Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 230 (2009) 161–187
www.elsevier.com/locate/entcs

Sheaves and Geometric Logic and Applications to Modular Verification of Complex Systems[1]

Viorica Sofronie-Stokkermans[2]

Max-Planck Institut für Informatik, Stuhlsatzenhausweg 85, Saarbrücken, Germany

Abstract

In this paper we show that states, transitions and behavior of concurrent systems can often be modeled as sheaves over a suitable topological space. In this context, geometric logic can be used to describe which local properties, of individual systems, are preserved, at a global level, when interconnecting the systems. The main area of application is to modular verification of complex systems. We illustrate the ideas by means of an example involving a family of interacting controllers for trains on a rail track.

Keywords: Geometric logic, sheaves, modular verification

1 Introduction

Complex systems, consisting of several components that interact, arise in a natural way in a wide range of applications. The components may be complex themselves (they may e.g. contain a database; may have their specific internal logic and an appropriate inference mechanism; a planning mechanism, etc.), or may be simple - but even then their composition can complicated because of the necessity to take into account the interaction between the single components. One of the main problems that arise in the verification of such complex systems is the state explosion problem: the state space can grow exponentially with the number of components. Symbolic representations of states and symbolic model checking have greatly increased the size of the systems that can be verified. However, many realistic systems are still too large to be handled. It is therefore important to find techniques that can be used to

[1] This work was partly supported by the German Research Council (DFG) as part of the Transregional Collaborative Research Center "Automatic Verification and Analysis of Complex Systems" (SFB/TR 14 AVACS). See www.avacs.org for more information.

[2] Email: sofronie@mpi-inf.mpg.de

1571-0661/
doi:10.1016/j.entcs.2009.02.024

further extend the size of the systems that can be verified. One possibility is to check properties in a modular way (i.e. verify them for the individual components, infer that they also hold in the system obtained by the interconnection of the individual components, and then use them to deduce additional properties of the system). Not all properties are preserved by interconnection: for instance deadlocks might occur when interconnecting deadlock free systems. The main goal of this paper is to offer an answer to an important question in verification:

Which properties of complex systems can be checked in a modular way?

To answer such questions, in this paper we use an analogy with phenomena in topology and algebraic geometry, where sheaves are used to describe locally defined objects which can be patched together into a global object. Thus, sheaf theory allows to establish links between "local" and "global" properties. We show that, given a family of interacting systems, states, actions, transitions, behavior in time can often be modeled by sheaves over a suitable topological space (where the topology expresses how the interacting systems share the information). Many properties of systems can be expressed as assertions about states, actions, transitions, behavior in time. The sheaf semantics allows us to prove, by using results from geometric logic, that those properties of systems that can be expressed by *cartesian axioms* are preserved after interconnecting the systems.

The starting point of our research is the work of Goguen [6], who uses sheaves to model behavior in an 'interval of observation', and Monteiro and Pereira [13], where behavior is modeled by sheaves of monoids. The idea of modeling states, actions and transitions by sheaves with respect to a topological space, and of using geometric logic for studying the link between properties of the components and properties of the systems that arises from their interconnection occurs, to the best of our knowledge, for the first time in our previous work [16,17,18]. We present an overview of our results in [17,18] together with new results which illustrate how sheaf theory can be used for the modular verification of complex systems. We illustrate all the notions introduced by means of a running example involving a family of interacting controllers controlling a subsets of consecutive trains on a linear, loop-free, rail track. The main contributions of the paper are summarized below:

- We start with a presentation of our previous results described in [16,17,18], where we showed that states, parallel actions, transitions and behavior in time can be modeled by sheaves. Concerning these topics, the main contribution of this paper consists in illustrating the various notions we use (definition of systems, states, parallel actions, transitions, conditions on transition relations, categorical constructions, covers, gluing and sheaf properties) by means of a running example.
- In addition to the model of behavior we considered in [16,17,18], we also analyze a description of behavior by traces of execution (modeled by free monoids and partially commutative monoids). We analyze gluing and sheaf properties also in this context. We pay special attention also in this case to identifying situations when the stalks of the sheaves are isomorphic to the behavior of the individual systems, whereas the global sections are isomorphic to the behavior of the colimit

of these systems. For this, we use results on sheaf representation in universal algebra. We establish links with existing results in the study of Petri nets and Mazurkiewicz traces [3] and on modeling behavior by sheaves of monoids [13].

- We use geometric logic for describing properties which can be checked modularly. We illustrate the ideas on the running example, and describe a simple complex system for trains for which safety and lifeness can be checked in a modular way.

Structure of the paper. The paper is structured as follows. In Section 2 we present a model for systems (including also their states, parallel actions and transitions). Section 3 contains the definition of a category of systems and the description of pullbacks and colimits in this category. In Section 4 we give a model for complex, interacting systems, and motivate the use of sheaf theory. Sections 5–8 describe our sheaf-theoretic semantics for states, parallel actions, transitions and behavior. In Section 9 geometric logic is used to test preservation of 'local' properties under connection of systems. Several examples are given in Section 10.

2 Systems

Our aim is to model interconnected systems. We assume systems are described by:

- a set X of control variables of the system, a set Γ of constraints on X expressed in a language $\mathcal{L}$,
- a set A of atomic actions, and a set C of constraints on A.

Let $\Sigma = (\mathsf{Sort}, O, P)$ be a signature, consisting of a set Sort of sorts, a set O of operation symbols and a set P of predicate symbols. For a (many-sorted) set of variables $X = \{X_s\}_{s\in\mathsf{Sort}}$ let $\mathsf{Fma}_\Sigma(X)$ be the set of formulae over Σ.
A Σ-*structure* is a structure $M = ((M_s)_{s\in\mathsf{Sort}}, \{f_M\}_{f\in O}, \{R_M\}_{R\in P})$ where if $f \in O$ has arity $s_1 \dots s_n \to s$ then $f_M : M_{s_1} \times \dots \times M_{s_n} \to M_s$ and if $R \in P$ has arity $s_1 \dots s_n$ then $R_M \subseteq M_{s_1} \times \dots \times M_{s_n}$. The class of all Σ-structures is denoted Str_Σ. If $M \in \mathsf{Str}_\Sigma$, $s : X \to M$ is a sort-preserving assignment, and $\phi \in \mathsf{Fma}_\Sigma(X)$, $(M, s) \models \phi$ (abbreviated by $s \models \phi$) is defined in the usual way (cf. [1], Ch. 1).

Definition 2.1 A *system* S is a tuple $(\Sigma, X, \Gamma, M, A, C)$, where

(i) $\Sigma = (\mathsf{Sort}, O, P)$ and $X = \{X_s\}_{s\in\mathsf{Sort}}$ are as specified above; together they define the *language* $\mathcal{L}_S$ *of the system* S;

(ii) $\Gamma \subseteq \mathsf{Fma}_\Sigma(X)$ is a set of constraints, which is closed with respect to the semantical consequence relation [3] $\models_M$;

(iii) $M \in \mathsf{Str}_\Sigma$;

(iv) A is a set of actions; for every $a \in A$, a set $X^a \subseteq X$ of variables on which a depends, and a transition relation $Tr^a \subseteq St^a \times St^a$, where $St^a = \{s_{|X^a} \mid s : X \to M, s \models \Gamma\}$ are specified;

[3] The relation $\models_M$ is defined by $\Gamma \models_M \phi$ if and only if for every assignment $s : X \to M$ of values in M to the variables in X, if $s \models \gamma$ for every $\gamma \in \Gamma$, then $s \models \phi$.

(v) C is a set of constraints on actions, expressed by boolean equations over $F_B(A)$ (the free boolean algebra generated by A) stating e.g. which actions can (or have to) be executed in parallel, and which cannot; C must contain all boolean equations that can be deduced from C.

In what follows, we may refer to any of the components of a system S by adding S as a subscript, e.g. Σ_S for its signature. X_S^a will denote the minimal set of variables on which $a \in A_S$ depends, and Tr_S^a the transition relation associated with a.

For the sake of simplicity, in the examples below we will only mention explicitly the axioms in Γ and C and not all their consequences.

Example 2.2 We consider a system consisting of n consecutive trains on a linear track controlled by a radio controller (cf. also [8]). The trains report their position to the controller at fixed time intervals Δt. The controller analyzes the distances between successive trains (we assume that certain security distance treshholds $l_0 < l_1 < \cdots < l_m < \ldots$ and corresponding maximal speed limits $\mathsf{maxSpeed}(1) < \cdots < \mathsf{maxSpeed}(m) < \ldots$, deemed to be safe for the trains, are known) and updates the movement modes of trains accordingly. A train with movement mode k can move in the next time interval Δt with an arbitrary speed between a minimal speed and the maximal speed limit of mode k, $\mathsf{maxSpeed}(k)$. The system is modeled as follows:

(i) *Language:* $\Sigma = (\mathsf{Sort}, O, P)$, where $\mathsf{Sort} = \{\mathsf{real}, \mathsf{nat}\}$;
- $O = \{+, -, \mathsf{minSpeed}, \mathsf{maxSpeed}, \mathsf{succ}\}$, where $+, -$:real, real→real, $\mathsf{minSpeed}$ is a constant of sort real, $\mathsf{maxSpeed}$ a function of arity $\mathsf{nat} \to \mathsf{real}$, and succ of arity $\mathsf{nat} \to \mathsf{nat}$.
- $P = \{\leq\}$, where $\leq$ has arity $\mathsf{real}, \mathsf{real}$.
- $X = \bigcup_{i=1}^{n} \{\mathsf{TrainIndex}_i, \mathsf{ActualPos}_i, \mathsf{RepPos}_i, \mathsf{Mode}_i\}$, where $\mathsf{TrainIndex}_i$ controls the number of train i on the line track, and $\mathsf{ActualPos}_i, \mathsf{RepPos}_i$ and Mode_i control the actual, resp. reported position and the movement mode of train i respectively.

(ii) *Constraints:* $\Gamma = \{\mathsf{succ}(\mathsf{TrainIndex}_i) = \mathsf{TrainIndex}_{i+1} \mid i \in \{1, \ldots, n-1\}\}$.

(iii) *Model* $M = (M_{\mathsf{nat}}, M_{\mathsf{real}}, +, -, \mathsf{minSpeed}, \mathsf{maxSpeed}, \mathsf{succ}, \leq)$, where $M_{\mathsf{nat}} = \mathbb{N}$; $M_{\mathsf{real}} = \mathbb{R}$; $+, -$ are addition and subtraction on $\mathbb{R}$, $\mathsf{succ} : \mathbb{N} \to \mathbb{N}$ is the successor function, $\mathsf{minSpeed} \in \mathbb{R}$, $\mathsf{maxSpeed} : \mathbb{N} \to \mathbb{R}$ associates with a mode $k \in \mathbb{N}$ the maximal allowed speed in mode k; $\leq$ is the order relation on $\mathbb{R}$.

(iv) *Actions:* $A = \{\mathsf{report}_i \mid i \in \{1, \ldots, n\}\} \cup \{\mathsf{update}\} \cup \{\mathsf{move}_i \mid i \in \{1, \ldots, n\}\}$.
- report_i depends on the variables $X^{r_i} = \{\mathsf{ActualPos}_i, \mathsf{RepPos}_i, \mathsf{Mode}_i\}$.

  If $s, s' : X \to M$ then $(s_{|X^{r_i}}, s'_{|X^{r_i}}) \in Tr^{r_i}$ iff $s(\mathsf{Mode}_i) = 0$
  $s'(\mathsf{RepPos}_i) = s(\mathsf{ActualPos}_i)$
  $s'(\mathsf{ActualPos}_i) = s(\mathsf{ActualPos}_i)$.
- update depends on $X^u = \bigcup_{i \in \{1,\ldots,n\}} \{\mathsf{ActualPos}_i, \mathsf{RepPos}_i, \mathsf{Mode}_i\}$.
  If $s, s' : X \to M$ then $(s_{|X^u}, s'_{|X^u}) \in Tr^{r_i}$ if and only if for all $i \in \{1, \ldots, n\}$ the following hold: (i) $s(\mathsf{Mode}_i) = 0$, (ii) $s'(\mathsf{ActualPos}_i) = s(\mathsf{ActualPos}_i)$, (iii) $s'(\mathsf{RepPos}_i) = s(\mathsf{ActualPos}_i)$, and (iv) $s'(\mathsf{Mode}_i)$ is updated according to the following rules: $s'(\mathsf{Mode}_1) > 0$ and for all $i \geq 2$:

if $l_k < s(\mathsf{RepPos}_{i-1}) - s(\mathsf{RepPos}_i) \leq l_{k+1}$ then $s'(\mathsf{Mode}_i) = k+1$.

- move_i depends on $X^{m_i} = \{\mathsf{ActualPos}_i, \mathsf{Mode}_i\}$. It is enabled at a state s iff $s(\mathsf{Mode}_i) > 0$ for all $i \in \{1, \ldots, n\}$; it changes $\mathsf{ActualPos}_i$ according to the value of Mode_i as follows, for $i \in \{1, \ldots, n\}$:

  $s'(\mathsf{ActualPos}_i) \in [\mathsf{RepPos}_i + \Delta t * \mathsf{minSpeed}, \mathsf{RepPos}_i + \Delta t * \mathsf{maxSpeed}(s(\mathsf{Mode}_i))]$;

  and it updates the value of Mode_i to 0: $s'(\mathsf{Mode}_i) = 0$ for $i \in \{1, \ldots, n\}$.

(v) *Constraints on actions:* $C = \{\mathsf{report}_1 = \mathsf{report}_2 = \cdots = \mathsf{report}_n = \mathsf{update}\} \cup \{\mathsf{report}_i \wedge \mathsf{move}_i = 0 \mid i \in \{1, \ldots, n\}\} \cup \{\mathsf{move}_1 = \cdots = \mathsf{move}_n\}$.

2.1 States, parallel actions

It is important to describe *the states* of a system and *the actions which can be performed in parallel* (which we here name admissible parallel actions).

Definition 2.3 Let $S = (\Sigma, X, \Gamma, M, A, C)$ be a system.

- A *state* of S is an assignment $s : X \to M$ satisfying all formulae in Γ. The *set of states* of the system S is $St(S) = \{s : X \to M \mid s \models \Gamma\}$.
- The *admissible parallel actions* of S are sets of actions, represented by maps $f : A \to \{0, 1\}$ that satisfy all constraints in C. The *set of admissible parallel actions* of S is the set $Pa(S) = \{f : A \to \{0, 1\} \mid f \text{ satisfies } C\}$.

Below we restrict our attention to *finite* systems, i.e. systems whose signatures, sets of control variables and sets of actions are finite; this suffices for practical applications and avoids having to consider infinitely many actions occurring in parallel.

