Sample solution for Pierce 3.5.17 "only if" direction

PROPOSITION If $\mathtt{t} \to^* \mathtt{v}$ then $\mathtt{t} \Downarrow \mathtt{v}$.

The solution in the back of the book is not quite right, as the errata note. There are a couple of better approaches.

Approach A

The first one uses structural induction on $\mathtt{t}$. To make things reasonably rigorous, we need a number of auxiliary lemmas. Each lemma analyzes what it means for a particular form of term to multi-step to a value and describes the implications for the subterms.

LEMMA 1. If $\mathtt{if}\ \mathtt{t}_1\ \mathtt{then}\ \mathtt{t}_2\ \mathtt{else}\ \mathtt{t}_3 \to^* \mathtt{v}$ then either $\mathtt{t}_1 \to^* \mathtt{true}$ and $\mathtt{t}_2 \to^* \mathtt{v}$, or $\mathtt{t}_1 \to^* \mathtt{false}$ and $\mathtt{t}_3 \to^* \mathtt{v}$.

This is essentially the same as Lemma A.8, except that we don't prove anything about the lengths of the evaluation sequences, since that is unnecessary for our proof of the proposition. The proof goes by induction on the length of the given evaluation sequence, as outlined in the book. All the following lemmas are proved the same way.

LEMMA 2. If $\mathtt{succ}\ \mathtt{t} \to^* \mathtt{v}$ then there exists $\mathtt{nv}$ such that $\mathtt{t} \to^* \mathtt{nv}$ and $\mathtt{v} = \mathtt{succ}\ \mathtt{nv}$.

LEMMA 3. If $\mathtt{pred}\ \mathtt{t} \to^* \mathtt{v}$ then there exists $\mathtt{nv}$ such that $\mathtt{t} \to^* \mathtt{nv}$ and either $\mathtt{nv} = \mathtt{v} = 0$ or $\mathtt{succ}\ \mathtt{v} = \mathtt{nv}$.

LEMMA 4. If $\mathtt{iszero}\ \mathtt{t} \to^* \mathtt{v}$ then there exists $\mathtt{nv}$ such that $\mathtt{t} \to^* \mathtt{nv}$ and either $\mathtt{nv} = 0$ and $\mathtt{v} = \mathtt{true}$, or $\mathtt{nv} = \mathtt{succ}\ \mathtt{nv}'$ for some $\mathtt{nv}'$ and $\mathtt{v} = \mathtt{false}$.

Now, to prove the main proposition that $\mathtt{t} \to^* \mathtt{v}$ implies $\mathtt{t} \Downarrow \mathtt{v}$, we proceed by structural induction on $\mathtt{t}$, as promised.

Case $\mathtt{t} = \mathtt{true}$

Since $\mathtt{t}$ is already a value (and hence a normal form), we have $\mathtt{v} = \mathtt{true}$, so the result follows by B-VALUE.

Cases $\mathtt{t} = \mathtt{false}$, $\mathtt{t} = 0$

Similar.

Case $\mathtt{t} = \mathtt{if}\ \mathtt{t}_1\ \mathtt{then}\ \mathtt{t}_2\ \mathtt{else}\ \mathtt{t}_3$

By Lemma 1, we have one of the following two sub-cases:

- $\mathtt{t}_1 \to^* \mathtt{true}$ and $\mathtt{t}_2 \to^* \mathtt{v}$

  By induction on sub-terms, $\mathtt{t}_1 \Downarrow \mathtt{true}$ and $\mathtt{t}_2 \Downarrow \mathtt{v}$, so the result follows by B-IFTRUE.

- $\mathtt{t}_1 \to^* \mathtt{false}$ and $\mathtt{t}_3 \to^* \mathtt{v}$

  Similar, using B-IFFALSE.

Case $\mathtt{t} = \mathtt{succ}\ \mathtt{t}'$

By Lemma 2, there exists a $\mathtt{nv}$ such that $\mathtt{t}' \to^* \mathtt{nv}$ and $\mathtt{v} = \mathtt{succ}\ \mathtt{nv}$. By induction, $\mathtt{t}' \Downarrow \mathtt{nv}$. The result follows by B-SUCC.

Case $\mathtt{t} = \mathtt{pred}\ \mathtt{t}'$

By Lemma 3, there exists $\mathtt{nv}$ such that $\mathtt{t}' \to^* \mathtt{nv}$ and either (a) $\mathtt{nv} = \mathtt{v} = 0$ or (b) $\mathtt{succ}\ \mathtt{v} = \mathtt{nv}$. By induction, $\mathtt{t}' \Downarrow \mathtt{nv}$. In case (a), the result follows by B-PREDZERO; in case (b), it follows by

B-PredSucc.

Case $\mathtt{t} = \mathtt{iszero\ t'}$

Similar, using Lemma 4 and B-IszeroZero or B-IszeroSucc. □

Approach B

An alternative, and probably simpler, approach to proving the main proposition is to do induction on the length of the derivation of $\mathtt{t} \to^* \mathtt{v}$, relying on the following lemma to show that prepending a small step preserves our ability to find a big step equivalent.

Lemma 5. If $\mathtt{t} \to \mathtt{t'}$ and $\mathtt{t'} \Downarrow \mathtt{v}$ then $\mathtt{t} \Downarrow \mathtt{v}$.

