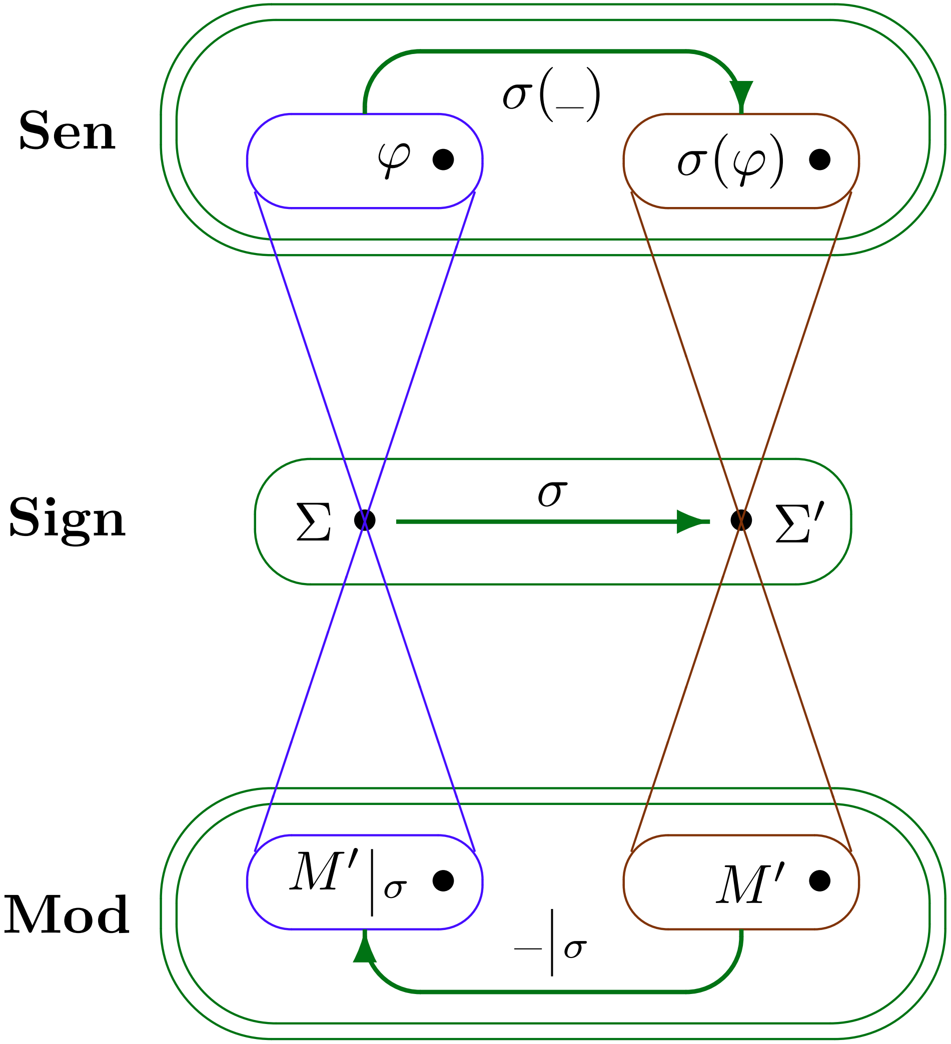
Heterogeneous Logical Environments for Distributed Specifications

Andrzej Tarlecki

Institute of Informatics, University of Warsaw
and
Institute of Computer Science, Polish Academy of Sciences
Warsaw, Poland

Based on joint work with **Till Mossakowski**,
with **María Victoria Cengarle**, **Alexander Knapp** and **Martin Wirsing**,
and with **Adam Warski**.

Working within an institution



imposing the *satisfaction condition:*

$$\boxed{M' \models_{\Sigma'} \sigma(\varphi) \text{ iff } M'|_\sigma \models_\Sigma \varphi}$$