Example 2.4 Consider the system S in Example 2.2 with $n \geq 2$. A state is a map $s : X \to M$ which satisfies Γ. For instance, any map $s : X \to M$ such that:

- $s(\mathsf{TrainIndex}_1) = 1, s(\mathsf{TrainIndex}_2) = 2, \ldots, s(\mathsf{TrainIndex}_n) = n$ or
- $s(\mathsf{TrainIndex}_1) = 100, s(\mathsf{TrainIndex}_2) = 101, \ldots, s(\mathsf{TrainIndex}_n) = 100 + (n-1)$.

is a state of S. If $s(\mathsf{TrainIndex}_1) = 1$ and $s(\mathsf{TrainIndex}_2) = 3$, s cannot be a state.

An admissible parallel action is a map $f : A \to \{0, 1\}$ which satisfies the constraints in C. Examples of admissible parallel actions are

(i) $f(\mathsf{report}_1) = f(\mathsf{report}_2) = \cdots = f(\mathsf{report}_n) = f(\mathsf{update}) = 1$, and 0 otherwise,

(ii) $f(\mathsf{move}_1) = \cdots = f(\mathsf{move}_n) = 1$ and 0 otherwise.

Any map f with $f(\mathsf{move}_1) = f(\mathsf{report}_1) = 1$, or with $f(\mathsf{report}_i) = 0$ but $f(\mathsf{update}) = 1$, is not an admissible parallel action, since it does not satisfy the constraints in C.

2.2 Transitions

Let $S = (\Sigma, X, \Gamma, M, A, C)$ be a system. Let $Tr_S(a) = \{(s_1, s_2) \mid s_1, s_2 \in St(S), (s_{1|X^a}, s_{2|X^a}) \in Tr^a, s_1(x) = s_2(x) \text{ if } x \notin X^a\}$. We extend the notion of

transition to parallel actions. For this we present two (non-equivalent) properties of transitions that express compatibility of the actions in an admissible parallel action:

(**Disj**) Let $f \in Pa(S), s \in St(S)$ such that for every $a \in f^{-1}(1)$ there is an $s^a \in St(S)$ with $(s_{|X^a}, s^a_{|X^a}) \in Tr^a$. Then for all $a, b \in f^{-1}(1)$ and $x \in X^a \cap X^b$, $s^a(x) = s^b(x)$ (the new local states agree on intersections). Then,

$$Tr_S(f) = \{(s,t) \mid s,t \in St(S), (s_{|X^a}, t_{|X^a}) \in Tr^a \text{ for every } a \text{ such that } f(a) = 1 \text{ and } s(x) = t(x) \text{ if } x \notin \bigcup_{a,f(a)=1} X^a\}.$$

The property (**Disj**) applies when a parallel action $f : A \to \{0,1\}$ is admissible iff its components do not consume common resources. This happens e.g. if for all $a_1, a_2 \in A$ with $f(a_1) = f(a_2) = 1$, either $a_1 = a_2 \in C$ or X^{a_1} and X^{a_2} are disjoint. In concurrency theory, this property is called "real parallelism" or "independence".

Example 2.5 Consider the example in Section 2.2. Let $f : A \to \{0,1\}$ be an admissible parallel action. We have two possibilities:

(i) $f(\mathsf{report}_1) = \cdots = f(\mathsf{report}_n) = f(\mathsf{update}) = 1$ and 0 otherwise.
The transition relation of this parallel action updates the value of each variable RepPos_i according to the transition relation of report_i, resp. update. The changes are not contradictory, since the effect of update agrees with the effect of $\mathsf{report}_1, \ldots, \mathsf{report}_n$ on the variables in $X^u \cap X^{r_i}$. Thus, (**Disj**) holds.

(ii) $f(\mathsf{report}_1) = \cdots = f(\mathsf{report}_n) = f(\mathsf{update}) = 0$ and $f(\mathsf{move}_1) = \cdots = f(\mathsf{move}_n) = 1$ and f is 0 otherwise. As the actions $\mathsf{move}_j, j = 1, \ldots, n$ depend on disjoint sets of variables, (**Disj**) is satisfied also in this case.
The transition relation of this parallel action updates the value of each variable $\mathsf{ActualPos}_i$. Since the sets of variables these actions depend upon, namely X^{m_i}, are mutually disjoint, these changes cannot be contradictory.

(**Indep**) Assume that if $a = b \in C$ then $X^a = X^b$ and $Tr^a = Tr^b$, and a and b can both be identified with one action: the parallel execution of a, b.
Let $f \in Pa(S), s \in St(S)$. We identify all $a, b \in A$ with $a = b \in C$ and $f(a) = f(b) = 1$. Let $\{b_1, \ldots, b_m\} \subseteq f^{-1}(1)$. We assume that:

(i) $g : A \to \{0,1\}$, defined by $g(a) = 1$ iff $a \in \{b_1, \ldots, b_m\}$, is in $Pa(S)$;
(ii) if $s \xrightarrow{b_1} s_1 \xrightarrow{b_2} s_2 \to \ldots \to s_{m-1} \xrightarrow{b_m} t$ then for every permutation σ of $\{1, \ldots, m\}$, there exist states $t^\sigma_1, \ldots, t^\sigma_{m-1}$ with $s \xrightarrow{b_{\sigma(1)}} t^\sigma_1 \xrightarrow{b_{\sigma(2)}} t^\sigma_2 \to \ldots \to t^\sigma_{m-1} \xrightarrow{b_{\sigma(m)}} t$

Then $Tr_S(f) = \{(s,t) \mid s,t \in St(S),$ and $\exists s_0, s_1, \ldots, s_{n-1}, s_n \in St(S)$ s.t. $s_0 = s, s_n = t,$ and $(s_{i-1}, s_i) \in Tr_S(a_i),$ for all $1 \le i \le n\}$.

It is easy to see that if $(s,t) \in Tr_S(f)$ then $s(x) = t(x)$ for every $x \notin \bigcup_{a,f(a)=1} X^a$. The property (**Indep**) reflects how transitions are interpreted when actions to be performed in parallel do consume common resources. It applies if the state reached after executing an action is uniquely determined: the fact that all components of a parallel action $f : A \to \{0,1\}$ can be applied at a state s is a necessary condition for f to be applicable at state s, but in general not sufficient (in addition, one

has to ensure that there are enough resources to perform all actions). Condition (**Indep**)(i) holds e.g. if C is the set of all consequences of a set C_0 consisting only of formulae of the form $a_1 = a_2$ and $a_1 \wedge a_2 = 0$. Condition (**Indep**)(ii) states that the final state does not depend on the order in which the actions are executed (it is related to the notions of interleaving and permutable actions used in concurrency).

Example 2.6 We consider a variant of Example 2.2, in which we assume that there is no control unit, but all trains have access to all information about the positions of all trains. The trains report all together and move all together. The actions are $A = \{\mathsf{report}_1, \ldots, \mathsf{report}_n\} \cup \{\mathsf{move}_1, \ldots, \mathsf{move}_n\}$, with constraints $C = \{\mathsf{report}_1 = \cdots = \mathsf{report}_n\} \cup \{\mathsf{move}_1 = \cdots = \mathsf{move}_n\} \cup \{\mathsf{report}_i \wedge \mathsf{move}_i = 0 \mid i \in \{1, \ldots, n\}\}$. Let $f : A \to \{0, 1\}$ be an admissible parallel action. Then $f^{-1}(1)$ is either $\emptyset$ or $\{\mathsf{report}_1, \ldots, \mathsf{report}_n\}$ or $\{\mathsf{move}_1, \ldots, \mathsf{move}_n\}$. As in all cases the actions in $f^{-1}(1)$ depend on disjoint sets of variables, the final state does not depend on the order in which the actions would be performed sequentially.

3 A category of systems

Essential to our model for communication is that systems have common subsystems through which information exchange is made. Let S, T be two systems. We say that S is a *subsystem* of T (denoted $S \rightarrowtail T$) if $\Sigma_S \subseteq \Sigma_T$, $X_S \subseteq X_T$, $A_S \subseteq A_T$, the constraints in Γ_S (resp. C_S) are consequences of the constraints in Γ_T (resp. C_T), and $M_S = M_{T|\Sigma_S}$ (the reduct of M_T to the signature Σ_S).

Let $S \rightarrowtail T$. If we regard a transition in T from the perspective of S, some variables in S may change their values with no apparent cause, namely if some action in A_T but not in A_S is performed, which depends on variables in X_S. If this cannot be the case, we call the subsystem $S \rightarrowtail T$ *transition-connected*. Formally:

Definition 3.1 S is a *transition-connected (t.c.) subsystem of* T (denoted $S \hookrightarrow T$) if $S \rightarrowtail T$ and the following two conditions hold:

(T_1) If $a \in A_T$ and $X_T^a \cap X_S \neq \emptyset$ then $a \in A_S$, and $X_S^a = X_T^a \cap X_S$.

(T_2) If $a \in A_S$, $s_1, s_2 \in St(T)$, and $(s_{1|X_T^a}, s_{2|X_T^a}) \in Tr_T^a$ then $(s_{1|X_S^a}, s_{2|X_S^a}) \in Tr_S^a$.

It is easy to see that the relation $\hookrightarrow$ is a partial order on systems.

Example 3.2 Consider the system $S = (\Sigma, X, \Gamma, M, A, C)$ in Example 2.2. Let $1 \leq k \leq l \leq n$ and $I = \{k, \ldots, l\}$. Consider the restriction $S_k^l = (\Sigma, X_k^l, \Gamma_k^l, M, A_k^l, C_k^l)$ of S to the consecutive trains controlled by the variables in $\{\mathsf{TrainIndex}_i \mid i \in I\}$.

- $X_k^l = \bigcup_{i \in I} \{\mathsf{TrainIndex}_i, \mathsf{ActualPos}_i, \mathsf{RepPos}_i, \mathsf{Mode}_i\}$,
- $\Gamma_k^l = \{\mathsf{succ}(\mathsf{TrainIndex}_i) = \mathsf{TrainIndex}_{i+1} \mid i \in \{k, \ldots, l-1\}\}$,
- $A_k^l = \{\mathsf{report}_i \mid i \in I\} \cup \{\mathsf{update}\} \cup \{\mathsf{move}_i \mid i \in I\}$, and
- C_k^l is the restriction of C to the actions in A_k^l:

  $C_k^l = \{\mathsf{report}_i{=}\mathsf{update} \mid i{\in}I\} \cup \{\mathsf{report}_i{\wedge}\mathsf{move}_i{=}0 \mid i{\in}I\} \cup \{\mathsf{move}_k{=}\ldots{=}\mathsf{move}_l\}$.

Condition (T_1) obviously holds: if an action of S depends on variables known in S_k^l,

then the action is known in S_k^l. Condition (T_2) obviously holds for $\{\mathsf{report}_i \mid i \in I\} \cup \{\mathsf{move}_i \mid i \in I\}$ and, for update, for all trains which follow a train known in S_k^l. For the first train (T_2) is a consequence of the fact that the mode update restrictions in S are stronger than those in S_k^l (any mode allowed in S is still allowed in S_k^l).

We define a category TcSys having as objects systems, and a morphism $S \hookrightarrow T$ between S and T whenever S is a t.c. subsystem of T. TcSys has *pullbacks* (infimums with respect to this order of t.c. subsystems of a given system; we will denote this operation by $\wedge$) and *colimits* of diagrams of t.c. subsystems of a given system.

Proposition 3.3 *The category* TcSys *has pullbacks.*

Proof: Let $S_1 \hookrightarrow S$ and $S_2 \hookrightarrow S$, where $S = (\Sigma, X, \Gamma, M, A, C)$, $S_i = (\Sigma_i, X_i, \Gamma_i, M_i, A_i, C_i)$. Then $M_i = M_{|\Sigma_i}$, and for every $a \in A_i$, $X_i^a = X_S^a \cap X_i$ (i = 1, 2) Hence, for every $a \in A_1 \cap A_2$, $X_1^a \cap X_2 = X_2^a \cap X_1 = X_S^a \cap X_1 \cap X_2$.

Let $S_{12} = (\Sigma_1 \cap \Sigma_2, X_1 \cap X_2, \Gamma_1 \cap \Gamma_2, M_{S|\Sigma_1 \cap \Sigma_2}, A_1 \cap A_2, C_1 \cap C_2)$, and such that for every $a \in A_1 \cap A_2$, $X_{12}^a = X_1^a \cap X_2 = X_2^a \cap X_1 = X_S^a \cap X_1 \cap X_2$, and $Tr_{12}^a = \{(s_{1|X_{12}^a}, s_{2|X_{12}^a}) \mid s_1, s_2 \in St(S_1), (s_{1|X_1^a}, s_{2|X_1^a}) \in Tr_{S_1}^a\} \cup \{(s_{1|X_{12}^a}, s_{2|X_{12}^a}) \mid s_1, s_2 \in St(S_2), (s_{1|X_2^a}, s_{2|X_2^a}) \in Tr_{S_2}^a\}$. It is easy to see that S_{12} is a transition-connected subsystem of both S_1 and S_2, and has the universality property of a pullback. □

Proposition 3.4 *Let $S = (\Sigma, X, M, \Gamma, A, C)$ be a system and $\{S_i \hookrightarrow S \mid i \in I\}$ a family of transition-connected subsystems of S, where for every $i \in I$, $S_i = (\Sigma_i, X_i, M_i, \Gamma_i, A_i, C_i)$. The colimit of this family in* $\mathsf{SYS_{il}}$ *is the system $\overline{S}$ with $\Sigma_{\overline{S}} = \bigcup_{i \in I} \Sigma_i$, $X_{\overline{S}} = \bigcup_{i \in I} X_i, M_{\overline{S}} = M_{|\bigcup_{i \in I} \Sigma_i}, \Gamma_{\overline{S}} = (\bigcup_{i \in I} \Gamma_i)^\bullet$ (the family of all logical consequences of $\bigcup_{i \in I} \Gamma_i$), $A_{\overline{S}} = \bigcup_{i \in I} A_i, C_{\overline{S}} = (\bigcup_{i \in I} C_i)^\bullet$ (the family of all logical consequences of $\bigcup_{i \in I} C_i$), and where for every $a \in \bigcup_{i \in I} A_i$ $X_{\overline{S}}^a = \bigcup_{a \in A_i} X_i^a$, and $Tr_{\overline{S}}^a = \{(s_{1|X_{\overline{S}}^a}, s_{2|X_{\overline{S}}^a}) \mid s_1, s_2 \in St(\overline{S})$, and for every $i \in I$ with $a \in A_i, (s_{1|X_i^a}, s_{2|X_i^a}) \in Tr_{S_i}^a\}$.*

Proof: (Sketch) One needs to show that for every $i \in I$, S_i is a transition-connected subsystem of $\overline{S}$, and that $\overline{S}$ satisfies the universality property of a colimit. The proof is long, but straightforward. □

Example 3.5 Consider the system S in Example 2.2, and two restrictions $S_1 = S_k^n$ and $S_2 = S_1^l$ constructed as in Example 3.2. The pullback of S_1 and S_2 is $S_{12} = S_k^l$ (defined as in Example 3.2 if $k \leq l$, or the system with the empty set of control variables and actions if $l < k$). The colimit $\overline{S}$ of the diagram $\{S_1, S_2, S_{12}\}$ (with transition-connected morphisms $S_k^l \hookrightarrow S_k^n, S_k^l \hookrightarrow S_1^l$ has the following components:

- $\Sigma_{\overline{S}} = \Sigma; M_{\overline{S}} = M$;
- $X_{\overline{S}} = \bigcup_{i \in \{1,\ldots,l\} \cup \{k,\ldots,n\}} \{\mathsf{TrainIndex}_i, \mathsf{ActualPos}_i, \mathsf{RepPos}_i, \mathsf{Mode}_i\}$,
- $\Gamma_{\overline{S}} = \{\mathsf{succ}(\mathsf{TrainIndex}_i) = \mathsf{TrainIndex}_{i+1} \mid i \in \{1, \ldots, l-1\} \cup \{k, \ldots, n-1\}\}^\bullet$,
- $A_{\overline{S}} = \bigcup_{i \in \{1,\ldots,l\} \cup \{k,\ldots,n\}} \{\mathsf{report}_i, \mathsf{move}_i\} \cup \{\mathsf{update}\}$;
- $C_{\overline{S}} = (\{\mathsf{report_i} = \mathsf{update} \mid i \in \{1, \ldots, l\} \cup \{k, \ldots, n\}\} \cup \{\mathsf{report}_i \wedge \mathsf{move}_i = 0 \mid i \in \{1, \ldots, l\} \cup \{k, \ldots, n\}\} \cup \{\mathsf{move}_1 = \cdots = \mathsf{move}_l\} \cup \{\mathsf{move}_k = \cdots = \mathsf{move}_n\})^\bullet$.

