Formal Specification F28FS2, Lecture 9
Relation operations; operation schema composition

Jamie Gabbay

February 24, 2015

Remember

- A relation is a set of maplets.
- A (partial) function is (partial) functional relation.

Remember:

$f : S \nrightarrow T = \mathbb{P}(S \times T)$ maps each $s : S$ to at most one thing on the right.

$f : S \rightarrow T$ maps each $s : S$ to precisely one thing on the right.

$f(s)$ (function application to an element). $R(U)$ (relational image of a set of elements).

If $S' \subseteq S$ and $T' \subseteq T$ then we have

- $S' \lhd f$ and $S' \unlhd f$ (domain restriction and anti-restriction) and
- $f \rhd T'$ and $f \unrhd T'$ (range restriction and anti-restriction).

Sequences

We have types $seq\ T \subseteq \mathbb{N}_1 \nrightarrow T$ (sequences; finite lists of elements in T) and $seq_1\ L$ (nonempty sequences) and $iseq\ L$ (injective sequences).

Know the predicates which characterises $seq\ T \subseteq \mathbb{N}_1 \nrightarrow T$ and similarly for $seq_1\ L$ and $iseq\ L$.

Suppose $L, L' : seq\ T$. Then we have:

- $head(L) : T$ (first element) and $tail(L) : seq\ T$ (rest of the list).
- $rev\ L$ (reverse L).
- $L \oplus L'$ (overwrite L with L').
- $L \frown L'$ (concatenate L and L').

Even more funky things to do with sequences

Suppose $L : seq\ T$.

$last(L) : T$ returns the last element of L. If L is empty $last(L)$ is undefined.

Recall that $[tom, dick, harry] = \{1 \mapsto tom, 2 \mapsto dick, 3 \mapsto harry\}$.

For example $last([tom, dick, harry]) = harry : T$.

$front(L) : seq\ T$ returns all but the last element of L. If L has fewer than two elements, $front(L)$ is undefined.

For example $front([tom, dick, harry]) = [tom, dick] : seq\ T$.

Filtering and squashing

Suppose $L : seq\ T$ and suppose $T' \subseteq T$ (note: equivalently we can suppose $T' : \mathbb{P}\, T$).

Then $L \upharpoonright T'$ is the sequence of elements in L that are also in T'.

Then $[tom, dick, harry] \upharpoonright \{tom, harry, jones\} = [tom, harry]$.

If $f : \mathbb{N}_1 \nrightarrow T$ is defined on finitely many elements, then $squash(f) : seq\ T$ is the sequence which returns the list of those elements. For example

$$squash(\{2 \mapsto dick, 3 \mapsto tom, 7 \mapsto harry\}) = \{1 \mapsto dick, 2 \mapsto tom, 3 \mapsto harry\}.$$

Generic constants

How to define things like *seq*, $\upharpoonleft$, *head*, *tail*, and so on?

T cat

$$\frown : seq\ T \times seq T \rightarrow seq\ T$$

$$\forall s, t : seq\ T \bullet$$
$$s \frown t = s \cup \{n \in dom(t) \bullet (n + \#s) \mapsto t(n)\}$$

Try defining *head*, *tail*, *last*, *front*, *rev*, and so on.

Squashing, defined explicitly in Z, just for fun:

T squash

$squash : (\mathbb{N} \rightarrow\!\!\!\!\!+ \; T) \rightarrow seq\ T$

$\forall f : \mathbb{N} \rightarrow\!\!\!\!\!+ \; T \bullet$

$\#squash(f) = \#f \wedge$

$\forall n : dom(f) \bullet squash(f)(\#(0..n \lhd f)) = f(n)$

Why is $\#squash(f) = \#f$ in there; what does it do?

Disjointness

Suppose $A_1, \ldots, A_n : \mathbb{P}S$.

$disjoint(A_1, \ldots, A_n)$ is true when

$$\forall\, i, j \in 1 \ldots n \bullet A_i \cap A_j \neq \varnothing \Rightarrow i = j$$

or equivalently (taking the contrapositive)

$$\forall\, i, j \in 1 \ldots n \bullet i \neq j \Rightarrow A_i \cap A_j = \varnothing.$$

In words:

"The elements of $(A_1, \ldots, A_n)$ are pairwise disjoint."

(The contrapositive of $P \Rightarrow Q$ is $\neg Q \Rightarrow \neg P$.
Exercise: using truth-tables verify that these are logically equivalent.)

Partition

If $U : \mathbb{P}S$ then the predicate '$(A_1, \ldots, A_n)$ *partition* U' holds when

$disjoint(A_1, \ldots, A_n)$

and furthermore

$\bigcup(A_1, \ldots, A_n) = U$.

In words

"$(A_1, \ldots, A_n)$ *partition* U is true when A_1 to A_n really do partition U."

For example $(\{1, 2\}, \{5\}, \{3, 4\})$ *partition* $\{1, 2, 3, 4, 5\}$ holds.

Labour-saving: *let*

Suppose we have some long expression — e.g. *primes*

$\{x : \mathbb{N} \mid (x \neq 0 \land \forall y, z : \mathbb{Z} \bullet y * z = x \Rightarrow 1 \in \{y, z\}) \bullet x\} : \mathbb{P}\mathbb{N}$

— which we use many times in another expression *BLAH*.

We can write this as *let primes* $= \{...\}$ *in BLAH*.

You can use this in your schemas, if you like.

Labour-saving: operation schema composition

A

$$a, a', c! : \mathbb{Z}$$

$$a' = a + 42$$
$$c! = a'$$

B

$$a, a', b? : \mathbb{Z}$$

$$b? < 10$$
$$a' = a + b?$$

Labour-saving: operation schema composition

Then $A;\ B$ is this:

$$
\begin{array}{|l}
\hline
\textit{A; B} \\
a, c! : \mathbb{Z} \\
a', b? : \mathbb{Z} \\
\hline
\exists\, d : \mathbb{Z} \bullet \\
d = a + 42 \land c! = d \land b? < 10 \land a' = d + b \\
\hline
\end{array}
$$