A Heterogeneous Approach to Service-oriented Systems Specification

Alexander Knapp*
Grzegorz Marczyński**
Martin Wirsing†
Artur Zawłocki**

*Universität Augsburg
**Uniwersytet Warszawski
†Ludwig-Maximilians-Universität München

Goals

- Declarative logical specification of services
  - for proving properties of operational models (like BPEL, BPMN, UML4SOA, &c.)
- Separation between individual service behaviour and orchestration
  - Loose coupling of services
  - Interaction structure can change over time
  - Number of services not known in advance
  - Local logics for specifying services, global logics for specifying interactions
- Institutional framework for integrating local and global logics
  - Heterogeneous service specifications
  - Connection to other languages described as institutions

Example: E-Course Management System

Student service(s), course manager service, course provider service(s)

1. Student enters data
2. Student service transfers data to course manager service
3. Course manager service contacts available course provider services
4. Course manager service collects provider data, selects possible courses
5. Course manager service provides student service with data
6. Optionally, student service registers student for selected courses

- Specification of individual services in local logic
  - independent of whether services are themselves composed or not
- Specification of choreography of services in global logic
  - Synchronisation predicate for describing changing communication structure
  - Quantification over services for unbounded number of participants

Local Logics

$\mathrm{aPCTL}^*(A)$: Action-based CTL* with past temporal operators and atomic propositions $a \in A$ interpreted over transitions

$$\begin{aligned}\varphi \ ::= {} & \bot \ \mid \ \varphi_1 \Rightarrow \varphi_2 \ \mid \ a \ \mid \\ & \mathsf{X}\,\varphi \ \mid \ \mathsf{Y}\,\varphi \ \mid \ \varphi_1 \,\mathsf{U}\, \varphi_2 \ \mid \ \varphi_1 \,\mathsf{S}\, \varphi_2 \ \mid \ \mathsf{A}\,\varphi\end{aligned}$$

Interpretation over runs $\pi = s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} \ldots$ of a labelled transition system $(A, S, s_0, \rightarrow)$ at position $0 \leq i \leq |\pi|$

- $\pi, i \models a$ iff $a_{i+1} = a$ and $i < |\pi|$
- $\pi, i \models \mathsf{X}\,\varphi$ iff $\pi, (i+1) \models \varphi$ and $i < |\pi|$
- $\pi, i \models \mathsf{Y}\,\varphi$ iff $\pi, (i-1) \models \varphi$ and $0 < i$
- $\pi, i \models \mathsf{A}\,\varphi$ iff $\pi', i \models \varphi$ for every run π' with $\pi\restriction_i = \pi'\restriction_i$

Parameterisation of next and previous operators for disregarding actions

- $\mathsf{X}_{\mathcal{A}}\,\varphi \ \equiv \ \mathsf{X}\,\big((\neg \bigvee_{a \in \mathcal{A}} a)\,\mathsf{U}\,\varphi\big)$

Local Logics: Example

Local specification of student service S

- Observable actions: $\mathcal{A}_S = \{ask!, answer?, choose!, register!\}$
- Axioms

  $\mathsf{G}\,(ask! \Rightarrow \mathsf{X}_{\mathcal{A}_S}\, answer?)$

  - After requesting a list of courses a reply is expected.

  $\mathsf{G}\,(answer? \Rightarrow \mathsf{Y}_{\mathcal{A}_S}\, ask!)$

  - A reply may be observed only as the next action after the request is sent.

  $\mathsf{G}\,(choose! \Rightarrow \mathsf{Y}_{\mathcal{A}_S}\, answer?)$

  - Choosing a course may be observed only after the reply is received.

  $\mathsf{G}\,(register! \Rightarrow \mathsf{Y}_{\mathcal{A}_S}\, choose!)$

  - Registering may be observed only after choosing a course.