If $k \leq l$ then $\overline{S}$ coincides with S. If $l < k-1$ then $X_{\overline{S}} \neq X$, so $\overline{S}$ is obviously different from S. Assume now that $l = k-1$. Then $X_{\overline{S}} = X, A_{\overline{S}} = A, C_{\overline{S}} = C$, but $\Gamma_{\overline{S}} \neq \Gamma$ (the constraint $\mathsf{succ}(\mathsf{TrainIndex}_{k-1}) = \mathsf{TrainIndex}_k$ cannot be recovered from $\Gamma_1^l \cup \Gamma_k^n$), hence $\overline{S}$ is different from S also in this case.

4 Modeling families of interacting systems

When analyzing concrete complex systems, we tend to be interested in a subcategory of TcSys, containing only the systems relevant for a given application. To this end, we assume a family InSys of interacting systems is specified, fulfilling:

(i) All $S \in \mathsf{InSys}$ are transition-connected subsystems of a system $\overline{S}$ with $A_{\overline{S}}$ finite.

(ii) InSys is closed under all pullbacks $S_1 \wedge S_2$ of t.c. subsystems S_1, S_2 of $\overline{S}$.

(iii) $(\mathsf{InSys}, \wedge)$ is a meet-semilattice.

The first condition enforces the compatibility of models on common sorts and the finiteness of A_S for every $S \in \mathsf{InSys}$; the second and third condition ensure that all systems by which communication is handled are taken into account. A system obtained by interconnecting some elements of InSys can either be seen as the set of all elements of InSys by whose interaction it arises (a subset of InSys which is downwards-closed with respect to $\hookrightarrow$) or as the colimit of such a family of elements. We define $\Omega(\mathsf{InSys})$ as consisting of all families of elements of InSys which are closed under transition connected subsystems. Clearly, $\Omega(\mathsf{InSys})$ is a topology on InSys.

Note: $\Omega(\mathsf{InSys})$ is the Alexandroff topology associated with the dual of the poset $(\mathsf{InSys}, \hookrightarrow)$. Since we assumed that InSys is finite and closed under pullbacks, this topology coincides with the Scott topology associated with the dual of $(\mathsf{InSys}, \hookrightarrow)$.

Example 4.1 Consider now the extension of the example in Section 2.2 considered in Example 3.5: Let $k \leq l \in \{1, \ldots, n\}$, let $I_1 = \{k, \ldots, n\}, I_2 = \{1, \ldots, l\}, I_{12} = \{k, \ldots, l\}$, and let $\mathsf{InSys} = \{S_1, S_2, S_{12}\}$ be the family consisting of the subsystems of $S = (\Sigma, X, \Gamma, M, A, C)$ described in Section 2.2 corresponding to the sets of trains with indices in I_1, I_2 and I_{12} respectively: $S_1 = S_k^n$, $S_2 = S_1^l, S_{12} = S_k^l$. Then InSys satisfies conditions (i), (ii) and (iii) above. The system obtained by interconnecting S_1, S_2, S_{12} can be regarded either as the set $\{S_1, S_2, S_{12}\}$ or as the colimit of the diagram defined by these systems, which coincides with the system S defined in Section 2.2. In this case, $\Omega(\mathsf{InSys})$ consists of the following sets $\{\emptyset, \{S_{12}\}, \{S_1, S_{12}\}, \{S_2, S_{12}\}, \{S_1, S_2, S_{12}\}\}$.

Our goal is to express the links between components of a system and the result of their interconnection. We start from the observation that compatible local states can be 'glued' into a global state (similar for parallel actions, transitions). For expressing such gluing condition in a general setting, we use sheaf theory.

4.1 Sheaf theory: An introduction

In what follows, notions from category theory are assumed known. For details cf. [9] or [12]. Categories and sheaves will be denoted in sans-serif style, e.g. Set, $\mathsf{Sh}(I)$.

Let I be a topological space, and $\Omega(I)$ the topology on I.

Definition 4.2 A *presheaf* on I is a functor $P : \Omega(I)^{op} \to \mathsf{Sets}$. Let $U \subseteq V$ be open sets in I, and $i_U^V : U \hookrightarrow V$ the inclusion morphism in $\Omega(I)$. The restriction to U, $P(i_U^V) : P(V) \to P(U)$ is denoted by ρ_U^V.
A *sheaf* on I is a presheaf $F : \Omega(I)^{op} \to \mathsf{Sets}$ that satisfies the following condition:

> for each open cover $(U_i)_{i\in I}$ of U and family of elements $s_i \in F(U_i)$ s.t. for all i, j, $\rho^{U_i}_{U_i\cap U_j}(s_i) = \rho^{U_j}_{U_i\cap U_j}(s_j)$, there is a unique $s \in F(U)$ with $\rho^U_{U_i}(s) = s_i$ for all i.

The morphisms of (pre)sheaves are natural transformations. We denote by $\mathsf{PreSh}(I)$ the category of presheaves over I and by $\mathsf{Sh}(I)$ the category of sheaves over I.

Definition 4.3 The *stalk* of a sheaf F on I at a point $i \in I$ is the colimit $F_i = \varinjlim_{i\in U} F(U)$, where U ranges over all open neighborhoods of i. The assignment $F \mapsto F_i$ defines the stalk functor at i, $\mathsf{Stalk}_i : \mathsf{Sh}(I) \to \mathsf{Set}$.

Sheaves can be defined also in a different way. An indexed system of sets $(F_i)_{i\in I}$ can alternatively be regarded as a map $f : F = \coprod_{i\in I} F_i \to I$, with the property that for every $x \in F$, $f(x) = i$ if and only if $x \in F_i$. If the index set I has a topology, then the set F can be endowed with a topology such that f is continuous (i.e. the sets in the family $(F_i)_{i\in I}$ are continuously indexed).

Definition 4.4 A *bundle* over I is a triple (F, f, I) where F and I are topological spaces and $f : F \to I$ is continuous. For every $i \in I$, $f^{-1}(i)$ will be denoted by F_i. Then $F = \coprod_{i\in I} F_i$. Let (F, f, I) and (G, g, I) be two bundles over I. A morphism between (F, f, I) and (G, g, I) is a continuous map $h : F \to G$ such that $g \circ h = f$. The *category of bundles* over I is denoted Sp/I.

Let LH/I be the full subcategory of Sp/I with objects (F, f, I), where $f : F \to I$ a local homeomorphism (i.e. for every $a \in F$ there are open neighborhoods U and U' of a respectively $f(a)$ such that $f : U \to U'$ is a homeomorphism).

Definition 4.5 Let (F, f, I) be a bundle over I. A *partial section* defined on a open subset $U \subseteq I$ is a continuous map $s : U \to F$ with the property that $f \circ s$ is the inclusion $U \subseteq I$. A section defined on I is called *global section*. The set of all partial sections over the open subset U of I will be denoted by $\Gamma(F, f)(U)$.

The following links between (pre)sheaves and bundles exist:

- For every bundle (F, f, I) let $\Gamma(F) = \{s : I \to F \mid s \text{ continuous and } f \circ s = id_I\}$, the set of all global sections of F. This defines a functor $\Gamma : \mathsf{Sp}/I \to \mathsf{PreSh}(I)$.
- Let F be a presheaf on I. For every $i \in I$ let F_i be the stalk of F at a point $i \in I$. The collection of stalks $(F_i)_{i\in I}$ is an I-indexed family of sets. Let $D(F)$ denote the disjoint union of the stalks, and let $\pi : D(F) \to I$ be the canonical

projection on I defined by $\pi(x) = i$ iff $x \in F_i$. For $s \in F(U)$ and $i \in U$, let s_i be the image of s in F_i. The map $\overline{s} : U \to D(F)$, $\overline{s}(i) = s_i$ defines a partial section of $\pi : D(F) \to I$; we impose on $D(F)$ the coarsest topology for which all such sections are continuous. $D(F) = (D(F), \pi, I)$ is a bundle. This construction defines a functor $D : \mathsf{PreSh}(I) \to \mathsf{Sp}/I$.

Theorem 4.6 (cf. [9,12]) *The functor $D : \mathsf{PreSh}(I) \to \mathsf{Sp}/I$ preserves finite limits and is left adjoint to $\Gamma : \mathsf{Sp}/I \to \mathsf{PreSh}(I)$. The functors D, Γ restrict to an equivalence of categories between $\mathsf{Sh}(I)$ and LH/I.*

$\Gamma \circ D : \mathsf{PreSh}(X) \to \mathsf{Sh}(X)$ is known as the *sheafification functor*.

Theorem 4.7 (cf. [9,12]) *The inclusion $\mathsf{Sh}(X) \to \mathsf{PreSh}(X)$ has a left adjoint, $\Gamma \circ D : \mathsf{PreSh}(X) \to \mathsf{Sh}(X)$. The sheafification functor $\Gamma \circ D$ preserves all finite limits.*

5 States, partial actions

Let InSys be a family of systems satisfying conditions (i), (ii), (iii) in Section 4, and $\Omega(\mathsf{InSys})$ be the topology on InSys consisting of all subsets InSys which are closed under t.c. subsystems. We define functors modeling states and parallel actions:

(St) $\mathsf{St} : \Omega(\mathsf{InSys})^{\mathrm{op}} \to \mathsf{Set}$ is defined as follows:
Objects: $\mathsf{St}(U) = \{(s_i)_{S_i \in U} \mid s_i \in St(S_i),$ and if $S_i \hookrightarrow S_j$ then $s_i = s_{j|X_i}\}$;
Morphisms: if $U_1 \overset{\iota}{\subseteq} U_2$, $\mathsf{St}(\iota) : \mathsf{St}(U_2) \to \mathsf{St}(U_1)$ is $\mathsf{St}(\iota)((s_i)_{S_i \in U_2}) = (s_i)_{S_i \in U_1}$.

(Pa) $\mathsf{Pa} : \Omega(\mathsf{InSys})^{\mathrm{op}} \to \mathsf{Set}$ is defined as follows:
Objects: $\mathsf{Pa}(U) = \{(f_i)_{S_i \in U} \mid f_i \in Pa(S_i),$ and if $S_i \hookrightarrow S_j$ then $f_i = f_{j|A_i}\}$;
Morphisms: if $U_1 \overset{\iota}{\subseteq} U_2$, $\mathsf{Pa}(\iota) : \mathsf{Pa}(U_2) \to \mathsf{Pa}(U_1)$ is $\mathsf{Pa}(\iota)((f_i)_{S_i \in U_2}) = (f_i)_{S_i \in U_1}$.

Example 5.1 Consider the family $\mathsf{InSys} = \{S_1, S_{12}, S_2\}$ in Example 3.5.

States. Any tuple (s_1, s_2, s_{12}), where $s_i \in St(S_i)$ for $i \in \{1, 2, 12\}$ and $s_{1|X_{12}} = s_{2|X_{12}} = s_{12}$, is an element in $\mathsf{St}(\mathsf{InSys})$. Assume first that $k \leq l$.

- Let $s_i : X_{S_i} \to M$ be such that $s(\mathsf{TrainIndex}_i) = i$ for all $i \in \{1, \ldots, l\}$, and such that $s_{1|X_{12}} = s_{2|X_{12}} = s_{12}$. Then $(s_1, s_2, s_{12}) \in \mathsf{St}(\mathsf{InSys})$.
- Let $s_1 : X_{S_1} \to M$ be defined by $s(\mathsf{TrainIndex}_i) = i$ for all $i \in \{1, \ldots, l\}$, and $s_2 : X_{S_2} \to M$ be defined by $s(\mathsf{TrainIndex}_i) = i + 1$ for all $i \in \{k, \ldots, n\}$. $s_1 \in St(S_1)$, $s_2 \in St(S_2)$, but they do not agree on the common control variables (in particular, $s_1(\mathsf{TrainIndex}_k) = k, s_2(\mathsf{TrainIndex}_k) = k + 1$). So $(s_1, s_2, s_{1|X_{S_{12}}}) \notin \mathsf{St}(\mathsf{InSys})$.

Assume now that $l < k$. Then S_{12} is the system with an empty set of control variables. Hence, $s_1 : X_{S_1} \to M$ defined by $s(\mathsf{TrainIndex}_i) = i$ for all $i \in \{1, \ldots, l\}$, and $s_2 : X_{S_2} \to M$, defined by $s(\mathsf{TrainIndex}_i) = i + 1$ for all $i \in \{k, \ldots, n\}$, agree on the common variables. Therefore $(s_1, s_2, s_{1|X_{S_{12}}}) \in \mathsf{St}(\mathsf{InSys})$.

Let $U = \{S_1, S_{12}, S_2\}$ and $U_1 = \{S_1, S_{12}\}$ be the two sets in $\Omega(\mathsf{InSys})$ which contain S_1, and let i be the inclusion between U_1 and U. Then $\mathsf{St}(i) : \mathsf{St}(U) \to \mathsf{St}(U_1)$ is defined by $St(i)(s_1, s_2, s_{12}) = \rho^U_{U_1}(s_1, s_2, s_{12}) = (s_1, s_{12})$.

