Modeling Interaction by Sheaves and Geometric Logic

Viorica Sofronie-Stokkermans[1] and Karel Stokkermans[2]

[1] Max-Planck Institut für Informatik, Saarbrücken, Germany
[2] Institut für Computerwissenschaften, Salzburg, Austria
email: sofronie@mpi-sb.mpg.de, stokkerm@cosy.sbg.ac.at

Abstract. In this paper we show that, given a family of interacting systems, many notions which are important for expressing properties of systems can be modeled as sheaves over a suitable topological space. In such contexts, geometric logic can be used to test whether "local" properties can be lifted to a global level. We develop a way to use this method in the study of interacting systems, illustrated by examples.

1 Introduction

Many properties of systems can be expressed as assertions about states, actions, transitions, behavior in time. In this paper we show that, given a family of interacting systems, under certain circumstances these notions can be modeled by sheaves over a suitable topological space (where the topology expresses how the interacting systems share the information). The main advantage is that this allows us to use geometric logic in order to study the links between the properties of the systems obtained by interconnecting families of interacting systems, and those of their components. This opens the way towards a possibility of verifying certain properties of complex systems in a modular way, thus increasing efficiency.

Among existing approaches to concurrency based on fiberings, sheaf and presheaf theory we mention [MP86], [Pfa91], [Gog92], [Lil93], [Mal94], [Win96], [CW96]. The starting point of our research is the work of Pfalzgraf [Pfa91] and the ideas of Goguen [Gog92] and Monteiro and Pereira [MP86]. 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 is, to the best of our knowledge, new. Preliminary results (in a more theoretically involved framework) appear in [Sof96]. The results presented here simplify and considerably extend those in [Sof96].

The paper is structured as follows. In Section 2 we present some basic notions from sheaf theory and geometric logic. Section 3 discusses the systems and communication between subsystems we want to model. Section 4 describes our sheaf-theoretic model; then geometric logic is used to test whether local properties can be lifted to a global level.

2 Preliminaries

We present results from sheaf theory and geometric logic which we will use in our work. For definitions we refer to [Joh82] or [MLM92]. Notions from category theory and many-sorted logic are assumed known. Categories and sheaves will usually be denoted in sans-serif style, e.g. Set, $\mathsf{Sh}(I)$.

Sheaf theory. Let I be a topological space, and $\Omega(I)$ the topology on I. A *presheaf* on I is a functor $P : \Omega(I)^{\mathrm{op}} \to \mathsf{Set}$. Let $U \subseteq V$ be open sets in I, and $i_U^V : U \hookrightarrow V$ the corresponding morphism in $\Omega(I)$. The restriction to U, $P(i_U^V) : P(V) \to P(U)$ will also be denoted by ρ_U^V. A *sheaf* on I is a presheaf $F : \Omega(I)^{\mathrm{op}} \to \mathsf{Set}$ satisfying the following property:

> 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 we have $\rho^{U_i}_{U_i \cap U_j}(s_i) = \rho^{U_j}_{U_i \cap U_j}(s_j)$, there is a unique $s \in F(U)$ with $\rho^U_{U_i}(s) = s_i$ for all i.

The *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 morphisms of sheaves are natural transformations of functors. $\mathsf{Sh}(I)$ will denote the category of sheaves on I. The assignment $F \mapsto F_i$ defines the stalk functor at i, $\mathsf{Stalk}_i : \mathsf{Sh}(I) \to \mathsf{Set}$.

Interpreting many-sorted first order languages 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 $X_1 \times \cdots \times X_n$ and 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 [MLM92], Ch. X.

Geometric formulae and axioms. A *geometric formula* is a formula built up from atomic formulae 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. A geometric axiom $(\forall x_1, \ldots, x_n)\ (\phi \Rightarrow \psi)$ is *satisfied in an interpretation M of $\mathcal{L}$ in* $\mathsf{Sh}(I)$ if $\{(x_1, \ldots, x_n) \mid \phi\}^M$ is a subobject of $\{(x_1, \ldots, x_n) \mid \psi\}^M$ in $\mathsf{Sh}(I)$.

