Constructive Logic (15-317), Fall 2016
Recitation 3: Verifications and proof terms

Evan Cavallo (`ecavallo@cs.cmu.edu`), Oliver Daids `ojd@andrew`, Giselle Reis `greis@andrew`

Solution 0: We have seen a lot of new concepts in class, and you might feel lost. Don't worry, things will start to connect now. In this homework we use only one proof and look at it through the lens of natural deduction with truth judgments, with verification judgments and proof terms. The story goes more or less like this. In natural deduction with truth judgments you can do (almost) anything you want. This includes constructing proofs that are somehow redundant. When annotating the proofs with proof terms, the redundancy can be detected by the presence of *redexes* (i.e., terms that can be reduced, like function applications). If we use the verification judgments, we are less flexible, but the proofs now give nicer and more concise proof terms, without these redexes (and also making proof search easier as a pleasant side effect ;).

Let φ be the following proof:

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \land (A \land A) \supset B}\,u}{(A \land A) \supset B\ \mathit{true}}\,\land E_2 \quad \dfrac{\dfrac{}{A\ \mathit{true}}\,w \quad \dfrac{}{A\ \mathit{true}}\,w}{A \land A\ \mathit{true}}\,\land I}{B\ \mathit{true}}\,\supset E}{A \supset B\ \mathit{true}}\,\supset I^w \quad \dfrac{\dfrac{}{A \land (A \land A) \supset B}\,u}{A\ \mathit{true}}\,\land E_1}{B\ \mathit{true}}\,\supset E}{A \land ((A \land A) \supset B) \supset B\ \mathit{true}}\,\supset I^u
$$

1 Verification

Task 1. Transform this proof into a proof using verification judgments, i.e., a proof of $A \land (A \land A \supset B) \supset B\ \uparrow$.

Solution 1: The point of this task is to show that, although the rules "look" the same for the verification judgments, they disallow the kind of proof like φ. In order to prove the verification, the proof must be:

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \land (A \land A \supset B)\ \downarrow}\,u}{A \land A \supset B\ \downarrow}\,\land E_2 \quad \dfrac{\dfrac{\dfrac{\dfrac{}{A \land (A \land A \supset B)\ \downarrow}\,u}{A\ \downarrow}\,\land E_1}{A\ \uparrow}\,\downarrow\uparrow \quad \dfrac{\dfrac{\dfrac{}{A \land (A \land A \supset B)\ \downarrow}\,u}{A\ \downarrow}\,\land E_1}{A\ \uparrow}\,\downarrow\uparrow}{A \land A\ \uparrow}\,\land I}{B\ \downarrow}\,\supset E}{B\ \uparrow}\,\downarrow\uparrow}{A \land (A \land A \supset B) \supset B\ \uparrow}\,\supset I^u
$$

2 Proof terms

Task 2. Annotate both proofs above with proof terms. For the verification judgments, consider that the proof terms used are the same as for the *true* judgments, and that on the $\downarrow\uparrow$ rule the proof terms of the premise and conclusion remain the same.

Solution 2: Note that the verification proof can be straightforwardly translated to a natural deduction proof with truth judgments.

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{u : A \wedge (A \wedge A) \supset B}\,u}{\mathbf{snd}\ u : (A \wedge A) \supset B\ \ true}\,\wedge E_2 \quad \dfrac{\dfrac{}{w : A\ \ true}\,w \quad \dfrac{}{w : A\ \ true}\,w}{\langle w, w\rangle\ A \wedge A\ \ true}\,\wedge I}{\mathbf{snd}\ u\ \langle w, w\rangle\ B\ \ true}\,\supset E}{\lambda w.\mathbf{snd}\ u\ \langle w, w\rangle : A \supset B\ \ true}\,\supset I^w \quad \dfrac{\dfrac{}{u : A \wedge (A \wedge A) \supset B}\,u}{\mathbf{fst}\ u : A\ \ true}\,\wedge E_1}{(\lambda w.\mathbf{snd}\ u\ \langle w, w\rangle)\mathbf{fst}\ u : B\ \ true}\,\supset E}{\lambda u.(\lambda w.\mathbf{snd}\ u\ \langle w, w\rangle)\mathbf{fst}\ u : A \wedge ((A \wedge A) \supset B) \supset B\ \ true}\,\supset I^u
$$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{u : A \wedge (A \wedge A \supset B) \downarrow}\,u}{\mathbf{snd}\ u : A \wedge A \supset B \downarrow}\,\wedge E_2 \quad \dfrac{\dfrac{\dfrac{\dfrac{}{u : A \wedge (A \wedge A \supset B) \downarrow}\,u}{\mathbf{fst}\ u : A \downarrow}\,\wedge E_1}{\mathbf{fst}\ u : A \uparrow}\,\downarrow\uparrow \quad \dfrac{\dfrac{\dfrac{}{u : A \wedge (A \wedge A \supset B) \downarrow}\,u}{\mathbf{fst}\ u : A \downarrow}\,\wedge E_1}{\mathbf{fst}\ u : A \uparrow}\,\downarrow\uparrow}{\langle \mathbf{fst}\ u, \mathbf{fst}\ u\rangle : A \wedge A \uparrow}\,\wedge I}{\mathbf{snd}\ u\ \langle \mathbf{fst}\ u, \mathbf{fst}\ u\rangle : B \downarrow}\,\supset E}{\mathbf{snd}\ u\ \langle \mathbf{fst}\ u, \mathbf{fst}\ u\rangle : B \uparrow}\,\downarrow\uparrow}{\lambda u.\mathbf{snd}\ u\ \langle \mathbf{fst}\ u, \mathbf{fst}\ u\rangle : A \wedge (A \wedge A \supset B) \supset B \uparrow}\,\supset I^u
$$

Task 3. What is the relation between these two terms?

Solution 3: The proof term obtained from the verification proof is equivalent to that of φ after one step reduction.

3 Tutch with proof terms

Tutch allows you to annotate your proof with proof terms by declaring it with `annotated proof`. An annotated proof is just like a regular Tutch proof, but each line `A` is annotated with the term that justifies it `M : A`.

```
annotated proof andComm : A & B => B & A =
begin
[ u : A & B;
  snd u : B;
  fst u : A;
  (snd u, fst u) : B & A];
fn u => (snd u, fst u) : A & B => B & A
end;
```

It is also possible to simply give the proof term. To give a proof term in Tutch, declare it with `term` rather than `proof`:

```
term andComm : A & B => B & A =
  fn u => (snd u, fst u);
```

For more examples, see Chapter 4 of the Tutch User's Guide. The proof terms are very similar to the ones given in lecture and are summarized in Section A.2.1 of the Guide.

Task 4. Give annotated proofs and the corresponding proof terms for both proofs above in tutch.

Solution 4: See source code.