Reasoning About Programs

Week 5 Tutorial - Induction over Recursively Defined Relations

Sophia Drossopoulou and Mark Wheelhouse

1st Question:

Consider the statement:

$$(*) \quad \forall n \in S_{\mathbb{N}}.\ [\ Odd(n) \ \rightarrow\ Even(\mathsf{Succ}\ n)\ ]$$

Recall the definitions of $S_{\mathbb{N}}$, Odd and $Even$ given in the lectures:

(R1) $\mathsf{Zero} \in S_{\mathbb{N}}$

(R2) $n \in S_{\mathbb{N}} \ \rightarrow\ \mathsf{Succ}\ n \in S_{\mathbb{N}}$

(R3) $Odd(\mathsf{Succ\ Zero})$

(R4) $Odd(n) \ \rightarrow\ Odd(\mathsf{Succ}(\mathsf{Succ}\ n))$

(R5) $Even(\mathsf{Zero})$

(R6) $Even(n) \ \rightarrow\ Even(\mathsf{Succ}(\mathsf{Succ}\ n))$

(a) Prove $(*)$ using induction over the definition of Odd.

(b) As a comparison, think about the proof of $(*)$ using induction over the definition of $S_{\mathbb{N}}$.

Warning The proof in part (b) will be more demanding than that in part (a). In fact, one part actually requires induction over the definition of Odd and $Even$.

A possible answer:

(a) Induction over the definition of Odd.

Recall from lectures that, taking $Q(n) \equiv Even(\mathsf{Succ}\ n)$, the induction principle for Odd gives:

$$\begin{array}{l} Even(\mathsf{Succ}(\mathsf{Succ\ Zero})) \\ \wedge \\ \ \forall n : S_{\mathbb{N}}.\ [\ Odd(n) \wedge Even(\mathsf{Succ}\ n) \ \rightarrow\ Even(\mathsf{Succ}(\mathsf{Succ}(\mathsf{Succ}\ n)))\quad] \\ \ \rightarrow \\ \forall n : S_{\mathbb{N}}.\ [\ Odd(n) \ \rightarrow\ Even(\mathsf{Succ}\ n)\ ] \end{array}$$

The proof therefore goes as follows:

Base Case:

To Show: $Even(\mathsf{Succ}(\mathsf{Succ\ Zero}))$

This follows from **(R5)** and **(R6)**.

Inductive Step

Take an arbitrary $n : S_{\mathbb{N}}$.
Assume $Odd(n)$
Inductive Hypothesis: $Even(\mathsf{Succ}\ n)$
To Show: $Even(\mathsf{Succ}(\mathsf{Succ}(\mathsf{Succ}\ n)))$

This follows directly from Inductive Hypothesis and **(R6)**.[1]

(b) Induction over the definition of $S_{\mathbb{N}}$.

This requires some thought. Namely, in the inductive step, we would need to be able to prove that:

$$\forall n : S_{\mathbb{N}}.\ (\ [Odd(n)\ \rightarrow\ Even(\mathsf{Succ}\ n)\ ]\ \rightarrow\ [\ Odd(\mathsf{Succ}\ n)\ \rightarrow\ Even(\mathsf{Succ}(\mathsf{Succ}\ n))\ ]\ )$$

The proof of the above is not immediately obvious!

One possibility is to strengthen the lemma from above, and instead prove:

$$(**)\ \forall n : S_{\mathbb{N}}.\ ([\ Odd(n) \veebar Even(n)\ ] \wedge [\ Odd(n)\ \rightarrow\ Even(\mathsf{Succ}\,n)\ ] \wedge [Even(n)\ \rightarrow\ Odd(\mathsf{Succ}\,n)\ ])$$

The proof of the lemma above can be done by induction over the definition of $S_{\mathbb{N}}$. But before proving (**) we need two auxiliary lemmas

