Software specification in CASL - The Common Algebraic Specification Language

Till Mossakowski, Lutz Schröder

January 2007

SFB/TR 8 SPATIAL COGNITION

Development Graphs

Development graphs $\mathcal{S} = \langle \mathcal{N}, \mathcal{L} \rangle$

Nodes in $\mathcal{N}$: (Σ^N, Γ^N) with

- Σ^N signature,
- $\Gamma^N \subseteq \mathbf{Sen}(\Sigma^N)$ set of local axioms.

Links in $\mathcal{L}$:

- global $M \xrightarrow{\sigma} N$, where $\sigma : \Sigma^M \to \Sigma^N$,
- local $M \overset{\sigma}{\dashrightarrow} N$ where $\sigma : \Sigma^M \to \Sigma^N$, or
- hiding $M \xrightarrow[h]{\sigma} N$ where $\sigma : \Sigma^N \to \Sigma^M$ going against the direction of the link.

Semantics of development graphs

$\mathbf{Mod}_{\mathcal{S}}(N)$ consists of those Σ^N-models n for which

1. n satisfies the local axioms Γ^N,
2. for each $K \xrightarrow{\sigma} N \in \mathcal{S}$, $n|_\sigma$ is a K-model,
3. for each $K \overset{\sigma}{\cdots\cdots\blacktriangleright} N \in \mathcal{S}$,
   $n|_\sigma$ satisfies the local axioms Γ^K,
4. for each $K \xrightarrow[h]{\sigma} N \in \mathcal{S}$,
   n has a σ-expansion k (i.e. $k|_\sigma = n$) that is a K-model.

Theorem links

Theorem links come in three versions:

- global theorem links $M \xrightarrow{\sigma} N$, where $\sigma\colon \Sigma^M \longrightarrow \Sigma^N$,
  - $\mathcal{S} \models M \xrightarrow{\sigma} N$ iff for all $n \in \mathbf{Mod}_\mathcal{S}(N)$, $n|_\sigma \in \mathbf{Mod}_\mathcal{S}(M)$.
- local theorem links $M \overset{\sigma}{\dashrightarrow} N$, where $\sigma\colon \Sigma^M \longrightarrow \Sigma^N$,
  - $\mathcal{S} \models M \overset{\sigma}{\dashrightarrow} N$ iff for all $n \in \mathbf{Mod}_\mathcal{S}(N)$, $n|_\sigma \models \Gamma^M$.

- $\mathcal{S} \models M \xrightarrow[h\ \theta]{\sigma} N$ iff for all $n \in \mathbf{Mod}_S(N)$,
  $n|_\sigma$ has a θ-expansion to some M-model.
  $\Sigma^M \xleftarrow{\theta} \Sigma \xrightarrow{\sigma} \Sigma^N$

- the calculus reduces these to local proof obligations.

Conservativity annotations

A global definition link $M \xrightarrow{\sigma} N$ can be marked to be conservative:

$$M \xrightarrow[c]{\sigma} N$$

This is a proof obligation expressing that

each M-model can be σ-expanded to an N-model

(that is, for each M-model m there is an N-model n such that $n|_\sigma = m$).

Local and global reachability

A node N is globally reachable from a node M via a signature morphism σ, $M \overset{\sigma}{\rightarrowtail\!\!\!\twoheadrightarrow} N$ for short, iff

- either $M = N$ and $\sigma = id$, or
- $M \xrightarrow{\sigma'} K$, and $K \overset{\sigma''}{\rightarrowtail\!\!\!\twoheadrightarrow} N$, with $\sigma = \sigma'' \circ \sigma'$.

A node N is locally reachable from a node M via a signature morphism σ, $M \overset{\sigma}{\rightarrowtail\cdots\!\twoheadrightarrow} N$ for short, iff $M \overset{\sigma}{\rightarrowtail\!\!\!\twoheadrightarrow} N$ or there is a node K with $M \overset{\sigma'}{\cdots\cdots\rightarrow} K$ and $K \overset{\sigma''}{\rightarrowtail\!\!\!\twoheadrightarrow} N$, such that $\sigma = \sigma'' \circ \sigma'$.