This lemma is best proved by structural induction on the derivation of $\mathtt{t} \to \mathtt{t'}$, casing over the rule used at the root of the derivation (what Pierce sometimes calls the "last rule used").

Case E-IfTrue: $\mathtt{t} = \mathtt{if\ true\ then\ t_2\ else\ t_3}$
$\mathtt{t'} = \mathtt{t_2}$

Since $\mathtt{true} \Downarrow \mathtt{true}$ by B-Value and $\mathtt{t_2} \Downarrow \mathtt{v}$, we can apply B-IfTrue to obtain $\mathtt{t} \Downarrow \mathtt{v}$.

Cases E-IfFalse,E-PredZero,E-IsZeroZero,E-IsZeroSucc:

Similar, using the corresponding B- rules.

Case E-PredSucc: $\mathtt{t} = \mathtt{pred\ succ\ nv}$
$\mathtt{t'} = \mathtt{nv}$

Similar, except that in order to apply B-PredSucc, we must first show $\mathtt{succ\ nv} \Downarrow \mathtt{succ\ v}$ by applying B-Succ to the given proof for $\mathtt{nv} \Downarrow \mathtt{v}$.

Case E-If: $\mathtt{t} = \mathtt{if\ t_1\ then\ t_2\ else\ t_3}$
$\mathtt{t'} = \mathtt{if\ t_1'\ then\ t_2\ else\ t_3}$
$\mathtt{t_1} \to \mathtt{t_1'}$
$\mathtt{if\ t_1'\ then\ t_2\ else\ t_3} \Downarrow \mathtt{v}$ (*)

There are two sub-cases, corresponding to the two rules which might have been used to build the derivation for (*).

- B-IfTrue was used, so $\mathtt{t_1'} \Downarrow \mathtt{true}$ and $\mathtt{t_2} \Downarrow \mathtt{v}$. Since $\mathtt{true}$ is a value, we can apply the inductive hypothesis to deduce that $\mathtt{t_1} \Downarrow \mathtt{true}$. Thus we can apply B-IfTrue to construct $\mathtt{if\ t_1\ then\ t_2\ else\ t_3} \Downarrow \mathtt{v}$.

- B-IfFalse was used, so $\mathtt{t_1'} \Downarrow \mathtt{false}$. Similar.

Case E-Succ: $\mathtt{t} = \mathtt{succ\ t_1}$
$\mathtt{t'} = \mathtt{succ\ t_1'}$
$\mathtt{t_1} \to \mathtt{t_1'}$
$\mathtt{succ\ t_1'} \Downarrow \mathtt{v}$ (*)

There are two sub-cases, corresponding to the rules which might have been used to build (*).

- B-Value was used, so $\mathtt{v} = \mathtt{succ\ t_1'}$. Then $\mathtt{t_1'}$ is also a value, so we can use B-Value to show that $\mathtt{t_1'} \Downarrow \mathtt{t_1'}$, and then apply the inductive hypothesis to conclude that $\mathtt{t_1} \Downarrow \mathtt{t_1'}$. Then we can apply B-Succ to construct $\mathtt{succ\ t_1} \Downarrow \mathtt{succ\ t_1'}$, i.e. $\mathtt{t} \Downarrow \mathtt{v}$.

- B-Succ was used, so $\mathtt{t_1'} \Downarrow \mathtt{nv}$ and $\mathtt{v} = \mathtt{succ\ nv}$. We can apply the inductive hypothesis to deduce that $\mathtt{t_1} \Downarrow \mathtt{nv}$. Thus we can apply B-Succ to construct $\mathtt{succ\ t_1} \Downarrow \mathtt{succ\ nv}$, i.e. $\mathtt{t} \Downarrow \mathtt{v}$.

Cases E-PRED,E-ISZERO:

Similar to E-IF. $\square$

Now to prove the main proposition that $\mathtt{t} \to^* \mathtt{v}$ implies $\mathtt{t} \Downarrow \mathtt{v}$, we proceed by (natural number) induction on the length of the derivation of $\mathtt{t} \to^* \mathtt{v}$. If the length is zero, $\mathtt{t} = \mathtt{v}$ is already a value, so we can apply B-VALUE to obtain $\mathtt{t} \Downarrow \mathtt{v}$. If the length is > 0, there is some $\mathtt{t}'$ such that $\mathtt{t} \to \mathtt{t}' \to^* \mathtt{v}$. By induction on the shorter derivation $\mathtt{t}' \to^* \mathtt{v}$, we get $\mathtt{t}' \Downarrow \mathtt{v}$. Then applying Lemma 5 immdiately gives $\mathtt{t} \Downarrow \mathtt{v}$. $\square$

As a minor alternative, we could prove the main proposition by structural induction on the derivation itself. If we do that, it is best to choose the following simpler formulation of the multi-step relation, which needs only two rules:

$$\mathtt{t} \to^* \mathtt{t} \qquad \text{(REFL)}$$

$$\frac{\mathtt{t} \to \mathtt{t}' \qquad \mathtt{t}' \to^* \mathtt{t}''}{\mathtt{t} \to^* \mathtt{t}''} \qquad \text{(STEP)}$$

These two rules obviously correspond to the zero and non-zero length cases of the proof above. It is simple to prove from these rules are equivalent to those of Exercise 3.5.10, so $\mathtt{t} \to \mathtt{t}'$ implies $\mathtt{t} \to^* \mathtt{t}'$, and $\to^*$ is transitive.