Geometric morphisms; preservation properties. Let $f : I \to J$ be a continuous map between topological spaces. The *direct image functor* $f_* : \mathsf{Sh}(I) \to \mathsf{Sh}(J)$ corresponding to f associates with every $F \in \mathsf{Sh}(I)$ the sheaf $f_*(F) : \Omega(J)^{\mathrm{op}} \to \mathsf{Set}$ defined by $f_*(F)(U) = F(f^{-1}(U))$; the *inverse image functor* $f^* : \mathsf{Sh}(J) \to \mathsf{Sh}(I)$ associated to f is defined as follows: for every $G \in \mathsf{Sh}(J)$, let $p : \coprod_{x \in J} G_x \to J$ be the bundle associated to G; $f^*(G) \in \mathsf{Sh}(I)$ is the sheaf associated to the bundle $f^*(p) : f^*(\coprod_{x \in J} G_x) \to I$ as obtained when constructing the pullback of f and p. f^* preserves finite limits and arbitrary colimits

(f^* is left adjoint to f_*); hence it preserves the interpretation of any geometric formula. Moreover, f^* preserves the interpretation of all geometric axioms. Since f_* is right adjoint to f^*, it preserves limits, but not unions or images (in general). However, f_* preserves, to some extent, existential quantification, as follows. Let $\mathbb{T}$ be a theory in the language $\mathcal{L}$. A variable 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 relative to* $\mathbb{T}$ is a formula built up from atomic formulae using only the connective $\wedge$ and the quantifier $\exists$ over $\mathbb{T}$-provably unique variables. A *cartesian axiom relative to* $\mathbb{T}$ is a formula of the form $(\forall x)(\phi(x) \Rightarrow \psi(x))$ where ϕ and ψ are cartesian formulae relative to $\mathbb{T}$. A *cartesian theory* is a theory whose axioms can be ordered such that each is cartesian relative to the preceding ones. Direct image functors preserve models of cartesian theories.

3 Systems

Our aim is modeling interconnected systems, whether hardware, software, or both. We assume a system S to be described by: a set X of control variables of the system, a set Γ of constraints on X, a set A of atomic actions, and a set C of constraints on A. This way of describing systems was influenced by the fact that, in many practical applications, the state of a system is determined by the values of certain control variables, among which dependencies may exist. An example and a detailed motivation can be found in [Sof96].

Definition 1. *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, 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 $s_1 \times \ldots \times s_n \to s$ then $f_M : M_{s_1} \times \ldots \times M_{s_n} \to M_s$ and if $R \in P$ has arity $s_1 \times \ldots \times s_n$ then $R_M \subseteq M_{s_1} \times \ldots \times M_{s_n}$. The class of Σ-structures is denoted Str_Σ.*

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. 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 in what follows by $s \models \phi$) is defined in the usual way (cf. e.g. [CK90], Ch. 1).

Definition 2. *A* system *S is a tuple $(\Sigma, X, \Gamma, M, A, C)$, where*

- *$\Sigma = (\mathsf{Sort}, O, P)$ and $X = \{X_s\}_{s\in\mathsf{Sort}}$ are as above; together they form the* language $\mathcal{L}_S$ of the system *S;*
- *$\Gamma \subseteq \mathsf{Fma}_\Sigma(X)$ is a set of constraints on variables, which is closed with respect to the semantical consequence relation[1] $\models_M$;*
- *$M \in \mathsf{Str}_\Sigma$;*
- *A is a set of actions; for every $a \in A$ we have a set $X^a \subseteq X$ of variables on which a depends, and a transition relation $Tr^a \subseteq Sat^a \times Sat^a$, where $Sat^a = \{s_{|X^a} \mid s : X \to M, s \models \Gamma\}$;*

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

– *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^a_S will denote the minimal set of variables on which $a \in A_S$ depends, and Tr^a_S the transition relation associated with a.

Definition 3 (States; Parallel actions). *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 is $Pa(S) = \{f : A \to \{0, 1\} \mid f$ 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 modeling the undesirable case of infinitely many actions occurring in parallel.