Truth is invariant under change of notation

and independent of any additional symbols around

Institution

- a category $\mathbf{Sign}$ of *signatures*
- a functor $\mathbf{Sen}\colon \mathbf{Sign} \to \mathbf{Set}$
  - $\mathbf{Sen}(\Sigma)$ is the set of Σ-*sentences*, for $\Sigma \in |\mathbf{Sign}|$
- a functor $\mathbf{Mod}\colon \mathbf{Sign}^{op} \to \mathbf{Cat}$
  - $\mathbf{Mod}(\Sigma)$ is the category of Σ-*models*, for $\Sigma \in |\mathbf{Sign}|$
- for each $\Sigma \in |\mathbf{Sign}|$, Σ-*satisfaction relation* $\models_\Sigma \subseteq |\mathbf{Mod}(\Sigma)| \times \mathbf{Sen}(\Sigma)$

subject to the *satisfaction condition*:

$$\boxed{M'|_\sigma \models_\Sigma \varphi \iff M' \models_{\Sigma'} \sigma(\varphi)}$$

where $\sigma\colon \Sigma \to \Sigma'$ in $\mathbf{Sign}$, $M' \in |\mathbf{Mod}(\Sigma')|$, $\varphi \in \mathbf{Sen}(\Sigma)$,
$M'|_\sigma$ stands for $\mathbf{Mod}(\sigma)(M')$, and $\sigma(\varphi)$ for $\mathbf{Sen}(\sigma)(\varphi)$.

Specifications

Basic specifications:

$$\boxed{\langle \Sigma, \Phi \rangle}$$

Structured specifications: built by *specification-building operations*, like:

union: $\boxed{SP_1 \cup SP_2}$

translation: $\boxed{\sigma(SP)}$

hiding: $\boxed{SP'|_\sigma}$

Semantics

Given a specification SP:

- its *signature*: $Sig[SP] \in |\mathbf{Sign}|$
- its *models*: $Mod[SP] \subseteq |\mathbf{Mod}(Sig[SP])|$

Specification morphism $\boxed{\sigma : SP \to SP'}$

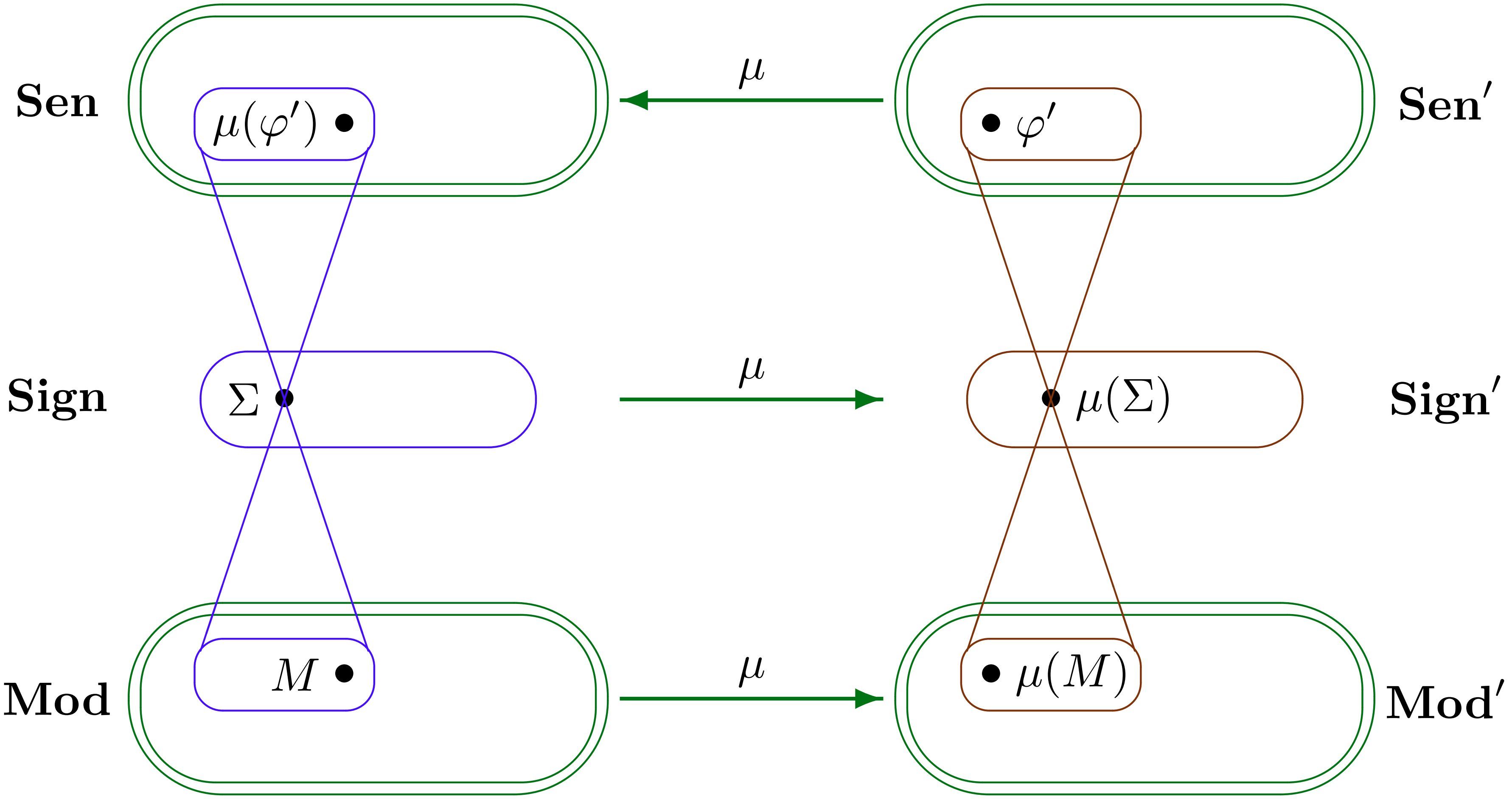
$\sigma : Sig[SP] \to Sig[SP']$ such that $\boxed{\text{for each } M' \in Mod[SP'], M'|_\sigma \in Mod[SP].}$