Parallel Actions. Any tuple (f_1, f_2, f_{12}), where $f_i \in Pa(S_i)$ for $i \in \{1, 2, 12\}$ and $f_{1|A_{12}} = f_{2|A_{12}} = f_{12}$, is an element in $\mathsf{Pa}(\mathsf{InSys})$. In particular:

- (f_1, f_2, f_{12}) with $f_j^{-1}(1) = \{\mathsf{report_i} \mid i \in I_j\} \cup \mathsf{update}$. These are admissible parallel actions in the corresponding systems, and $f_{1|A_{12}} = f_{2|A_{12}} = f_{12}$. Then $(f_1, f_2, f_{12}) \in \mathsf{Pa}(\mathsf{InSys})$.

Tuples (f_1, f_2, f_{12}) which do not satisfy these conditions are not in $\mathsf{Pa}(\mathsf{InSys})$:

- (f_1, f_2, f_{12}) with $f_j^{-1}(1) = \{\mathsf{report_i} \mid i \in I_j\} \cup \mathsf{update} \cup \{\mathsf{move}_i \mid i \in I_j\}$ is not in $\mathsf{Pa}(\mathsf{InSys})$, because the components are not admissible parallel actions.
- (f_1, f_2, f_{12}) with $f_1^{-1}(1) = \{\mathsf{report_i} \mid i \in I_1\} \cup \mathsf{update}$ and $f_2^{-1}(1) = \{\mathsf{move}_i \mid i \in I_2\}$ is not in $\mathsf{Pa}(\mathsf{InSys})$, because the components do not agree on A_{12}.

Theorem 5.2 ([18]) *The functors* St *and* Pa *are sheaves on* InSys. *For each* $S_i \in \mathsf{InSys}$, *the stalk at* S_i *of* St *(resp.* Pa*) is in bijection with* $St(S_i)$ *(resp.* $Pa(S_i)$*). Moreover, for each* $U \in \Omega(\mathsf{InSys})$, $\mathsf{St}(U)$ *(resp.* $\mathsf{Pa}(U)$*) is in bijection with* $St(S_U)$ *(resp.* $Pa(S_U)$*), where* S_U *is the colimit of the diagram defined by* U.

Example 5.3 Let $\mathsf{InSys} = \{S_1, S_{12}, S_2\}$ as defined in Example 4.1 (with $k \leq l$):

(1) An example of an open cover for $U = \{S_1, S_2, S_{12}\}$ is $\{U_1, U_2, U_{12}\}$, where $U_1 = \{S_1, S_{12}\}, U_2 = \{S_2, S_{12}\}, U_{12} = \{S_{12}\}$. Let $(s_1, s_{12}) \in St(U_1)$ and $(t_2, t_{12}) \in St(U_2)$ be such that $\rho^{U_1}_{U_{12}}(s_1, s_{12}) = \rho^{U_2}_{U_{12}}(t_2, t_{12})$. Then $s_{12} = t_{12}$ and there is a unique element $(s_1, t_2, s_{12}) \in St(U)$ such that $\rho^{U}_{U_1}(s_1, t_2, s_{12}) = (s_1, s_{12})$ and $\rho^{U}_{U_2}(s_1, t_2, s_{12}) = (t_2, t_{12})$. Similar for Pa.

(2) The stalk of St at S_1 is the colimit of the diagram $\mathsf{St}(U) \overset{\mathsf{St}(i)}{\rightarrow} \mathsf{St}(U_1) \overset{\mathsf{St}(id)}{\rightarrow} \mathsf{St}(U_1)$ and hence in bijection with $\mathsf{St}(U_1)$. Similarly for Pa.

(3) It can be seen that $\mathsf{St}(U)$ is in bijection with $St(S)$, where S is the system in the example in Section 2.2: Let $(s_1, s_2, s_{12}) \in \mathsf{St}(U)$. Then $s : X \rightarrow M$ defined by $s(x) = s_i(x)$ iff $x \in X_i$ is well defined (due to the definition of $\mathsf{St}(U)$) and in $St(S)$. Conversely, if $s \in St(S)$, then $(s_{X_1}, s_{X_2}, s_{|X_{12}}) \in \mathsf{St}(U)$.

Also $\mathsf{Pa}(U)$ is in bijection with $Pa(S)$: If $(f_1, f_2, f_{12}) \in \mathsf{Pa}(U)$ then $f : A \rightarrow \{0, 1\}$ defined by $f(x) = f_i(x)$ iff $x \in A_i$ is well defined (due to the definition of $\mathsf{Pa}(U)$). It can also be checked that if $f_1 \models C_1$ and $f_2 \models C_2$ then $f \models C$. Thus, $f \in Pa(S)$. The converse is immediate.

Assume now that S_1, S_2, S_{12} are as in Example 3.5 but $l < k$, say $l = k - 1$. The open cover and stalk construction in (1) and (2) above are the same. However, $\mathsf{St}(U)$ is in bijection with $St(\overline{S})$, where $\overline{S}$ is the colimit of the diagram defined by U as described in Example 3.5 which in this case is different from S. In particular, $s : X \rightarrow M$ with $s(\mathsf{TrainIndex}_1) = 1, s(\mathsf{TrainIndex}_2) = 2, \ldots, s(\mathsf{TrainIndex}_{k-1}) = k-1$ and $s(\mathsf{TrainIndex}_k) = k + 1, \ldots, s(\mathsf{TrainIndex}_{n-1}) = n$ is a state of $\overline{S}$, but not of S.

6 Transitions

Let InSys be a family of systems satisfying conditions (i), (ii), (iii) in Section 4. We define a functor modeling transitions:

(Tr) $\mathsf{Tr} : \Omega(\mathsf{InSys})^{\mathrm{op}} \to \mathsf{Set}$ is defined as follows:

Objects: $\mathsf{Tr}(U) = \{(f, s, s') \mid f = (f_i)_{S_i \in U} \in \mathsf{Pa}(U), s = (s_i)_{S_i \in U} \in \mathsf{St}(U), s' = (s'_i)_{S_i \in U} \in \mathsf{St}(U), (s_i, s'_i) \in Tr_{S_i}(f_i)$, for all $S_i \in U\}$;

Morphisms: if $U_1 \overset{\iota}{\subseteq} U_2$, $\mathsf{Tr}(\iota) : \mathsf{Tr}(U_2) \to \mathsf{Tr}(U_1)$ is defined by $\mathsf{Tr}(\iota)((f, s, s')) = (\mathsf{Pa}(\iota)(f), \mathsf{St}(\iota)(s), \mathsf{St}(\iota)(s'))$,

where, for every S_i in InSys and $f_i \in Pa(S_i)$, $Tr_{S_i}(f_i)$ is the transition relation associated to f_i in S_i as explained in Section 3.

Example 6.1 Consider the family $\{S_1, S_{12}, S_2\}$ in Example 4.1. With the notation introduced in Example 4.1, let:

- $s_j(\mathsf{ActualPos}_i) = a_i$, $s_j(\mathsf{RepPos}_i) = r_i, s_j(\mathsf{Mode}_i) = m_i$, for $i \in I_j$;
- f_j be such that $f_j^{-1}(1) = \{\mathsf{report}_\mathsf{i} \mid i \in I_j\} \cup \mathsf{update}$, and
- s'_j be defined by: $s'_j(\mathsf{ActualPos}_i) = a_i, s'_j(\mathsf{RepPos}_i) = a_i, s'_j(\mathsf{Mode}_i) = m'_i$, where m'_i is computed according to the transition rules for update in Example 2.2.

Then: $f_i \in Pa(S_i), s_i, s'_i \in St(S_i), (s_i, s'_i) \in Tr(S_i)$ for $i \in \{1, 2, 12\}$, $f_{1|A_{12}} = f_{2|A_{12}} = f_{12}$ and $s_{1|X_{12}} = s_{2|X_{12}} = s_{12}$.
Hence, $((f_1, s_1, s'_1), (f_2, s_2, s'_2), (f_{12}, s_{12}, s'_{12}))$ is in $\mathsf{Tr}(\mathsf{InSys})$.

Theorem 6.2 ([18]) *The functor* $\mathsf{Tr} : \Omega(\mathsf{InSys})^{op} \to \mathsf{Set}$ *is a subsheaf of* $\mathsf{Pa}\times\mathsf{St}\times\mathsf{St}$. *Moreover:*

- *For every* $S_i \in \mathsf{InSys}$, *the stalk of* Tr *at* S_i *is in bijection with* $Tr(S_i) = \{(f, s, s') \mid (s, s') \in Tr_{S_i}(f)\}$.
- *If the transitions obey either (***Disj***) or (***Indep***), then, for every* $U \in \Omega(\mathsf{InSys})$, $\mathsf{Tr}(U)$ *is in bijection with* $Tr(S_U) = \{(f, s, s') \mid (s, s') \in Tr_{S_U}(f)\}$, *where* S_U *is the colimit of the diagram defined by* U.

Example 6.3 Consider the family $\{S_1, S_{12}, S_2\}$ in Example 4.1. Let $((f_1, s_1, s'_1), (f_2, s_2, s'_2), (f_{12}, s_{12}, s'_{12})) \in \mathsf{Tr}(U)$. Let $f : A \to \{0, 1\}$ be defined by $f(x) = f_i(x)$ iff $x \in A_i$ is well defined. Then $f \in Pa(S)$. Similarly, $s, s' : X \to M$, defined by $(s(x) = s_i(x)$ and $s'(x) = s'_i(x))$ iff $x \in X_i$ are well defined and in $St(S)$.

As shown in Example 2.5, the transitions in all systems S_1, S_2, S_{12} obey condition (**Disj**). The changes of the components of parallel actions are not contradictory and affect only the variables the actions depend upon. Thus, (s, s') is in the transition induced (according to rule (**Disj**)) by f. Hence, $(s, s') \in Tr_S(f)$. The converse is an immediate consequence of the fact that, as showed in Example 3.2, S_1, S_2, S_{12} are transition-connected subsystems of S.

7 Behavior in time

In [6], the behavior of a given system S in time is modeled by a functor $F : \mathcal{T}^{op} \to \mathsf{Set}$, where $\mathcal{T}$ is the basis for the topology on $\mathbb{N}$ consisting of all the sets $\{0, 1, \ldots, n\}, n \in \mathbb{N}$. Intuitively, for every $T \in \mathcal{T}$, $F(T)$ represents the succession of the states of the systems "observed" during the interval of time T. We analyze various alternative possibilities of modeling behavior.

7.1 Behavior as successions of states and actions

Since we are interested in actions as well as states, we present a different description of behavior. Let $\mathcal{T}$ consist of $\mathbb{N}$ together with all sets $\{0, 1, \ldots, n\}, n \in \mathbb{N}$. The behavior in an interval $T \in \mathcal{T}$ of a complex system obtained by interconnecting a family InSys (satisfying conditions (i)–(iii) in Section 4) is modeled by all successions of pairs (state, action) of the component subsystems that can be observed during T, i.e. by the functor $\mathsf{B}_T : \Omega(\mathsf{InSys})^{\mathrm{op}} \to \mathsf{Set}$ defined as follows:

Objects: for $U \in \Omega(\mathsf{InSys})$, $\mathsf{B}_T(U) = \{h : T \to \mathsf{St}(U) \times \mathsf{Pa}(U) \mid K(h, T)\}$,

Morphisms: for $U_1 \overset{\iota}{\subseteq} U_2$ by $\mathsf{B}_T(\iota) : \mathsf{B}_T(U_2) \to \mathsf{B}_T(U_1)$, where if $h \in \mathsf{B}_T(U_2)$,

$$\mathsf{B}_T(\iota)(h) = (\mathsf{St}(\iota) \times \mathsf{Pa}(\iota)) \circ h : T \xrightarrow{h} \mathsf{St}(U_2) \times \mathsf{Pa}(U_2) \xrightarrow{\mathsf{St}(\iota) \times \mathsf{Pa}(\iota)} \mathsf{St}(U_1) \times \mathsf{Pa}(U_1).$$

Here $K(h, T)$ expresses the fact that for every n, if $n, n+1 \in T$ and $h(n) = (s, f)$, $h(n+1) = (s', f')$ then $(f, s, s') \in \mathsf{Tr}(U)$.

Example 7.1 We illustrate the definition above. Let $T = \mathbb{N}$, and let $U = \{S_1, S_2, S_{12}\}$ as in Example 4.1. We represent an element h in $\mathsf{B}_T(\mathsf{InSys})$ as a table (first row: arguments i of h, second row: the value $h(i)$, i.e. a pair of tuples):

i	$h(i)$																	
	$\mathsf{St}(U)$									$\mathsf{Pa}(U)$								
	$\mathsf{St}(S_1)$			$\mathsf{St}(S_{12})$			$\mathsf{St}(S_2)$			$\mathsf{Pa}(S_1)$			$\mathsf{Pa}(S_{12})$			$\mathsf{Pa}(S_2)$		
	$(i \in I_1)$			$(i \in I_{12})$			$(i \in I_2)$			$(i \in I_1)$			$(i \in I_{12})$			$(i \in I_2)$		
	ActPos_i	RepPos_i	Mode_i	(restr.)			ActPos_i	RepPos_i	Mode_i	rep_i	upd	move_i	(restr.)			rep_i	upd	move_i
0	a_i	r_i	m_i	a_i	r_i	m_i	a_i	r_i	m_i	1	1	0	1	1	0	1	1	0
1	a_i	a_i	m'_i	a_i	a_i	m'_i	a_i	a_i	m'_i	0	0	1	0	0	1	0	0	1
2	a'_i	a_i	m'_i	a'_i	a_i	m'_i	a'_i	a_i	m'_i	1	1	0	1	1	0	1	1	0
3	a'_i	a'_i	m''_i	a'_i	a'_i	m''_i	a'_i	a'_i	m''_i	1	1	0	1	1	0	1	1	0
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...

Theorem 7.2 ([18]) *Let $B_T(S) = \{h : T \to St(S) \times Pa(S) \mid K_S(h, T)\}$, where $K_S(h, T)$ expresses the fact that for every n, if $n, n+1 \in T$ and $h(n) = (s, f)$, $h(n+1) = (s', f')$ then $(s, s') \in Tr_S(f)$. Then:*

- *For every $T \in \mathcal{T}$, $\mathsf{B}_T : \Omega(\mathsf{InSys})^{op} \to \mathsf{Set}$ is a sheaf.*
- *For every $S_i \in \mathsf{InSys}$, the stalk at S_i is in bijection with $B_T(S_i)$.*

- *If the transitions obey (***Disj***) or (***Indep***), then, for every $U \in \Omega(\mathsf{InSys})$, $\mathsf{B}_T(U)$ is in bijection with $B_T(S_U)$, where S_U is the colimit of the diagram defined by U.*

7.2 Behavior: Admissible Parallel Actions as Words

If we ignore the states, the behavior of any system S can be expressed by a subset L_S of the free monoid $Pa(S)^*$ over the set of possible actions of S, where:

$$L_S = \{f_1 \dots f_n \mid \exists h : \{0,\dots,n\} \to St(S) \times Pa(S), \exists s_i \in St(S), \text{ s.t.} \\ \forall i \in \{0,\dots,n-1\}, (s_i, s_{i+1}) \in Tr_S(f_i)\} \subseteq Pa(S)^*.$$

Consider the family $\{Pa(S_i)^* \mid S_i \in \mathsf{InSys}\}$. If $S_i, S_j \in \mathsf{InSys}$ and $S_i \hookrightarrow S_j$, let $\rho_{S_i}^{S_j} : Pa(S_j) \to Pa(S_i)$ be the restriction to S_i. The restriction extends to a homomorphism of monoids, $p_i^j : Pa(S_j)^* \to Pa(S_i)^*$. If there is no risk of confusion, in what follows we will abbreviate $p_i^j(w_j)$ by $w_{j|S_i}$. Let $M(\mathsf{InSys})$ be defined by:

$$M(\mathsf{InSys}) = \{(w_i)_{S_i \in \mathsf{InSys}} \mid w_i \in Pa(S_i)^* \text{ and } \forall S_i \hookrightarrow S_j, p_i^j(w_j) = w_i\}.$$

It can be seen that $M(\mathsf{InSys})$ is the limit of the diagram $\{Pa(S_i)^* \mid S_i \in \mathsf{InSys}\}$ (with the morphisms p_i^j for every $S_i \hookrightarrow S_j$).

