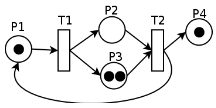
ADT : Proofs



October 15rd 2015

David Lawrence Edmundo Lopez Alexis Marechal

Today we will study the relation between a model and its specification in the domain of AADTs, and two methodologies to prove theorems in this domain: equational and inductive proofs.

Consider the following AlPiNA ADT for the natural numbers :

```
ADT nat
Sorts
  nat;
Generators
  zero: nat;
  suc : nat -> nat;
Operations
  + : nat, nat -> nat;
Axioms
  x + zero = x;
  x + suc(y) = suc(x+y);
Variables
  x : nat;
  y : nat;
```

Exercise 1 : Algebraic specification

1. Given the previous AlPiNA code, define formally the algebraic specification that it represent.

Exercise 2 : Σ algebras and models

1. Is the well known set of natural numbers $\mathbb{N}$ a Σ-algebra, if Σ is the signature of the above specification ?

Exercise 3 : Deductive proof (equational proof)

use only axioms and deduct from..

and theorem basic

1. Make a *detailed* proof of the following theorem :

```
x + suc(zero) = suc(x)
```

Exercise 4 : Inductive proof

Consider the following theorem :

```
suc (zero) + x = suc(x)
```

1. Is it possible to prove it in the same way as the theorem from exercise 3 ? Why ?
2. *(Finitely generated by the generators algebra)* Make a detailed proof of this theorem by taking into account that $\mathbb{N}$ is finitely generated by the generators of the AADT.
3. *(Finitely generated algebra)* How would you do this proof if $\mathbb{N}$ was only finitely generated ?

Exercise 5 : Another algebra

Consider a new set that we will call $\mathbb{N}' = \mathbb{N} \cup \{*, *'\}$, with a unary operation $suc^{\mathbb{N}'}$ and a binary operation $+^{\mathbb{N}'}$ defined respectively in tables 1 and 2.

$suc^{\mathbb{N}'}(n)$	
$n \in \mathbb{N}$	$n+1$
$n = *$	$*$
$n = *'$	$*'$

Table 1 – Behavior of the operation $suc^{\mathbb{N}'}$ in $\mathbb{N}'$.

$+^{\mathbb{N}'}(m,n)$	$n \in \mathbb{N}$	$n = *$	$n = *'$
$m \in \mathbb{N}$	$m+n$	$*'$	$*$
$m = *$	$*$	$*$	$*$
$m = *'$	$*'$	$*'$	$*'$

Table 2 – Behavior of the operation $+^{\mathbb{N}'}$ in $\mathbb{N}'$.

For instance, these tables indicate that :
$suc^{\mathbb{N}'}(2) = 3$, $suc^{\mathbb{N}'}(*) = *$ and $suc^{\mathbb{N}'}(*') = *'$,
$+^{\mathbb{N}'}(2,3) = 5$, $+^{\mathbb{N}'}(1,*) = *'$, $+^{\mathbb{N}'}(*,1) = *$ and $+^{\mathbb{N}'}(*',*) = *'$.

1. *(Model)* Is this new set $\mathbb{N}'$ a model of the AADT nat ?
2. *(Proofs)* Make the proofs in the exercises 3 and 4 for $\mathbb{N}'$.