Toward heterogeneous specifications

Linking institutions with each other

. . . various maps between institutions. . .

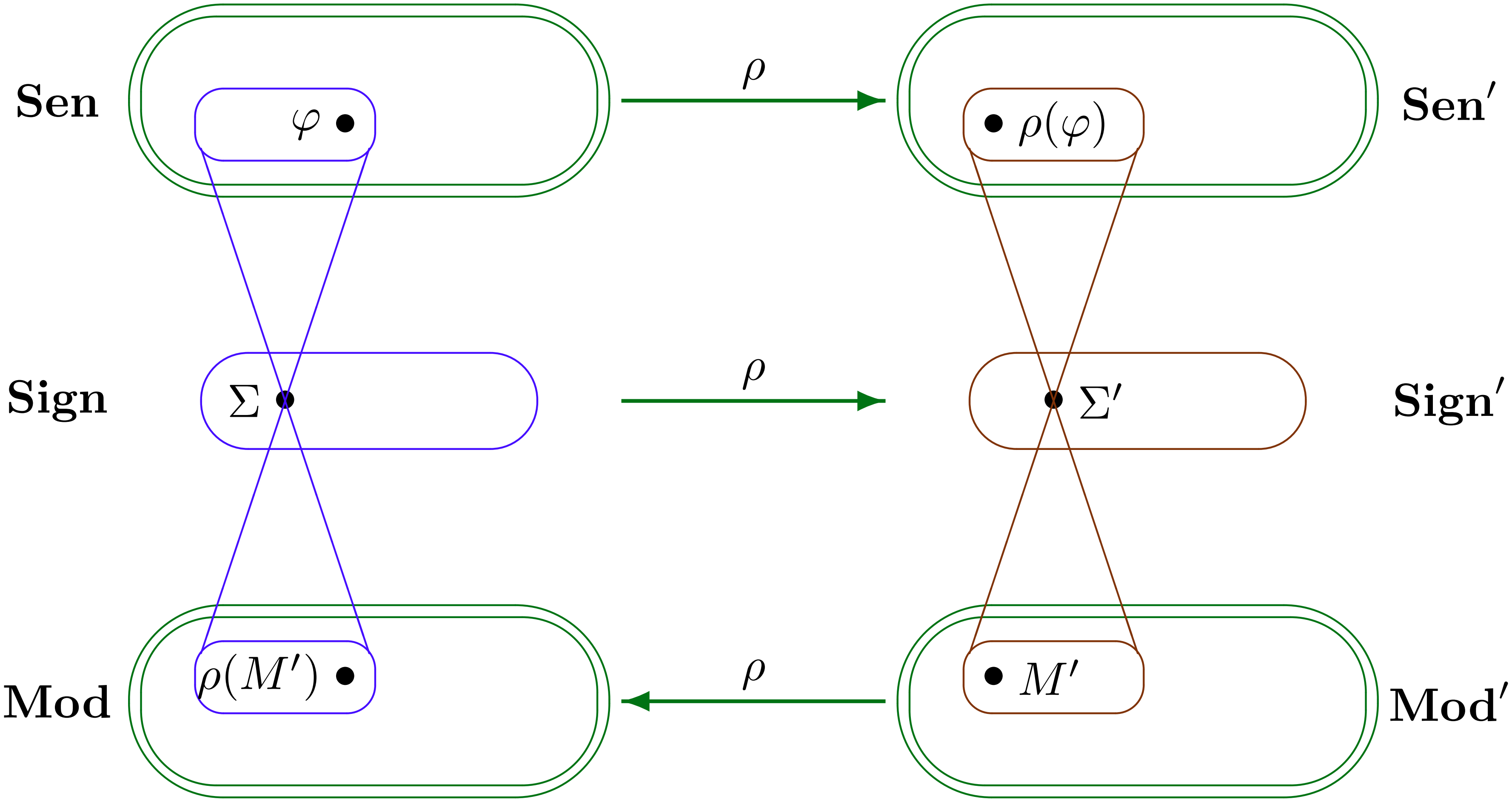
Institution morphism: $\mu\colon \mathbf{I} \longrightarrow \mathbf{I}'$