Theorem 7.3 *Let $M : \Omega(\mathsf{InSys})^{op} \to \mathsf{Sets}$ be defined as follows:*

Objects: $M(U) = \{(w_i)_{S_i \in V} \mid w_i \in Pa(S_i)^*, w_{i|S_j} = w_j$ *for every* $S_j \hookrightarrow S_i\}$,

Morphisms: *if* $\iota : U_1 \subseteq U_2$, $M(\iota) : M(U_2) \to M(U_1)$ *is defined for every* $(w_i)_{S_i \in U_2}$ *by* $M(\iota)((w_i)_{S_i \in U_2}) = (w_i)_{S_i \in U_1}$.

Then M is a sheaf of monoids. $M(V)$ is the limit of the diagram $\{Pa(S_i)^* \mid S_i \in V\}$ (with morphisms $p_i^j : Pa(S_j)^* \to Pa(S_i)^*$ whenever $S_i \hookrightarrow S_j$).

Proof: Let $U \in \Omega(\mathsf{InSys})$ and $\{U_k \mid k \in K\}$ be a cover for U. Let $\{w_k\}_{k \in K}$ be a family of elements, such that for every $k \in K$, $w_k = (w_k^i)_{S_i \in U_k}$ and for every $k_1, k_2 \in K$, if $S_i \in U_{k_1} \cap U_{k_2}$ then $w_{k_1}^i = w_{k_2}^i$.

We define $w = (w_i)_{Si \in U}$ as follows: for every $S_i \in U$, $S_i \in U_k$ for some k. Then w_i is defined to be w_k^i. Note that w_i is well defined because of the compatibility of the family $\{w_k\}_{k \in K}$, and $p_{U_k}^U(w) = w_k$ for every $k \in K$. The uniqueness of w follows from the fact that for every $w' = (w_i')_{S_i \in U}$ such that $p_{U_k}^U(w') = w_k$ for every $k \in K$ we have $w_i' = w_i^k$ for every $S_i \in U_k$.

The fact that $M(V)$ is the limit of the diagram $\{Pa(S_i)^* \mid S_i \in V\}$ (with the corresponding morphisms) can be checked without difficulty. □

Remark: Let S be the colimit of the diagram defined by U. The connection between $Pa(S)^*$ and $M(U)$ is rather loose: Let $p : Pa(S)^* \to M(U)$ be defined by $p(f_1 \dots f_n) = ((f_1 \dots f_n)_{|S_i})_{S_i \in U} \in M(U)$. If we identify the empty action with the empty word ϵ, p may not be injective as can be seen from the following example:

Example 7.4 Let S_1 and S_2 be as defined in Example 4.1, where trains are indexed by $I_1 = \{k_1, \dots, n\}$ and $I_2 = \{1, \dots, k_2\}$ and $k_2 < k_1$, with the difference that update is omitted as in Example 2.6. Let $\mathsf{InSys} = \{S_1, S_2, \emptyset\}$. Let $w_1 = f_1 f_2$ and $w_2 = f_2 f_1$, where $f_1^{-1}(1) = \{\mathsf{report}_i \mid i \in I_1\}$ and $f_2^{-1}(1) = \{\mathsf{move}_j \mid j \in I_2\}$. Note

that $f_{1|A_1}^{-1}(1) = \{\mathsf{report}_i \mid i \in I_1\}$, $f_{2|A_1}^{-1}(1) = f_{1|A_2}^{-1}(1) = \emptyset$, and $f_{2|A_2}^{-1}(1) = \{\mathsf{move}_j \mid j \in I_2\}$. Thus, $p(w_1) = ((f_1 f_2)_{|S_1}, (f_1 f_2)_{|S_2}, (f_1 f_2)_{|\emptyset}) = ((f_{1|A_1} f_{2|A_1}), (f_{1|A_2} f_{2|A_2}), \epsilon) = (f_1\epsilon, \epsilon f_2, \epsilon) = (\epsilon f_1, f_2\epsilon, \epsilon) = ((f_{2|A_1} f_{1|A_1}), (f_{2|A_2} f_{1|A_2}), \epsilon) = p(w_2)$, but $w_1 \neq w_2$.

The next example shows that $p : Pa(S)^* \to M(U)$ is not necessarily onto: There may exist compatible families (even if we only consider singleton parallel actions) of sequences of actions that cannot be "glued together" to a sequence of actions on $Pa(S)$. A similar result appears in [13] (in that case, no parallelism is allowed).

Example 7.5 Let S_1, S_2, S_3 be three systems all having the same language, the same constraints on variables and the same model for the variables, such that

$$A_{S_1} = \{a, b, d\}, \quad A_{S_2} = \{b, c, e\}, \quad A_{S_3} = \{a, c, f\}$$
$$C_{S_1} = \{a \wedge b = 0\} \quad C_{S_2} = \{b \wedge c = 0\} \quad C_{S_3} = \{a \wedge c = 0\}$$

Let S be the system obtained by interconnecting S_1, S_2, S_3. Then $A_S = \{a, b, c, d, e, f\}, C_S = \{a \wedge b = 0, b \wedge c = 0, a \wedge c = 0\}$. Consider $w_1 = ab \in Pa(S_1)^*$, $w_2 = bc \in Pa(S_2)^*$, $w_3 = ca \in Pa(S_3)^*$. It is easy to see that $p_{12}^1(w_1) = p_{12}^2(w_2) = b$, $p_{23}^2(w_2) = p_{23}^3(w_3) = c$, $p_{13}^1(w_1) = p_{13}^3(w_3) = a$, but there is no $w \in Pa(S)^*$ such that $w_{|S_i} = w_i, i = 1, 2, 3$.

We investigate therefore other ways of modelling behavior for which tighter links between local and global behavior exist.

7.3 Behavior: Partially Commutative Monoids

In what follows we assume that the constraints on actions are all of the form $a_i \wedge a_j = 0$ (they state which actions cannot be performed in parallel).

Definition 7.6 Let S be a system with the property that the constraints on actions are all of the form $a_i \wedge a_j = 0$. The *dependence graph* of S is the graph (A_S, D_S) having as set of vertices A_S, and where D_S is defined by $(a_1, a_2) \in D_S$ if $a_1 = a_2$ or $a_1 \wedge a_2 = 0 \in C_S$.

For every system S with dependence graph (A_S, D_S) we denote by $M(S) = M(A_S, D_S)$ the free partially commutative monoid defined by (A_S, D_S), i.e. the quotient of A_S^* by the congruence relation generated by $a_1 a_2 = a_2 a_1$ for every $(a_1, a_2) \in (A_S \times A_S) \backslash D_S$. For basic properties of (free) partially commutative monoids we refer e.g. to [3], pp.9-29 and 67-79.

For every $S_i \in \mathsf{InSys} \backslash \emptyset$, let $M(S_i) = A_{S_i}^*/\theta_i$ (where θ_i is the congruence defined as explained above from $(A_{S_i} \times A_{S_i}) \backslash D_{S_i}$) be the partially commutative monoid associated with the dependence graph of S_i. Let S be the colimit of the diagram defined by InSys. Then $A_S = \bigcup_{S_i \in \mathsf{InSys}} A_i$ and $D_S = \bigcup_{S_i \in \mathsf{InSys}} D_i$. Hence, for every $S_i \in \mathsf{InSys}$ there is a canonical projection $p_i : M(S) \to M(S_i)$ which is onto. Let $ker(p_i)$ be the kernel of p_i. Then $M(S_i) \simeq M(S)/ker(p_i)$.

If $S_i \hookrightarrow S_j$, then we denote the canonical projection by $p_i^j : M(S_j) \to M(S_i)$, and if $S_i, S_j \in \mathcal{S}$, then $p_{ij}^j : M(S_j) \to M(S_i \cap S_j)$, and $p_{ij}^i : M(S_i) \to M(S_i \cap S_j)$ are

the canonical mappings. Note that all homomorphisms $p^i_j : M(S_i) \to M(S_j)$ and $p^i_{ij} : M(S_i) \to M(S_i \cap S_j)$ are onto. We know that for all $S_j \hookrightarrow S_i$, $p^i_j \circ p_i = p_j$.

Example 7.7 Consider a family of two systems of trains S_1, S_2 over disjoint sets I_1, I_2 of trains as in Example 4.1 but with $l < k$. We simplify the description by replacing all actions that need to be executed at the same time with one action. The system S_i ($i \in \{1,2\}$) obtained this way has two actions update_i and move_i The constraints are $C_i = \{\mathsf{update}_i \wedge \mathsf{move}_i = 0\}$. Thus $\theta_i = id$, so $M(S_i) = A^*_{S_i}$.
Let S be the system obtained by the interconnection of S_1 and S_2.
$A_S = \{\mathsf{update}_1, \mathsf{update}_2, \mathsf{move}_1, \mathsf{move}_2\}$ and $C_S = C_1 \cup C_2$.

$$D_S = \{(\mathsf{update}_1, \mathsf{update}_1), (\mathsf{update}_2, \mathsf{update}_2), (\mathsf{move}_2, \mathsf{move}_2), (\mathsf{move}_1, \mathsf{move}_1), (\mathsf{update}_1, \mathsf{move}_1), (\mathsf{move}_1, \mathsf{update}_1), (\mathsf{update}_2, \mathsf{move}_2), (\mathsf{move}_2, \mathsf{update}_2)\}$$

$$(A_S \times A_S)\backslash D_S = \{(\mathsf{update}_1, \mathsf{update}_2), (\mathsf{update}_2, \mathsf{update}_1), (\mathsf{update}_1, \mathsf{move}_2), (\mathsf{move}_2, \mathsf{update}_1), (\mathsf{move}_1, \mathsf{update}_2), (\mathsf{update}_2, \mathsf{move}_1), (\mathsf{move}_1, \mathsf{move}_2), (\mathsf{move}_2, \mathsf{move}_1)\}$$

Thus, $M(S) = A^*_S/\theta$, where θ is the congruence generated by $(A_S \times A_S)\backslash D_S$.

Applying a method due to [2] (cf. Appendix A) – where sheaves of algebras are constructed, whose stalks are quotients of a given algebra – we deduce for partially commutative monoids results similar to those given in [13] for monoids. The results are similar to results on Petri Nets and Mazurkiewicz traces presented in [3].

Let (F, f, InSys) be defined by $F = \coprod_{S_i \in \mathsf{InSys}} M(S_i)$, and $f : F \to \mathsf{InSys}$ be the natural projection. Assume that a subbasis for the topology on F is $\mathcal{SB} = \{[m](U) \mid U \in \Omega(\mathsf{InSys}), m \in M(S)\}$, where $[m](U) = \{p_i(m) \mid i \in U\}$.

We first show that $\Omega(\mathsf{InSys})$ has the property that for every $m_1, m_2 \in M(S)$, if $p_i(m_1) = p_i(m_2)$ then there exists an open neighborhood U of S_i in $\Omega(\mathsf{InSys})$ such that for every $S_j \in U$, $p_j(m_1) = p_j(m_2)$ (i.e. it is an S-topology).

Lemma 7.8 $\Omega(\mathsf{InSys})$ *is a S-topology (cf. Definition A.2).*

Proof: We show that for every $m_1, m_2 \in M(S)$, if $p_i(m_1) = p_i(m_2)$ then there exists an open neighborhood U of S_i in $\Omega(\mathsf{InSys})$ s.t. for every $S_j \in U$, $p_j(m_1) = p_j(m_2)$. Let $m_1, m_2 \in M(S)$ with $p_i(m_1) = p_i(m_2)$. Let $U = \downarrow S_i = \{S_j \in \mathsf{InSys} \mid S_j \hookrightarrow S_i\}$. $U \in \Omega(\mathsf{InSys})$ and $p_j(m_1) = p^i_j(p_i(m_1)) = p^i_j(p_i(m_2)) = p_j(m_2)$ for every $S_j \in U$. □

Let $\alpha : M(S) \to \Gamma(I, F_A)$ be defined by $\alpha(m) = ([m]_{\theta_i})_{i \in I}$. Since $\Omega(\mathsf{InSys})$ is an S-topology, by Theorem A.1 and Corollary A.3 in Appendix A we have:

(1) (F, f, InSys) is a sheaf of algebras,
(2) The stalk at $S_i \in \mathsf{InSys}$ is isomorphic to $M(S_i)$,
(3) In $M(S) \xrightarrow{\alpha} \Gamma(\mathsf{InSys}, F) \leq \prod_{S_i \in \mathsf{InSys}} M(S_i) \xrightarrow{\pi_i} M(S_i)$
  (3.i) $\pi_i \circ \alpha$ is an epimorphism,
  (3.ii) $M(S)$ is a subdirect product of $\{M(S_i)\}_{S_i \in \mathsf{InSys}}$ iff α is a monomorphism.

Lemma 7.9 *Let* $s : \mathsf{InSys} \to \coprod_{S_i \in \mathsf{InSys}} M(S_i)$ *be such that* $s(S_i) \in M(S_i)$ *for every*

$S_i \in \mathsf{InSys}$. *Let* $m \in M(S)$ *and* $U \in \Omega(\mathsf{InSys})$. *Then* $S_i \in s^{-1}([m](U))$ *if and only if* $S_i \in U$ *and* $s(S_i) = p_i(m)$.