Institutions

Institution $\mathbb{I} = (\mathit{Sign}, \mathit{Mod}, \mathit{Sen}, \langle \models_\Sigma \rangle_{\Sigma \in |\mathit{Sign}|})$

- category Sign of signatures Σ
- functor $\mathit{Mod} : \mathit{Sign}^{\mathrm{op}} \to \mathrm{Class}$ for classes of Σ-models
  - for $\sigma : \Sigma \to \Sigma'$ $\mathit{Mod}(\sigma)$ σ-reduct map
- functor $\mathit{Sen} : \mathit{Sign} \to \mathrm{Set}$ for sets of Σ-sentences
  - for $\sigma : \Sigma \to \Sigma'$ $\mathit{Sen}(\sigma)$ translation map
- family $\langle \models_\Sigma \subseteq \mathit{Mod}(\Sigma) \times \mathit{Sen}(\Sigma) \rangle_{\Sigma \in |\mathit{Sign}|}$ of satisfaction relations
- Satisfaction condition for all $\sigma : \Sigma \to \Sigma'$, Σ'-models M', Σ-sentences φ

$$\mathit{Mod}(\sigma)(M') \models_\Sigma \varphi \iff M' \models_{\Sigma'} \mathit{Sen}(\sigma)(\varphi)$$

- For $\Sigma \in |\mathit{Sign}|$, $\mathit{Ax} \subseteq \mathit{Sen}(\Sigma)$ $\mathit{Sp} = (\Sigma, \mathit{Ax})$ specification in $\mathbb{I}$
  - $M \models \mathit{Sp}$, if $M \in \mathit{Mod}(\Sigma)$ and $M \models_\Sigma \varphi$ for all $\varphi \in \mathit{Ax}$
- Sp' refines Sp along $\sigma : \Sigma \to \Sigma'$
  - $\mathit{Mod}(\sigma)(M') \models \mathit{Sp}$ for all M' with $M' \models \mathit{Sp}'$

Local Logic Institution $\mathbb{L}$

- Category of signatures $\mathit{Sign}^{\mathbb{L}}$

  Set for action names

- Model functor $\mathit{Mod}^{\mathbb{L}} : \mathrm{Set}^{\mathrm{op}} \to \mathrm{Class}$

  Local $\mathcal{A}$-models $M = (T, \langle a^M \rangle_{a \in \mathcal{A}})$

  labelled transition system $T = (A, S, s_0, \to)$, actions $a^M \in A$

  f-reduct map for $f : \mathcal{A} \to \mathcal{B}$: $(T, \langle b^M \rangle_{b \in \mathcal{B}})|f = (T, \langle f(a)^M \rangle_{a \in \mathcal{A}})$

- Sentence functor $\mathit{Sen}^{\mathbb{L}} : \mathrm{Set} \to \mathrm{Set}$

  $\mathcal{A}$-sentences: formulae in $\mathrm{aPCTL}^*(\mathcal{A})$

  translation map for $f : \mathcal{A} \to \mathcal{B}$: replacing a by $f(a)$

- Satisfaction relation for local $\mathcal{A}$-model $M = (T, \langle a^M \rangle_{a \in \mathcal{A}})$, $\mathcal{A}$-sentence φ

  $M \models^{\mathbb{L}}_{\mathcal{A}} \varphi$ iff $T \models (\varphi)^M$

Proposition $\mathbb{L} = (\mathit{Sign}^{\mathbb{L}}, \mathit{Mod}^{\mathbb{L}}, \mathit{Sen}^{\mathbb{L}}, \models^{\mathbb{L}})$ is an institution.

Global Logics

Similar to local logics, but taking into account

- classes of services $\mathcal{C}$
- action names $\mathcal{A}_c$ for each service class $c \in \mathcal{C}$
- service variables k
  - service k does a yields action proposition $k.a$
- synchronisation of actions in services
  - $k_1.a_1 \sim k_2.a_2$ says that k_1 and k_2 do a_1 resp. a_2 together

$$\begin{array}{rl} \varphi ::= & \bot \mid \varphi_1 \Rightarrow \varphi_2 \mid \\ & \mathsf{X}\,\varphi \mid \mathsf{Y}\,\varphi \mid \varphi_1\,\mathsf{U}\,\varphi_2 \mid \varphi_1\,\mathsf{S}\,\varphi_2 \mid \mathsf{A}\,\varphi \mid \\ & \forall k : c \cdot \varphi \mid k_1 = k_2 \mid k.a \mid k_1.a_1 \sim k_2.a_2 \end{array}$$

Parameterisation of next and previous operators for disregarding actions

- $\mathsf{Y}_k^{\mathcal{A}_c}\,\varphi \equiv \mathsf{Y}\,\neg(\bigvee_{a\in\mathcal{A}_c} k.a)\,\mathsf{S}\,\varphi$

Global Logics: Example

Global specification of e-course management system

- Service classes $\mathcal{C} = \{student, course, mngm\}$
- Action names $\mathcal{A}_S$, $\mathcal{A}_C$, $\mathcal{A}_M$
- Axioms

  $\exists s : student \cdot s.ask!$

  - Initial condition: There is a student asking for courses.