Proof rules: Structural rules

$$\frac{K \overset{\sigma \circ \tau}{\dashrightarrow} M \text{ for each } K \overset{\tau}{\rightarrowtail\!\!\dashrightarrow\!\!\twoheadrightarrow} N \qquad L \xrightarrow[h\ \theta]{\sigma \circ \tau} M \text{ for each } L \xrightarrow[h]{\theta} K \text{ and } K \overset{\tau}{\rightarrowtail\!\!\twoheadrightarrow} N}{N \xrightarrow{\sigma} M}$$

Glob-Decomposition

$$\frac{M \overset{\sigma}{\rightarrowtail\!\!\twoheadrightarrow} N}{M \xrightarrow{\sigma} N}$$

Subsumption

$$\frac{K \xrightarrow{\sigma} L \quad L \xrightarrow{\theta} M}{K \xrightarrow{\theta \circ \sigma} M}$$

Composition

Proof rules: Basic Inference

$$\frac{Th_{\mathcal{S}}(N) \vdash_{\Sigma^N} \sigma(\varphi) \text{ for each } \varphi \in \Gamma^M}{M \overset{\sigma}{\dashrightarrow} N}$$

Basic Inference

For $N \in \mathcal{N}$, the theory $Th_{\mathcal{S}}(N)$ of N is defined by

$$\Gamma^N \cup \bigcup_{K \overset{\sigma}{\rightarrowtail\!\!\dashrightarrow} N} \sigma(\Gamma^K)$$

Proof rule: Hide-Theorem-Shift

$$
\dfrac{
\begin{array}{ccc}
M' & \xrightarrow{\sigma'} & N' \\
 & & \theta' \uparrow c \\
 & & N
\end{array}
}{
\begin{array}{ccc}
 & & N' \\
 & & \theta' \uparrow c \\
M' & \xrightarrow[h\ \theta]{\sigma} & N
\end{array}
}
\qquad
\begin{array}{ccc}
\Sigma^{M'} & \xrightarrow{\sigma'} & \Sigma^{N'} \\
\theta \uparrow & & \theta' \uparrow \\
\Sigma & \xrightarrow{\sigma} & \Sigma^{N}
\end{array}
$$

$$\sigma' \circ \theta = \theta' \circ \sigma$$

Used for proving hiding theorem links (that arise when hiding is present at the source of a theorem link).

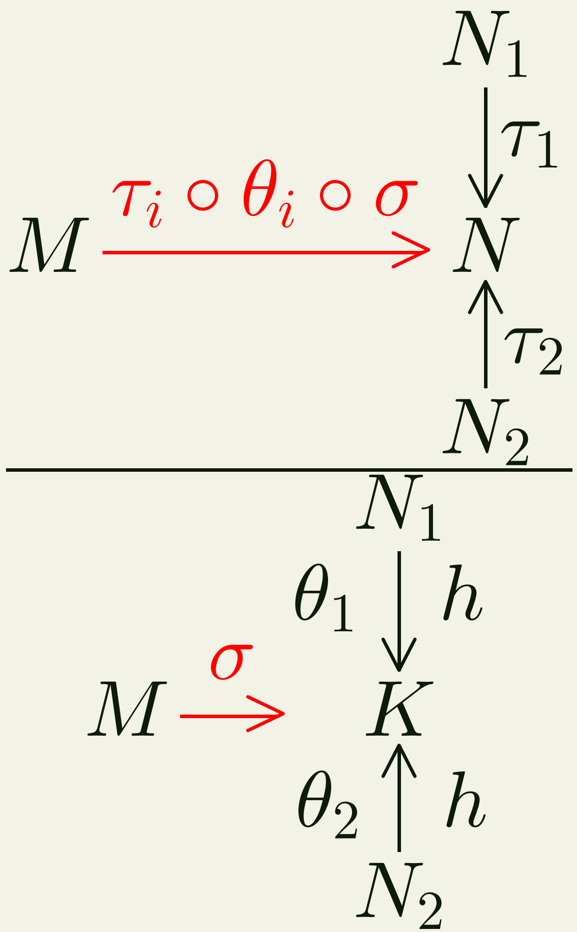
Proof rule: Theorem-Hide-Shift (simplified)