with the *satisfaction condition* lurking again:

$$\boxed{M \models \mu(\varphi) \ \text{ iff } \ \mu(M) \models' \varphi'}$$

Institution comorphism: $\rho\colon \mathbf{I} \longrightarrow \mathbf{I}'$



with the *satisfaction condition* lurking again:

$$\rho(M') \models \varphi \text{ iff } M' \models' \rho(\varphi)$$

Moving between institutions: a taxonomy of maps

morphisms μ	$\mathbf{Sen} \longleftarrow \mathbf{Sen}'$ $\mathbf{Sign} \longrightarrow \mathbf{Sign}'$ $\mathbf{Mod} \longrightarrow \mathbf{Mod}'$	*semi-morphisms* μ	$\mathbf{Sen} \qquad \mathbf{Sen}'$ $\mathbf{Sign} \longrightarrow \mathbf{Sign}'$ $\mathbf{Mod} \longrightarrow \mathbf{Mod}'$
comorphisms ρ	$\mathbf{Sen} \longrightarrow \mathbf{Sen}'$ $\mathbf{Sign} \longrightarrow \mathbf{Sign}'$ $\mathbf{Mod} \longleftarrow \mathbf{Mod}'$	*semi-comorphisms* ρ	$\mathbf{Sen} \qquad \mathbf{Sen}'$ $\mathbf{Sign} \longrightarrow \mathbf{Sign}'$ $\mathbf{Mod} \longleftarrow \mathbf{Mod}'$
forward morphisms	$\mathbf{Sen} \longrightarrow \mathbf{Sen}'$ $\mathbf{Sign} \longrightarrow \mathbf{Sign}'$ $\mathbf{Mod} \longrightarrow \mathbf{Mod}'$		
forward comorphisms	$\mathbf{Sen} \longleftarrow \mathbf{Sen}'$ $\mathbf{Sign} \longrightarrow \mathbf{Sign}'$ $\mathbf{Mod} \longleftarrow \mathbf{Mod}'$		

plus *theoroidal* versions,

plus *weak* versions, plus . . .

Mastering the diversity

Morphism

$$\begin{tikzcd}
& \mathbf{Set} & \\
& \xleftarrow{\alpha} & \\
\mathbf{Sign}^{(op)} \arrow[uur, "\mathbf{Sen}"] \arrow[ddr, "\mathbf{Mod}"'] \arrow[rr, "\Phi"] & & \mathbf{Sign}'^{(op)} \arrow[uul, "\mathbf{Sen}'"'] \arrow[ddl, "\mathbf{Mod}'"] \\
& \xrightarrow{\beta} & \\
& \mathbf{Cat} &
\end{tikzcd}$$

