

Schemas

Using Z

Woodcock & Davies

Schema language

The **schema language** is used to structure and compose mathematical descriptions: collating pieces of information, encapsulating them, and naming them for re-use.

It is the second component of the Z notation, the first being the **mathematical language** of logic and set theory.

Declaration and constraint

Any mathematical description will involve declarations of identifiers, and constraints upon them.

In a formal specification, groups of identifiers may be used to describe compound objects or related properties. These identifiers will often be declared—and constrained—together.

We may simplify our formal specifications by factoring out patterns of declaration and constraint.

Examples

Both of the following mathematical expressions involve a declaration and a constraint:

$$\{ a, b : \mathbb{N} \mid a = 2 * b \bullet a \mapsto b \}$$

$$\exists c : \mathbb{N} \mid c \neq 1 \bullet c < 2$$

Example

A formal specification might involve the given types

sold : *Seat* \leftrightarrow *Customer*

seating : \mathbb{P} *Seat*

and the constraint

$\text{dom } \textit{sold} \subseteq \textit{seating}$

Schemas

A **schema** is a pattern of declaration and constraint.

We will define schemas, and use them as declarations, as predicates, and as sets.

Notation

We may write schemas in horizontal form:

$[\textit{declaration} \mid \textit{constraint}]$

or in vertical form:

<i>declaration</i>
<i>constraint</i>

In the vertical form, we may elide the semicolons between declarations and the conjunctions between predicates.

Examples

$[a : \mathbb{Z}; c : \mathbb{P} \mathbb{Z} \mid c \neq \emptyset \wedge a \in c]$

$a : \mathbb{Z}$
$c : \mathbb{P} \mathbb{Z}$
$c \neq \emptyset$
$a \in c$

Naming schemas

We may give names to schemas, and use these names to refer to the corresponding pattern of declaration and constraint. The definition

$$\textit{Name} \hat{=} \textit{Exp}$$

introduces a schema name *Name* which is equivalent to *Exp*, which must be a schema expression.

Example

$$\textit{Schema} \hat{=} [a : \mathbb{Z}; c : \mathbb{P}\mathbb{Z} \mid c \neq \emptyset \wedge a \in c]$$

$$\textit{Schema} \hat{=} \begin{array}{|l} a : \mathbb{Z} \\ c : \mathbb{P}\mathbb{Z} \\ \hline c \neq \emptyset \\ a \in c \end{array}$$

Notation

We may write the second definition above as:

Schema
$a : Z$
$c : \mathbb{P}Z$
$c \neq \emptyset$
$a \in c$

Example

BoxOffice
$\text{sold} : \text{Seat} \leftrightarrow \text{Customer}$
$\text{seating} : \mathbb{P} \text{Seat}$
$\text{dom sold} \subseteq \text{seating}$

Equivalence

Two schemas are said to be **equivalent** if they declare the same set of identifiers—with the same types—and impose a logically equivalent constraint upon them.

Example

$seating : \mathbb{P} \textit{Seat}$
$sold : \textit{Seat} \leftrightarrow \textit{Customer}$
$\text{dom } sold \subseteq seating$
$sold \in \textit{Seat} \leftrightarrow \textit{Customer}$

Using schemas

We may use a schema name:

- in place of a **declaration**: after quantifiers, in set comprehensions, and in lambda and mu expressions
- in place of a **predicate**; in this case, only the constraint part is important
- in place of a **set**

Examples

\forall *Schema* • $a \in \mathbb{N}$

$\exists a : \mathbb{Z}; c : \mathbb{P} \mathbb{Z}$ • *Schema*

Question

What is the type of the following function?

λ *BoxOffice* • *seating* \ *dom sold*

Bindings

A binding is a mapping from **names** to **values**. The **names** are names of identifiers; the **values** are values of expressions of the appropriate type.

Notation

The binding that associates the name of identifier x with the value of expression e , and the name of y with the value of f can be written

$$\langle x \rightsquigarrow e, y \rightsquigarrow f \rangle$$
Example
$$S ::= \langle a \rightsquigarrow 2, c \rightsquigarrow \{1, 2, 3\} \rangle$$

Schemas as sets

A schema corresponds to a set of bindings.

Each binding in this set associates the identifiers declared in the schema with values in such a way that the constraint part of the schema is satisfied.

If this set is maximal within the specification, then it is said to be a [schema type](#).

Example

The following bindings are associated with *Schema*:

$\langle a \rightsquigarrow 1, c \rightsquigarrow \{0, 1, 2\} \rangle$

$\langle a \rightsquigarrow 0, c \rightsquigarrow \mathbb{Z} \rangle$

$\langle a \rightsquigarrow -3, c \rightsquigarrow \{-3\} \rangle$

Example

The following definition introduces a schema type:

```
SchemaType  
  a : Z  
  c : P Z
```

Question

What is the type of the following set?

```
{ Schema | c ∈ {0, 1} }
```

Characteristic binding

If *Schema* is the name of a schema, then we write $\theta Schema$ to denote the characteristic binding of *Schema*.