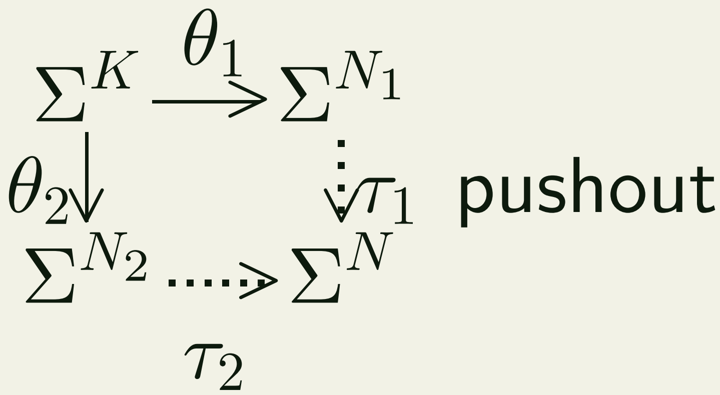
$$\frac{M \xrightarrow{\theta \circ \sigma} N}{\begin{array}{ccc} & & N \\ & & \theta \big\downarrow h \\ M & \xrightarrow{\sigma} & K \end{array}}$$

$$\Sigma^M \xrightarrow{\sigma} \Sigma^K \xrightarrow{\theta} \Sigma^N$$

Used for proving theorem links when hiding is present at the target of the theorem link.

Proof rule: Theorem-Hide-Shift (two hidings)



