On Structural Induction and Homework 3

Peter Höfner

1 Introduction

Exercise 2 of Homework 3 (`http://www.cse.unsw.edu.au/~rvg/6752/homework.html`) was considered very hard. One reason is that many students are not familiar with *structural induction*. The purpose of this short note is to recapitulate the basic principles of structural induction and to present one solution for Exercise 2. As usual, there may be other correct solutions for the same exercise; hence the presented solution should not be considered as the only solution.

2 On Structural induction

A good overview of structural induction is provided by Wikipedia (`https://en.wikipedia.org/wiki/Structural_induction`).

Structural Induction is a generalisation of induction over the natural numbers, which should be familiar to anybody who took a basic course in mathematics at university.

Induction over the natural numbers is a proof technique to establish results for *all* natural numbers. An induction (over natural numbers) is done in two steps. The first, known as the *base case*, is to prove the statement (proof goal) for a "first" natural number. (Often the base case considers the number "0" or "1", but is not limited to these numbers.) The second step, called *induction step* is to prove that the statement holds for any given number (larger than the number used in the base case). This is done by assuming that the statement holds for a number n—this assumption is called *induction hypothesis*. Using this hypothesis one has to show that the statement holds for $n+1$. If these two steps can be shown, the statement holds for all natural numbers larger than or equal to the number used for the base case. (Sometimes it is necessary to expand the hypothesis to all natural numbers between the number used in the base case and n; it is easy to see that this expansion generalises classical induction on natural numbers.) The key to apply induction over natural numbers is the fact that any number can be split into strictly smaller numbers.

Structural induction generalises this idea and works on any recurse data type (any structure that can be split into smaller fragments). Structural induction is a proof technique to establish results for *all* elements of a recursively defined structure (or a well-founded structure). All 'indivisible' elements will form the base case. For example, any list can be built from the empty list and all lists containing only a single element, using list concatenation.

A structural induction is done in two steps. The first, known as the *base case*, is to prove the statement (proof goal) for the small indivisible elements. The second step, called *induction step* is to prove that the statement holds for all structures that can be built from the base elements. This is done by assuming that the statement holds for elements n_1 to n_k and then to prove that is holds for all structures that are built up from these elements.

Exercise 2 of Homework 3

Having the basics of structural induction in mind, we can now look at an example, namely Exercise 2 of Homework 3.

Exercise. Let $Cl = \texttt{tick}.Cl$ and $Cl2 = \texttt{tick}.\texttt{tick}.Cl2$. Show that no modal formula (of HML) distinguishes these clocks.

Solution. The idea is to use structural induction. The syntax of Hennesy-Milner-Logic was given by

$$\Phi = \texttt{true} \mid \texttt{false} \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \neg\Phi \mid [K]\Phi \mid \langle K\rangle\Phi$$

It is easy to see that $\vee$ can be defined using $\neg$ and $\wedge$, hence we will not consider $\vee$ later on. In principle, $[K]\Phi$ can be expressed as $\langle K\rangle\Phi$ and could be skipped as well (to keep the proof short); for completeness I include the case for $\langle K\rangle\Phi$.

Looking at the syntax we easily see that the only 'indivisible' element is `true` (`false` can be expressed by means of `true`). So the base case has to consider true; however, for all processes P, $P \models \texttt{true}$ holds, so the claim is trivial.

$$Cl \models \texttt{true} \quad \Leftrightarrow \quad Cl2 \models \texttt{true}$$

The induction hypothesis states that for HML-formulas Φ_1 and Φ_2 cannot distinguish Cl and $CL2$ That is

$$\begin{aligned} Cl \models \Phi_1 \quad &\Leftrightarrow \quad Cl2 \models \Phi_1 \text{ , and} \\ Cl \models \Phi_2 \quad &\Leftrightarrow \quad Cl2 \models \Phi_2 \text{ .} \end{aligned}$$

Based on this hypothesis we now have to show that the formulas $\Phi_1 \wedge \Phi_2$, $\neg\Phi_1$, $[K]\Phi_1$ and $\langle K\rangle\Phi_1$ cannot distinguish CL and $CL2$ either.