Transitions. Let $S = (\Sigma, X, \Gamma, M, A, C)$ be a system. Let $Tr_S(a) = \{(s_1, s_2) \mid s_1, s_2 \in St(S), (s_{1|X^a}, s_{2|X^a}) \in Tr^a, s_1(x) = s_2(x)$ if $x \notin X^a\}$. In order to extend this notion of transition to parallel actions we present two non-equivalent properties of transitions that express compatibility of the actions in an admissible parallel action, (**Disj**) and (**Indep**).

(Disj) Let $f \in Pa(S), s \in St(S)$ such that for every $a \in A$ with $f(a) = 1$ there is an $s^a \in St(S)_{|X^a}$ with $(s_{|X^a}, s^a) \in Tr^a$. Then for all $a, b \in A_S$ and $x \in X^a \cap X^b$, $s^a(x) = s^b(x)$, i.e. the new local states "agree on intersections". The transition induced by f is $Tr_S(f) = \{(s, t) \mid s, t \in St(S), (s_{|X^a}, t_{|X^a}) \in Tr^a$ for every a such that $f(a) = 1$, and $s(x) = t(x)$ if $x \notin \bigcup_{a, f(a)=1} X^a\}$.

(Indep) We assume that if $a = b \in C$ then $X^a = X^b$ and $Tr^a = Tr^b$, and a and b can be both identified with one action: the parallel execution of a, b. Let $f \in Pa(S), s \in St(S)$. We identify all elements $a, b \in A$ with $a = b \in C$ and $f(a) = f(b) = 1$. Let now $f^{-1}(1) = \{a_1, \dots, a_n\}$. Let $\{b_1, \dots, b_m\}$ be an arbitrary subset of $f^{-1}(1)$. We assume that:
  (i) $g : A \to \{0, 1\}$, defined by $g(a) = 1$ if and only if $a \in \{b_1, \dots, b_m\}$, is in $Pa(S)$;
  (ii) $s \xrightarrow{b_1} s_1 \xrightarrow{b_2} s_2 \cdots \xrightarrow{b_{m-1}} s_{m-1} \xrightarrow{b_m} t$ implies that for every permutation σ of $\{1, \dots, m\}$, there exist states $t^\sigma_1, \dots, t^\sigma_{m-1}$ such that $s \xrightarrow{b_{\sigma(1)}} t^\sigma_1 \xrightarrow{b_{\sigma(2)}} t^\sigma_2 \cdots \xrightarrow{b_{\sigma(m-1)}} t^\sigma_{m-1} \xrightarrow{b_{\sigma(m)}} t$ (the final state t is the same).

The transition induced by f is $Tr_S(f) = \{(s, t) \mid s, t \in St(S)$, and there exist $s = s_0, s_1, \dots, s_{n-1}, s_n = t \in St(S)$ such that $(s_{i-1}, s_i) \in Tr_S(a_i)$, for all $1 \leq i \leq n\}$. It is easy to see that if $(s, t) \in Tr_S(f)$ then for every $x \notin \bigcup_{a, f(a)=1} X^a$, $s(x) = t(x)$.

The property (**Disj**) applies when a parallel action $f : A \to \{0,1\}$ is admissible if and only if its components do not consume common resources. This happens for example 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. The property (**Indep**) reflects how transitions of parallel actions are interpreted when actions to be performed in parallel do consume common resources. It specifically applies if the state reached after executing an action is uniquely determined. In this case, 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 be sure that there are enough resources to perform all actions. Condition (**Indep**)(i) holds for instance 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 order in which the actions are executed is not relevant for determining the final state.

3.1 Communication between subsystems

Systems are usually related to other systems. We assume that, in order for two systems to be able to *communicate* they need a *"dictionary"*. Elements that are equal according to the dictionary are identified, so communicating systems are here supposed to share *common control variables* and *common actions*. We further assume that the values of the common control variables "sensed" simultaneously by two or more systems are the same. Essential to our model is that systems have common subsystems by which communication is handled (not the use of "dictionaries" or "translations"), and we focus on this aspect.

Definition 4. *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 $M_S = U^{\Sigma_T}_{\Sigma_S}(M_T)$ (where $U^{\Sigma_T}_{\Sigma_S} : \mathsf{Str}_{\Sigma_T} \to \mathsf{Str}_{\Sigma_S}$ is the forgetful functor).*

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, we have the following definition.

