

# Proof 1

October 18, 2013

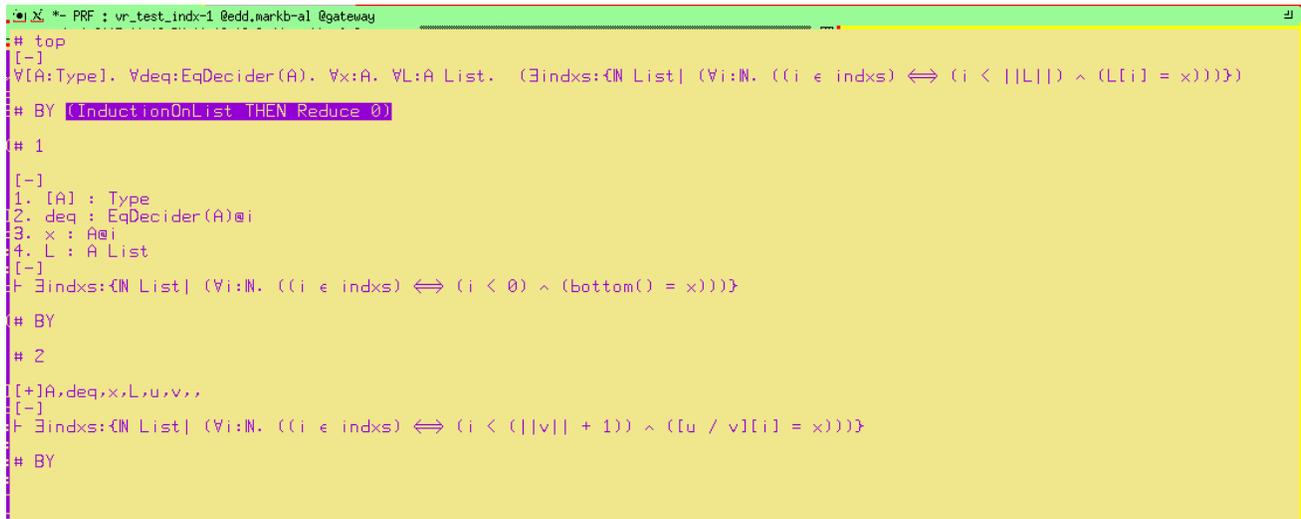
In this document we present a proof of

$$\begin{aligned} \text{INDXS} = & \forall A : \text{Type}. \\ & \forall x : A. \\ & \forall \text{lst} : \text{List}(A). \\ & \exists \text{indx} : \text{List}(\mathbb{N}). \\ & \forall i : \mathbb{N}. \quad i \in_{\mathbb{N}} \text{indx} \\ & \iff \\ & i < ||\text{lst}|| \wedge x = \text{lst}[i] \in A \end{aligned}$$

that generates the following program:

```
let rec indexes x lst =
  match lst with
  [] -> []
| h :: t ->
  let l = List.map (fun x -> x + 1) (indexes x t)
  in if x = h then 0 :: l else l ;;
```

We prove our goal by induction on L. We get two subgoals: (1) the base case, and (2) the induction case.



```
PRF : vr_test_indx-1 @edd.markb-al @gateway
# top
[-]
∀[A:Type]. ∀deq:EqDecider(A). ∀x:A. ∀L:A List. (∃indx:ℕ List) (∀i:ℕ. ((i ∈ indx) ⇔ (i < ||L||) ∧ (L[i] = x)))
# BY (inductionOnList THEN Reduce 0)
# 1
[-]
1. [A] : Type
2. deq : EqDecider(A)@i
3. x : A@i
4. L : A List
[-]
⊢ ∃indx:ℕ List) (∀i:ℕ. ((i ∈ indx) ⇔ (i < 0) ∧ (bottom() = x)))
# BY
# 2
[+]A,deq,x,L,u,v,,
[-]
⊢ ∃indx:ℕ List) (∀i:ℕ. ((i ∈ indx) ⇔ (i < (||v|| + 1)) ∧ ([u / v][i] = x)))
# BY
```