Lemma 1 *For any $n \in S_{\mathbb{N}}$:*

- $Odd(n)\quad \longleftrightarrow\quad [\ \ n = \mathsf{Succ\,Zero}\ \vee\ \exists m \in S_{\mathbb{N}}.[\ n = \mathsf{Succ}(\mathsf{Succ}\ m)\ \wedge Odd(m)\ ]\ ]$

Lemma 2 *For any $n \in S_{\mathbb{N}}$:*

- $Even(n)\quad \longleftrightarrow\quad [\ \ n = \mathsf{Zero}\ \vee\ \exists m \in S_{\mathbb{N}}.[\ n = \mathsf{Succ}(\mathsf{Succ}\ m)\ \wedge Even(m)\ ]\ ]$

Lemma 1 follows from **(R3)** and **(R4)** and from the fact that *Odd* is the *smallest* relation satisfying **(R3)** and **(R4)**. Similarly, lemma 2 follows from **(R5)** and **(R6)** and from the fact that *Even* is the smallest relation satisfying **(R5)** and **(R6)**.

We now proceed to prove (**):

Base Case

To Show $[\ Odd(\mathsf{Zero}) \veebar Even(\mathsf{Zero})\ ]\ \wedge\ [\ Odd(\mathsf{Zero})\ \rightarrow\ Even(\mathsf{Succ\ Zero})\ ]\ \wedge\ [Even(\mathsf{Zero}) \rightarrow Odd(\mathsf{Succ\ Zero})\ ]$

From lemma 1 we obtain that $(A)\ \neg Odd(\mathsf{Zero})$.

Now, we have that $Even(\mathsf{Zero})$ (by **(R5)**), and using (A), we also obtain that $Odd(\mathsf{Zero}) \veebar Even(\mathsf{Zero})$.

Also, from (A) we obtain that $Odd(\mathsf{Zero}) \rightarrow Even(\mathsf{Succ\ Zero})$.

Finally, we have that $Odd(\mathsf{Succ\ Zero})$ (by **(R3)**), and therefore we also have that $Even(\mathsf{Zero})\ \rightarrow\ Odd(\mathsf{Succ\ Zero})$.

[1] Note that in the inductive step we did not need to use the assumption that $Odd(n)$.

Inductive Step Take $n \in S_{\mathbb{N}}$, arbitrary.

Inductive Hypothesis $[\, Odd(n) \veebar Even(n)\,] \wedge [Odd(n) \;\to\; Even(\mathsf{Succ}\, n)\,] \wedge [\, Even(n) \;\to\; Odd(\mathsf{Succ}\, n)\,]$

To Show $[\, Odd(\mathsf{Succ}\, n) \veebar Even(\mathsf{Succ}\, n)\,] \;\wedge\; [Odd(\mathsf{Succ}\, n) \;\to\; Even(\mathsf{Succ}\,(\mathsf{Succ}\, n))\,] \;\wedge\; [\, Even(\mathsf{Succ}\, n) \;\to\; Odd(\mathsf{Succ}\,(\mathsf{Succ}\, n))\,]$

We proceed by cases.

1st Case $Odd(n) \wedge \neg Even(n)$.

Then, by application of the induction hypothesis we obtain that (A) $Even(\mathsf{Succ}\, n)$. By application of lemmas 1 and 2 we obtain (B) $\neg Odd(\mathsf{Succ}\, n)$.[2] From (A) and (B) we obtain the first conjunct that is to be shown.

From (B) we obtain the second conjunct that is to be shown.

And from $Odd(n)$ and **(R40)** we obtain $Odd(\mathsf{Succ}\,(\mathsf{Succ}\, n))$ which gives the third conjunct that is to be shown.

2nd Case $\neg Odd(n) \wedge Even(n)$.

Similar to 1st Case.

