Sample Solution to COMP 523 Homework 1

Joshua Dunfield
McGill University

February 1, 2008

1 Exercise 1

Making the suggested change breaks several theorems in TAPL chapter 3:

- Theorem 3.5.4, Determinacy of One-Step Evaluation, fails:

  $$\frac{}{\texttt{pred}\ (\texttt{succ}\ (\texttt{pred}\ \texttt{z})) \rightarrow \texttt{pred}\ \texttt{z}}\ \text{(new rule)}$$

  but also

  $$\dfrac{\dfrac{\dfrac{}{\texttt{pred}\ \texttt{z} \rightarrow \texttt{z}}\ \text{E-PRED-ZERO}}{\texttt{succ}\ (\texttt{pred}\ \texttt{z}) \rightarrow \texttt{succ}\ \texttt{z}}\ \text{E-SUCC}}{\texttt{pred}\ (\texttt{succ}\ (\texttt{pred}\ \texttt{z})) \rightarrow \texttt{pred}\ (\texttt{succ}\ \texttt{z})}\ \text{E-PRED}$$

- Theorem 3.5.12 fails: since there is no longer a rule with $\texttt{pred}\ (\texttt{succ}\ \mathit{nv})$ on the left, terms of the form ... $\texttt{pred}\ (\texttt{succ}\ \texttt{t})$ get stuck. (The $\texttt{t}$ may evaluate to a value, yielding $\texttt{pred}\ (\texttt{succ}\ \mathit{nv})$, a stuck term.)

  To be painfully explicit,

  $$\texttt{pred}\ (\texttt{succ}\ \texttt{z})$$

  is stuck, which we verify by looking at every rule and seeing if it can derive $\texttt{pred}\ (\texttt{succ}\ \texttt{z}) \rightarrow \texttt{t}$ for some $\texttt{t}$.

  - Rule E-PRED-SUCC no longer exists.
  - Rule E-PRED-ZERO does not match (it derives $\texttt{pred}\ \texttt{z} \rightarrow \texttt{z}$, but we have $\texttt{pred}\ (\texttt{succ}\ \texttt{z})$).
  - Rule E-SUCC does not match.
  - Rule E-PRED matches if $\texttt{succ}\ \texttt{z} \rightarrow \texttt{t}'$ for some $\texttt{t}'$. Now we see if one can derive $\texttt{succ}\ \texttt{z} \rightarrow \texttt{t}'$. The only plausible candidate is E-SUCC, which would conclude $\texttt{succ}\ \texttt{z} \rightarrow \texttt{succ}\ \texttt{t}'$ if $\texttt{z} \rightarrow \texttt{t}'$; however, $\texttt{z} \rightarrow \texttt{t}'$ cannot be derived. Therefore E-PRED cannot derive $\texttt{pred}\ (\texttt{succ}\ \texttt{z}) \rightarrow \texttt{t}$.
  - Rules E-IF-TRUE, E-IF-FALSE, E-IF do not match.
  - Rules E-ISZERO-ZERO, E-ISZERO-SUCC, and E-ISZERO do not match.

  We have shown that there exists no $\texttt{t}$ such that $\texttt{pred}\ (\texttt{succ}\ \texttt{z}) \rightarrow \texttt{t}$. Since $\texttt{pred}\ (\texttt{succ}\ \texttt{z})$ is not a value, $\texttt{pred}\ (\texttt{succ}\ \texttt{z}) \rightarrow^* \texttt{t}$ is not derivable. Therefore 3.5.12, Termination of Evaluation, fails.

1.1 Grading notes

More than one theorem fails, but the homework only asked for one, so that was enough to (potentially) get full credit. The above solution is much more verbose than was required.

2 Exercise 2

Theorem 1. *If v is a value and $v \to^* v'$ then $v = v'$.*

Proof. By reflexivity of $\to^*$, we have $v \to^* v$. It is given that $v \to^* v'$. All values are in normal form (Theorem 3.5.7), so v and v' are in normal form. By Theorem 3.5.11 (Uniqueness of Normal Forms), $v = v'$. □

One can also prove this "from scratch":

Proof. By case analysis on the number of steps in $v \to^* v'$.

