Bank Account Example

First we must define some basic global data types.

Basic data types: $[INT, STRING]$.

Then we can define the schema "Person". It will have two state variables (data): name and address.

Person

$$name : STRING$$
$$address : STRING$$

No constraints are needed here.

Our second schema is "Account". State variables (data): owner, balance.

Account

$$owner : Person$$
$$balance : INT$$

$$balance \geqslant 0$$

We must define the constraint that balance cannot be negative.

The last state schema that we will define here is "Bank".

Bank

$$ownership : Person \leftrightarrow Account$$

The relation "ownership" defines a set of pairs $(person, account)$. We allow one person to have multiple bank accounts.

Now we have to define schemas for two operations: withdraw and deposit.

Withdraw

$$\Delta Account$$
$$amount? : NAT$$
$$person? : Person$$

$$person? = owner$$

$$balance' = balance - amount$$

Here, the condition $person? = owner$ represents a precondition for the operation, and the expression $balance' = balance - amount$ captures its effect.

The operation "deposit" can be defined in a similar way.

Concrete values (constants) may be defined using a schema like this:

JoeDoe

$$Person$$

$$name = Joe\ Doe$$

$$address = New\ York$$

We include the schema "Person", effectively reusing all the declared state variables.

Instance of the "Bank" schema:

GoldmanSachs

Bank

$ownership = \{(JoeDoe, AccountJD)\}$

We assume that "AccountJD" is an existing constant of the schema "Account".