Event B: Modeling and Reasoning with Data Structures[1]

Manuel Carro
manuel.carro@upm.es

Universidad Politécnica de Madrid &
IMDEA Software Institute

[1] Theory, text, examples borrowed from J. R. Abrial: see http://wiki.event-b.org/index.php/Event-B_Language

Strategy

- Data structures involving pointers formalized with relations, functions.
- Specific axioms of these specific data structures give *properties* of these functions that model the data structures.
- Specific forms of these axioms (capturing induction on the data structures) are well-suited to be used in automated proofs.
- We will focus on formalizing:
  - Infinite lists.
  - Finite lists.
  - Infinite trees.
  - Finite trees.

Infinite lists

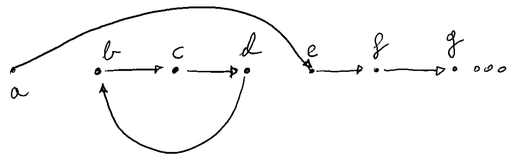
- Set V of list nodes.
- Initial node f.
- Bijective *next* function

axm_1 : $f \in V$

axm_2 : $n \in V \mathrel{\rightarrowtail\mkern-18mu\twoheadrightarrow} V \setminus \{f\}$

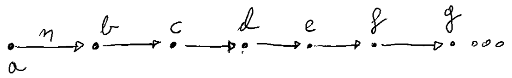
Note: isomorphic to natural numbers with $V = \mathbb{N}$, $f = 0$, $n = succ$.

Avoiding cycles



$S = \{b, c, d\} \quad n[S] = \{b, c, d\}$

$S \subseteq n[S]$



$S = \{b, c, d\} \quad n[S] = \{c, d, e\}$

$S \not\subseteq n[S]$

Avoiding cycles

- If a list has a cycle, then there is a $S \subseteq V$ s.t. $S \subseteq n[S]$.
- On the other hand, it is always the case that $\varnothing \subseteq n[\varnothing]$.
- So we insist that this is the only case:

$$\text{axm\_3} : \forall S \cdot S \subseteq V \land S \subseteq n[S] \Rightarrow S = \varnothing$$

- It can be used to prove properties in infinite lists.

From absence of cycles to induction

$\forall S \cdot S \subseteq V \land S \subseteq n[S] \Rightarrow S = \emptyset$

S can be written $S = V \setminus T$ (for some T). Then:

Redundant

$\forall S \cdot S = V \setminus T \land \boxed{S \subseteq V} \land S \subseteq n[S] \Rightarrow S = \emptyset$

$\forall S \cdot S = V \setminus T \land S \subseteq n[S] \Rightarrow \boxed{S = \emptyset}$

From absence of cycles to induction

$\forall S \cdot S = V \setminus T \land S \subseteq n[S] \Rightarrow \boxed{S = \emptyset}$

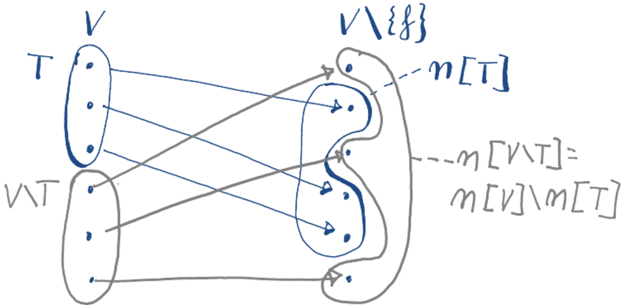
$V \setminus T = \emptyset \quad \equiv V \subseteq T$

$\forall S \cdot S = V \setminus T \land S \subseteq n[S] \Rightarrow V \subseteq T$

From absence of cycles to induction

$$\forall S \cdot S = V \setminus T \land S \subseteq \boxed{n[S]} \Rightarrow V \subseteq T$$

n bijective: $n[V \setminus T] = n[V] \setminus n[T]$
(because $n[S]$ and $n[T]$ don't intersect)



From absence of cycles to induction

$$S \subseteq n[S] \rightsquigarrow V \setminus T \subseteq n[V \setminus T] = n[V] \setminus n[T]$$

By definition: $f \in V$, $f \notin n[V \setminus T]$

Since $V \setminus T \subseteq n[V \setminus T]$, $f \notin V \setminus T$

Therefore $f \in T$ so that $f \notin V \setminus T$

And $n[V] = V \setminus \{f\}$

From absence of cycles to induction

$$V \setminus T \subseteq n[V] \setminus n[T]$$

$$\boxed{V \setminus T} \subseteq (V \setminus \{f\}) \setminus \boxed{n[T]}$$

... we will have no elements here

If we remove too much from here ...