- Case: $v \to^* v'$ in zero steps. By inversion $v = v'$, which was to be shown.
- Case: $v \to^* v'$ in one or more steps. By inversion, there exists v_1 such that $v \to v_1 \to^* v'$. But there is no rule that can possibly conclude $v \to v_1$, so this case is impossible. □

3 Exercise 3

We must show $e \Downarrow v$ if and only if $e \to^* v$. We first show the left-to-right direction.

Remark 1. Note that rule B-Z is not really adequate to prove the right-to-left direction; we replace it as follows:

$$\cancel{\frac{}{z \Downarrow z}\ \text{B-Z}} \qquad \frac{}{v \Downarrow v}\ \text{B-V}$$

Equivalently, we could add rules for `true` and `false`, but B-V leads to shorter proofs. Since the assignment said "we concentrate here on the fragment for natural numbers", it was fine to only consider z.

3.1 Left-to-right direction: If $e \Downarrow v$ then $e \to^* v$

Lemma 2. *If $e \to^* e'$ then* $\texttt{succ}\ e \to^* \texttt{succ}\ e'$.

Proof. By induction on the number of steps in $e \to^* e'$.

If zero steps, we have $e = e'$. By reflexivity, $\texttt{succ}\ e \to^* \texttt{succ}\ e$, but $e = e'$ so in fact $\texttt{succ}\ e \to^* \texttt{succ}\ e'$, which was to be shown.

If one or more steps, we have $e \to^* e''$ and $e'' \to e'$. The derivation of $e \to^* e''$ has one less step than the given derivation of $e \to^* e'$, so we can apply the induction hypothesis, yielding $\texttt{succ}\ e \to^* \texttt{succ}\ e''$. We already know $e'' \to e'$. By rule E-SUCC, $\texttt{succ}\ e'' \to \texttt{succ}\ e'$. We now have

$$\texttt{succ}\ e \to^* \texttt{succ}\ e'' \quad \text{and} \quad \texttt{succ}\ e'' \to \texttt{succ}\ e'$$

By transitivity, $\texttt{succ}\ e \to^* \texttt{succ}\ e'$, which was to be shown. □

Lemma 3. *If $e \to^* e'$ then* $\texttt{iszero}\ e \to^* \texttt{iszero}\ e'$.

Proof. Similar to Lemma 2, using rule E-ISZERO instead of E-SUCC. □

Remark 2. This tactic of saying a proof is similar to another one, *except* for some specific differences, is encouraged. (Mentioning the differences is evidence that you actually did the proof.)

Lemma 4. *If $e \to^* e'$ then* $\texttt{pred}\ e \to^* \texttt{pred}\ e'$.

Proof. Similar to Lemma 2, using rule E-PRED instead of E-SUCC. □

Theorem 5. *If $e \Downarrow v$ then $e \to^* v$.*

Proof. By structural induction on the derivation of $e \Downarrow v$. We write one case for each of the 6 rules that can derive judgments of the form $e \Downarrow v$.

- **Case** B-V: $\dfrac{}{v \Downarrow v}$

  Here we have $e = v$, and need to show $v \to^* v$, i.e. that v evaluates to v in zero or more steps. This follows by reflexivity of $\to^*$.

- **Case** B-SUCC: $\dfrac{e' \Downarrow v'}{\underbrace{\texttt{succ}\ e'}_{e} \Downarrow \underbrace{\texttt{succ}\ v'}_{v}}$

  We have a derivation of $e' \Downarrow v'$ that is smaller than the given derivation, so we can apply the induction hypothesis, concluding

  $$e' \to^* v'$$

  By Lemma 2, $\texttt{succ}\ e' \to^* \texttt{succ}\ v'$, which was to be shown.