Span of comorphisms

$$\begin{tikzcd}
& & \mathbf{Set} & & \\
& \xleftarrow{\alpha} & \bullet \arrow[u, "\mathbf{Sen}'"'] & \xrightarrow{=} & \\
\mathbf{Sign}^{(op)} \arrow[uurr, "\mathbf{Sen}"] \arrow[ddrr, "\mathbf{Mod}"'] & & \mathbf{Sign}^{(op)} \arrow[ll, "="'] \arrow[rr, "\Phi"] \arrow[u, "\Phi"'] \arrow[d, "\Phi^{op}"'] & & \mathbf{Sign}'^{(op)} \arrow[uull, "\mathbf{Sen}'"'] \arrow[ddll, "\mathbf{Mod}'"] \\
& \xrightarrow{\beta} & \bullet \arrow[d, "\mathbf{Mod}'"'] & \xleftarrow{=} & \\
& & \mathbf{Cat} & &
\end{tikzcd}$$

Heterogeneous logical environments

A collection of institutions
linked by
(forward) (semi-) (co-) morphisms

A collection of institutions
linked by comorphisms

A diagram $\mathcal{HIE}$ in the category $co\mathcal{INS}$
(of institutions and institution comorphisms)

EXAMPLES:

- a dozen of logics, one for each kind of UML diagrams
- the HETS family of institutions
- Mossakowski's diagram of algebraic and other institutions
- ...

Heterogeneous specifications

- Move to a **universal institution** $\mathbf{UI}$
  (encode institutions in $\mathcal{HIE}$ using comorphisms into $\mathbf{UI}$, compatible with maps within $\mathcal{HIE}$; then work in $\mathbf{UI}$)
- **Focused heterogeneous specifications**
  (specifications that reside in an institution, but may involve specifications from other institutions in $\mathcal{HIE}$)
- **Distributed heterogeneous specifications**
  (specification diagrams over $\mathcal{HIE}$)

Focused heterogeneous specifications

Translation: introduces new structure to specification models, following an institution comorphism $\rho\colon \mathbf{I} \to \mathbf{I}'$; for any $\mathbf{I}$-specification SP,

Also along institution morphisms

$$\boxed{\rho(SP)}$$

is an $\mathbf{I}'$-specification with $Sig[\rho(SP)] = \rho(Sig[SP])$ and $Mod[\rho(SP)] = \{M' \in |\mathbf{Mod}'(\rho(Sig[SP]))| \mid \rho(M') \in Mod[SP]\}$.

Hiding: hides extra structure of specification models, following an institution morphism $\mu\colon \mathbf{I}' \to \mathbf{I}$; for any $\mathbf{I}'$-specification SP',

Also w.r.t. institution comorphisms

$$\boxed{SP'|_{\mu}}$$

is an $\mathbf{I}$-specification with $Sig[SP'|_{\mu}] = \mu(Sig[SP'])$ and $Mod[SP'|_{\mu}] = \{\mu(M') \mid M' \in Mod[SP']\}$.

Essentially: everything as for specifications within a single institution

Heterogeneous specification (co)morphisms

Heterogeneous specification (co)morphism from (simpler) $\mathbf{I}$-specification SP to (richer) $\mathbf{I}'$-specification SP'

$$\boxed{\langle \rho, \sigma' \rangle : SP \to SP'}$$

where $\rho : \mathbf{I} \to \mathbf{I}'$ is an institution comorphism, and $\sigma' : \rho(Sig[SP]) \to Sig[SP']$ is an $\mathbf{I}'$-signature morphism such that $\boxed{\text{for all } M' \in Mod[SP'],\ \rho(M'|_{\sigma'}) \in Mod[SP]}$

This yields a category $co\mathcal{HSPEC}$ of heterogeneous specifications over $\mathcal{HIE}$.

. . . Grothendieck construction. . .

Distributed heterogeneous specifications

- A *distributed heterogeneous specification* $\mathcal{HSP}$ is a diagram of heterogeneous specifications in $co\mathcal{HSPEC}$, $\mathcal{HSP} : \mathcal{J} \rightarrow co\mathcal{HSPEC}$.

Notation:

- for $i \in |\mathcal{J}|$, $\mathcal{HSP}_i$ is the specification $\mathcal{HSP}(i)$
- for $e : i \rightarrow j$ in $\mathcal{J}$, $\mathcal{HSP}_e = \langle \rho_e, \sigma_e \rangle : \mathcal{HSP}_i \rightarrow \mathcal{HSP}_j$ is the heterogeneous specification morphism $\mathcal{HSP}(e)$.