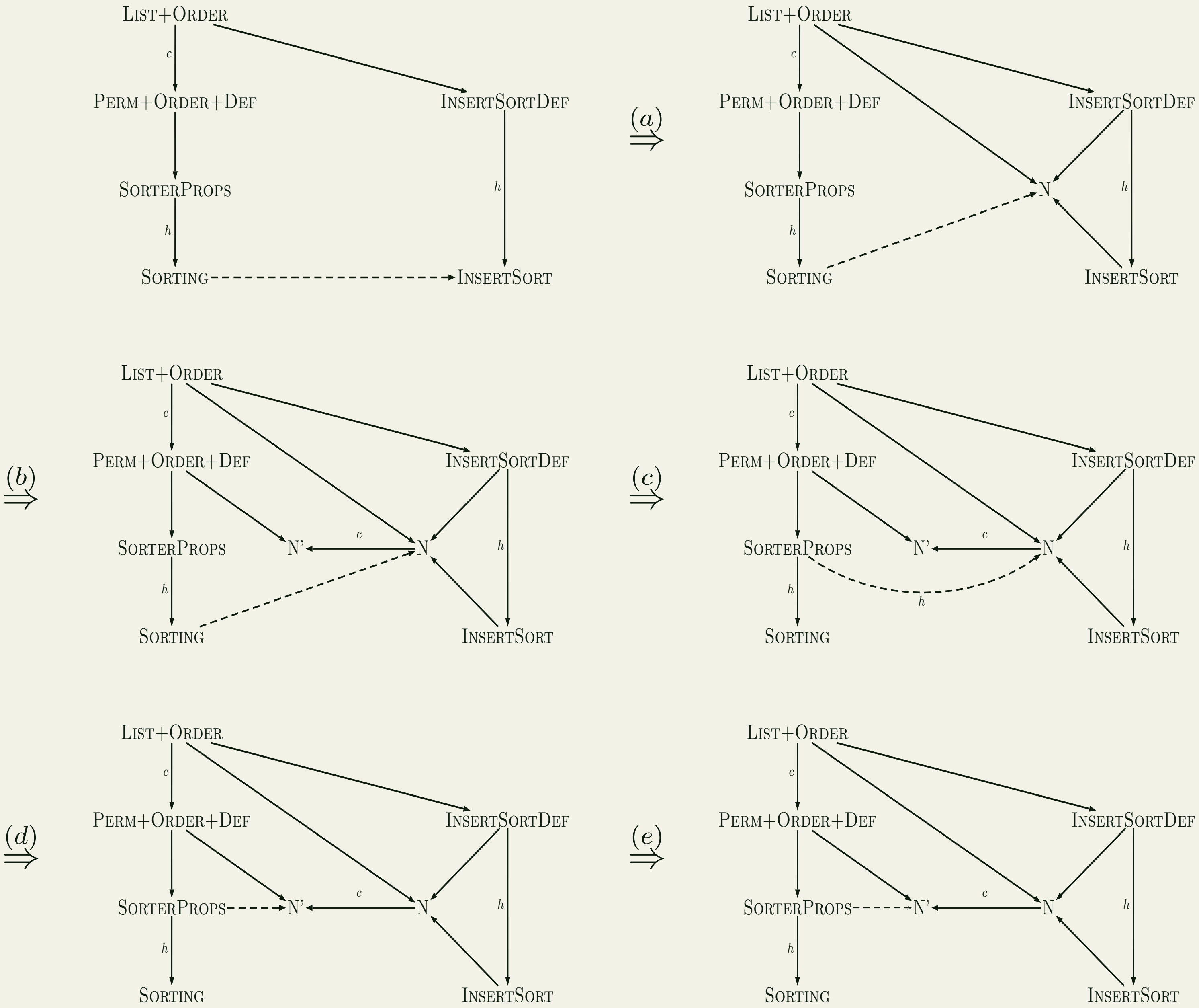


Proof rule: Theorem-Hide-Shift (general)