- **Case** B-ISZERO: $\dfrac{e' \Downarrow z}{\underbrace{\texttt{iszero}\ e'}_{e} \Downarrow \underbrace{\texttt{true}}_{v}}$

  We have $e' \Downarrow z$ by a smaller derivation than the given one. By induction hypothesis, $e' \to^* z$. By Lemma 3, $\texttt{iszero}\ e' \to^* \texttt{iszero}\ z$. By rule E-ISZERO-ZERO, $\texttt{iszero}\ z \to \texttt{true}$. We have $\texttt{iszero}\ e' \to^* \texttt{iszero}\ z \to \texttt{true}$, so by transitivity,

  $$\underbrace{\texttt{iszero}\ e'}_{e} \to^* \underbrace{\texttt{true}}_{v}$$

- **Case** B-ISSUCC: $\dfrac{e' \Downarrow \texttt{succ}\ v}{\texttt{iszero}\ e' \Downarrow \texttt{false}}$

  Similar to the previous case, applying E-ISZERO-SUCC instead of E-ISZERO-ZERO.

- **Case** B-PRED-ZERO: $\dfrac{e' \Downarrow z}{\underbrace{\texttt{pred}\ e'}_{e} \Downarrow \underbrace{z}_{v}}$

  By i.h., $e' \to^* z$. By Lemma 4, $\texttt{pred}\ e' \to^* \texttt{pred}\ z$. By rule E-PRED-ZERO, $\texttt{pred}\ z \to z$. We now have:

  $$\texttt{pred}\ e' \to^* \texttt{pred}\ z \to z$$

  By transitivity, $\texttt{pred}\ e' \to^* z$, which was to be shown.

- **Case** B-PRED-SUCC: $\dfrac{e' \Downarrow \texttt{succ}\ v}{\underbrace{\texttt{pred}\ e'}_{e} \Downarrow v}$

  By i.h., $e' \to^* \texttt{succ}\ v$. By Lemma 4, $\texttt{pred}\ e' \to^* \texttt{pred}\ (\texttt{succ}\ v)$.

  By rule E-PRED-SUCC, $\texttt{pred}\ (\texttt{succ}\ v) \to v$. By transitivity, $\texttt{pred}\ e' \to^* v$, which was to be shown. □

3.2 Right-to-left direction: If $e \to^* v$ then $e \Downarrow v$

Lemma 6. *For all values v, we can derive $v \Downarrow v$.*

Proof. By induction on the structure of v.

- Case: $v = z$. The result follows by rule B-V.
- Case: $v = \texttt{true}$. The result follows by rule B-V.
- Case: $v = \texttt{false}$. The result follows by rule B-V.
- Case: $v = \texttt{succ}\ v'$. By induction hypothesis, $v' \Downarrow v'$. By rule B-SUCC, $\texttt{succ}\ v' \Downarrow \texttt{succ}\ v'$.
- Case: $v = \texttt{iszero}\ v'$. The term $\texttt{iszero}\ v'$ is not a value, so this case is impossible and there is nothing to be done.
- Case: $v = \texttt{pred}\ v'$. Similarly impossible. □

Lemma 7. *If $\texttt{succ}\ e' \to^* v$ in n steps then $e' \to^* v'$ in m steps, where $v = \texttt{succ}\ v'$, and: if $n > 0$ then $m < n$; if $n = 0$ then $m = 0$.*

Proof. By induction on the number of steps n in the given derivation of $\texttt{succ}\ e' \to^* v$.

If $n = 0$, we have $v = \texttt{succ}\ e'$. Let $v' = e'$. Then $e' \to^* v'$ (by reflexivity), in 0 steps, satisfying the obligation that if $n = 0$ then $m = 0$.

If in one or more steps, we have some e such that

$$\texttt{succ}\ e' \to e \to^* v$$

The only rule that can derive $\texttt{succ}\ e' \to e$ is E-SUCC. By inversion, $e' \to e''$ where $e = \texttt{succ}\ e''$.

By i.h., $e'' \to^* v'$ in m steps, where $m < n - 1$ and $v = \texttt{succ}\ v'$.