- A *distributed heterogeneous model* of $\mathcal{HSP}$ is a family $\mathcal{M} = \langle M_i \rangle_{i \in |\mathcal{J}|}$ of models *compatible with* $\mathcal{HSP}$.

That is, such that

- for $i \in |\mathcal{J}|$, $M_i \in Mod[\mathcal{HSP}_i]$
- for $e : i \rightarrow j$ in $\mathcal{J}$, $M_i = \rho_e(M_j|_{\sigma_e})$.

$\mathcal{HSP}$ *is (globally) consistent*
if it has a (distributed) model

Implementing distributed specifications

To implement $\mathcal{HSP} : \mathcal{J} \to co\mathcal{HSPEC}$ by $\mathcal{HSP}' : \mathcal{J}' \to co\mathcal{HSPEC}$, provide:

- a *covering function* $f : |\mathcal{J}| \to |\mathcal{J}'|$, and
- a *distributed constructor* $\kappa = \langle \kappa_i : Mod[\mathcal{HSP}'_{f(i)}] \to Mod[\mathcal{HSP}_i] \rangle_{i \in |\mathcal{J}|}$.

So that for each $i \in |\mathcal{J}|$, we have $\mathcal{HSP}_i \underset{\kappa_i}{\leadsto} \mathcal{HSP}'_{f(i)}$.

THEN:

$$\boxed{\mathcal{HSP} \underset{\langle \kappa, f \rangle}{\leadsto} \mathcal{HSP}'}$$

if for each distributed heterogeneous model $\mathcal{M}' = \langle M'_{i'} \rangle_{i' \in |\mathcal{J}'|}$ of $\mathcal{HSP}'$, $\kappa_f(\mathcal{M}') = \langle \kappa_i(M'_{f(i)}) \rangle_{i \in |\mathcal{J}|}$ is a distributed heterogeneous model of $\mathcal{HSP}$.

STRUCTURE MAY CHANGE! INSTITUTIONS MAY CHANGE!

WE NEED TO ARRIVE AT A SINGLE “IMPLEMENTATION” INSTITUTION

“Natural” implementations of distributed specifications

Fact: *For any* $\mathcal{HSP} : \mathcal{J} \rightarrow co\mathcal{HSPEC}$ *and* $\mathcal{HSP}' : \mathcal{J}' \rightarrow co\mathcal{HSPEC}$, *given*

- *a functor* $F : \mathcal{J} \rightarrow \mathcal{J}'$
- *a natural transformation* $\tau : \mathcal{HSP} \rightarrow F;\mathcal{HSP}'$ *with* $\tau_i = \langle \rho_i, \sigma_i \rangle : \mathcal{HSP}_i \rightarrow \mathcal{HSP}'_{F(i)}$ *for* $i \in |\mathcal{J}|$

we have

$$\boxed{\mathcal{HSP} \underset{\langle \kappa, f \rangle}{\rightsquigarrow} \mathcal{HSP}'}$$

where

- $f = |F| : |\mathcal{J}| \rightarrow |\mathcal{J}'|$
- $\kappa = \langle \rho_i(\_|_{\sigma_i}) : Mod[\mathcal{HSP}'_{F(i)}] \rightarrow Mod[\mathcal{HSP}_i] \rangle_{i \in |\mathcal{J}|}$

Understanding (distributed) UML specifications

> *UML specifications consist of a number of diagrams of various kinds, each forming a specification in a different logic.*

NECESSARY TASKS:

- Build the heterogeneous logical environment of UML.
- Give a meaning to UML heterogeneous distributed specifications in such an environment.

(Some) UML diagram logics

Institution of Static Structures $\mathcal{ISS}$ (class diagrams) with:

- signatures that name classes, attributes, methods and associations typed as expected,
- sentences that essentially are class diagrams,
- models that are sets of states and interpret attributes and methods as functions and associations as relations.

Institution of Interaction $\mathcal{IINT}$ (interaction diagrams) with:

- signatures that name classes and messages (typed by classes),
- sentences that essentially are interaction diagrams
- models that for each interpretation of class names as sets of object instances and messages as sets of message instances, and for each valuation of variables, yield sets of permitted and forbidden traces, respectively.

Institution of OCL $\mathcal{OCL}$ (OCL specifications) with:

- signatures that name classes, queries and methods (typed as expected)
- sentences as in OCL (invariants, pre/postconditions, etc)
- models that are state transition systems, with sets of objects as states and transitions labelled by method invocations (and possibly their results).

