UNIVERSITÉ DE GENÈVE
FACULTÉ DES SCIENCES
Département d'informatique

Master of Computer Science

Software modeling and verification
Home Work 3

ADT : proofs and rewriting

Author :
Mohammad Oday Darwich

Professors :
M. Didier Buchs
M. David Lawrence

5 janvier 2016

0.1 Introduction

The goal of this TP is to cover two aspects in the domain of ADTs : proofs (both deductive and inductive) and rewriting systems.
The aim of **Proofs in algebraic specifications** is the proof of specification properties in a systematic way. So how to proceed from the axioms :

- Use equational rules (reflexivity,symmetry, transitivity)
- Use functional composition rules
- Use variable substitution rules)

$\rightarrow$ we obtain equational theorems

0.2 Exercice 1 : Proof

Make a detailed and precise proof of the following theorem by using the ADTs in listings 1 and 2.

```
s($x) divide s($x) = s(zero)
```

Here we have $P(\$x) = s(\$x)\ divide\ s(\$x) = s(zero)$ $P(\$x)$ represent some statement about \$x. The statement is either true or false, depending on \$x.
The proof will take three place :
- **Claim :** $\forall x$, $P(\$x)$ is true.
- **Base Casse :** Prove the base case of the set satisfies the property $P(\$x)$
- **Induction Step :** We assume that $P(\$x)$ is true for any \$x (**The induction hypothesis**) then we prove that the rules of the inductive step preserves the property $P(\$x)$

1. **Proove** : $P(\$x) = s(\$x)\ divide\ s(\$x) = s(zero)$
2. **Claim** : $\forall x$, $P(\$x)$ is true
3. **Proove by induction for** $\$x\ ge\ \$x = true$ **?** 3

   - **Base Case :** $\$x = zero$ then we have **To proove** : $zero\ ge\ zero = true$
     With the axiom below ↷

     ```
     $x ge zero = true;
     ```

     Substitution $\$x\ by\ zero$ then
     $zero\ ge\ zero = true$ then ✓

   - **Iduction Step :**
     To proove : $s(\$x)\ ge\ s(\$x) = true$

   - So we **Assume :** $zero\ ge\ zero = true$
     With the axiom below ↷

     ```
     s($x) ge s($y) = $x ge $y;
     ```

     Substitution $\$x\ by\ \$x\ and\ \$y\ by\ \$x$ then
     $s(\$x)\ ge\ s(\$x) = \$x\ ge\ \$x$

     Transitivity for the latter and with what we Assumed then
     s(\$x) ge s(\$x) = true then ✓
     3 Prooved $\$x\ ge\ \$x = true$✓, and with **Substitution** $\$x\ by\ s(\$x)$ then $s(\$x)\ ge\ s(\$x) = true$ ✓

As we have prooved in 3 and with the axim below $\curvearrowright$

```
if ge($x, $y) = true then $x divide $y = s(($x minus $y) divide $y);
```

Doing the **Substitution** $\$x\ by\ s(\$x)\ and\ \$y\ by\ s(\$x)$ then

```
if s($x) ge s($x) = true then s($x) divide s($x) = s((s($x) minus s($x)) divide s($x)) "A"
```

and with what we prooved 3 and the substitution we arrive to

```
s($x) divide s($x) = s((s($(x) minus s($x)) divide s($x)) "B"
```

4. **Proove by induction for** $\$x\ minus\ \$x = zero$ **? 4**

   – **Base Case :** $\$x \ = \ zero$ then we have **To proove** : $zero\ minus\ zero \ = zero$
   With the axiom below $\curvearrowright$

```
$x minus zero = $x;
```

   Substitution $\$x\ by\ zero$ then
   $zero\ minus\ zero = zero$ then ✓

   – **Iduction Step :**
   To proove : $s(\$x)\ mins\ s(\$x) \ = zero$

   • So we **Assume :** $\$x\ minus\ \$x \ = zero$
   With the axiom below $\curvearrowright$

```
s($x) minus s($y) = $x minus $y;
```

   Substitution $\$x\ by\ \$x\ and\ \$y\ by\ \$x$ then
   $s(\$x)\ minus\ s(\$x) \ = \ \$x\ minus\ \$x$

   Transitivity for the latter and with what we Assumed then
   $s(\$x)\ minus\ s(\$x) \ = zero$ then ✓
   4 Prooved $\$x\ minus\ \$x = zero$ ✓, and with **Substitution** $\$x\ by\ s(\$x)$ then $s(\$x)\ minus\ s(\$x) \ = zero$ ✓
   As we have prooved in 4 and with the right part (after the =) of the axim below $\curvearrowright$

```
if ge($x, $y) = true then $x divide $y = s(($x minus $y) divide $y);
```