We have $e' \to e''$ and $e'' \to^* v'$ in m steps, so

$$e' \to^* v'$$

in $m + 1$ steps. We have $m < n - 1$, so $m + 1 < n$, the last part of what was to be shown. □

Lemma 8. *If $\texttt{pred}\ e' \to^* v$ then $e' \to^* v'$ in fewer steps, where either $v' = v = z$ or $v' = \texttt{succ}\ v$.*

Proof. By induction on the number of steps n in the derivation of $\texttt{pred}\ e' \to^* v$.

If in zero steps, $v = \texttt{pred}\ e'$, but that is impossible since $\texttt{pred}\ e'$ is not a value.

If in one or more steps, we have $\texttt{pred}\ e' \to e \to^* v$. We proceed by cases on the rule used to conclude $\texttt{pred}\ e' \to e$. Three rules have conclusions that can match $\texttt{pred}\ e' \to e$.

- **Case** E-PRED-SUCC: $\dfrac{}{\texttt{pred}\ (\underbrace{\texttt{succ}\ nv}_{e'}) \to \underbrace{nv}_{e}}$

  $nv = e$ is a value, which is a normal form, so the only way we could have $e \to^* v$ is in zero steps: $e = v$. Let $v' = \texttt{succ}\ nv$. Since we have $nv = e$ and $e = v$, substituting yields $v' = \texttt{succ}\ v$. By reflexivity, $\underbrace{\texttt{succ}\ nv} \to^* \texttt{succ}\ v$, that is, $e' \to^* v'$.

- **Case** E-PRED-ZERO: $\dfrac{}{\underbrace{\texttt{pred}\ z}_{e'} \to \underbrace{z}_{e}}$

  $z = e$ is a value, which is a normal form, so we must have $e \to^* v$ in zero steps: $e = v = z$. Let $v' = v$. Then $e \to^* v'$.

- **Case** E-PRED: $\dfrac{e' \to e''}{\texttt{pred}\, e' \to \underbrace{\texttt{pred}\, e''}_{e}}$

  We have $\texttt{pred}\, e'' \to^* v$ in one less step than the given derivation. By i.h., $e'' \to^* v'$ in at least two fewer steps than the given derivation, where either $v' = v = z$ or $v' = \texttt{succ}\, v$.

  We have $e' \to e''$ as a subderivation, and $e'' \to^* v'$. Therefore $e' \to^* v'$, in at most one less step than the given derivation. □

Lemma 9. *If* $\texttt{iszero}\, e' \to^* v$ *then* $e' \to^* nv$ *in fewer steps, where either* $nv = z$ *and* $v = \texttt{true}$*, or* $nv = \texttt{succ}\, nv'$ *and* $v = \texttt{false}$*.*

Proof. By induction on the number of steps in the given derivation.

If zero steps, $v = \texttt{iszero}\, e'$, but terms of the form $\texttt{iszero}\, e'$ are not values, so this case is impossible.

If in n steps where $n > 0$, we have $\texttt{iszero}\, e' \to e''$ and $e'' \to^* v$. We proceed by cases on the rule used to derive $\texttt{iszero}\, e' \to e''$; there are three possible rules.

- **Case** E-ISZERO-ZERO: by inversion, $e' = z$, a numeric value, and $v = \texttt{false}$. $z \to^* z$ in zero steps.
- **Case** E-ISZERO-SUCC: by inversion, $e' = \texttt{succ}\, nv$, a numeric value, and $v = \texttt{true}$. $\texttt{succ}\, nv \to^* \texttt{succ}\, nv$ in zero steps.
- **Case** E-ISZERO: $\dfrac{e' \to e_1}{\texttt{iszero}\, e' \to \underbrace{\texttt{iszero}\, e_1}_{e''}}$

  We have $e'' \to^* v$, that is, $\texttt{iszero}\, e_1 \to^* v$, in $n-1$ steps. By i.h., $e_1 \to^* nv$ in fewer than $n-1$ steps, where either $nv = z$ and $v = \texttt{true}$ or $nv = \texttt{succ}\, nv'$ and $v = \texttt{false}$. We have as a subderivation $e' \to e_1$. By transitivity, $e' \to^* nv$ in at most $n-1$ steps. □

Theorem 10. *If* $e \to^* v$ *then* $e \Downarrow v$*.*

Proof. By induction on the number of steps in $e \to^* v$.

