Homework # 8 SOLUTION
due April 15, 13:00

Please turn in the answers to problems (§2) on paper in class, and send the SASyLF parts (§3,4) to `scmalte@inf.ethz.ch` before the 1pm deadline.

1   Reading

Please read Chapter 15 in your textbook.

2   Problems

Please do the following problems

- Exercise 15.2.1

- Exercise 15.2.3

Check your answers against the solutions in the book, but do *not* turn them in.
   Please do the following problems:

- Exercise 15.5.1 (proof sketch only required)

  > In the proof of preservation, we have a typing and an evaluation and need to show that the result is typed. We have two rules for `as`, (original) T-ASCRIBE and (new) T-DOWNCAST and two evaluation rules: (original) E-ASCRIBE1, and (new) E-DOWNCAST. The latter evaluation rule *replaces* the former E-ASCRIBE. Here's how the cases are handled in the new proof:
  >
  > **T-Ascribe and E-Ascribe1** By the induction hypothesis, the new term has the correct type (or a subtype) and we can apply `T-Ascribe` again, perhaps after applying T-SUB if the new type was a subtype.
  >
  > **T-Downcast and E-Ascribe1** Similar except that we won't need to add T-SUB.
  >
  > ***either* and E-Downcast** The typing we get from E-DOWNCAST is precisely what is needed.

- Exercise 15.5.2 (the "program" should use the combined syntax of Chapters 13 and 15).

  > 1. $(\lambda$ r:Ref {a:Top}. (!r).a)(ref {})
  >
  > 2. $(\lambda$ r1:Ref {a:Top}. $(\lambda$ r2:Ref Top . r2 = {}) r1, (!r1).a)(ref {a={}})

Turn in your answers to these problems.

3   Proofs

Adding T-SUB drastically changes a type system, especially the canonical forms lemmas. You are provided with proof of type soundness for the simply-typed lambda calculus with records. You need to change the proofs to add subtyping.
   The skeleton file for this homework, not only includes records and the proof of soundness but also the subtyping relation. You need to do several things:

- Modify the canonical forms definitions so that it handles the results of Lemma 15.3.3 and Lemma 15.3.6. (This work is done for you in comments.)

- Prove the subtyping inversion lemma (Lemma 15.3.2). (You may use the solution on page 519 to help.)

- Rewrite the canonical forms lemma to generate the updated definitions. (And fix the helper lemmas that generate typings.)

- Fix the proofs of progress and preservation to handle the updated canonical forms. (And add the cases for T-SUB, which are easy inductive cases.)

4   Mechanization

Take a paper published recently[1] in a prestigious venue[2] (best if one of the papers you have discussed in an earlier homework), and represent the syntax and judgments for evaluation in SASyLF. If the system requires the use of identifiers that aren't bound variables, then either use natural numbers, as we do for records, or just list three possibilities, as in:

    id ::= a | b | c

This assignment should be not too simple nor too hard. If the syntax and judgments in the paper are too simple, choose a different paper. If they are too hard, you may select a subset. Check with the instructors if you are not sure. For an example, see the master solution to Homework 7.5. You may also ask a paper to be assigned to you.

---

[1]Within last five years
[2]Top journal or conference; ask if unsure