   Doing the **Substitution** $\$x\ by\ s(\$x)\ and\ \$y\ by\ s(\$x)$ then

```
if s($x) ge s($x) = true then s($x) divide s($x) = s((s($x) minus s($x)) divide s($x)) "A"
```

   and with what we prooved 4 and the substitution we arrive to

```
if s($x) ge s($x) = true then s($x) divide s($x) = ( (s($x) minus s($x)) divide s($x) ) ~ s( zero divide s($x) ) "C"
```

5. Now i want to reduce the left part of what i arrived just before " $s(zero\ divide\ s(\$x))$" to zero (if did it then the theorem 0.2 i want to proof is true.

6. I see that with the second case of the axiom *divide* i will try to reduce it.

```
if ge($x, $y) = false then $x divide $y = zero;
```

I want to arrive to $zero\ divides(\$x) = zero$, after doing substitution in this axiom above, so i see that i have to proove that $ge(zero, s(\$x))$

- **To proove** : $ge(zero, s(\$x) = false$
  from the axiom below ↷

```
zero ge s($x) = false;
```

so it's false (right) ✓and with the axiom mentioned first in point 6.
Doing the **Substitution** $\$x$ *by zero and* $\$y$ *by* $s(\$x)$ then from the left part of what it's on 4

```
zero divide s($x) = zero; "G"
```

then Doing **Transitivity** at last of the point 4. "C" 4 and "G" 6 then

```
s(zero divide s($x) )= s( zero ) "H"
```

then the Theorem is Prooved 1

```
s($x) divide s($x) = s(zero)
```

0.3 Exercise 2 : Rewriting systems and Stratagem

As we see in the RewritingPresentation.pdf on the exercice, we see that in the re-writing system the orientation is important.
and probles come with wrong orientation cause two probleme the confluence and the termination, *the confluence property which it's is verified if a rewrite system converge it to a unique value (course S87/79)* and it was resolved with Knuth-Bendix but the second problem was not resolved yet ☹ !

We see that in the Listing 1 if we re-write the first 2 axioms in the orientation (left to right)

```
false = not(true);
true = not(false);
```

we will have $false_{\rightarrow_1} not(true) {\rightarrow_2} not(not(false)) {\rightarrow_1} not(not(not(true)))_{\rightarrow_1}$... and so on, so on...
so with continuing re-writing, it will to be more and more complex and then we see the problem on non termination.

0.4 Exercise 3 : The terrifying journey of a little girl

To lunch stratagem we open the command prompt and we put the directory of .../bin
then we put the command

$$stratagem\ transition - system\ filename.ts$$

or

$$stratagem.bat\ transition - system\ filename.ts$$

Question 1 Applying the transition

```
continue_the_terrifying_journey_with_fear    = One(Try_to_reach_light_switch_with_fear(), 1)
```

it will call

```
Try_to_reach_light_switch_with_fear    = ForEachRoom(Freeze())
```

and the latter will call Freeze() foreachroom, but the freeze will work $\iff$ there are a ghost and if there is a ghost in the next section of the corridor, the girl will freeze and close her eyes and here is the question what to do if there are no ghost ? we can do nothing wo it will fail then the function calling freeze will fail also, then all will fail so to not let the system fail we apply *One* because The strategy *One()* is non deterministic so if we apply it it take one of the sub terms and it apply the strategy for this sub term and if all result all fail then it will fail. so as strategies can fail if there is no possible rule application, we use an order on the rules to provide with deterministic behaviours.

Question 2 ForEachRoom(V) = Choice(One(ForEachRoom(V), 2), V) it a recursive strategies and it's to repeat the term for the ∞ if it's needed.

Question 3 There are seven state because to do the journey the little girl will pass by 7 state, between get out of her bedroom and walk taking a steps between entities$_s$*pace* and reach the light switch at the end of the corridor.

Question 4 when we change the initial state in the third empty space of the corridor to ghost we obtain 8 states, That mean that to reach the light the girl take one more state.

Question 5 if we had a ghost in the first empty space has follow we get one state so the thing is that the girl will do just one step is to get out but it will freeze because of ghost and freezing as we said in the first question will fail the system.
so it do one step and the system fail.

0.5 References

ref : http ://goo.gl/gCQro3