If zero, we have $e = v$. The result follows by Lemma 6.

Otherwise, we proceed by cases on the form of e.

- If $e = \texttt{succ}\, e'$, then by Lemma 7, $e' \to^* v'$, in fewer steps, and $v = \texttt{succ}\, v'$. Since $e' \to^* v'$ in fewer steps than the given derivation, we can apply the i.h., yielding $e' \Downarrow v'$. By B-SUCC, $\texttt{succ}\, e' \Downarrow \texttt{succ}\, v'$, that is, $e \Downarrow v$.
- If $e = \texttt{pred}\, e'$, then by Lemma 8, $e' \to^* v'$, in fewer steps, and either $v' = v = z$ or $v' = \texttt{succ}\, v$.
  - If $v' = v = z$: By i.h., $e' \Downarrow v'$, that is, $e' \Downarrow z$. By B-PRED-ZERO, $\texttt{pred}\, e' \Downarrow z$. Substituting gives us $e \Downarrow v$.
  - If $v' = \texttt{succ}\, v$: By i.h., $e' \Downarrow v'$, that is, $e' \Downarrow \texttt{succ}\, v$. By B-PRED-SUCC, $\texttt{pred}\, e' \Downarrow v$.
- If $e = \texttt{iszero}\, e'$, then by Lemma 9, $e' \to^* nv$ in fewer steps. By i.h., $e' \Downarrow nv$. A numeric value nv is, by definition, either z or $\texttt{succ}\, nv'$ for some nv'.

  If $nv = z$, the lemma also tells us that $v = \texttt{true}$. Applying B-ISZERO to $e' \Downarrow nv$ yields $\texttt{iszero}\, e' \Downarrow \texttt{true}$, which is $e \Downarrow v$, which was to be shown.

  The $nv = \texttt{succ}\, nv'$ case is similar to the $nv = z$ case, with the lemma giving us $v = \texttt{false}$ and applying B-ISZERO-SUCC instead of B-ISZERO.
- If e is a value (z, $\texttt{true}$, or $\texttt{false}$), we have a contradiction: $e \to^* v$ in more than zero steps, but values are normal forms. This case is therefore impossible. □

4 General comments

- If you're proving something by induction, say that you are, and say what you're inducting on. You *can* leave out "structural" or "the structure of" if you want: "By induction on the derivation of ..." is fine. Then induct on that, not on something else, no matter how convenient that seems for that one case...
- You don't need to explicitly state the induction hypothesis. That's clear from the statement of what you're inducting on.

  Similarly, you don't need to explicitly separate base and inductive cases when you're inducting on the structure of a derivation. This isn't necessary; in most situations, you just go straight into a case analysis on the rule concluding the derivation.

  I'm guessing some of you were told to write inductive proofs this way when you learned how to do proofs by induction on natural numbers. It made more sense then, because the cases were exactly $\mathfrak{n} = 0$ and $\mathfrak{n} > 0$: one base case, one inductive case, and you had to label those cases *somehow*. It makes much less sense when you're inducting on the structure of a derivation, because you can have many "base cases" (one for each rule with no premises) and many "inductive cases" (one for each rule with one or more premises).

  If you find it helpful to write out the i.h. explicitly, or to label cases, you can. But you don't have to.
- Clearly distinguish lemmas from "main" proofs. Otherwise, it's hard to see where the lemma ends and the main proof resumes. If you're writing by hand, it's OK to stick the lemma within a main proof, but indent it or something so it's clearly separated.
- Distinguish between applying a rule (when you know the premises and want to obtain the conclusion) and inverting a rule (when you know the conclusion and know that some particular rule was applied to reach it).
- Please feel free to contact me (joshua.dunfield [at] gmail.com) if you have any questions.