The base case is trivial, the list of indexes is the empty list []:

```

❌ *- PRF : vr_test_indx-1 @edd,markb-al @gateway
* top 1

[-]
1. [A] : Type
2. deq : EqDecider(A)@i
3. x : A@i
4. L : A List
[-]
├ ∃indxs:⟦N List⟧ (∀i:ℕ. ((i ∈ indxs) ⇔ (i < 0) ∧ (bottom() = x))))}

* BY (With '['] (D 0)· THEN Auto)

```

In the induction case, we first check whether or not  $x$  is equal to  $u$ , the head of our list  $L$ . We obtain two subgoals. In the first branch, we get to assume that  $x$  and  $u$  are equal and in the other branch we get to assume that they are different.

```

❌ *- PRF : vr_test_indx-1 @edd,markb-al @gateway
# top 2

[-]
1. [A] : Type
2. deq : EqDecider(A)@i
3. x : A@i
4. L : A List
5. u : A
6. v : A List
7. ∃indxs:⟦N List⟧ (∀i:ℕ. ((i ∈ indxs) ⇔ (i < ||v||) ∧ (v[i] = x))))}
[-]
├ ∃indxs:⟦N List⟧ (∀i:ℕ. ((i ∈ indxs) ⇔ (i < (||v|| + 1)) ∧ ((u / v)[i] = x))))}

# BY (D (-1) THEN (VrBoolCase 'deq x u'· THEN Auto))

# 2 1

[+]indxs,,,
[-]
├ ∃indxs:⟦N List⟧ (∀i:ℕ. ((i ∈ indxs) ⇔ (i < (||v|| + 1)) ∧ ((u / v)[i] = x))))}

# BY

# 2 2

[+]indxs,,,
[-]
├ ∃indxs:⟦N List⟧ (∀i:ℕ. ((i ∈ indxs) ⇔ (i < (||v|| + 1)) ∧ ((u / v)[i] = x))))}

# BY

```

If  $x$  is equal to  $u$  then the list of indexes is  $0 :: \text{map } (\text{fun } x \Rightarrow x + 1) \text{ indxs}$ , where  $\text{indxs}$  is the list of positions of  $x$  in the tail of  $L$ . The `SpReasoner` tactic proves several of the simple subgoals. We are left with two subgoals in this branch. Both of them are trivial.

```

X *- PRF : vr_test_indx-1 @edd.markb-al @gateway
# top 2 1

[-]
1. [A] : Type
2. deq : EqDecider(A)@i
3. x : A@i
4. L : A List
5. u : A
6. v : A List
7. indx : ℕ List
8. [%3] : ∀i:ℕ. ((i ∈ indx) ↔ (i < ||v||) ∧ (v[i] = x))
9. ↑(deq x u)
[-]
⊢ ∃indx:(ℕ List) (∀i:ℕ. ((i ∈ indx) ↔ (i < (||v|| + 1)) ∧ ([u / v][i] = x)))}

# BY (With "[0 / map(λx.(x + 1);indx)]" (D 0)· THEN Auto THEN SpReasoner)

# 2 1 1

[+]deq,,x,L,u,
[+]v,indx,,,i,y,,,,
[-]
⊢ v[i - 1] = x

# BY

# 2 1 2

[+]deq,,x,
[+]L,u,v,indx,,,i,,,,
[-]
⊢ (i = 0) ∨ (∃y:ℕ. ((y ∈ indx) ∧ (i = (y + 1))))

# BY

```

In the first subgoal we just need to know that  $i - 1$  is equal to  $y$  to finish the proof:

```

X *- PRF : vr_test_indx-1 @edd,markb-al @gateway
* top 2 1 1

[+]A,deq,,x,L,u,
[-]
7. v : A List
8. indxs : ℕ List
9. ∀i:ℕ. ((i ∈ indxs) ⇔ (i < ||v||) ∧ (↑(deq v[i] x)))
10. ↑(deq x u)
11. i : ℕ@i
12. y : ℕ
13. y < ||v||
14. ↑(deq v[y] x)
15. i = (y + 1)
16. 0 < (y + 1)
[-]
⊢ v[i - 1] = x

* BY (Assert 「(i - 1) = y」. THEN Auto)