Proof: Note that $s^{-1}([m](U)) = \{S_i \in \mathsf{InSys} \mid s(S_i) \in [m](U)\} = \{S_i \in \mathsf{InSys} \mid s(S_i) \in \{p_j(m) \mid S_j \in U\}\}$. We first prove the direct implication. Assume that $S_i \in s^{-1}([m](U))$. Then $s(S_i) = p_j(m)$ for some $S_j \in U$. Since $f \circ s(S_i) = S_i$, it follows that $S_i = f(s(S_i)) = f(p_j(m)) = S_j$, hence $S_i \in U$ and $s(S_i) = p_i(m)$. To prove the converse, assume that $S_i \in U$ and $s(S_i) = p_i(m)$. Then $s(S_i) \in \{p_j(m) \mid S_j \in U\}$, hence $S_i \in s^{-1}([m](U))$. □

Lemma 7.10 *Let* τ *be the topology on* $F = \coprod_{S_i \in \mathsf{InSys}} M(S_i)$ *generated by* $\mathcal{SB} = \{[m](U) \mid U \in \Omega(\mathsf{InSys}), m \in M(S)\}$ *as a subbasis. Then* $s : \mathsf{InSys} \to \coprod_{S_i \in \mathsf{InSys}} M(S_i)$ *such that for every* $S_i \in \mathsf{InSys}$, $s(S_i) \in M(S_i)$ *is continuous if and only if for every* $S_i, S_j \in \mathsf{InSys}$ *such that* $S_j \hookrightarrow S_i$, $p_j^i(s(S_i)) = s(S_j)$.

Proof: Since $\mathcal{SB}$ is a subbasis for the topology on $F = \coprod_{S_i \in \mathsf{InSys}} M(S_i)$, $s : \mathsf{InSys} \to \coprod_{S_i \in \mathsf{InSys}} M(S_i)$ is continuous iff for every $[m](U) \in \mathcal{SB}$, $s^{-1}([m](U)) \in \Omega(\mathsf{InSys})$. We first prove the direct implication. Assume that $s : \mathsf{InSys} \to \coprod_{S_i \in \mathsf{InSys}} M(S_i)$ is continuous. Let $S_i, S_j \in \mathsf{InSys}$ be such that $S_j \hookrightarrow S_i$. We prove that $p_j^i(s(S_i)) = s(S_j)$. Let $U = \ \downarrow S_i \in \Omega(\mathsf{InSys})$ and let $m \in M(S)$ be such that $p_i(m) = s(S_i)$ (the existence of m is ensured by the fact that $p_i : M(S) \to M(S_i)$ is onto). From the continuity of s we know that $s^{-1}([m](\downarrow S_i)) \in \Omega(\mathsf{InSys})$. Obviously, $S_i \in s^{-1}([m](\downarrow S_i))$. Therefore, since $S_j \hookrightarrow S_i$, $S_j \in s^{-1}([m](\downarrow S_i))$, hence, by Lemma 7.9, $s(S_j) = p_j(m)$. Therefore, $s(S_j) = p_j(m) = p_j^i(p_i(m)) = p_j^i(s(S_i))$.

Conversely, assume that for every $S_i, S_j \in \mathsf{InSys}$ such that $S_j \hookrightarrow S_i$ it holds that $p_j^i(s(S_i)) = s(S_j)$. We prove that s is continuous. Let $[m](U) \in \mathcal{SB}$, where $m \in M(S)$ and $U \in \Omega(\mathsf{InSys})$. We prove that $s^{-1}([m](U)) \in \Omega(\mathsf{InSys})$. Let $S_i \in s^{-1}([m](U))$. Then $S_i \in U$ and $s(S_i) = p_i(m)$. Let $S_j \hookrightarrow S_i$. Then $S_j \in U$ and by the hypothesis, $s(S_j) = p_j^i(s(S_i)) = p_j^i(p_i(m)) = p_j(m)$. Thus, $S_j \in s^{-1}([m](U))$. Therefore $s^{-1}([m](U)) \in \Omega(\mathsf{InSys})$. □

Lemma 7.11 *The set* $\Gamma(\mathsf{InSys}, F)$ *of global sections of* F *has the form* $\Gamma(\mathsf{InSys}, F) = \{(m_i)_{S_i \in \mathsf{InSys}} \mid m_i \in M(S_i)$ *and* $\forall S_j \hookrightarrow S_i \in \mathsf{InSys}, p_j^i(m_i) = m_j\}$.

Proof: We know that $\Gamma(\mathsf{InSys}, F) = \{s : \mathsf{InSys} \to \coprod_{S_i \in \mathsf{InSys}} M(S_i) \mid s$ continuous and $s(S_i) \in M(S_i), \forall S_i \in \mathsf{InSys}\}$. (The elements of $\Gamma(\mathsf{InSys}, F)$ are tuples $(s(S_i))_{S_i \in \mathsf{InSys}}$.) Let first $s \in \Gamma(\mathsf{InSys}, F)$. Then s is continuous and, by Lemma 7.10, for all $S_i, S_j \in \mathsf{InSys}$ with $S_j \hookrightarrow S_i$, $p_j^i(s(S_i)) = s(S_j)$. Conversely, let $(m_i)_{S_i \in \mathsf{InSys}}$ be such that for every $S_i, S_j \in \mathsf{InSys}, m_i \in M(S_i)$ if $S_j \hookrightarrow S_i$ then $p_j^i(m_i) = m_j$. Let $s : \mathsf{InSys} \to \coprod_{S_i \in \mathsf{InSys}} M(S_i)$ be defined by $s(S_i) = m_i$ for every $S_i \in \mathsf{InSys}$. Then, whenever $S_j \hookrightarrow S_i \in \mathsf{InSys}$, $p_j^i(s(S_i)) = s(S_j)$ and, by Lemma 7.10, s is continuous. □

Theorem 7.12 *Let* (F, f, InSys) *be defined as above. Then* (F, f, InSys) *is a sheaf space of algebras. The stalk at* $S_i \in \mathsf{InSys}$ *is isomorphic to* $M(S_i)$*; the set of global sections is* $\Gamma(\mathsf{InSys}, F) = \{(m_i)_{S_i \in \mathsf{InSys}} \mid m_i \in M(S_i),$ *and* $\forall S_i \hookrightarrow S_j, p_i^j(m_j) = m_i\}$. *Additionally the following hold:*

(1) If InSys *is finite, then*

(i) $M(S) \hookrightarrow \Gamma(\mathsf{InSys}, F) \leq \prod_{S_i \in \mathsf{InSys}} M(S_i) \stackrel{\pi_i}{\to} M(S_i)$ *is a subdirect product.*

(ii) The embedding $M(S) \hookrightarrow \Gamma(\mathsf{InSys}, F)$ *is an isomorphism iff every chordless cycle in the dependence graph* G_S *of* S *is a cycle in a subgraph* G_{S_i} *for some* $S_i \in \mathsf{InSys}$.

(2) If InSys *is infinite, and if for every* $a \in A_S$ *there are at most finitely many* $S_i \in \mathsf{InSys}$ *with* $a \in A_i$, *then there is an injective morphism* $M(S) \to \bigoplus_{S_i} M(S_i)$, *where* $\bigoplus_{S_i} M(S_i) = \{(w_i)_{i \in I} \mid w_i \in M(S_i), w_i = \varepsilon \text{ a.e.}\}$ *is the weak product of the family* $\{M(S_i)\}_{S_i \in \mathsf{InSys}}$.

Proof: The form of $\Gamma(\mathsf{InSys}, F)$ follows from Lemma 7.11. (1)(i) and (2) are a consequence of Theorem B.1 and the subsequent comments in Appendix B. (1)(ii) is a direct consequence of Theorem 3.3.2 in [3]. □

Example 7.13 First consider the family of systems in Example 7.7. The dependency graph of S, $G_S = (A_S, D_S)$ contains the following non-trivial chordless cycles:

(i) $(\mathsf{update}_1, \mathsf{move}_1, \mathsf{update}_1)$ and $(\mathsf{move}_1, \mathsf{update}_1, \mathsf{move}_1)$ (all cycles in G_{S_1})

(ii) $(\mathsf{update}_2, \mathsf{move}_2, \mathsf{update}_2)$ and $(\mathsf{move}_2, \mathsf{update}_2, \mathsf{move}_2)$ (all cycles in G_{S_2}).

Thus, in this case the embedding in Theorem 7.12(1)(ii) is an isomorphism.

Example 7.14 Consider the systems in Example 7.5. The dependency graphs are:

- $G_{S_1} = (A_1, D_1)$, with $D_1 = \{(a,a), (b,b), (d,d), (a,b), (b,a)\}$,
- $G_{S_2} = (A_2, D_2)$, with $D_2 = \{(b,b), (c,c), (e,e), (b,c), (c,b)\}$,
- $G_{S_3} = (A_3, D_3)$, with $D_3 = \{(a,a), (c,c), (f,f), (a,c), (c,a)\}$).

$G_S = (A_1 \cup A_2 \cup A_3, D_1 \cup D_2 \cup D_3)$ contains the chordless cycle (a, b, c, a) which is not contained in any of the subgraphs $G_{S_i}, i \in \{1, 2, 3\}$. Thus, the embedding in Theorem 7.12(1)(ii) is not an isomorphism.

8 Other concepts and their sheaf semantics

Time. One possibility for expressing time internally in the category $\mathsf{Sh}(\mathsf{InSys})$ is to model time by the sheafification $\mathbb{N}$ of the constant presheaf $\mathcal{N} : \Omega(\mathsf{InSys})^{\mathrm{op}} \to \mathsf{Set}$ (defined for every U by $\mathcal{N}(U) = \mathbb{N}$), which can be constructed as follows:

- Let $\mathcal{N}^+ : \Omega(\mathsf{InSys})^{op} \to \mathsf{Sets}$, defined by $\mathcal{N}^+(U) = \mathbb{N}$ if $U \neq \emptyset$ and $\mathcal{N}^+(\emptyset) = 1$ (for the empty cover there is exactly one matching family; the empty one).
- Let $\mathbb{N} = (\mathcal{N}^+)^+ : \Omega(\mathsf{InSys})^{op} \to \mathsf{Sets}$. An element of $(\mathcal{N}^+)^+(U)$ is an equivalence class of sets of elements $i_j \in \mathcal{N}(U_j)$ for some open covering $\{U_j \mid j \in J\}$ of U, which match $(i_{j_1} = i_{j_2})$ whenever the overlap $U_{j_1} \cap U_{j_2}$ is nonempty. Thus, these elements "glue" together to give a function $i : U \to \mathbb{N}$, with the property that every point of U has some open neighborhood on which the function is constant.

For every $U \in \Omega(\mathsf{InSys})$, $\mathbb{N}(U) = \{i : U \to \mathbb{N} \mid f \text{ locally constant}^{4}\}$. There exist $\mathsf{Sh}(\mathsf{InSys})$-arrows $1 \xrightarrow{0} \mathbb{N} \xrightarrow{s} \mathbb{N}$; the sheaf $\mathbb{N}$ is the natural number object in $\mathsf{Sh}(\mathsf{InSys})$.

Other constructions. Various other sheaves and natural transformations can be defined by using standard categorical constructions in $\mathsf{Sh}(\mathsf{InSys})$. We can e.g. define a natural transformation $\mathsf{B}_{\mathbb{N}} \times \mathbb{N} \xrightarrow{\mathsf{a}} \mathsf{St} \times \mathsf{Pa}$ whose components $\mathsf{B}_{\mathbb{N}}(U) \times \mathbb{N}(U) \xrightarrow{\mathsf{a}_U} \mathsf{St}(U) \times \mathsf{Pa}(U)$ are defined by $\mathsf{a}_U(h, (n_i)_{S_i \in U}) = ((s_i^i)_{S_i \in U}, (f_i^i)_{S_i \in U})$, for every $U \in \Omega(\mathsf{InSys})$, where for every $S_i \in U$, $h(n_i) = ((s_j^i)_{S_j \in U}, (f_j^i)_{S_j \in U})$. [5]

Theorem 8.1 ([18]) *For every $S_i \in \mathsf{InSys}$, $\mathsf{Stalk}_{S_i}(\mathsf{a})$ is (up to isomorphism) the map $B_T(S_i) \times \mathbb{N} \xrightarrow{\mathsf{a}_{S_i}} St(S_i) \times Pa(S_i)$, defined by $\mathsf{a}_{S_i}(h, n) = h(n)$.*

9 Geometric logic and properties of systems

We provide interpretations for properties of systems (i.e. statements about states, actions, behavior) both concretely (in the category of sets) and in a category of sheaves, and establish links between the set-theoretical (both for individual systems and for their interconnections) and the sheaf-theoretical interpretation. These links are then used to prove preservation of truth when interconnecting systems.

9.1 Many-sorted first order languages and their interpretation in $\mathsf{Sh}(I)$

Let $\mathcal{L}$ be a many-sorted first-order language consisting of a collection of sorts and collections of function and relation symbols. Terms and atomic formulae from $\mathcal{L}$ are defined in the standard way; compound formulae are constructed by using the connectives $\vee, \wedge, \Rightarrow, \neg$ and the quantifiers $\exists, \forall$, for every sort X. An *interpretation M of $\mathcal{L}$ in* $\mathsf{Sh}(I)$ is constructed by associating:

- a sheaf X^M on I to every sort X,
- a subsheaf $R^M \subseteq X_1^M \times \cdots \times X_n^M$ to every relation symbol R of arity $X_1 \times \cdots \times X_n$,
- an arrow $f^M : X_1^M \times \cdots \times X_n^M \to Y^M$ in $\mathsf{Sh}(I)$ to every function symbol f with arity $X_1 \times \cdots \times X_n \to Y$.

Each term $t(x_1, \ldots, x_n)$ of sort Y is (inductively) interpreted as an arrow $t^M : X_1^M \times \cdots \times X_n^M \to Y^M$; and every formula $\phi(x_1, \ldots, x_n)$ with free variables $FV(\phi) \subseteq \{x_1, \ldots, x_n\}$, where x_i is of sort X_i, gives rise to a subsheaf $\{(x_1, \ldots, x_n) \mid \phi(x_1, \ldots, x_n)\}^M \subseteq X_1^M \times \cdots \times X_n^M$. For details we refer to [12], Ch. X.

Definition 9.1 A *geometric formula* is a formula built from atomic formulae by using only the connectives $\vee$ and $\wedge$ and the quantifier $\exists$. A *geometric axiom* is a formula of the form $(\forall x_1, \ldots, x_n)(\phi \Rightarrow \psi)$ where ϕ and ψ are geometric formulae.

---

[4] $f{:}U \to X$ is locally constant if $\forall x \in U$ there is an open neighborhood $U_1 \subseteq U$ of x on which f is constant. This means that 'local clocks' of the systems in U synchronize for systems sharing common subsystems.

[5] The map a_U has as arguments a behaviour along $\mathbb{N}$ of the family of systems in U, $h \in \mathsf{B}_{\mathbb{N}}(U)$, and a tuple consisting of 'local clocks' of the systems in U which synchronize on systems sharing common subsystems. a_U returns the pair $((s_i^i)_{S_i \in U}, (f_i^i)_{S_i \in U})$ where (s_i^i, f_i^i) is the pair state/parallel action in the behavior corresponding to the system S_i in U, at the time point indicated by the local clock n_i of S_i.