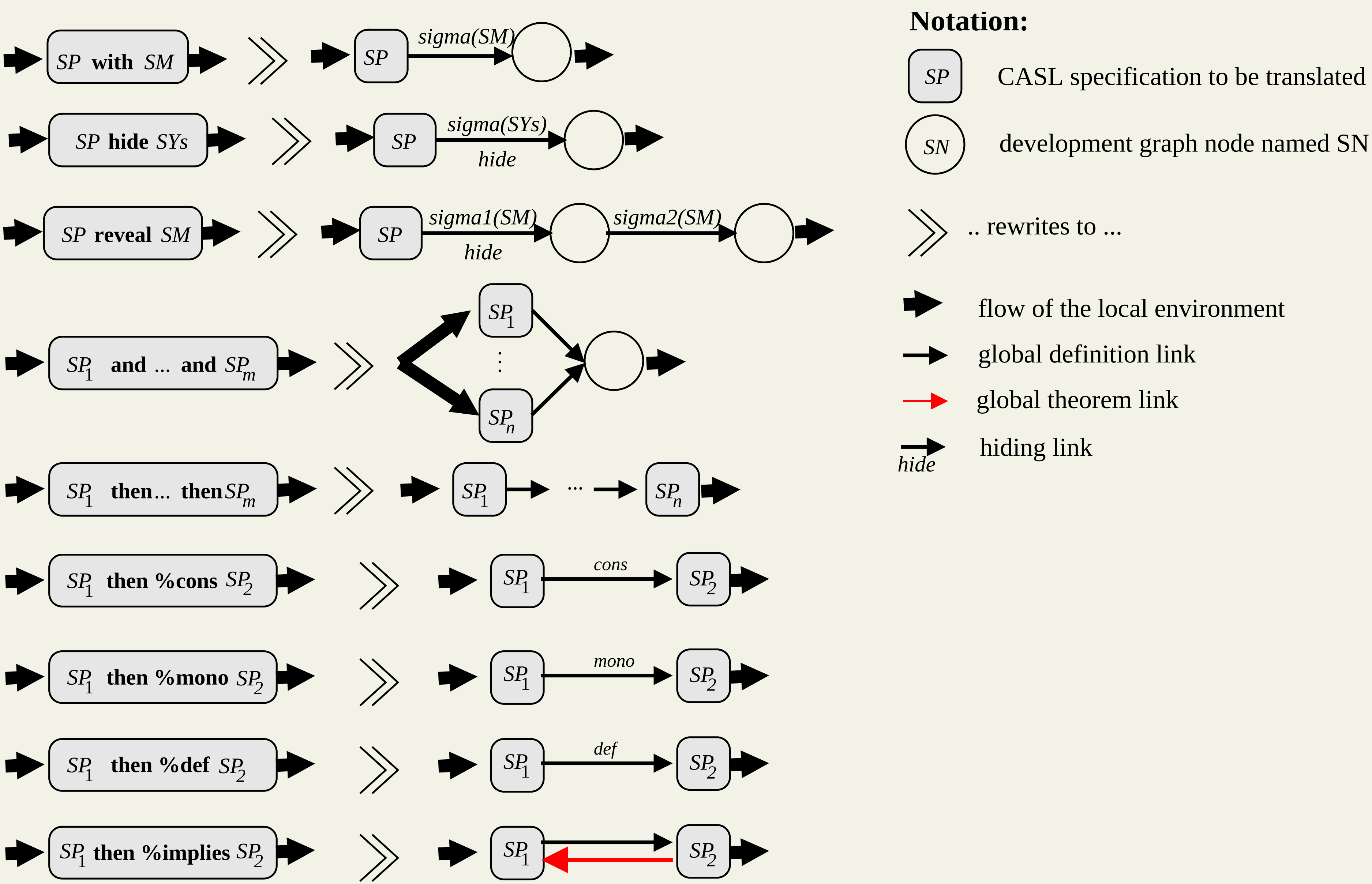
$$\frac{\begin{array}{ccc} & G(i) & \\ & \downarrow \mu_i & (i \in |J|) \\ M \xrightarrow{\mu_{\langle N \rangle} \circ \sigma} & C & \end{array}}{\text{---}\; D \;\text{---}}$$