```

The second subgoals comes from having to prove that  $i$  is a member of  $0 :: \text{map } (\text{fun } x \Rightarrow x + 1) \text{ indxs}$  given that  $i$  is less than the length of  $0 :: \text{map } (\text{fun } x \Rightarrow x + 1) \text{ indxs}$  and that the  $i$ 's element of that list is  $x$ . Proving that  $i$  is a member of  $0 :: \text{map } (\text{fun } x \Rightarrow x + 1) \text{ indxs}$  boils down to proving that either  $i$  is 0 or that  $i - 1$  is in  $\text{indxs}$ :

```

X *- PRF : vr_test_indx-1 @edd,markb-al @gateway
* top 2 1 2

[+]A,deq,,x,
[-]
5. L : A List
6. u : A
7. v : A List
8. indxs : ℕ List
9. ∀i:ℕ. ((i ∈ indxs) ⇔ (i < ||v||) ∧ (v[i] = x))
10. ↑(deq x u)
11. i : ℕ@i
12. i < (||v|| + 1)@i
13. ↑(deq v[i - 1] x)
14. ¬(i ≤ 0)
[-]
⊢ (i = 0) ∨ (∃y:ℕ. ((y ∈ indxs) ∧ (i = (y + 1))))

* BY ((OrRight THENA Auto) THEN InstConcl 「i - 1」. THEN Auto)

```

Now, if  $x$  is not equal to  $u$  then the list of indexes is  $\text{map } (\text{fun } x \Rightarrow x + 1) \text{ indxs}$ , where  $\text{indxs}$  is the list

of positions of  $x$  in the tail of  $L$ . Again, our `SpReasoner` tactic proves several of the simple subgoals, and we are left with two trivial subgoals (see below).

```

X *- PRF : vr_test_indx-1 @edd,markb-al @gateway
# top 2 2

[-]
1. [A] : Type
2. deq : EqDecider(A)@i
3. x : A@i
4. L : A List
5. u : A
6. v : A List
7. indxs : ℕ List
8. [%3] : ∀i:ℕ. ((i ∈ indxs) ⇔ (i < ||v||) ∧ (v[i] = x))
9. ¬↑(deq x u)
[-]
F ∃indxs:(ℕ List) (∀i:ℕ. ((i ∈ indxs) ⇔ (i < (||v|| + 1)) ∧ ([u / v][i] = x)))}

# BY (With (map(λx.(x + 1);indxs) (D 0) THEN Auto THEN SpReasoner)

# 2 2 1

[+]deq,,x,L,u,
[+]v,indxs,,i,y,,,,
[-]
F v[i - 1] = x

# BY

# 2 2 2

[+]deq,,x,
[+]L,u,v,indxs,,i,,,,
[-]
F ∃y:ℕ. ((y ∈ indxs) ∧ (i = (y + 1)))

# BY

```

```

X *- PRF : vr_test_idx-1 @edd,markb-al @gateway
* top 2 2 1

[+]A,deq,,x,L,u,
[-]
7. v : A List
8. indxs : IN List
9.  $\forall i:\mathbb{N}. ((i \in \text{indxs}) \iff (i < ||v||) \wedge (\uparrow(\text{deq } v[i] \ x)))$ 
10.  $\neg \uparrow(\text{deq } x \ u)$ 
11.  $i : \mathbb{N}@i$ 
12.  $y : \mathbb{N}$ 
13.  $y < ||v||$ 
14.  $\uparrow(\text{deq } v[y] \ x)$ 
15.  $i = (y + 1)$ 
16.  $0 < (y + 1)$ 
[-]
 $\vdash v[i - 1] = x$ 

* BY (Assert  $\uparrow(i - 1) = y^1$ . THEN Auto)

```

```

X *- PRF : vr_test_idx-1 @edd,markb-al @gateway
* top 2 2 2

[+]A,deq,,x,
[-]
5. L : A List
6. u : A
7. v : A List
8. indxs : IN List
9.  $\forall i:\mathbb{N}. ((i \in \text{indxs}) \iff (i < ||v||) \wedge (v[i] = x))$ 
10.  $\neg \uparrow(\text{deq } x \ u)$ 
11.  $i : \mathbb{N}@i$ 
12.  $i < (||v|| + 1)@i$ 
13.  $\uparrow(\text{deq } v[i - 1] \ x)$ 
14.  $\neg(i \leq 0)$ 
[-]
 $\vdash \exists y:\mathbb{N}. ((y \in \text{indxs}) \wedge (i = (y + 1)))$ 

* BY (InstConcl  $\uparrow(i - 1)$ . THEN Auto)

```