2nd Question:

(This is part of the 2016/2017 exam question). Consider the functions `f`, `g`, and `h`, defined below:

```
f :: Int -> Int
f n =
   | 0<=n && n<3 = 10 + 10*n
   | otherwise   = f(n-1)*f(n-3)

g :: Int -> Int
g n =
   | 0<=n && n<3 = 10 + 10*n
   | otherwise   = h(n,2,30,20,10)

h :: (Int,Int,Int,Int,Int) -> Int
h(n,cnt,k1,k2,k3)
   | n==cnt     = k1
   | otherwise  = h(n,cnt+1,k1*k3,k1,k2)
```

[2] To be precise, in order to deduce (B) we would need to apply a form of strong induction, ie in the inductive hypothesis we would be proving that (**) $\forall n : S_{\mathbb{N}}.\ ([\ Odd(n) \veebar Even(n)\ ] \wedge [\ Odd(n) \to Even(\mathsf{Succ}\ n)\ ] \wedge [Even(n) \to Odd(\mathsf{Succ}\ n)\ ] \wedge [\ Odd(\mathsf{Succ}\ n) \veebar Even(\mathsf{Succ}\ n)\ ] \wedge [\ Odd(\mathsf{Succ}\ n) \to Even(\mathsf{Succ}(\mathsf{Succ}\ n))\ ] \wedge [Even(\mathsf{Succ}\ n) \to Odd(\mathsf{Succ}(\mathsf{Succ}\ n))\ ] \longrightarrow [\ Odd(\mathsf{Succ}(\mathsf{Succ}\ n)) \veebar Even(\mathsf{Succ}(\mathsf{Succ}\ n))\ ] \wedge [\ Odd(\mathsf{Succ}(\mathsf{Succ}\ n)) \to Even(\mathsf{Succ}(\mathsf{Succ}(\mathsf{Succ}\ n)))\ ] \wedge [Even(\mathsf{Succ}(\mathsf{Succ}\ n)) \to Odd(\mathsf{Succ}(\mathsf{Succ}(\mathsf{Succ}\ n)))\ ])$. We leave this as exercise – after all, the point on part b was to demonstrate how much easier the proof is by induction over the definition of *Odd* and *Even*.

We will study various proof steps in establishing that

$$(A)\quad \forall n:\mathbb{N}.\ \mathtt{f}\,n \ = \ \mathtt{g}\,n.$$

In particular:

(i) Assume a predicate $P \subseteq \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$, and write out the inductive principle as applied to the definition of $\mathtt{h}$, which implies that:

$(B)\quad \forall n, cnt, k1, k2, k3, r:\mathbb{Z}.\ [\ \mathtt{h}(n, cnt, k1, k2, k3) = r \ \to\ P(n, cnt, k1, k2, k3, r)\ ]$

(ii) Write out the proof schema that allows us to prove that:

$(C)\quad \forall n, cnt, k1, k2, k3, r:\mathbb{Z}.$
$[\ \ \mathtt{h}(n, cnt, k1, k2, k3) = r \ \to$
$[\,n\geq 3 \wedge cnt\geq 2 \wedge k1{=}\mathtt{f}(cnt) \wedge k2{=}\mathtt{f}(cnt{-}1) \wedge k3{=}\mathtt{f}(cnt{-}2)\ \to\ r = \mathtt{f}(n)\ ]\ \ ]$

After that, fill in the proofs (*this was not required in the exam*)

(iii) For which values of $n:\mathbb{Z}$ does the term $\mathtt{g}\,n$ terminate?

(iv) Prove termination for values you have specified in your answer in part (iii).

(v) Prove (A).

A possible answer:

(i) $\forall n, k1, k2, k3:\mathbb{Z}.\, P(n, n, k1, k2, k3, k1)$
$\wedge$
$\forall n, cnt, k1, k2, k3, r:\mathbb{Z}.$
$[\,n{\neq}cnt \wedge \mathtt{h}(n, cnt{+}1, k1{*}k3, k1, k2) = r \wedge P(n, cnt{+}1, k1{*}k3, k1, k2, r)\ \to\ P(n, cnt, k1, k2, k3, r)\,]$
$\longrightarrow$
$\forall n, cnt, k1, k2, k3, r:\mathbb{Z}.\,[\ \mathtt{h}(n, cnt, k1, k2, k3) = r \ \to\ P(n, cnt, k1, k2, k3, r)\ ]$

(ii) **Base Case** Take $n, k1, k2, k3, r:\mathbb{Z}$, arbitrary.