Definition 5. *S is a* transition-connected (t.c.) subsystem of T *(denoted $S \hookrightarrow T$) if $S \rightarrowtail T$ and the following two conditions hold:*

(T1) *for every $a \in A_T$, if $X^a_T \cap X_S \neq \emptyset$ then $a \in A_S$, and $X^a_S = X^a_T \cap X_S$;*
(T2) *for every $a \in A_S$ and every $s_1, s_2 \in St(T)$, if $(s_{1|X^a_T}, s_{2|X^a_T}) \in Tr^a_T$ then $(s_{1|X^a_S}, s_{2|X^a_S}) \in Tr^a_S$.*

It is easy to see that the relation $\hookrightarrow$ is a partial order on systems. We define a category TcSys with as objects systems and a morphism $S \hookrightarrow T$ between S and T whenever S is a t.c. subsystem of T.

Theorem 1. 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.*

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

- All $S \in \mathsf{InSys}$ are t.c. subsystems of a system $\overline{S}$ with $A_{\overline{S}}$ finite.
- InSys is closed (in TcSys) under pullbacks of subsystems of $\overline{S}$.
- $(\mathsf{InSys}, \wedge)$ 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 make sure that all systems by which communication is handled are taken into account.

A system obtained by interconnecting some elements of InSys can be seen either 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 t.c. subsystems. It is a topology on InSys.

4 Modeling by sheaves

We show that the notions of states, (parallel) actions, behavior, and time can be represented as sheaves over the topological space $(\mathsf{InSys}, \Omega(\mathsf{InSys}))$ previously defined. The fact that these notions can be expressed as sheaves with respect to an appropriate Grothendieck topology on a category of systems was already noticed in [Sof96]. We now show that the abstract framework presented there can be simplified. The main advantage of this simplification is that we can now express many properties of systems in the internal logic of the topos of sheaves over InSys. Geometric logic is then used to study how properties are preserved when interconnecting systems: interpretations corresponding to individual systems are obtained by using stalk functors, and interpretations corresponding to their interconnection are obtained by using the global section functors and colimits.

Definition 6 (States; Parallel actions).

(St) $\mathsf{St} : \Omega(\mathsf{InSys})^{op} \to \mathsf{Set}$ *is defined on objects by* $\mathsf{St}(U) = \{(s_i)_{S_i \in U} \mid s_i \in St(S_i)$, *and if* $S_i \hookrightarrow S_j$ *then* $s_i = s_{j|X_i}\}$, *and is such that for* $U_1 \overset{\iota}{\subseteq} U_2$, $\mathsf{St}(\iota) : \mathsf{St}(U_2) \to \mathsf{St}(U_1)$ *is defined by* $\mathsf{St}(\iota)((s_i)_{S_i \in U_2}) = (s_i)_{S_i \in U_1}$.

(Pa) $\mathsf{Pa} : \Omega(\mathsf{InSys})^{op} \to \mathsf{Set}$ *is defined on objects by* $\mathsf{Pa}(U) = \{(f_i)_{S_i \in U} \mid f_i \in Pa(S_i)$, *and if* $S_i \hookrightarrow S_j$ *then* $f_i = f_{j|A_i}\}$*; moreover, for* $U_1 \overset{\iota}{\subseteq} U_2$, $\mathsf{Pa}(\iota) : \mathsf{Pa}(U_2) \to \mathsf{Pa}(U_1)$ *is* $\mathsf{Pa}(\iota)((f_i)_{S_i \in U_2}) = (f_i)_{S_i \in U_1}$.

Theorem 2. *The functors* St *and* Pa *are sheaves on* InSys*. For every* $S_i \in \mathsf{InSys}$*, the stalk at* S_i *is in bijection with* $St(S_i)$ *resp.* $Pa(S_i)$*. Moreover, for every* $U \in \Omega(\mathsf{InSys})$, $\mathsf{St}(U)$ *(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.

