Reasoning About Programs

Week 5 PMT - Induction over Recursively Defined Sets, Relations and Functions
To discuss during PMT - do NOT hand in

Sophia Drossopoulou and Mark Wheelhouse

1st Question:

Consider the following inductive definition of the set $S \subseteq \mathbb{Z} \times \mathbb{Z}$:

(R1) $(3, 5) \in S$

(R2) If $(z_1, z_2) \in S$ then $(z_2, z_1) \in S$

(R3) If $(z_1, z_2) \in S$ then $(z_1 + 2, z_2) \in S$

(R4) If $(z_1, z_2) \in S$ then $(-z_1, z_2) \in S$

(a) Show the derivation of the following facts:

(i) $(3, 7) \in S$

(ii) $(-3, 3) \in S$

(b) Write the inductive principle for the set S for a property P defined over $\mathbb{Z} \times \mathbb{Z}$, which guarantees that $\forall (m, n) \in S.\, P(m, n)$.

(c) Write out the proof schema for $\quad (*) \;\; S \subseteq \mathbb{Z}^{odd} \times \mathbb{Z}^{odd}$,
where $\mathbb{Z}^{odd}$ stands for the odd integers.

Only state what is taken arbitrary, what is assumed, and what is to be shown.

Hint: You may want to reword $(*)$ as $\quad (**) \;\; \forall (m, n) \in S.\ (m, n) \in \mathbb{Z}^{odd} \times \mathbb{Z}^{odd}$.

A possible answer:

(a) Derivations of membership to S:

(i) $(3, 7) \in S$ can be derived as follows

(1)	$(3, 5) \in S$	by **(R1)**
(2)	$(5, 3) \in S$	by (1) and **(R2)**
(3)	$(7, 3) \in S$	by (2) and **(R3)**
(4)	$(3, 7) \in S$	by (3) and **(R2)**

(ii) $(-3, 3) \in S$ can be derived as follows

(1)	$(3, 5) \in S$	by **(R1)**
(2)	$(5, 3) \in S$	by (1) and **(R2)**
(3)	$(-5, 3) \in S$	by (2) and **(R4)**
(4)	$(-3, 3) \in S$	by (3) and **(R3)**

(b) The induction principle for the set S for a property $P \subseteq \mathbb{Z} \times \mathbb{Z}$ is:

$$\begin{array}{ll} & P(3,5) \\ \wedge & \forall (z_1, z_2) \in S.\ [P(z_1, z_2) \to P(z_2, z_1)] \\ \wedge & \forall (z_1, z_2) \in S.\ [P(z_1, z_2) \to P(z_1 + 2, z_2)] \\ \wedge & \forall (z_1, z_2) \in S.\ [P(z_1, z_2) \to P(-z_1, z_2)] \\ \to & \\ \multicolumn{2}{l}{\forall (z, z') \in S.\, P(z, z')} \end{array}$$

(c) We prove (**) following the induction principle outlined in part (**??**). We take $P \subseteq \mathbb{Z} \times \mathbb{Z}$ to be $P(z_1, z_2) \equiv (z_1, z_2) \in \mathbb{Z}^{odd} \times \mathbb{Z}^{odd}$.

We outline the structure of the proof, but do not fill the cases.

Base Case (R1):

To Show: $(3,5) \in \mathbb{Z}^{odd} \times \mathbb{Z}^{odd}$.

...

Inductive Step (R2):

Take arbitrary $(z_1, z_2) \in S$.
Inductive Hypothesis: $(z_1, z_2) \in \mathbb{Z}^{odd} \times \mathbb{Z}^{odd}$
To Show: $(z_2, z_1) \in \mathbb{Z}^{odd} \times \mathbb{Z}^{odd}$

...

Inductive Step (R3):

Take arbitrary $(z_1, z_2) \in S$.
Inductive Hypothesis: $(z_1, z_2) \in \mathbb{Z}^{odd} \times \mathbb{Z}^{odd}$
To Show: $(z_1 + 2, z_2) \in \mathbb{Z}^{odd} \times \mathbb{Z}^{odd}$

...

Inductive Step (R4):

Take arbitrary $(z_1, z_2) \in S$.
Inductive Hypothesis: $(z_1, z_2) \in \mathbb{Z}^{odd} \times \mathbb{Z}^{odd}$
To Show: $(-z_1, z_2) \in \mathbb{Z}^{odd} \times \mathbb{Z}^{odd}$

...