Condition: $n[T] \subseteq T$

From absence of cycles to induction

All together:

$$\forall S \cdot S = \boxed{V} \setminus \boxed{T} \land f \in T \land n[T] \subseteq T \Rightarrow V \subseteq T$$

Fixed Variable

If we expand $n[T] \subseteq T$:

$$\text{thm\_2} : \forall T \cdot f \in T \land (\forall x \cdot x \in T \Rightarrow n(x) \in T) \Rightarrow V \subseteq T$$

- T the set of elements with some property P: $T = \{x | P(x)\}$
- If:
  - Initial node f has the property ($f \in T$), and
  - For every element with the property ($x \in T$), the next one has this property ($n(x) \in T$), then
  - All elements have the property ($V \subseteq T$).

Using thm_2 to prove list properties

- We want to prove $P(x)$ for all $x \in V$.
- Elements for which P holds: $T = \{x | x \in V \wedge p(X)\}$.
- We want to prove that $T = V$.
- Since clearly $T \subseteq V$, it is enough to prove $V \subseteq T$.
- We do that by instantiating T in thm_2.

$$\begin{array}{cc} f \in \{x|x \in V \wedge P(x)\} & \wedge \\ \forall x \cdot x \in \{x|x \in V \wedge P(x)\} \Rightarrow n(x) \in \{x|x \in V \wedge P(x)\} & \Rightarrow \\ V \subseteq \{x|x \in V \wedge P(x)\} & \end{array}$$

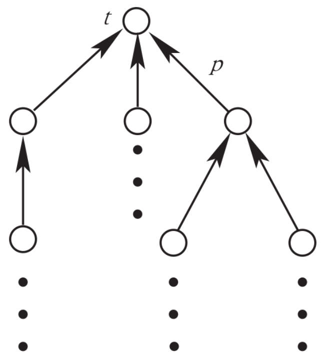
- $f \in \{x|x \in V \wedge P(x)\} \equiv P(f)$.
- Second part equivalent to $\forall x \cdot x \in V \wedge P(x) \Rightarrow P(n(x))$.
- The RHS is equivalent to $\forall x \cdot x \in V \Rightarrow P(x)$.
- Instantiating thm_2 gives a scheme to prove by induction in infinite lists.

Finite lists

- Basically as infinite lists, but including a last (l) element and a different axiom 2:

$$\begin{array}{rl} \text{axm\_4}: & l \in V \\ \text{axm\_5}: & \text{finite}(V) \\ \text{axm\_2}': & n \in V\setminus\{l\} \rightarrowtail\!\!\!\!\twoheadrightarrow V\setminus\{f\} \end{array}$$

Infinite trees



- t is the root.
- p relates every node with its parent (it is a surjection).
- There should not be cycles.

$$\begin{array}{rl} \text{axm\_1}: & t \in V \\ \text{axm\_2}: & p \in V\setminus\{t\} \twoheadrightarrow V \\ \text{axm\_3}: & \forall S \cdot S \subseteq p^{-1}[S] \Rightarrow S = \varnothing \end{array}$$

Induction rule:

$$\forall T \cdot t \in T \wedge p^{-1}[T] \subseteq T \Rightarrow V \subseteq T$$

Instantiation to prove properties:

$$\begin{array}{ll} \forall T \cdot & T \subseteq V \wedge t \in T \wedge \\ & (\forall x \cdot x \in V\setminus\{t\} \wedge p(x) \in T \Rightarrow x \in T) \\ & \Rightarrow V \subseteq T \end{array}$$

Finite trees

- t is the root.
- p relates every node with its parent.
- L is the set of tree leaves.
- There should not be cycles.

$$\begin{array}{rl} \text{axm\_1}: & t \in V \\ \text{axm\_2}: & L \subseteq V \\ \text{axm\_3}: & p \in V\setminus\{t\} \twoheadrightarrow V\setminus L \\ \text{axm\_4}: & \forall S \cdot S \subseteq p^{-1}[S] \Rightarrow S = \varnothing \end{array}$$