In this binding, each of the named identifiers is associated with its value in the current scope.

Example

$$\theta Schema = \langle a \rightsquigarrow a, c \rightsquigarrow c \rangle$$

Question

Is there any difference between θ Schema and θ SchemaType?

Characteristic tuples

Where a schema is used as part of a declaration, the characteristic binding for that schema is used as the corresponding part of the characteristic tuple.

Example

$$\{ \text{Schema}; b : \mathbb{Z} \} = \{ \text{Schema}; b : \mathbb{Z} \bullet (\emptyset \text{Schema}, b) \}$$

Schemas as sets (again)

When we use a schema name *Schema* as a set, we are referring to the following set of bindings:

$$\{ \text{Schema} \bullet \emptyset \text{Schema} \}$$

Example

$\{ \text{Schema} \bullet \emptyset \text{Schema} \}$

$\{ a : \mathbb{Z}; c : \mathbb{P}\mathbb{Z} \mid c \neq \emptyset \wedge a \in c \bullet \langle a \rightsquigarrow a, c \rightsquigarrow c \rangle \}$

Component selection

If s is an object of schema type and x is one of the named components in s , then $s.x$ is the value associated with x in s .

For example, if s is the binding $\langle x \rightsquigarrow v \rangle$, then $s.x = v$.

Example

Date

month : *Month*

day : 1 .. 31

month \in {*sep, apr, jun, nov*} \Rightarrow *day* \leq 30

month = *feb* \Rightarrow *day* \leq 29

marina's_birthday : *Date*

marina's_birthday.month = *jan*

marina's_birthday.day = 28

Schemas as declarations

When a schema name is used in place of a declaration, the named identifiers are introduced under the given constraint.

Example

$\exists \textit{Date} \bullet \textit{day} = 31$

$\exists \textit{day} : 1..31; \textit{month} : \textit{Month} \mid$

$(\textit{month} \in \{\textit{sep}, \textit{apr}, \textit{jun}, \textit{nov}\} \Rightarrow \textit{day} \leq 30) \wedge$

$\textit{month} = \textit{feb} \Rightarrow \textit{day} \leq 29 \bullet$

$\textit{day} = 31$

Question

What are the elements of the following set?

$$\{ \textit{Date} \mid \textit{day} = 31 \bullet \textit{month} \}$$
Question

What are the elements of the following set?

$$\{ \textit{d} : \textit{Date} \mid \textit{d.day} = 31 \bullet \textit{d.month} \}$$

Schemas as predicates

When a schema name is used in place of a predicate, a statement is made about the identifiers declared in the schema.

This statement is logically equivalent to the constraint information in **the whole** of the schema.

Example

$\forall \textit{day} : \mathbb{Z}; \textit{month} : \textit{Month} \bullet \textit{Date} \Rightarrow \textit{day} \leq 31$

$\forall \textit{day} : \mathbb{Z}; \textit{month} : \textit{Month} \bullet$

$(\textit{day} \in 1..31 \wedge$

$(\textit{month} \in \{\textit{sep}, \textit{apr}, \textit{jun}, \textit{nov}\} \Rightarrow \textit{day} \leq 30) \wedge$

$\textit{month} = \textit{feb} \Rightarrow \textit{day} \leq 29) \Rightarrow$

$\textit{day} \leq 31$

Normalisation

A schema in which there is no constraint information in the declaration part is said to be **in normal form**.

It is sometimes useful to replace a schema with an equivalent schema in normal form.

Example

<i>NormalDate</i>
<i>month</i> : Month
<i>day</i> : \mathbb{Z}
$day \in 1..31$
$month \in \{sep, apr, jun, nov\} \Rightarrow day \leq 30$
$month = feb \Rightarrow day \leq 29$

Note

The declaration part of a normalised schema is that of a schema type.

DateType _____
month : *Month*
day : \mathbb{Z}

Question

If we define

NotDate _____
month : *Month*
day : $1..31$

$\neg ((\textit{month} \in \{\textit{sep}, \textit{apr}, \textit{jun}, \textit{nov}\} \Rightarrow \textit{day} \leq 30) \wedge$
 $(\textit{month} = \textit{feb} \Rightarrow \textit{day} \leq 29))$

is the following statement true or false?