2nd Question:

Consider the function $Min : S_{\mathbb{N}} \times S_{\mathbb{N}} \to S_{\mathbb{N}}$, defined as follows:

(R1) $\forall n \in S_{\mathbb{N}}.\ Min(\mathsf{Zero}, n) = \mathsf{Zero}$

(R2) $\forall n \in S_{\mathbb{N}}.\ Min(n, \mathsf{Zero}) = \mathsf{Zero}$

(R3) $\forall n, n', m \in S_{\mathbb{N}}.\ [\ Min(n, n') = m\ \to\ Min(\mathsf{Succ}\ n, \mathsf{Succ}\ n') = \mathsf{Succ}\ m)]$

Assume a ternary relation $P \subseteq S_{\mathbb{N}} \times S_{\mathbb{N}} \times S_{\mathbb{N}}$. Consider the assertion:

$$(*) \quad \forall n, n', m \in S_{\mathbb{N}}.\ [\ m = Min(n, n') \to P(n, n', m)\ ]$$

(a) State the induction principle over the definition of Min which would guarantee $(*)$.

(b) To compare with the previous, also write out the inductive principle over $S_{\mathbb{N}}$ which would guarantee $(*)$. Apply induction on n.

(c) Use your solution from part a) to prove that $\forall i, j, k \in S_{\mathbb{N}}. [\ Min(i, j) = k \rightarrow k = Min(j, i)]$

A possible answer:

(a)

$$\begin{array}{l}
\forall n' \in S_{\mathbb{N}}.\ P(\mathsf{Zero}, n', \mathsf{Zero}) \\
\wedge \\
\forall n \in S_{\mathbb{N}}.\ P(n, \mathsf{Zero}, \mathsf{Zero}) \\
\wedge \\
\forall n, n', m \in S_{\mathbb{N}}. [\, m = Min(n, n') \wedge P(n, n', m) \ \rightarrow\ P(\mathsf{Succ}\ n, \mathsf{Succ}\ n', \mathsf{Succ}\ m)\ ] \\
\rightarrow \\
\forall n, n', m \in S_{\mathbb{N}}.\ [\ m = Min(n, n') \rightarrow P(n, n', m)\ ]
\end{array}$$

(b)

$$\begin{array}{l}
\forall n', m \in S_{\mathbb{N}}. [\, m = Min(\mathsf{Zero}, n') \rightarrow\ P(\mathsf{Zero}, n', m)\ ] \\
\wedge \\
\forall k \in S_{\mathbb{N}}.\ (\ \ \forall n', m \in S_{\mathbb{N}}. [\ m = Min(k, n') \rightarrow P(n, n', m)\ ]\ \rightarrow \\
\qquad\qquad\quad \forall n', m \in S_{\mathbb{N}}. [\ m = Min(\mathsf{Succ}\, k, n') \rightarrow P(\mathsf{Succ}\, k, n', m)\ ]\ \ ) \\
\rightarrow \\
\forall n, n', m \in S_{\mathbb{N}}.\ [\ m = Min(n, n') \rightarrow P(n, n', m)\ ]
\end{array}$$

Comment Notice that in part (a) the assumption of the inductive principle consists of three conjuncts, while in the part (b) it only consists of two. This may seem surprising initially. It is due to the fact that the induction in part (a) is on the definition of Min which consists of three cases, while the induction in part (b) is on the definition of $S_{\mathbb{N}}$ which consists of two cases.

(c) We are proving $\forall i, j, k \in S_{\mathbb{N}}. [\ Min(i, j) = k \rightarrow P(i, j, k)]$ where $P(i, j, k) \equiv k = Min(j, i)$

Therefore, the proof is as follows:

Base Case (R1): To Show: $\forall j \in S_{\mathbb{N}}.\ \mathsf{Zero} = Min(j, \mathsf{Zero})$.

follows from **(R2)**

Base Case (R2): To Show: $\forall i \in S_{\mathbb{N}}.\ \mathsf{Zero} = Min(\mathsf{Zero}, i)$

follows from **(R1)**

Inductive Step (R3): Take arbitrary $i, j, k \in S_{\mathbb{N}}$.

Inductive Hypothesis: $k = Min(i, j)\ \wedge\ k = Min(j, i)$
To Show: $\mathsf{Succ}\ k = Min(\mathsf{Succ}\ j, \mathsf{Succ}\ i)$

From the Ind. Hyp. we have $k = Min(j, i)$. By application of **(R3)**, we obtain $\mathsf{Succ}\ k = Min(\mathsf{Succ}\ j, \mathsf{Succ}\ i)$

3rd Question - Challenge - only if you have time

Remember that we said that for inductively defined sets A, and predicates P_1, $P_2 \subseteq A$, where P_1 is inductively defined, assertions of the form $\forall a : A.[\ P_1(a) \to P_2(a)\ ]$ could be proven either by induction on the definition of A, or by induction on the definition of P_1.

In this exercise, we shall *prove* that any proof over the the definition of Odd has its counterpart in a proof over the definition of $S_{\mathbb{N}}$.