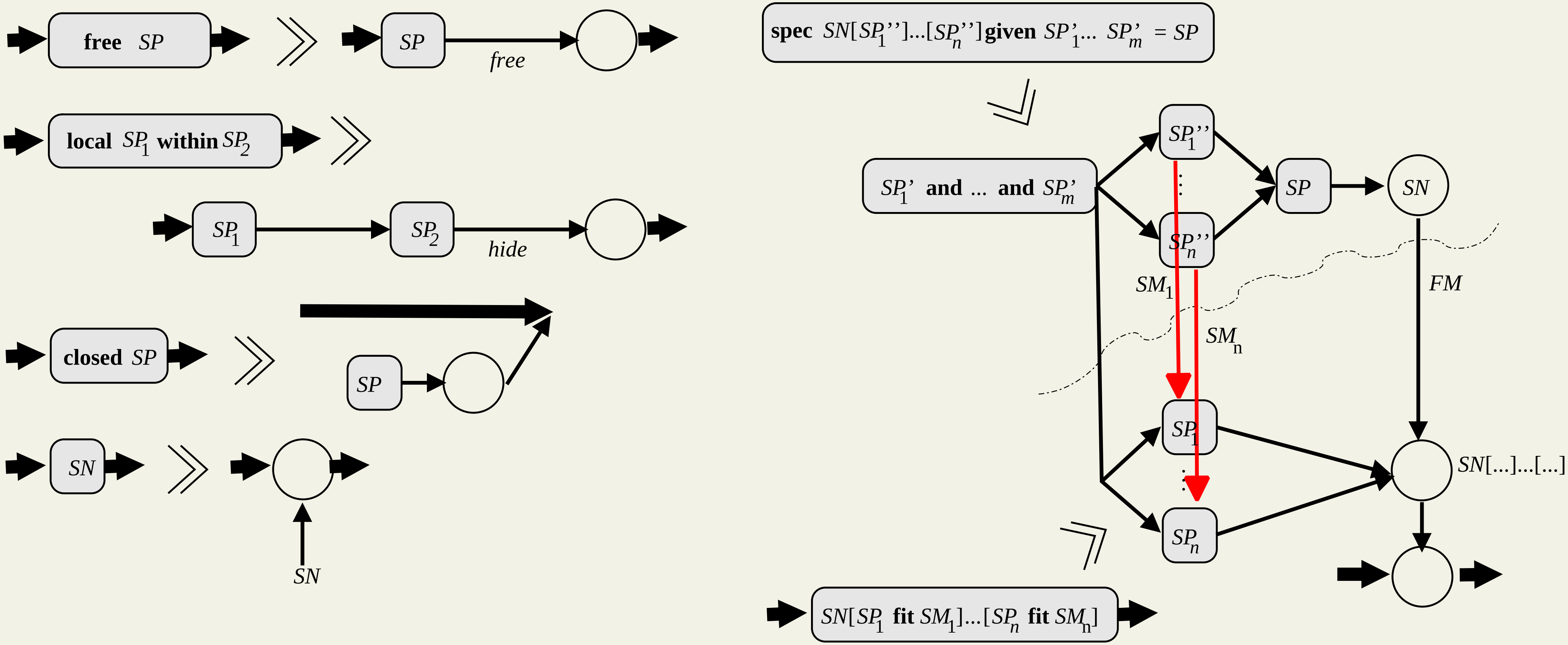
$$M \xrightarrow{\sigma} N$$

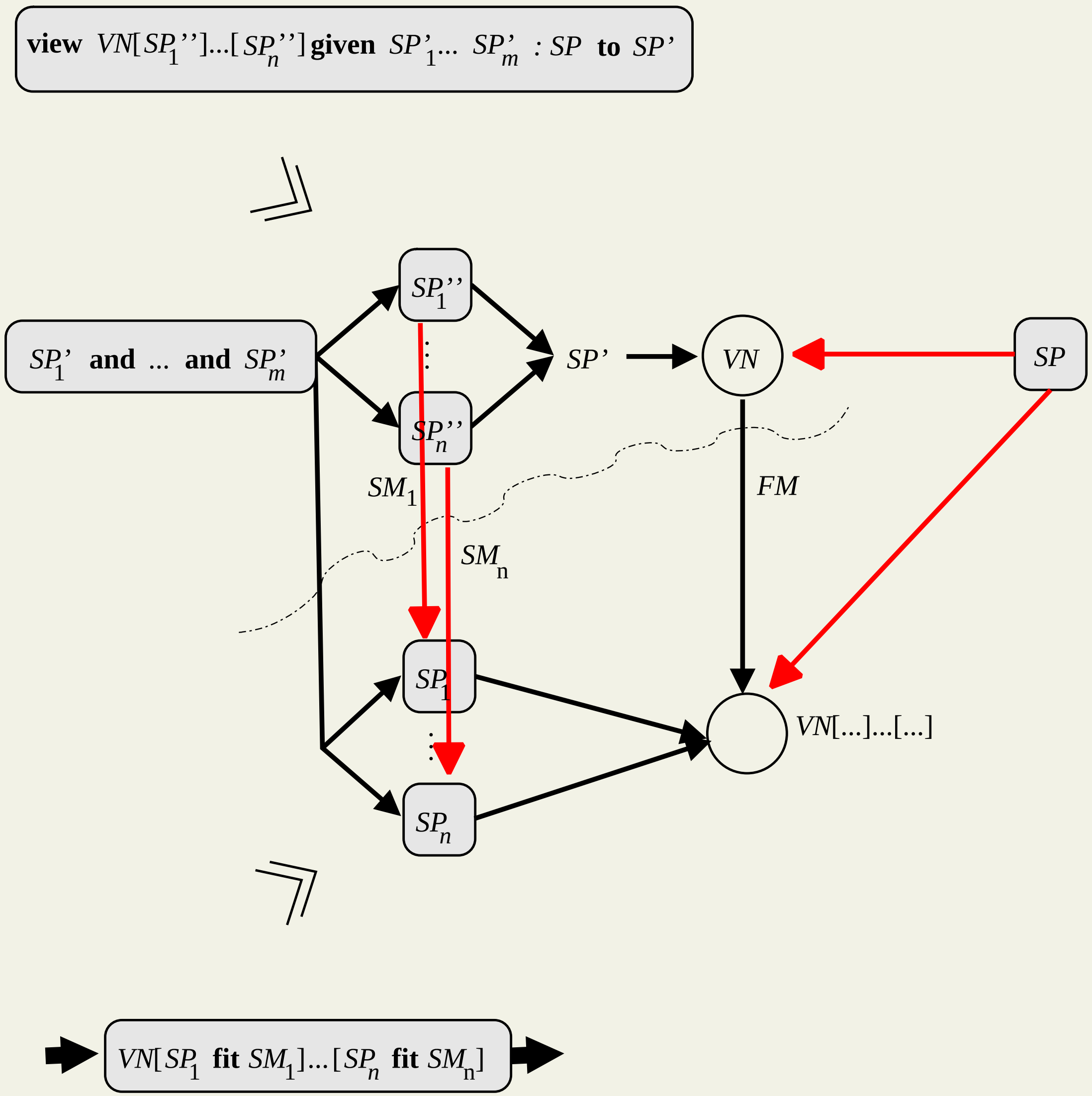
(μ_i) a weakly amalgamable cocone for "zig-zag path diagram" D