Linking (some) UML diagram logics

- $\mathcal{ISS} \to \mathcal{IINT}$ and $\mathcal{ISS} \to \mathcal{OCL}$: easy, obvious comorphisms can be given.
- Relating $\mathcal{IINT}$ and $\mathcal{OCL}$ is more difficult; a sink of comorphisms

$$\mathcal{IINT} \longrightarrow \mathcal{OCL}{+}\mathcal{IINT} \longleftarrow \mathcal{OCL}$$

can be given to capture the expected consistency requirements.

BTW: Spans of comorphisms capture sharing requirements.

BTW: Consistency may be better captured by spans of morphisms.

Completing distributed specifications

UML lists specifications over various logics in its heterogeneous logical environment. Compatibility can be captured by (co)morphisms, to be added as follows:

Given a sink of institution comorphisms $\rho_1 \colon \mathbf{I}_1 \to \mathbf{I}$ and $\rho_2 \colon \mathbf{I}_2 \to \mathbf{I}$, for each $\mathbf{I}_1$-specification SP_1 and $\mathbf{I}_2$-specification SP_2, add $\mathbf{I}$-specification

$$\boxed{SP = \rho_1(SP_1) \textbf{ and } \rho_2(SP_2)}$$

with the span of heterogeneous specification comorphisms

$$\boxed{\langle \rho_1, \iota_1 \rangle : SP_1 \to SP \text{ and } \langle \rho_2, \iota_2 \rangle : SP_2 \to SP}$$

Union of signatures of $\rho_1(SP_1)$ and $\rho_2(SP_2)$ is required (with inclusions ι_1 and ι_2).

Models $M_1 \in Mod[SP_1]$ and $M_2 \in Mod[SP_2]$ are compatible if $M_1 = \rho_1(M|_{\iota_1})$ and $M_2 = \rho_2(M|_{\iota_2})$ for some $\mathbf{I}$-model M (witnessing consistency of M_1 and M_2).

Dually for sharing requirements captured by spans of comorphisms

Morphism-based heterogeneous specifications

Heterogeneous logical environment

A collection of institutions linked by morphisms

A diagram $\mathcal{HIE}$ in the category $\mathcal{INS}$ (of institutions and institution morphisms)

Define: another category $\mathcal{HSPEC}$ of heterogeneous specifications over $\mathcal{HIE}$, with *heterogeneous specification morphism* from (simpler) $\mathbf{I}$-specification SP to (richer) $\mathbf{I}'$-specification SP' $\boxed{\langle \mu, \sigma \rangle : SP \to SP'}$ where $\mu : \mathbf{I}' \to \mathbf{I}$ is an institution morphism, and $\sigma : Sig[SP] \to \mu(Sig[SP'])$ is an $\mathbf{I}$-signature morphism such that $\boxed{\text{for all } M' \in Mod[SP'],\ \mu(M')|_\sigma \in Mod[SP]}$

Problem: $\mathcal{HSPEC}$ over $\mathcal{HIE}$ and $co\mathcal{HSPEC}$ over $span(\mathcal{HIE})$ are quite different!

BTW: adjunctions between signature categories help

Mix them well!

Mixed heterogeneous logical environments

Problem: $\mathcal{INS}$ and $co\mathcal{INS}$ do not mix well...

Work with heterogeneous logical environments as
$\mathcal{INS} + co\mathcal{INS}$ *"mixed" diagrams of institutions*

Problem: $\mathcal{HSPEC}$ and $co\mathcal{HSPEC}$ do not mix well...

Work with distributed heterogeneous specifications as
$\mathcal{HSPEC} + co\mathcal{HSPEC}$ *"mixed" diagrams of specifications*

Another overall option:

Work within a category of institutions with
relational links between them. . .

Sample other further work

- keep building up the environment of relevant institutions and (forward) (semi-)(co)morphisms between them;

  complete UML heterogeneous environment!

- work systematically with semi-(co)morphisms between institutions;
- going to the limits;
- relational links between institutions
- expected results and methods for distributed heterogeneous specifications;
- proof theoretic links between institutions linked semantically;
- architectural heterogeneous specifications;
- programming links between "programming" institutions linked semantically;
- . . .