  $\forall s : student \cdot \mathsf{G}\,(s.ask! \Rightarrow \exists m : mngm \cdot s.ask! \sim m.ask? \wedge$
  $\quad \mathsf{F}\,(s.answer? \wedge m.answer!))$

  - A student asking for courses is connected to a management service and sometime will receive a reply.

  $\forall m : mngm \cdot \mathsf{G}\,((\mathsf{Y}_m^{\mathcal{A}_M}\, m.select!) \Rightarrow \exists c : course \cdot m.request! \sim c.request?)$

  - When selecting courses, at least one course is available (i.e., connected to a management service).

Global Frames

Global frame $G = (N, \langle T_n \rangle_{n \in N}, S, s_0, \rightarrow)$

- set of service names N
- a labelled transition system $T_n = (A_n, S_n, s_{0,n}, \rightarrow_n)$ for each $n \in N$
- set of global configurations $S \subseteq (\prod_{n \in N} S_n) \times \mathit{Sync}(\langle T_n \rangle_{n \in N})$
  - synchronisations $\mathit{Sync}(\langle T_n \rangle_{n \in N})$ equivalence relations over actions from different T_n
- initial global configuration $s_0 \in S$
- global transition relation $\rightarrow \subseteq S \times \wp(\coprod_{n \in N} A_n) \times S$
  - $(\langle s_n \rangle_{n \in N}, \sim) \xrightarrow{A} (\langle s'_n \rangle_{n \in N}, \sim')$ has $A \in (\coprod_{n \in N} A_n)/\sim$ and takes all synchronised actions in A locally simultaneously
  - Progress condition: all transitions from synchronised local transitions are possible

Interpretation of Global Logics

- Global frame $(N, \langle T_n \rangle_{n \in N}, S, s_0, \rightarrow)$
- Assignment of service names to classes $\nu(c) \subseteq N$ for $c \in \mathcal{C}$
- Assignment of variables $\xi(k) \in N$

Interpretation over runs $\rho = \langle s_0, \sim_0 \rangle \xrightarrow{[a_1]_{\sim_0}} \langle s_1, \sim_1 \rangle \xrightarrow{[a_2]_{\sim_1}} \ldots$ of global frame at position $0 \leq i \leq |\rho|$ w.r.t. ξ

- $\rho, i, \xi \models k.a \quad$ iff $\quad \xi(k).a \in [a_{i+1}]_{\sim_i}$ and $i < |\rho|$
- $\rho, i, \xi \models \mathsf{X}\, \varphi \quad$ iff $\quad \rho, (i+1), \xi \models \varphi$ and $i < |\rho|$
- $\rho, i, \xi \models k_1.a_1 \sim k_2.a_2 \quad$ iff $\quad \xi(k_1).a_1 \sim_i \xi(k_2).a_2$
- $\rho, i, \xi \models \forall k : c \cdot \varphi \quad$ iff $\quad \rho, i, \xi\{k \mapsto n\} \models \varphi$ for all $n \in \nu(c)$

Global Logic Institution

- Category of signatures $\mathit{Sign}^{\mathbb{G}}$

  objects $\Gamma = (\mathcal{C}, \langle \mathcal{A}_c \rangle_{c \in \mathcal{C}})$ for service classes, action names per class

  morphisms γ componentwise
- Model functor $\mathit{Mod}^{\mathbb{G}} : (\mathit{Sign}^{\mathbb{G}})^{\mathrm{op}} \to \mathrm{Class}$

  Global Γ-models $M = (G, \langle c^M \rangle_{c \in \mathcal{C}}, \langle a_n^M \rangle)$

  global frame $G = (N, \langle T_n \rangle_{n \in N}, S, s_0, \to)$

  $c^M \subseteq N$, $a_n^M \in A_n$ $(n \in c^M$ for $a \in \mathcal{A}_c)$

  γ-reduct map by relabelling
- Sentence functor $\mathit{Sen}^{\mathbb{G}} : \mathit{Sign}^{\mathbb{G}} \to \mathrm{Set}$

  $\mathcal{A}$-sentences: closed formulae in global logic

  translation map for γ by renaming (taking variables into account)
- Satisfaction relation for global Γ-model M and Γ-sentence φ

  $M \models_{\Gamma}^{\mathbb{G}} \varphi \quad$ iff $\quad G \models (\varphi)^M$

Proposition $\mathbb{G} = (\mathit{Sign}^{\mathbb{G}}, \mathit{Mod}^{\mathbb{G}}, \mathit{Sen}^{\mathbb{G}}, \models^{\mathbb{G}})$ is an institution.