Let $\mathbb{T}$ be a theory in the language $\mathcal{L}$. A variable in a geometric formula is called $\mathbb{T}$-*provably unique* if its value in every model of $\mathbb{T}$ is uniquely determined by the values of the remaining free variables.

A *cartesian formula w.r.t.* $\mathbb{T}$ is a formula constructed from atomic formulae using only the connective $\wedge$ and the quantifier $\exists$ over $\mathbb{T}$-provably unique variables. A *cartesian axiom w.r.t.* $\mathbb{T}$ is a formula of the form $(\forall x)(\phi(x) \Rightarrow \psi(x))$ where ϕ and ψ are cartesian formulae w.r.t. $\mathbb{T}$. A *cartesian theory* is a theory whose axioms can be ordered such that each is cartesian w.r.t. the preceding ones.

A geometric axiom $(\forall x_1 \dots x_n)(\phi \Rightarrow \psi)$ is *satisfied in an interpretation* M *in* $\mathsf{Sh}(I)$ if $\{(x_1, \dots, x_n)|\phi\}^M$ is a subobject of $\{(x_1, \dots, x_n)|\psi\}^M$ in $\mathsf{Sh}(I)$.

9.2 Stalk functors, global section functors; preservation of truth

Stalk functors. For every $S_i \in \mathsf{InSys}$ let $f_i : \{*\} \to \mathsf{InSys}$ be defined by $f_i(*) = S_i$. The inverse image functor corresponding to f_i, the stalk functor $\mathsf{Stalk}_{S_i} = f_i^* : \mathsf{Sh}(\mathsf{InSys}) \to \mathsf{Set}$, associates to every sheaf $F \in \mathsf{Sh}(\mathsf{InSys})$ the stalk at S_i, F_{S_i}. For all $S_i \in \mathsf{InSys}$, f_i^* preserves the validity of geometric axioms. The stalk functors f_i^* are collectively faithful, so they reflect the validity of geometric axioms.

Global section functor. Consider the unique map $g : \mathsf{InSys} \to \{*\}$. The direct image functor, $g_* : \mathsf{Sh}(\mathsf{InSys}) \to \mathsf{Set}$, is the global section functor $g_*(F) = F(\mathsf{InSys})$ for every $F \in \mathsf{Sh}(\mathsf{InSys})$. Thus, the global section functor preserves the interpretation of every cartesian axiom.

9.3 A geometric logic for reasoning about complex systems

Let $\mathcal{L}$ be a fixed many-sorted language including at least sorts like st(ate), pa(rallel-action), b(ehavior), t(ime); constants like $s_0 : \mathsf{st}$ (initial state), $0 : \mathsf{t}$ (initial moment of time); function symbols like $\mathsf{appl} : \mathsf{b} \times \mathsf{t} \to \mathsf{st} \times \mathsf{pa}$, $\mathsf{p}_1 : \mathsf{st} \times \mathsf{pa} \to \mathsf{st}$, $\mathsf{p}_2 : \mathsf{st} \times \mathsf{pa} \to \mathsf{pa}$; relation symbols like tr(ansition) $\subseteq \mathsf{pa} \times \mathsf{st} \times \mathsf{st}$, $=_X \subseteq X \times X$ for every sort X, etc. Let M be an interpretation of $\mathcal{L}$ in $\mathsf{Sh}(\mathsf{InSys})$ such that $\mathsf{st}^M = \mathsf{St}$, $\mathsf{pa}^M = \mathsf{Pa}$, $\mathsf{b}^M = \mathsf{B}_{\mathbb{N}}$, $\mathsf{t} = \mathbb{N}$, $\mathsf{appl}^M = \mathsf{a}$, ${\mathsf{p}_1}^M = \pi_1, {\mathsf{p}_2}^M = \pi_2$ (the canonical projections), $\mathsf{tr}^M = \mathsf{Tr}$. For every sort X, we interpret $=_X : X \times X \to \Omega$ as usual.

Theorem 9.2 ([18]) $\mathsf{Sh}(\mathsf{InSys})$ *satisfies a geometric axiom in the interpretation* M *if and only if* Set *satisfies it in all interpretations* $f_i^*(M)$. *If* $\mathsf{Sh}(\mathsf{InSys})$ *satisfies a cartesian axiom, this is also true in* Set *in the interpretation* $g_*(M)$ *(*$f_i^*(M)$ *and* $g_*(M)$ *interpret a sort* X *as* $f_i^*(X^M)$ *resp.* $g_*(X^M)$*).*

From Theorems 6.2 and 7.2 we know that for every $S_i \in \mathsf{InSys}$, $f_i^*(\mathsf{St}) = \mathsf{St}_{S_i} \simeq St(S_i)$ and $f_i^*(\mathsf{Pa}) = \mathsf{Pa}_{S_i} \simeq Pa(S_i)$; if S is the system obtained by interconnecting all elements in InSys, $g_*(\mathsf{St}) = \mathsf{St}(\mathsf{InSys}) \simeq St(S)$, and $g_*(\mathsf{Pa}) = \mathsf{Pa}(\mathsf{InSys}) \simeq Pa(S)$. The same holds for Tr and B_T. Moreover, $f_i^*(\mathbb{N}) = \mathbb{N}$, $g^*(\mathbb{N}) = \mathbb{N}(\mathsf{InSys})$, and, by Theorem 8.1, $f_i^*(\mathsf{appl}) = \mathsf{a}_{S_i} : B_{\mathbb{N}}(S_i) \times \mathbb{N} \to St(S_i) \times Pa(S_i)$. Hence, statements about states, actions and transitions in $\mathsf{Sh}(\mathsf{InSys})$ are translated by f_i^* (resp. g_*) to corresponding statements about states, actions and transitions in S_i (resp. S).

We illustrate the ideas above by several classes of properties of systems (adapted from [11]) which we express in the language $\mathcal{L}$. For instance, if h is a possible behavior and j a moment in time, then $h(j)$ can be expressed in $\mathcal{L}$ by $\mathsf{appl}(h, j)$; the state of h at j can be expressed by $\mathsf{s}(h, j)$, where $\mathsf{s} = \mathsf{p}_1 \circ \mathsf{appl} : \mathsf{b} \times \mathbf{t} \stackrel{\mathsf{appl}}{\to} \mathsf{st} \times \mathsf{pa} \stackrel{\mathsf{p}_1}{\to} \mathsf{st}$.

(a) Safety properties are of the form $(\forall h : \mathsf{b})(\forall j : \mathsf{t})(P(\mathsf{s}(h, 0)) \Rightarrow Q(\mathsf{s}(h, j)))$, where P and Q are formulae in $\mathcal{L}$. As examples we mention:
partial correctness: $(\forall h : \mathsf{b})(\forall j : \mathsf{t})[(P(\mathsf{s}(h, 0)) \wedge \mathsf{Final}(\mathsf{s}(h, j))) \Rightarrow Q(\mathsf{s}(h, j))]$;
global invariance of Q: $(\forall h : \mathsf{b})(\forall j : \mathsf{t})[P(\mathsf{s}(h, 0)) \Rightarrow Q(\mathsf{s}(h, j))]$.

(b) Liveness properties have the form $(\forall h : \mathsf{b})[P(\mathsf{s}(h, 0)) \Rightarrow (\exists j : \mathsf{t})Q(\mathsf{s}(h, j))]$. With s_0 denoting the initial and s_f a final state, examples are: *total correctness and termination:* $(\forall h : \mathsf{b})[P(\mathsf{s}(h, 0)) \Rightarrow (\exists j : \mathsf{t})(\mathsf{Final}(\mathsf{s}(h, j)) \wedge Q(\mathsf{s}(h, j)))]$; *accessibility:* $(\forall h : \mathsf{b})[(\mathsf{s}(h, 0) = s_0) \Rightarrow (\exists j : \mathsf{t})(\mathsf{s}(h, j) = s_f)]$.

(c) Precedence properties: $(\forall h : \mathsf{b})(\forall j : \mathsf{t})[(P(\mathsf{s}(h, 0)) \wedge A(\mathsf{s}(h, j))) \Rightarrow Q(\mathsf{s}(h, j))]$.

Theorem 9.3 ([18]) *Assume that the following conditions are fulfilled:*

(1) The final states form a subsheaf $\mathsf{St}_f \subseteq \mathsf{St}$ interpreting a sort $\mathsf{st_f}$ of $\mathcal{L}$. (This happens e.g. if in the definition of a system final states are specified by additional constraints, and in defining colimits this information is also used.)

(2) The properties P, Q, A can be expressed in $\mathcal{L}$ (using the sorts, constants, function and relation symbols mentioned at the beginning of Section 9), and can be interpreted in $\mathsf{Sh}(\mathsf{InSys})$ and also in Set (to express, for every S_i in InSys, the corresponding property of S_i, or S).

The truth of formulae describing safety, liveness and precedence properties (as in (a),(b),(c) above) is preserved under inverse image functors if in the definitions of the property P (c.q. Q, A) only conjunction, disjunction and existential quantification occur. The truth of these formulae is additionally preserved by direct image functors if only conjunction and unique existential quantification occur in them.

9.4 Example 1: Safety of train systems controlled by a radio controller

Consider the example in Section 4.1: Let $k \leq l \in \{1, \ldots, n\}$, $I_1 = \{k, \ldots, n\}, I_2 = \{1, \ldots, l\}$, and $I_{12} = \{k, \ldots, l\}$. Let $\mathsf{InSys} = \{S_1, S_2, S_{12}\}$ be the family consisting of the subsystems of S described in Section 2.2 corresponding to the sets of trains with indices in I_1, I_2 and I_{12}. Let Γ_s^j, $j \in \{1, 2, 12\}$ be the following constraints encoding collision freeness of S_j (where $\Rightarrow$ denotes logical implication):

$$\Gamma_s^j = \{\mathsf{succ}(\mathsf{TrainIndex}_i) = \mathsf{TrainIndex}_k \Rightarrow \mathsf{ActualPos}_i < \mathsf{ActualPos}_k - \mathsf{L} \mid i, k \in I_j\}.$$

For every $S_j \in \{1, 2, 12\}$ let $\mathsf{SafeSt}(S_j) = \{s : X_j \to M_j \mid s \models \Gamma_j \cup \Gamma_s^j\}$ be the set of safe states of S_j [6]. Let $\mathsf{SafeState} : \Omega(\mathsf{InSys}) \to \mathsf{Sets}$ be defined on objects by $\mathsf{SafeState}(U) = \{(s_j)_{S_j \in U} \mid s_j \in \mathsf{SafeSt}(S_j)$, and $s_{j|X_i} = s_i$ whenever $S_i \hookrightarrow S_j\}$, and on morphisms by restriction. We can define a set of similar constraints Γ_s and a similar set of safe states $\mathsf{SafeSt}(S)$ for the system S, where:

[6] We denote by Γ_j the restriction of Γ (cf. Definition 2.2) to X_j

$\Gamma_s = \{\mathsf{succ}(\mathsf{TrainIndex}_i) = \mathsf{TrainIndex}_k \Rightarrow \mathsf{ActualPos}_i < \mathsf{ActualPos}_k - \mathsf{L} \mid i, k \in \{1, \ldots, n\}\}$.

If $I_1 \cap I_2 \neq \emptyset$ then $\Gamma_s^1 \cup \Gamma_s^2 = \Gamma_s$ [7]. Analogously to Theorem 6.2 we can show:

Theorem 9.4 *The following hold:*

(i) $\mathsf{SafeState}$ *is a sheaf. Moreover,* $\mathsf{SafeState}$ *is a subsheaf of* St.

(ii) *For each* $S_i \in \mathsf{InSys}$, *the stalk of* $\mathsf{SafeState}$ *at* S_i *is in bijection with* $\mathsf{SafeSt}(S_i)$.

(iii) $\mathsf{SafeState}(\mathsf{InSys})$ *is in bijection with* $\mathsf{SafeSt}(S)$.

Collision freeness can be expressed as follows:

$$\mathsf{CollFree} \quad (\forall h : \mathsf{b})(\forall j : \mathsf{t})\ [\mathsf{SafeState}(\mathsf{s}(h, 0)) \Rightarrow \mathsf{SafeState}(\mathsf{s}(h, j))].$$

This formula contains only atomic formulae and the implication symbol. Therefore, by Theorem 9.3, its truth is preserved both under inverse image functors and under direct image functors, and it is reflected by the stalk functors:

- Assume that S_1, S_2, S_{12} satisfy $\mathsf{CollFree}$. Then for all $h \in B_{\mathbb{N}}(S_j)$, $t \in \mathbb{N}$, if $\pi_1(h(0)) \in \mathsf{SafeSt}(S_j)$ then $\pi_1(h(t)) \in \mathsf{SafeSt}(S_j)$. Due to the form of the formula $\mathsf{CollFree}$, its truth is reflected by the stalk functors $f_j^* : \mathsf{Sh}(\mathsf{InSys}) \to \mathsf{Set}$. It therefore follows that $\mathsf{Sh}(\mathsf{InSys})$ satisfies, internally, the formula $\mathsf{CollFree}$.
- The truth of $\mathsf{CollFree}$ is preserved by the global section functor $g_* : \mathsf{Sh}(\mathsf{InSys}) \to \mathsf{Set}$, defined by $g(F) = F(\mathsf{InSys})$. Therefore, (in Set) the following holds:

$$\forall h \in B_{\mathbb{N}}(\mathsf{InSys}), \forall t \in \mathbb{N}(\mathsf{InSys})\ [\pi_1(h(0)) \in \mathsf{SafeState}(\mathsf{InSys}) \Rightarrow \pi_1(h(t)) \in \mathsf{SafeState}(\mathsf{InSys})]$$

As, by Theorems 9.4 and 7.2, $\mathsf{SafeState}(\mathsf{InSys})$ is in bijective correspondence with $\mathsf{SafeSt}(S)$ and $\mathsf{B}_{\mathbb{N}}(\mathsf{InSys})$ is in bijective correspondence with $B_{\mathbb{N}}(S)$, we obtain:

$\forall h \in B_{\mathbb{N}}(S)$, $\forall t \in \mathbb{N}$, if $\pi_1(h(0)) \in \mathsf{SafeSt}(S)$ then $\pi_1(h(t)) \in \mathsf{SafeSt}(S)$.

Corollary 9.5 *Consider a family of consecutive trains on a linear track without loops. Assume that each train i controls both its position and the position of its predecessor, and accordingly determines its movement mode. We obtain a family* $\{S_i \mid i \in \{2, \ldots, n\}\}$ *of systems consisting of two successor trains each (each defined as in Example 2.2 for* $n = 2$*). Let U consist of this family of systems together with their intersections. The colimit of this family is the system S described in Example 3.5. By Theorem 9.3, if collision freeness can be guaranteed for all the systems in U, then the system S is collision free.*

For suitably chosen $\mathsf{minSpeed}, \mathsf{maxSpeed}$ and update interval Δt all 2-train systems are collision free (for an automatic proof ideas from [8] can be used). Therefore, the n-train system in Example 2.2 can be proved to be collision free for these values.