To Show: $n \geq 3 \wedge cnt{\geq}2 \wedge k1{=}\mathtt{f}(n) \wedge k2{=}\mathtt{f}(n{-}1) \wedge k2{=}\mathtt{f}(n{-}2)\ \to\ k1 = \mathtt{f}(n)$.

Proof of Base Case - not required in the exam

Follows easily, as we are asked to show that $\ldots \wedge k1{=}\mathtt{f}(n) \wedge \ldots\ \to\ k1{=}\mathtt{f}(n)$

Inductive Step

Take arbitrary $n, cnt, k1, k2, k3, r:\mathbb{Z}.$.
Assume that
(ass1) $\quad n \neq cnt$
(ass2) $\quad \mathtt{h}(n, cnt{+}1, k1{*}k3, k1, k2) = r.$
Inductive Hypothesis:

$n{\geq}3 \wedge cnt{+}1{\geq}2 \wedge k1{*}k3{=}\mathtt{f}(cnt{+}1) \wedge k1{=}\mathtt{f}(cnt) \wedge k2{=}\mathtt{f}(cnt{-}1)\ \to\ r = \mathtt{f}(n)$

To Show:
$n{\geq}3 \wedge cnt{\geq}2 \wedge k1{=}\mathtt{f}(cnt) \wedge k2{=}\mathtt{f}(cnt{-}1) \wedge k3{=}\mathtt{f}(cnt{-}2)\ \to\ r = \mathtt{f}(n)$

Proof of Inductive Step - not required in exams

We assume moreover that
(ass3) $\quad n{\geq}3$

(ass4) $cnt! \geq 2$
(ass5) $k1 = \mathtt{f}(cnt)$
(ass6) $k2 = \mathtt{f}(cnt-1)$
(ass7) $k3 = \mathtt{f}(cnt-2)$
And we want to prove that $r = \mathtt{f}(n)$.

We have that

(F1)	$\mathtt{f}(cnt+1) = \mathtt{f}(cnt) * \mathtt{f}(cnt-2)$	because, from (ass4), we have $cnt+1 \geq 3$, and by def. $\mathtt{f}$
(F2)	$k1 * k3 = \mathtt{f}(cnt+1)$	by (F1), (ass5) and (ass7)
(F3)	$cnt+1 \geq 2$	from (ass4)
	$r = \mathtt{f}(n)$	from (ass3), (F3), (F2), (ass5), (ass6) and Inductive Hypothesis

(iii) The term $\mathtt{g}\,n$ terminates for all $n : \mathbb{N}$.

(iv) $\mathtt{g}\,n$ terminates immediately for $0 \leq n \leq 2$
$\mathtt{h}(n, cnt, k1, k2, k3)$ terminates when $n \geq cnt$ – we can show this by mathematical induction on $n - cnt$. Therefore, $\mathtt{g}\,n$ also terminates for $n \geq 2$.
Therefore, $\mathtt{g}\,n$ terminates for all $n : \mathbb{N}$.

(v)

(F1)	$n \geq 3 \longrightarrow \mathtt{h}(n, 2, 30, 20, 10) = \mathtt{f}\ n$	from (C), by substituting cnt by 2, and substituting $k1$ by $f\ 2$, and $k2$ by $f\ 1$ and $k3$ by $f\ 0$
(F2)	$n \geq 3 \longrightarrow \mathtt{g}\ n = \mathtt{f}\ n$	(F1) and def. $\mathtt{g}$
(F2)	$0 \leq n < 3 \longrightarrow \mathtt{f}\,n = \mathtt{g}\,n$	from def. $\mathtt{f}$ and $\mathtt{g}$.

(A) follows from (F2) and (F3).

Thank you to Linna Wang (2015) and Joe Rackham (2017) for noticing that in Question 1 the proof over $S_{\mathbb{N}}$ requires some deeper thought in the base case.