I/O Relations and Domain Expressions in the MID

SFWR ENG 2B03

2003

Robert L. Baber

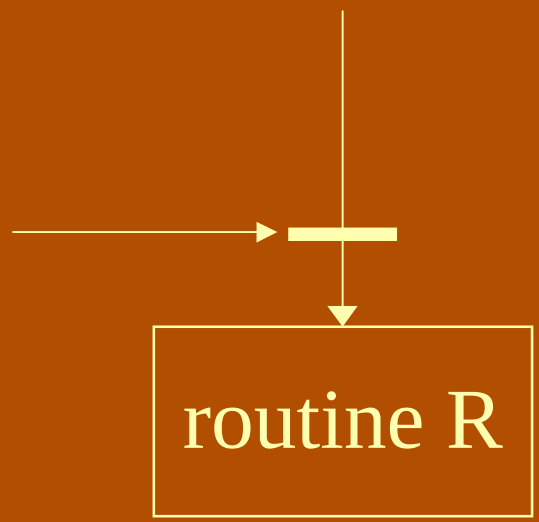
Routine R in module M

module M

The I/O relation in the MID for routine R refers to values of concrete state variables and formal parameters as control passes this interface.

State variables:

ASV: abstract
CSV: concrete



Permitted references in the I/O relation

The I/O relation in the MID refers to values

- of concrete state variables and formal parameters
- before and after execution routine R.

The concrete state variables *must* belong to the module *in which routine R is declared*.

The I/O relation may contain references to *mathematical* functions (no internal state).

Prohibited references in the I/O relation

No other variable name, no routine name may appear in the I/O relation.

No exceptions

The I/O relation does *not* give an internal view of the routine or any part of it.

Domain

The same restrictions apply also to the expression defining the domain of routine R.

Only references to values of concrete state variables and formal parameters *before* executing routine R are permitted.

Routine semantics in the MID

I/O relations and domain expressions in the routine semantics sections of the MID are

- *mathematical* expressions,
- *not* program code, program statements, pseudocode or anything similar.

No reference to routines, state variables of other modules, local variables, etc. may appear in domain expressions or I/O relations.

Deriving an I/O relation, domain for a MID

If the abstraction relation is a function from the concrete to the abstract state variables, express it as the conjunction of terms of the form

$$ASVi = fi(CSV1, CSV2, \ldots)$$

Then, in the I/O relation or domain expression involving the abstract state variables (e.g. from the MIS), substitute fi(CSV1, CSV2, …) for ASVi, etc. The result will be an expression involving only the concrete state variables. It will be the desired domain expression or I/O relation.

Goal of the I/O relation and domain

These expressions represent an external view from "above" – *from the standpoint of the caller*.

They also represent a view to "above", i.e. *from the routine to its caller*.

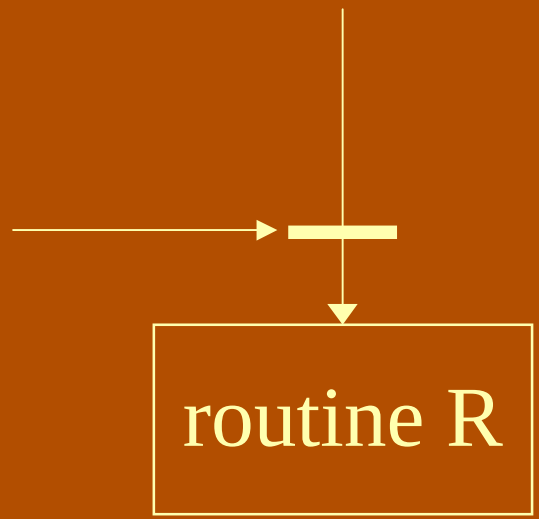
They specify the interface between the routine and its caller.

They *define what* the routine does, but say *nothing about how* it does it.

Routine R in module M

module M

The I/O relation in the MID for routine R refers to values of concrete state variables and formal parameters as control passes this interface.



State variables:

ASV: abstract
CSV: concrete