Case $\Phi_1 \wedge \Phi_2$: Using the semantic definition of $\wedge$, the induction hypothesis and the definition again, the statement is easy to show.

$$\begin{aligned} & Cl \models \Phi_1 \wedge \Phi_2 \\ \Leftrightarrow \quad & \{\!|\text{semantic definition of } \wedge \text{ as shown in the lecture}|\!\} \\ & Cl \models \Phi_1 \text{ and } Cl \models \Phi_2 \\ \Leftrightarrow \quad & \{\!|\text{induction hypothesis}|\!\} \\ & Cl2 \models \Phi_1 \text{ and } Cl2 \models \Phi_2 \\ \Leftrightarrow \quad & \{\!|\text{semantic definition of } \wedge \text{ as shown in the lecture}|\!\} \\ & Cl2 \models \Phi_1 \wedge \Phi_2 \end{aligned}$$

Case $\neg\Phi_1$: The case for negation is even simpler:

$$\begin{aligned} & Cl \models \neg\Phi_1 \\ \Leftrightarrow \quad & \{\!|\text{semantic definition of } \neg \text{ as shown in the lecture}|\!\} \\ & \text{not } (Cl \models \Phi_1) \\ \Leftrightarrow \quad & \{\!|\text{induction hypothesis}|\!\} \\ & \text{not } (Cl2 \models \Phi_1) \\ \Leftrightarrow \quad & \{\!|\text{semantic definition of } \neg \text{ as shown in the lecture}|\!\} \\ & Cl2 \models \neg\Phi_1 \end{aligned}$$

The remaining two cases are the most interesting ones, since they consider the modal operators of HML. We assume K to be an arbitrary set.

Case $[K]\Phi_1$: As before we 'unfold' the formula using the semantic definition. This splits the formula into smaller parts where we can use the induction hypothesis.

Unfolding yields the following equivalences

$$\begin{aligned} Cl \models [K]\Phi_1 &\Leftrightarrow \forall F \in \{E \mid Cl \xrightarrow{b} E,\ b \in K\}.\ F \models \Phi_1 \text{ , and} \\ Cl2 \models [K]\Phi_1 &\Leftrightarrow \forall F \in \{E \mid Cl2 \xrightarrow{b} E,\ b \in K\}.\ F \models \Phi_1 \text{ .} \end{aligned}$$

Both Cl and $Cl2$ can only perform a `tick`-action. Depending on whether $\texttt{tick} \in K$ we can determine the sets that show up in the above calculations.

$\underline{\texttt{tick} \notin K}$: In this case $\{E \mid Cl \xrightarrow{b} E,\ b \in K\} = \{E \mid Cl2 \xrightarrow{b} E,\ b \in K\} = \emptyset$, and hence the claim follows immediatly.

$$\begin{aligned} & Cl \models [K]\Phi_1 \\ \Leftrightarrow\ & \forall F \in \{E \mid Cl \xrightarrow{b} E,\ b \in K\}.\ F \models \Phi_1 \\ \Leftrightarrow\ & \forall F \in \emptyset.\ F \models \Phi_1 \\ \Leftrightarrow\ & \forall F \in \{E \mid Cl2 \xrightarrow{b} E,\ b \in K\}.\ F \models \Phi_1 \\ \Leftrightarrow\ & Cl2 \models [K]\Phi_1 \end{aligned}$$

(We do not even use the induction hypothesis.)

$\underline{\texttt{tick} \in K}$: Since the process can only do a single transition, the sets contain a single element.

$$\begin{aligned} Cl \models [K]\Phi_1 &\Leftrightarrow \forall F \in \{Cl\}.\ F \models \Phi_1 \Leftrightarrow Cl \models \Phi_1 \text{ , and} \\ Cl2 \models [K]\Phi_1 &\Leftrightarrow \forall F \in \{\texttt{tick}.Cl2\}.\ F \models \Phi_1 \Leftrightarrow \texttt{tick}.Cl2 \models \Phi_1 \text{ .} \end{aligned}$$

If we could show that $Cl2$ and $\texttt{tick}.Cl2$ are undistinguishable, then we would be done:

$$\begin{aligned} & Cl \models [K]\Phi_1 \\ \Leftrightarrow\ & \{\!|\text{see above}|\!\} \\ & Cl \models \Phi_1 \\ \Leftrightarrow\ & \{\!|\text{induction hypothesis}|\!\} \\ & Cl2 \models \Phi_1 \\ \Leftrightarrow\ & \{\!|\text{assumption: for all } \Phi\text{: } \texttt{tick}.Cl2 \models \Phi \Leftrightarrow Cl2 \models \Phi|\!\} \\ & \Leftrightarrow \texttt{tick}.Cl2 \models \Phi_1 \\ \Leftrightarrow\ & \{\!|\text{see above}|\!\} \\ & Cl2 \models [K]\Phi_1 \end{aligned}$$

Therefore it remains to show the assumption, which will be done in a separate lemma below.

Case $\langle K\rangle\Phi_1$: This case is similar to the previous one: replace all occurrences of $[K]$ by $\langle K\rangle$, and $\forall$ by $\exists$.

We now show the remaining assumption.

Lemma. For all formulas Φ we have $\texttt{tick}.Cl2 \models \Phi \Leftrightarrow Cl2 \models \Phi$.