Remark: The condition that the systems consist of successive trains and overlap over one extremity is needed for recovering the successor constraints on trains for the colimit. We obtain similar links between global and local properties also with a cover consisting of one-train systems. However, then the colimit of the system

[7] Note that if $I_1 \cap I_2 = \emptyset$ then some of the constraints of Γ_s cannot be deduced from Γ_s^1 and Γ_s^2

defined by such a cover is different of the system S; we would obtain a link between the safety of the systems consisting of one train only and the safety of a system in which all trains are on independent tracks.

9.5 Example 2: Lifeness

We adapt the example in the previous section and give an example of lifeness property which can be expressed by means of a cartesian theory, and thus can be checked modularly. Assume that the constraints Γ'_j on for system S_j consist of Γ_j (defined as Γ^l_k in Example 3.2) and the constraint $(\bigwedge_{i\in I_j} \mathsf{Mode}_i = 0) \vee (\prod_{i\in I_j} \mathsf{Mode}_i > 0)$. As in Theorem 9.4 we can prove that this defines a subsheaf St'_j of St; the following constraints define subsheaves of St' with properties similar to those of $\mathsf{SafeState}$:

- $\Gamma^j_{su} = \Gamma'_j \cup \Gamma^j_s \cup \{\mathsf{Mode}_i = 0 \mid i \in I_j\}$ defines a sheaf $\mathsf{SafeStateUpdate}$;
- $\Gamma^j_{\mathsf{CanMove}} = \Gamma'_j \cup \{\mathsf{Mode}_i > 0 \mid i \in I_j\}$ defines a sheaf $\mathsf{CanMove}$;
- $\Gamma^j_{\mathsf{CannotMove}} = \Gamma'_j \cup \{\mathsf{Mode}_i = 0 \mid i \in I_j\}$ defines a sheaf $\mathsf{CannotMove}$.

For $S_i \in \mathsf{InSys}$ let $\mathsf{Minimal}(S_i) = \{(h, j) \mid s(h, j) \in \mathsf{CanMove}(S_i)$ and $\forall k(s(h, k) \in \mathsf{CanMove}(S_i) \rightarrow k \geq j)\}$, characterizing the minimal moment in time j w.r.t. a behavior h at which all trains in system S_i can move. These definitions can be used to define a subsheaf $\mathsf{MinimalCanMove} \subseteq \mathsf{B}_{\mathbb{N}} \times \mathbb{N}$ with properties similar to those of $\mathsf{St}, \mathsf{Pa}, \mathsf{Tr}, \mathsf{B}$. A form of lifeness can be expressed by the following cartesian axioms:

$$\forall h : \mathsf{b}\ (\mathsf{SafeStateUpdate}(\mathsf{s}(h, 0)) \rightarrow \exists j : \mathsf{t}\ \mathsf{MinimalCanMove}(h, j))$$
$$\forall h : \mathsf{b}, \forall i : \mathsf{t}\ (\mathsf{MinimalCanMove}(h, i) \rightarrow \mathsf{CanMove}(\mathsf{s}(h, i)))$$
$$\forall h : \mathsf{b}, \forall i, k : \mathsf{t}\ (\mathsf{MinimalCanMove}(h, i) \wedge \mathsf{CanMove}(\mathsf{s}(h, k)) \rightarrow i \leq k)$$

(where the existential quantified variable in the first axiom is provably unique modulo the second and third axiom), and can thus be checked modularly.

10 Conclusion

We showed that a family InSys of interacting systems closed under pullbacks can be endowed with a topology which models the way these systems interact. States, parallel actions, transitions, and behavior can be described as sheaves on this topological space. We then used geometric logic to determine which kind of properties of systems in InSys are preserved when interconnecting these systems. The main advantage of our approach is that it enables us to verify properties of complex systems in a modular way. We illustrated the ideas by means of a running example, involving systems of trains controlled by interacting controllers. In future work we plan to look at other applications, including geographically distributed systems, controlled by geographically fixed controllers, whose domains overlap.

We think that there should exist relationships between the approach described in this paper and other new approaches to the study of concurrency such as, for instance, higher dimensional automata (cf. [14,15]) or approaches based on methods from geometry and algebraic topologicy in particular homotopic methods (cf. [7]). Links between algebraic topology and concurrency as well as links with higher dimensional automata between have been studied e.g. by Gaucher, Goubault, Fa-

jstrup, and Raussen (cf. e.g. [5,4]). We would like to compare our approach with the methods mentioned above. Using homological and especially homotopic methods seems to be the next natural step after the sheaf semantics given in this paper.

Acknowledgement

Many thanks to the referees for their helpful comments.

References

[1] C.C. Chang and H.J. Keisler. *Model Theory*. North-Holland, Amsterdam, 3rd edition, 1990.

[2] B.A. Davey. Sheaf spaces and sheaves of universal algebras. Math. Zeitschrift, 134:275–290, 1973.

[3] V. Diekert. Combinatorics on Traces. In *LNCS 454*. Springer Verlag, 1990.

[4] L. Fajstrup, M. Raussen, E. Goubault. Algebraic topology and concurrency, I. *Theoretical Computer Science* 357, pages 241–278, 2006.

[5] P. Gaucher, É. Goubault. Topological Deformation of Higher Dimensional Automata. *Homology, Homotopy, Appl.*, 5(2):39–82, 2003.

[6] J.A. Goguen. Sheaf semantics for concurrent interacting objects. *Mathematical Structures in Computer Science*, 11:159–191, 1992.

[7] M. Herlihy, N. Shavit.. The topological structure of asynchronous computation. *Journal of the ACM*, 46: 858-923, 1999.

[8] S. Jacobs and V. Sofronie-Stokkermans. Applications of hierarchical reasoning in the verification of complex systems. Electronic Notes in Computer Science 174(8), pages 39-54, 2007. (Selection of the papers presented at the IJCAR'06 workshop Pragmatics of Decision Procedures in Automated Reasoning (PDPAR'06).)

[9] P. Johnstone. *Stone Spaces*. Cambridge Studies in Advanced Mathematics 3. Cambridge University Press, 1982.

[10] P.H. Krauss and D.M. Clark. Global subdirect products. *Memoirs of the AMS*, 17(210):1–109, 1979.

[11] F. Kröger. *Temporal Logic of Programs*, volume 8 of *EATCS Monographs on Theoretical Computer Science*. Springer Verlag, 1987.

[12] S. Mac Lane and I. Moerdijk. *Sheaves in Geometry and Logic*. Universitext. Springer Verlag, 1992.

[13] L. Monteiro and F. Pereira. A sheaf theoretic model for concurrency. *Proc. Logic in Computer Science (LICS'86)*, 1986.

[14] V. Pratt. Modeling concurrency with geometry. *Proc. 18th Symposium on Principles of Programming Languages* pages 311-322, ACM Press New York USA, 1991.

[15] V. Pratt. Higher-dimensional automata revisited. *Mathematical Structures in Computer Science*, 10(4), 2000.

[16] V. Sofronie. Towards a sheaf theoretic approach to cooperating agents scenarios. In J. Calmet, J.A. Campbell, and J. Pfalzgraf, editors, *Proc. of the International Conference Artificial Intelligence and Symbolic Mathematical Computation (AISMC-3)*, LNCS 1138, pages 289–304. Springer Verlag, 1996.

[17] V. Sofronie-Stokkermans. *Fibered Structures and Applications to Automated Theorem Proving in Certain Classes of Finitely-Valued Logics and to Modeling Interacting Systems*. PhD thesis, RISC-Linz, J. Kepler University Linz, 1997.

[18] V. Sofronie-Stokkermans and K. Stokkermans. *Modeling Interaction by Sheaves and Geometric Logic*. In G. Ciobanu and Gh. Paun eds, Proc. International Conference Fundamentals of Computation Theory (FCT'99), LNCS 1684, pages 512-523, Springer Verlag, 1999.

A Appendix. Sheaves of algebras

Let A be an algebra of similarity type Σ, $(\theta_i)_{i\in I}$ a family of congruences on A, and τ a topology on I. The following problem was addressed and solved in [2]: In which situation does a sheaf exist with fibers $A_i = A/\theta_i$ such that for every $a \in A$ the map $[a] : I \to \coprod_{i\in I} A_i$ is a global section? Two constructions are possible:

Construction 1 Let (F_A, f, I) be defined by $F_A = \coprod_{i\in I} A/\theta_i$, and $f : F_A \to I$ be the natural projection. Assume that a subbasis for the topology on F_A is $\{[a](U) \mid U \in \tau, a \in A\}$, where $[a](U) = \{[a](i) \mid i \in U\} = \{[a]_{\theta_i} \mid i \in U\}$.

Construction 2 Let $G_A : \tau \to \Sigma Alg$ be defined on objects by $G_A(U) = A/\theta_U$, where $\theta_U = \bigwedge_{i\in U} \theta_i$ and on morphisms, for every $V \subseteq U$ by the canonical morphism $G_A(U) = A/\theta_U \to A/\theta_V = G_A(V)$, $a_{\theta_U} \mapsto a_{\theta_V}$.

Let $G_i = \varinjlim_{i\in U} G_A(U)$ be the stalks of G_A, and for every $i \in I$ let $g_i : G_i \to A_i$ be the unique morphism that arises from the universality property of the colimit. Note that $g_i(\rho_i^U(a)) = a_{\theta_i}$ for every $U \in \tau$ and every $i \in I$. G_A is a presheaf of algebras. Let (SG_A, g, I) be the associated sheaf.

In Construction 1, the stalk at i is isomorphic to A_i, but (F_A, f, I) might be not a sheaf space. In Construction 2, (SG_A, g, I) is a sheaf space, but $g_i : G_i \to A_i$ may not be an isomorphism.

Theorem A.1 ([2]) *The following conditions are equivalent:*

(1) If $[a]_{\theta_i} = [b]_{\theta_i}$ then there is an open neighborhood U of i such that for every $j \in U$, $[a]_{\theta_j} = [b]_{\theta_j}$.
(2) (F_A, f, I) is a sheaf of algebras.
(3) For every $i \in I$, $g_i : G_i \to A_i$ is an isomorphism.

Definition A.2 If $(\theta_i)_{i\in I}$ is a family of congruences on an algebra A, then any topology on I that satisfies (1) is called an *S-topology*.

Corollary A.3 ([2]) *Assume that the topology on I is an S-topology with respect to the family of congruences $(\theta_i)_{i\in I}$. Then (F_A, f, I) and (SG_A, g, I) are isomorphic sheaves of algebras for which*

(1) The stalk at i is isomorphic to $A_i = A/\theta_i$,
(2) The map $\alpha : A \to \Gamma(I, F_A)$ defined by $\alpha(a) = ([a]_{\theta_i})_{i\in I}$ is a homomorphism,
(3) In $A \xrightarrow{\alpha} \Gamma(I, F_A) \leq \prod_{i\in I} A/\theta_i \xrightarrow{p_i} A/\theta_i$:
  (i) $p_i \circ \alpha$ is an epimorphism, and
  (ii) A is a subdirect product of the family $(A/\theta_i)_{i\in I}$ iff $\bigwedge_{i\in I} \theta_i = \Delta_A$ (i.e. iff α is a monomorphism).

The coarsest S-topology on I can be constructed as follows:

Lemma A.4 ([2], [10]) *Let $A \hookrightarrow \prod_{i\in I} A_i \xrightarrow{p_i} A_i$ be a subdirect product. The coarsest S-topology on I is generated by the sets $E(a,b)=\{i\in I \mid p_i(a)=p_i(b)\}$ as a subbasis.*

Lemma A.5 ([10]) *Let $A \hookrightarrow \prod_{i\in I} A_i \xrightarrow{p_i} A_i$ be a subdirect product and τ_1, τ_2 be two topologies on I. If $\tau_1 \subseteq \tau_2$ and τ_1 contains the equalizer topology induced by A (generated by the sets $E(a,b)$ as a subbasis), then $\Gamma(F_A, (I, \tau_1)) \subseteq \Gamma(F_A, (I, \tau_2))$.*

Even if the topology on I is an S-topology, A is not necessarily isomorphic to the algebra $\Gamma(I, F_A)$. A necessary and sufficient condition for A to be isomorphic to an algebra of global sections of a sheaf with fibers $A_i = A/\theta_i$, for $i \in I$ is given below:

Definition A.6 A family $(c_i)_{i\in I}$ of elements of A is said to be *global* with respect to $(\theta_i)_{i\in I}$ if for every $i \in I$ there exist $a_1^i, \ldots, a_n^i, b_1^i, \ldots, b_n^i \in A$ such that:

(i) $(a_j^i, b_j^i) \in \theta_i$ for every $j = 1, \ldots, n$,
(ii) If $(a_j^i, b_j^i) \in \theta_k$ for every $j = 1, \ldots, n$ then $(c_k, c_i) \in \theta_k$.

Theorem A.7 ([2]) *Let $(\theta_i)_{i\in I}$ be a family of congruences on an algebra A such that A is a subdirect product of $(A/\theta_i)_{i\in I}$. Endow I with its coarsest S-topology. Then $\alpha : A \to \Gamma(I, F_A)$ is an isomorphism iff for every family of elements $(c_i)_{i\in I}$ global with respect to $(\theta_i)_{i\in I}$, there is a $c \in A$ with $(c, c_i) \in \theta_i$ for every $i \in I$.*

B Appendix. Partially commutative monoids

If $G = (A, D)$ is a dependency graph, we denote by $M(G)$ the quotient A^*/θ, where θ is the congruence generated by $\{(a_1a_2, a_2a_1) \mid (a_1, a_2) \notin D\}$ (a free partially commutative monoid).

Theorem B.1 (Corollary 1.4.5 in [3]) *Let G be an undirected graph and $\{G_j \mid j \in J\}$ be a* finite *family of subgraphs of G. For $j \in J$ let $\pi_j : M(G) \to M(G_j)$ be the canonical projection and $\pi : M(G) \to \prod_{j\in J} M(G_j)$ be the homomorphism into the direct product defined by $\pi(t) = (\pi_j(t))_{j\in J}$. Then π is injective iff $G = \bigcup_{j\in J} G_j$.*

If $\{M_j \mid j \in J\}$ is a family of non-trivial free partially commutative monoids then $\prod_{j\in J} M_j$ is free partially commutative iff J is finite [3]. If $\{G_j \mid j \in J\}$ is not finite, then – assuming that for every vertex x of G there are finitely many $j \in J$ such that x is a vertex of G_j – there is an injective morphism $M(G) \hookrightarrow \bigoplus_{j\in J} M(G_j)$, where $\bigoplus_{j\in J} M(G_j) = \{(m_j)_{j\in J} \mid m_j \in M(G_j)$ for all $j \in J, m_j = \varepsilon$ a.e. [8] $\}$ [3], p.27.

[8] a.e. means *almost everywhere*