List+Order
Perm+Order+Def
InsertSortDef
SorterProps
Sorting
InsertSort
c
h
h
(a)
⟹
List+Order
Perm+Order+Def
InsertSortDef
SorterProps
N
Sorting
InsertSort
c
h
h
(b)
⟹
List+Order
Perm+Order+Def
InsertSortDef
SorterProps
N'
N
Sorting
InsertSort
c
c
h
h
(c)
⟹
List+Order
Perm+Order+Def
InsertSortDef
SorterProps
N'
N
Sorting
InsertSort
c
c
h
h
h
(d)
⟹
List+Order
Perm+Order+Def
InsertSortDef
SorterProps
N'
N
Sorting
InsertSort
c
c
h
h
(e)
⟹
List+Order
Perm+Order+Def
InsertSortDef
SorterProps
N'
N
Sorting
InsertSort
c
c
h
h

Translation of CASL Specifications to Development Graphs


SP with SM
SP
sigma(SM)
SP hide SYs
SP
sigma(SYs)
hide
SP reveal SM
SP
sigma1(SM)
hide
sigma2(SM)
SP1 and ... and SPm
SP1
SPn
SP1 then... then SPm
SP1
...
SPn
SP1 then %cons SP2
SP1
cons
SP2
SP1 then %mono SP2
SP1
mono
SP2
SP1 then %def SP2
SP1
def
SP2
SP1 then %implies SP2
SP1
SP2
Notation:
SP
CASL specification to be translated
SN
development graph node named SN
.. rewrites to ...
flow of the local environment
global definition link
global theorem link
hide
hiding link


free SP
SP
free
local SP1 within SP2
SP1
SP2
hide
closed SP
SP
SN
SN
spec SN[SP''1]...[SP''n] given SP'1... SP'm = SP
SP'1 and ... and SP'm
SP''1
SP''n
SP
SN
SM1
SMn
FM
SP1
SPn
SN[...]...[...]
SN[SP1 fit SM1]...[SPn fit SMn]


view VN[SP1'']...[SPn''] given SP'1... SP'm : SP to SP'
SP'1 and ... and SP'm
SP1''
SPn''
SP'
VN
SP
FM
SM1
SMn
SP1
SPn
VN[...]...[...]
VN[SP1 fit SM1]...[SPn fit SMn]