Homework # 1

due February 25, 13:00

The natural language proof (§2) and inversion exercises (§3) should be done on paper and submitted at the *beginning* of the lecture on Tuesday, February 25th. The SASyLF proofs (§4,5) should be submitted as attachments by email to `scmalte@inf.ethz.ch` *before* 1pm on Tuesday, February 25th. Please use UTF-8 text encoding for your SASyLF files.

1 Reading

Please read Chapters 1–3 in your textbook through the end of 3.3

2 Problems

Please do the following problem from the book:

2.2.7 (transitive closure) full natural language proof required

This is such an elementary result that sometimes it is hard to explicitly go through the steps. To get an idea of how to write such a proof, please read the accompanying handout.

Solution:

To prove that R^+ is indeed the transitive closure of R, we need to show that (1) $R^+ \supseteq R$, obvious since $R^+ \supseteq R_0 = R$, (2) R^+ is transitive and (3) it is the smallest transitive relation including R.

2. We wish to prove that R^+ is transitive. Thus suppose $(s,t), (t,u) \in R^+$. We need to prove that $(s,u) \in R^+$.

   We first prove a lemma about the R_i sets: If $i \leq j$, then $R_i \subseteq R_j$. We prove this by induction on $j - i$.

   > Suppose $i = j$, then $R_i = R_j$ and thus $R_i \subseteq R_j$.
   > Next suppose $i < j$ and hence $i + 1 \leq j$. Now by induction (since $j - (i+1) < j - i$), we have $R_{i+1} \subseteq R_j$. Further, by definition of R_{i+1} we have $R_{i+1} = R_i \cup ...$ and thus $R_i \subseteq R_{i+1}$. By the transitivity of $\subseteq$, we have $R_i \subseteq R_j$. QED

   An element is in a union, even an infinite union, if and only if it is in one of the sets included in the union. Thus the two elements (s,t) and (t,u) must be in at least one of the sets making up the infinite union. Suppose we have i, j such that $(s,t) \in R_i$ and $(t,u) \in R_j$. Let $k = i + j$. Since i and j are natural numbers, we have $i \leq k$ and $j \leq k$ and thus (by the lemma) $R_i \subseteq R_k$ and $R_j \subseteq R_k$ and thus both elements are in R_k.

   Now the definition of R_{k+1} implies that it includes (s,u) whenever $(s,t), (t,u) \in R_k$. Since this is indeed the case, we can conclude $(s,u) \in R_{k+1}$ and thus $(s,u) \in R^+$. Thus R^+ is transitive.

3. Next, we have to prove that for any $R' \supseteq R$ that is transitive, we must have $R^+ \subseteq R'$. We will prove this fact by showing that every $R_i \subseteq R'$ by induction on i. First we have $R_0 \subseteq R'$ since $R_0 = R$ and $R \subseteq R'$ which is one of the two facts known about R'.

   Next, suppose $R_i \subseteq R'$. We will prove that $R_{i+1} \subseteq R'$. Every element of R_{i+1} is either in R_i and hence in R' or is (s, u) for some $(s, t), (t, u)\ inR_i$. Now since $R_i \subseteq R'$, we must have that $(s, t), (t, u)\ inR'$ too and thus by the transitivity of R', we have $(s, u) \in R'$. Thus every element in R_{i+1} is in R'.

   Now that we know that all $R_j \subseteq R'$, the union of all these sets R^+ must also be included in R' (by definition of union). QED

3 Inversion

Suppose we have the following definition of natural numbers:

$n ::= \mathsf{z} \mid \mathsf{s}\, n$

And further, the following definition of addition:

$$\textsc{PlusZero}\ \frac{}{\mathsf{z} + n = n} \qquad \textsc{PlusSucc}\ \frac{n_1 + n_2 = n_3}{\mathsf{s}\, n_1 + n_2 = \mathsf{s}\, n_3}$$

For each of the following possibilities, give the cases that are possible inverting this relation just *once*.

For example:

$A + B = B$

We have two cases:

1. (PlusZero) $A = \mathsf{z}$
2. (PlusSucc) $A = \mathsf{s}\, D$, $B = \mathsf{s}\, E$ and we have the additional relation $D + (\mathsf{s}\, E) = E$.

   (As it happens, this case is impossible, but one level of inversion is not enough to prove this fact.)

1. $A + B = C$

   Either:

   (a) (PlusZero) $A = \mathsf{z}$ and $B = C$, or

   (b) (PlusSucc) $A = \mathsf{s}\, D$, $C = \mathsf{s}\, E$ and $D + B = E$.

2. $\mathsf{s}\,\mathsf{z} + B = C$

   The only case possible is (PlusSucc), so we must have $C = \mathsf{s}\, D$ and $\mathsf{z} + B = D$.

3. $A + \mathsf{z} = C$.

   Either:

   (a) (PlusZero) $A = C = \mathsf{z}$, or

   (b) (PlusSucc) $A = \mathsf{s}\, D$, $C = \mathsf{s}\, E$ and $D + \mathsf{z} = E$.

4. $A + A = C$

   > Either:
   >
   > (a) (PlusZero) $A = C = \mathsf{z}$, or
   >
   > (b) (PlusSucc) $A = \mathsf{s}\,D$, $C = \mathsf{s}\,E$ and $D + \mathsf{s}\,D = E$.

5. $A + B = \mathsf{z}$

   > The only possibility is PlusZero, which means $A = B = \mathsf{z}$.

4 Natural Numbers

Using the following definition of "greater than" on natural numbers as defined in §3.

```
judgment gt: n > n

------- gt-one
s n > n

n1 > n2
--------- gt-more
s n1 > n2
```

Prove the following theorems in SASyLF:

1. For any n, we have $(\mathsf{s}\,n) > 0$.
2. "Greater than" is transitive.
3. If $\mathsf{s}\,n_1 > \mathsf{s}\,n_2$ then $n_1 > n_2$.
4. If $n > n$ then we have a contradiction.
   For this you need to define a contradiction judgment, e.g.:

   ```
   judgment absurd: contradiction
   ```

Put your SASyLF text in a file `gt.slf`. Include your full name in a comment at the start of the file.

5 Terms

Define the boolean term language (`true`, `false` and `if`) and define equality (with only one rule) over the terms and then prove the following theorems:

1. If `if` t_0 `then` t_1 `else` t_2 `==` `if` t_0' `then` t_1' `else` t_2', then t_0 `==` t_0'.
2. If t_0 `==` t_0', t_1 `==` t_1', and t_2 `==` t_2' then `if` t_0 `then` t_1 `else` t_2 `==` `if` t_0' `then` t_1' `else` t_2'.

Put your solution in a file `term.slf`, again with your full name at the start.