Here what we will do:
Remember that we defined $S_{\mathbb{N}}$, and the predicate $Odd \subseteq S_{\mathbb{N}}$ inductively as follows:

R1 $zero \in S_{\mathbb{N}}$

R2 $\forall n.[n \in S_{\mathbb{N}} \ \to \ \mathsf{Succ}\ n \in S_{\mathbb{N}}]$

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

R4 $\forall n \in S_{\mathbb{N}}.[\ Odd(n) \ \to \ Odd(\mathsf{Succ}\ (\mathsf{Succ}\ n))\ ]$

And as we already discussed, the principle of induction applied on the definition of Odd gives:

IPO For any predicate $P \subseteq S_{\mathbb{N}}$

$$
\begin{array}{l}
P(\mathsf{Succ\ Zero}) \\
\wedge \\
\forall m \in S_{\mathbb{N}}.[\ Odd(m) \ \wedge \ P(m) \to P(\mathsf{Succ}(\mathsf{Succ}\ m))\ ] \\
\to \\
\forall n \in S_{\mathbb{N}}.[\ Odd(n) \to P(n)\ ]
\end{array}
$$

On the other hand, the principle of induction applied on the definition of $S_{\mathbb{N}}$ gives:

IPS For any predicate $P \subseteq S_{\mathbb{N}}$

$$
\begin{array}{l}
Odd(\mathsf{Zero}) \to P(\mathsf{Zero}) \\
\wedge \\
\forall m \in S_{\mathbb{N}}.[\quad [\,Odd(m) \to P(m)\,] \to [\,Odd(sc(m)) \to P(\mathsf{Succ}\ m)\,]\quad] \\
\to \\
\forall n \in S_{\mathbb{N}}.[\ Odd(n) \to P(n)\ ]
\end{array}
$$

Assume that **IPO** holds. Show that **IPS** holds. **Hint:** Take ideas from the proof of equivalence of mathematical and strong induction.

A possible answer:

Take any arbitrary predicate $R \subseteq S_{\mathbb{N}}$ such that

(A) $Odd(zero) \to R(zero)$

(B) $\forall m \in S_{\mathbb{N}}.[\,Odd(m) \to R(m)\,] \to [\,Odd(\mathsf{Succ}\ m) \to R(\mathsf{Succ}\ m)\,]$

Prove that

(α) $\forall n \in S_{\mathbb{N}}. [\, Odd(n) \to R(n) \,]$

We define a new predicate $R' \subseteq S_{\mathbb{N}}$ as follows:

(D) $R'(m) \equiv Odd(m) \to R(m)$

We then can prove the following two properties:

(E) $R'(\mathsf{Succ\ Zero})$
Namely, **(B)** applied to $zero$ gives that
$$[Odd(zero) \to R(zero)\,] \to [\,Odd(\mathsf{Succ\ Zero}) \to R(\mathsf{Succ\ Zero})\,],$$
and because $Odd(zero) = false$, the above gives
$$Odd(\mathsf{Succ\ Zero}) \to R(\mathsf{Succ\ Zero}).$$
The latter is equivalent with $R'(\mathsf{Succ\ Zero})$.

(F) $\forall m \in S_{\mathbb{N}}. [\, Odd(m) \wedge R'(m) \to R'(\mathsf{Succ}\ (\mathsf{Succ}\ m))\,]$.
Namely, take an arbitrary $m \in S_{\mathbb{N}}$. Assume $Odd(m) \wedge R'(m)$ holds, and aim to show $R'(\mathsf{Succ}\ (\mathsf{Succ}\ m))$.
Because $R'(m)$, by application of the definition **(D)** we obtain: $Odd(m) \to R(m)$. We can apply **(B)** twice, and obtain $Odd(\mathsf{Succ}\ (\mathsf{Succ}\ m)) \to R(\mathsf{Succ}\ (\mathsf{Succ}\ m))$. By application of the definition **(D)** on the latter, we obtain $R'(\mathsf{Succ}\ (\mathsf{Succ}\ m))$.

By applying **IPO** to **(E)** and **(F)**, we obtain

(G) $\forall n \in S_{\mathbb{N}}. [\, Odd(n) \to R'(n) \,]$

By application of the definition in **(D)**, we have that
$$\forall n \in S_{\mathbb{N}}. [\, Odd(n) \to R'(n) \,] \;\equiv\; \forall n \in S_{\mathbb{N}}. [\, Odd(n) \to (Odd(n) \to R(n)) \,],$$
By the rules of logic, we have
$$\forall n \in S_{\mathbb{N}}. [\, Odd(n) \to (Odd(n) \to R(n)) \,] \equiv \forall n \in S_{\mathbb{N}}. [\, Odd(n) \to R(n) \,].$$
Using the two results from above together with **(G)**, we obtain:

(α) $\forall n \in S_{\mathbb{N}}. [\, Odd(n) \to R(n) \,]$

Thank you

to Constantine Mateescu for feedback on the 2nd Question.