Institution Co-Morphisms

Representation (embedding) of an institution $\mathbb{I}$ in an institution $\mathbb{I}'$

Institution co-morphism $(\Phi, \alpha, \beta) : \mathbb{I} \to \mathbb{I}'$

- functor $\Phi : \mathit{Sign} \to \mathit{Sign}'$
- natural transformation $\alpha : \mathit{Sen} \to \Phi; \mathit{Sen}'$
- natural transformation $\beta : \Phi; \mathit{Mod}' \to \mathit{Mod}$
- satisfaction condition for all $\Sigma \in |\mathit{Sign}|$, $M' \in \mathit{Mod}'(\Phi(\Sigma))$, $\varphi \in \mathit{Sen}(\Sigma)$

$$M' \models'_{\Phi(\Sigma)} \alpha_\Sigma(\varphi) \iff \beta_\Sigma(M') \models_\Sigma \varphi$$

Relating Local and Global Logics

Global model induces several local models, one for each service

- Construct “powerset” institution $\wp(\mathbb{L})$ with same signatures and sentence functor as $\mathbb{L}$, but a set of $\mathbb{L}$-models as $\wp(\mathbb{L})$-models

Define

- $\Gamma(\mathcal{A}) = (\{*\}, \{* \mapsto \mathcal{A}\})$ for every set $\mathcal{A} \in |\mathit{Sign}^{\mathbb{L}}|$
  - with “dummy” service class name $*$
- $\alpha_{\mathcal{A}}(\varphi) = \forall k : * \cdot \varphi$ for all $\varphi \in \mathit{Sen}^{\mathbb{L}}(\mathcal{A})$
- $\beta_{\mathcal{A}}(M) = \{M\restriction_n \mid n \in *^M\}$ for all $M \in \mathit{Mod}^{\mathbb{G}}(\Gamma(\mathcal{A}))$
  - $M\restriction_n$ projects M to service n

Proposition $(\Gamma, \alpha, \beta) : \wp(\mathbb{L}) \to \mathbb{G}$ is an institution-comorphism.

Heterogeneous Service Specifications

Given

- $\mathcal{C}$ set of service classes
- Local signature $\mathcal{A}_c$ for each $c \in \mathcal{C}$
- Local specification Sp_c for each $c \in \mathcal{C}$
- Global specification Sp over $(\mathcal{C}, \langle \mathcal{A}_c \rangle_{c \in \mathcal{C}})$

Heterogeneous service specification $(\langle c : Sp_c \rangle_{c \in \mathcal{C}}, Sp)$

- Signature $\Gamma = (\mathcal{C}, \langle \mathcal{A}_c \rangle_{c \in \mathcal{C}})$
- Class of models

$$\{M \in Mod^{\mathbb{G}}(\Gamma) \mid (\forall c \in \mathcal{C} \,.\, M \models \alpha_{\mathcal{A}_c}(Sp_c)\{* \mapsto c\} \wedge M \models Sp\}$$

- Transfer of notion of refinement

Example: $Sp_{eCM} = (\langle student : Sp_S, course : Sp_C, mngm : Sp_M \rangle, Sp)$

Refinement: Example

Course selection in two phases

1. Management service selects continuations of previously taken courses
2. Management service chooses new feasible courses

Local refinement of management service

- Extended signature $\mathcal{A}_{M_1} = \mathcal{A}_M \cup \{selContinuation!, selFeasible!\}$
- Additional axiom

$$\mathsf{G}\,(reply? \land \neg \mathsf{X}_{\mathcal{A}_M}\, reply? \Rightarrow \\ \mathsf{X}_{\mathcal{A}_{M_1}}\,(selContinuation! \land \mathsf{X}_{\mathcal{A}_{M_1}}\,(selFeasible! \land \mathsf{F}\, select!))$$

- Refinement in $\mathbb{L}$ since other axioms relative to $\mathcal{A}_M$

From this refinement as heterogeneous service specification

Conclusions and Outlook

Institution-based heterogeneous formal specification of service-oriented systems

- Local logic for individual services
- Global logic for service interactions
- Integration of local and global logic

Future work

- Other choices of local/global logics
  - State predicates
  - Requirements for local institution w.r.t. global institution
- Asynchronous communication
  - focus on loose coupling
- Architectural specifications
  - independent implementation