Proof. The proof is again by structural induction. The induction base (`true`) is trivial since, for all process P, $P \models \texttt{true}$ (as before).

So, let's assume that $\texttt{tick}.Cl2 \models \Phi_1 \Leftrightarrow Cl2 \models \Phi_1$ and $\texttt{tick}.Cl2 \models \Phi_2 \Leftrightarrow Cl2 \models \Phi_2$—the induction hypothesis.

Since the reasoning is similar to the calculations shown before, I keep the explanations short.

Case $\Phi_1 \wedge \Phi_2$:

$$
\begin{array}{ll}
 & Cl2 \models \Phi_1 \wedge \Phi_2 \\
\Leftrightarrow & \{\!|\text{semantics}|\!\} \\
 & Cl2 \models \Phi_1 \text{ and } Cl2 \models \Phi_2 \\
\Leftrightarrow & \{\!|\text{induction hypothesis}|\!\} \\
 & \texttt{tick}.Cl2 \models \Phi_1 \text{ and } \texttt{tick}.Cl2 \models \Phi_2 \\
\Leftrightarrow & \{\!|\text{semantics}|\!\} \\
 & \texttt{tick}.Cl2 \models \Phi_1 \wedge \Phi_2
\end{array}
$$

Case $\neg\Phi_1$:

$$
\begin{array}{ll}
 & Cl2 \models \neg\Phi_1 \\
\Leftrightarrow & \{\!|\text{semantics}|\!\} \\
 & \text{not } (Cl2 \models \Phi_1) \\
\Leftrightarrow & \{\!|\text{induction hypothesis}|\!\} \\
 & \text{not } (\texttt{tick}.Cl2 \models \Phi_1) \\
\Leftrightarrow & \{\!|\text{semantics}|\!\} \\
 & \texttt{tick}.Cl2 \models \neg\Phi_1
\end{array}
$$

Case $[K]\Phi_1$: I only show the case if $\texttt{tick} \in K$, the other case is the same as above.

$$
\begin{array}{ll}
 & Cl2 \models [K]\Phi_1 \\
\Leftrightarrow & \{\!|\text{semantics}|\!\} \\
 & \forall F \in \{E \mid Cl2 \xrightarrow{b} E,\ b \in K\}.\ F \models \Phi_1 \\
\Leftrightarrow & \{\!|\text{definition of } Cl2|\!\} \\
 & \forall F \in \{\texttt{tick}.Cl2\}.\ F \models \Phi_1 \\
\Leftrightarrow & \{\!|\text{set theory}|\!\} \\
 & \texttt{tick}.Cl2 \models \Phi_1 \\
\Leftrightarrow & \{\!|\text{induction hypothesis}|\!\} \\
 & Cl2 \models \Phi_1
\end{array}
$$

$$
\begin{array}{ll}
\Leftrightarrow & \{\!|\text{set theory}|\!\} \\
& \forall F \in \{Cl2\}.\ F \models \Phi_1 \\
\Leftrightarrow & \{\!|\text{definition of prefix}|\!\} \\
& \forall F \in \{E \mid \texttt{tick}.Cl2 \xrightarrow{b} E,\ b \in K\}.\ F \models \Phi_1 \\
\Leftrightarrow & \{\!|\text{semantics}|\!\} \\
& \texttt{tick}.Cl2 \models [K]\Phi_1
\end{array}
$$

Case $\langle K\rangle\Phi_1$: Similar to the previous case—again I only consider $\texttt{tick} \in K$

$$
\begin{array}{ll}
& Cl2 \models \langle K\rangle\Phi_1 \\
\Leftrightarrow & \{\!|\text{semantics}|\!\} \\
& \exists F \in \{E \mid Cl2 \xrightarrow{b} E,\ b \in K\}.\ F \models \Phi_1 \\
\Leftrightarrow & \{\!|\text{definition of } Cl2|\!\} \\
& \exists F \in \{\texttt{tick}.Cl2\}.\ F \models \Phi_1 \\
\Leftrightarrow & \{\!|\text{set theory}|\!\} \\
& \texttt{tick}.Cl2 \models \Phi_1 \\
\Leftrightarrow & \{\!|\text{induction hypothesis}|\!\} \\
& Cl2 \models \Phi_1 \\
\Leftrightarrow & \{\!|\text{set theory}|\!\} \\
& \exists F \in \{Cl2\}.\ F \models \Phi_1 \\
\Leftrightarrow & \{\!|\text{definition of prefix}|\!\} \\
& \exists F \in \{E \mid \texttt{tick}.Cl2 \xrightarrow{b} E,\ b \in K\}.\ F \models \Phi_1 \\
\Leftrightarrow & \{\!|\text{semantics}|\!\} \\
& \texttt{tick}.Cl2 \models \langle K\rangle\Phi_1
\end{array}
$$