operatorname{double}(\operatorname{suc} n) = \operatorname{suc}(\operatorname{suc}(\operatorname{double} n))$$

(Az) $$n + 0 = n$$

(As) $$n + \operatorname{suc} m = \operatorname{suc}(n + m)$$

(Mz) $$n \times 0 = 0$$

(Ms) $$n \times \operatorname{suc} m = (n \times m) + n$$

for any $n, m \in \mathbb{N}$. You may also assume the facts I give proofs of in the supplementary document called 'Proofs by induction: a guide'. Also, some of the later proofs will require on earlier ones. Remember too that '2' abbreviates '$\operatorname{suc}(\operatorname{suc} 0)$'.

> (a) By induction. Base case: $\operatorname{double} 0 = 0$ (Dz)
> $= 0 + 0$ (Az)

Induction step: suppose $\mathrm{double}\, n = n + n$. Then

$$\begin{aligned}
\mathrm{double}(\mathrm{suc}\, n) &= \mathrm{suc}(\mathrm{suc}(\mathrm{double}\, n)) && \text{(Ds)}\\
&= \mathrm{suc}(\mathrm{suc}(n + n)) && \text{(IH)}\\
&= \mathrm{suc}(n + \mathrm{suc}\, n) && \text{(As)}\\
&= \mathrm{suc}\, n + \mathrm{suc}\, n && \text{(Thm. 2 from ‘Guide’)}
\end{aligned}$$

(b) By induction on n, for arbitrary m.

Base case: $m + 0 = m$ (Az)

$= 0 + m$ (Thm. 1 from ‘Guide’)

Induction step: suppose $m + n = n + m$. Then

$$\begin{aligned}
m + \mathrm{suc}\, n &= \mathrm{suc}(m + n) && \text{(As)}\\
&= \mathrm{suc}(n + m) && \text{(IH)}\\
&= \mathrm{suc}\, n + m && \text{(Thm. 2 from ‘Guide’)}
\end{aligned}$$

(c) I'm afraid I messed up here: I meant to write $n \times 2$ rather than $2 \times n$. Given what I actually wrote, the easiest way to prove this one goes by way of problems (a) and (f), so I should have put this one after (f): apologies!

Once we have (a) and (f), we can reason as follows:

$$\begin{aligned}
2 \times n &= n \times 2 && \text{(by (f))}\\
&= \mathrm{n} \times 1 + n && \text{(Ms)}\\
&= (\mathrm{n} \times 0 + n) + n && \text{(Ms)}\\
&= (0 + n) + n && \text{(Mz)}\\
&= n + n && \text{(Thm. 1)}\\
&= \mathrm{double}\, n && \text{(by (a))}
\end{aligned}$$

Note that this is not itself an inductive proof, though of course it relies on the results of other inductive proofs!

(d) By induction. Base case: $0 \times 0 = 0$ by (Mz).

Induction step: suppose $0 \times n = 0$. Then

$$\begin{aligned}
0 \times \mathrm{suc}\, n &= (0 \times n) + 0 && \text{(Ms)}\\
&= 0 + 0 && \text{(IH)}\\
&= 0 && \text{(Az)}
\end{aligned}$$

(e) By induction on m, for an arbitrary n.

Base case: $\mathrm{suc}\, n \times 0 = 0$ (Mz)

$= 0 + 0$ (Az)

$= (n \times 0) + 0$ (Mz)

Induction step: suppose that $\operatorname{suc} n \times m = (n \times m) + m$. Then

$$\begin{aligned}
\operatorname{suc} n \times \operatorname{suc} m &= (\operatorname{suc} n \times m) + \operatorname{suc} n && \text{(Ms)}\\
&= ((n \times m) + m) + \operatorname{suc} n && \text{(IH)}\\
&= n \times m + (m + \operatorname{suc} n) && \text{(Thm. 3)}\\
&= n \times m + \operatorname{suc}(m + n) && \text{(As)}\\
&= n \times m + \operatorname{suc}(n + m) && \text{(b)}\\
&= n \times m + (n + \operatorname{suc} m) && \text{(As)}\\
&= ((n \times m) + n) + \operatorname{suc} m && \text{(Thm. 3)}\\
&= (n \times \operatorname{suc} m) + \operatorname{suc} m && \text{(Ms)}
\end{aligned}$$

(f) By induction on n, for an arbitrary m.

Base case: $0 \times m = 0$ (by part (d)) $= m \times 0$ (by (Mz)).

Induction step: suppose $n \times m = m \times n$. Then

$$\begin{aligned}
(\operatorname{suc} n) \times m &= (n \times m) + m && \text{(part (e))}\\
&= (m \times n) + m && \text{(IH)}\\
&= m \times \operatorname{suc} n && \text{(Ms)}
\end{aligned}$$

(g) By induction on n, generalizing over m.

Base case: we want to show that for all m, if $\operatorname{double} m = \operatorname{double} 0$ then $m = 0$. Suppose for contradiction that for a certain m, $\operatorname{double} m = \operatorname{double} 0$ although $m \neq 0$. Since every number other than 0 is a successor, we have $m = \operatorname{suc} m'$ for some m, hence $\operatorname{double} m = \operatorname{suc}\operatorname{suc}\operatorname{double} m'$. But then $\operatorname{double} m \neq 0$ since 0 is not a successor, contradicting our assumption.

Induction step: suppose as the induction hypothesis that for any m, if $\operatorname{double} m = \operatorname{double} n$, then $m = n$. To show that the same is true of $\operatorname{suc} n$, suppose $\operatorname{double} m = \operatorname{double}\operatorname{suc} n$. Then we have $\operatorname{double} m = \operatorname{suc}\operatorname{suc}\operatorname{double} n$. This can't happen if $m = 0$, since then we'd have $\operatorname{double} m = 0$ and 0 isn't a successor. So we must have $m = \operatorname{suc} m'$ for some m', and hence $\operatorname{double} m = \operatorname{suc}\operatorname{suc}\operatorname{double} m' = \operatorname{suc}\operatorname{suc}\operatorname{double} n$. But then by the injectivity of suc, we have $\operatorname{suc}\operatorname{double} m' = \operatorname{suc}\operatorname{double} n$ and hence $\operatorname{double} m' = \operatorname{double} n$, so by the induction hypothesis $m' = n$. But then $m = \operatorname{suc} m' = \operatorname{suc} n$

4. (10% extra credit) Open the Lean Natural Numbers Game at `https://www.ma.imperial.ac.uk/~buzzard/xena/natural_number_game/` and play through (at least) the levels 'Tutorial World', 'Addition World', and 'Multiplication World'. To show that you've completed the levels, send us a screenshot of the last level of Multiplication World open on your computer screen, with your name showing somewhere in the screenshot (e.g. in a text editor window).

Note that the facts you're proving in these levels of the game overlap a lot with the ones you're asked to prove in problem 2. So, you might find it helpful to play the game first and tackle problem 2 afterwards. Whichever order you do it in, it should be instructive to look at your proofs in problem 2 with your solutions to the game, and see how they have the same mathematical content.

There are solutions at `https://github.com/adyavanapalli/natural-number-game-solutions`.