$\vee \textit{DateType} \mid \neg \textit{Date} \bullet \textit{NotDate}$

Renaming

If *old* is one of the identifiers declared in *Schema*, then the schema *Schema*[*new*/*old*] is the schema that

- declares *new* instead of *old*
- imposes the same constraint upon *new* as it did upon *old*

Example

The schema *Date*[*dd*/*day*, *mm*/*month*] is equivalent to

<i>mm</i> : <i>Month</i>
<i>dd</i> : 1 .. 31
<i>mm</i> ∈ { <i>sep</i> , <i>apr</i> , <i>jun</i> , <i>nov</i> } ⇒ <i>dd</i> ≤ 30
<i>mm</i> = <i>feb</i> ⇒ <i>dd</i> ≤ 29

Decoration

If *Schema* is a schema, then *Schema'* is the schema that declares the same identifiers as *Schema*, and imposes the same constraint, **except** that every identifier is decorated with a prime symbol (').

Example

Schema' is equivalent to

$a' : \mathbb{Z}$
$c' : \mathbb{P}\mathbb{Z}$
$c' \neq \emptyset$
$a' \in c'$

Example

BoxOffice' is equivalent to

$seating' : \mathbb{P} Seat$ $sold' : Seat \leftrightarrow Customer$ $dom\ sold' \subseteq seating'$
--

Equality of bindings

Two bindings are equal if they map the same identifiers to equal values.

$$\langle X \rightsquigarrow V \rangle = \langle X \rightsquigarrow W \rangle \Leftrightarrow V = W$$

Decoration of characteristic bindings

If b is a characteristic binding, then b' is a binding in which the same names are associated with primed values.

$$\langle X \rightsquigarrow X \rangle' = \langle X \rightsquigarrow X' \rangle$$

Binding decoration binds more loosely than θ :

$$\theta Schema' = (\theta Schema)'$$

Example

The decorated binding $\theta Schema'$ is

$$\langle a \rightsquigarrow a', c \rightsquigarrow c' \rangle$$

The characteristic binding $\theta(Schema')$ is

$$\langle a' \rightsquigarrow a', c' \rightsquigarrow c' \rangle$$

Decoration and schema types

Decoration does not change the type of a binding: $\theta Schema'$ is an object of schema type $Schema$.

The declaration $Schema'$ may be used to introduce $\theta Schema'$: it declares every variable in the decorated binding.

Example

The declaration $Schema$; $Schema'$ may be used to introduce two objects of schema type $Schema$:

$\langle a \rightsquigarrow a, c \rightsquigarrow c \rangle$ and $\langle a \rightsquigarrow a', c \rightsquigarrow c' \rangle$

Question

Is the following proposition true or false?

$$\forall a' : \mathbb{Z}; c' : \mathbb{P} \mathbb{Z} \bullet$$

$\exists \text{Schema}' \in \text{Schema}$

Quantification over schema types

We will sometimes encounter quantified expressions in which the components of the declaration schema do not appear; a characteristic binding is used instead.

Where this is the case, we may avoid unnecessary expansion by reasoning at the level of schemas and bindings.

Substitution of bindings

A pair of bindings from the same schema type may be used to specify a renaming; the effect is that of a partial decoration.

The substituted schema

$\text{SchemaA}[\theta\text{SchemaB}' / \theta\text{SchemaB}]$

may be obtained from SchemaA by decorating the identifiers that appear in $\theta\text{SchemaB}$.

Example

Suppose that NewSchema is defined by

NewSchema
$a :: \mathbb{Z}$
$b :: \mathbb{Z}$
$c :: \mathbb{P}\mathbb{Z}$
$b \notin c$

NewSchema[\emptyset *Schema'* / \emptyset *Schema*] is equivalent to

$a' : \mathbb{Z}$
$b : \mathbb{Z}$
$c' : \mathbb{P}\mathbb{Z}$
$b \notin c'$

Universal introduction

$$\frac{\begin{array}{c} [\emptyset S \in S]^{[i]} \\ \vdots \\ p \end{array}}{A S \bullet P} \quad [\text{V-intro}^{[i]}]$$

Provided that $\emptyset S$ is not free in the other assumptions.

Universal elimination

$$\frac{\theta S' \in S \quad A \ S \bullet P}{P[\theta S'/\theta S]} \quad [V\text{-elim}]$$

Existential introduction

$$\frac{\theta S' \in S \quad P[\theta S'/\theta S]}{\exists S \bullet P} \quad [E\text{-intro}]$$

Existential elimination

$$\frac{\begin{array}{c} [\theta S \in S]^{[i]} \\ [P]^{[i]} \\ \vdots \\ \exists S \bullet P \quad Q \end{array}}{Q} \quad [\exists\text{-elim}^{[i]}]$$

Provided that θS is not free in the other assumptions and that θS is not free in Q .

Summary

- schema language
- schemas as sets
- schemas as declarations
- schemas as predicates
- decoration
- schema types