1 Arbitrarily Branching Trees

spec ArbitrarilyBranchingTrees =

free types $Tree ::= node(TreeList);$

$TreeList ::= notree \mid \_\_ \circ \_\_(TreeList, Tree);$

preds $edge : Tree \times Tree;$

$path : Tree \times Tree;$

vars $l : TreeList; \quad t, t' : Tree$

axioms

$\neg edge(node(notree), t);$ %Ax1

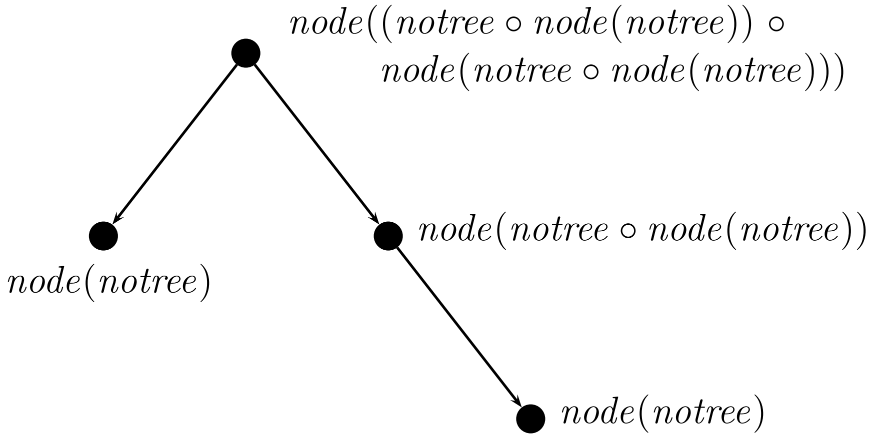
$edge(node(l \circ t), t);$ %Ax2

$t \neq t' \;\Rightarrow\; (edge(node(l \circ t), t') \Leftrightarrow edge(node(l), t'));$ %Ax3

$path(t, t') \;\Leftrightarrow\; (edge(t, t') \vee \exists t'' : Tree \bullet (edge(t, t'') \wedge path(t'', t')));$ %Ax4

end

2 An Example Tree



3 Transitivity of *path*

spec ArbitrarilyBranchingTrees2 =
ArbitrarilyBranchingTrees

then %implies

axiom

$\forall x, y, z : Tree \bullet (path(x, y) \wedge path(y, z)) \Rightarrow path(x, z);$

end

On the logical level, the %implies keyword is nothing but a comment. This means, the extending spec is conjunctively added to the original one as if the

%implies was not there. On the pragmatical level (i.e., when working with a tool), a proof obligation should be generated to check that the extending spec indeed follows from the original one. We will do this proof by hand below.

4 Proof by Induction

Given
A free type T
A well-founded ordering $<$ on the ground terms of type T

Then
To prove

$$\forall x : T \bullet \phi(x)$$

it is sufficient to show for all ground terms t of type T:

$$\phi(t') \text{ for all } t' < t \qquad \text{implies} \qquad \phi(t)$$

5 In This Example

Ordering:
$t' < t$ iff t' has less symbols than t

Induction Schema:
To prove

$$\forall x : \mathit{Tree} \bullet \phi(x)$$

show

$$\begin{array}{l} \phi(\mathit{node}(\mathit{notree})) \\ \phi(\mathit{node}(l)) \wedge \phi(t) \ \Rightarrow \ \phi(\mathit{node}(l \circ t)) \end{array}$$

6 Proof

We are showing $\forall x : \mathit{Tree} \bullet \phi(x)$ with

$$\phi(x) \equiv \forall y, z : \mathit{Tree} \bullet (\mathit{path}(x, y) \wedge \mathit{path}(y, z)) \Rightarrow \mathit{path}(x, z)$$

6.1 Lemma

First, we need a small lemma. The Lemma says that

$$\mathit{edge}(\mathit{node}(l), x) \Rightarrow \mathit{edge}(\mathit{node}(l \circ t), x)$$

Proof is by case distinction. If $x = t$ then $\mathit{edge}(\mathit{node}(l \circ t), x)$ is an immediate consequence of Ax2. If $x \neq t$ then the Lemma follows from the right-to-left direction of Ax3.

6.2 Induction Start

For the start, we have to show $\phi(node(notree))$, which is short for:

$$\forall y, z : Tree \bullet (path(node(notree), y) \wedge path(y, z)) \Rightarrow path(node(notree), z) \quad (0)$$

In the premiss of (0), the first conjunct $path(node(notree), y)$ requires by Ax4 either $edge(node(notree, y))$ or $edge(node(notree, t''))$ for some node t''. Both is impossible in this one-node tree by Ax1. Thus the premiss of (0) is false and we have proven (0).

6.3 Induction Step

The induction schema chosen above has two induction hypotheses. Thus, during the proof, we can assume that $\phi(node(l))$ holds, which is short for

$$\forall y, z : Tree \bullet (path(node(l), y) \wedge path(y, z)) \Rightarrow path(node(l), z) \quad \text{(IH1)}$$

We can also assume that $\phi(t)$ holds, which is short for

$$\forall y, z : Tree \bullet (path(t, y) \wedge path(y, z)) \Rightarrow path(t, z) \quad \text{(IH2)}$$

To complete induction, we have to show $\phi(node(l \circ t))$ holds, which is short for

$$\forall y, z : Tree \bullet (\underbrace{path(node(l \circ t), y)}_{(1)} \wedge \underbrace{path(y, z)}_{(2)}) \Rightarrow \underbrace{path(node(l \circ t), z)}_{(3)} \quad (*)$$

This is an implication, so altogether we will assume (1),(2),(IH1), and (IH2). From this we have to show (3). For this, we take a closer look at (1) and make a case distinction following Ax4.

Case 1: There is a direct edge from $node(l \circ t)$ **to** y

We have not only $path(node(l \circ t), y)$ but even $edge(node(l \circ t), y)$ and together with (2) this gives us (3) by Ax4. We have proven (*).

Case 2: There is no direct edge from $node(l \circ t)$ **to** y

We have $path(node(l \circ t), y)$ but not $edge(node(l \circ t), y)$. This means (by Ax4) that there must be some node u such that

$$\underbrace{path(node(l \circ t), u)}_{(4)} \wedge \underbrace{path(u, y)}_{(5)}$$

Case 2a: $u = t$

With $u = t$ (5) becomes $path(t, y)$. Using this together with (2) in (IH2) gives us $path(t, z)$. Adding Ax2 ($path(node(l \circ t), t)$) we obtain $path(node(l \circ t), z)$ by (IH1). This is (3) and we have proven (*).

Case 2b: $u \neq t$

Keeping in mind that $u \neq t$, we derive by Ax3 from (4) that $edge(node(l), u)$. From this with (5) and Ax4: $path(node(l), y)$. From this with (2) and (IH1): $path(node(l), z)$.

Here we again get to distinguish two cases.

Case 2b1: There is a direct edge $edge(node(l), z)$

With Lemma we get $edge(node(l \circ t), z)$ and per Ax4 we obtain (3). We have proven (*).

Case 2b2: $\neg edge(node(l), z)$

Per Ax4 there is some node v such that

$$edge(node(l), v) \wedge path(v, z)$$

This can be transformed with Lemma into

$$edge(node(l \circ t), v) \wedge path(v, z)$$

from where with Ax4 we obtain (3). We have proven (*).