Proof: *(Sketch)* The fact that St and Pa are sheaves follows immediately from the definition of a sheaf. The fact that there exists a bijection between $\mathsf{St}(U)$ (resp. $\mathsf{Pa}(U)$) and $St(S_U)$ (resp. $Pa(S_U)$), where S_U is the colimit of the diagram defined by $U \in \Omega(\mathsf{InSys})$, follows from the definition of the colimit, taking into account that (i) if S_1 is a t.c. subsystem of S_2 and ϕ is a formula of S_1 then a state s of S_2 satisfies ϕ if and only if its restriction to S_1 satisfies ϕ; and (ii) for every $U \in \Omega(\mathsf{InSys})$, every family $\{s_i\}_{S_i \in U}$ of states which are compatible on the common variables can be "glued" to a (unique) state of the colimit S_U of the diagram defined by U. It can be shown that the stalk of St at S_i is $\mathsf{St}(\downarrow S_i)$. Since the colimit of the diagram defined by $\downarrow S_i = \{S_j \in \mathsf{InSys} \mid S_j \hookrightarrow S_i\}$ is S_i, $\mathsf{St}(\downarrow S_i)$ is in bijection with $St(S_i)$. The same results hold also for Pa. $\square$

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

Definition 7 (Transition).

(Tr) $\mathsf{Tr} : \Omega(\mathsf{InSys})^{op} \to \mathsf{Set}$ *is defined on objects by* $\mathsf{Tr}(U) = \{(f, s, s') \mid f = (f_i)_{S_i \in U} \in \mathsf{Pa}(U), s = (s_i)_{S_i \in U}, s' = (s'_i)_{S_i \in U} \in \mathsf{St}(U), (s_i, s'_i) \in Tr_{S_i}(f_i),$ *for all* $S_i \in U\}$ *and is such that for* $U_1 \overset{\iota}{\subseteq} U_2$, $\mathsf{Tr}(\iota) : \mathsf{Tr}(U_2) \to \mathsf{Tr}(U_1)$ *is defined by* $\mathsf{Tr}(\iota)((f, s, s')) = (\mathsf{Pa}(\iota)(f), \mathsf{St}(\iota)(s), \mathsf{St}(\iota)(s'))$.

Theorem 3. *The functor* $\mathsf{Tr} : \Omega(\mathsf{InSys})^{op} \to \mathsf{Set}$ *is a subsheaf of* $\mathsf{Pa} \times \mathsf{St} \times \mathsf{St}$. *For every* $S_i \in \mathsf{InSys}$*, the stalk 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.

Proof: *(Idea)* The fact that Tr is a subsheaf of $\mathsf{Pa} \times \mathsf{St} \times \mathsf{St}$ follows immediately. A careful analysis shows that if the transitions obey either (**Disj**) or (**Indep**), then (i) for every $U \in \Omega(\mathsf{InSys})$, every family of local (compatible) transitions in the systems $S_i \in U$ can be glued to a global transition of S_U, where S_U is the colimit of the diagram defined by U; and (ii) for every $S_i \in U$, the restrictions of a transition in S_U to S_i is a transition in S_i. The fact that the stalk at S_i is in bijection with $Tr(S_i)$ can be proved as in Theorem 2. $\square$

We now define the behavior in time of a complex system. Our ideas are influenced by those in [Gog92], where objects are modeled by functors $F : \mathcal{T}^{\mathrm{op}} \to \mathsf{Set}$, where $\mathcal{T}$ is a "base for observation", and behavior is described componentwise. Here, we propose a slightly different way of modeling behavior. In what follows, time is assumed to be discrete, and all actions take a constant, unit amount of time. We will assume that $\mathcal{T}$ is the basis for the topology on $\mathbb{N}$ consisting of $\mathbb{N}$ together with all sets $\{0, 1, \ldots, n\}, n \in \mathbb{N}$. The behavior in the interval $T \in \mathcal{T}$ of a complex system is modeled by all successions of pairs (state, action) of the component subsystems that can be observed during T. We show that behavior over an arbitrary but fixed time interval T, can be modeled by a sheaf. It may be interesting to combine sheaf conditions with respect to time and with respect to the structure of a system; this is planned for future work.

Definition 8 (Behavior). *Let $T \in \mathcal{T}$ be arbitrary but fixed. The behavior in the time interval T is modeled by $\mathsf{B}_T : \Omega(\mathsf{InSys})^{op} \to \mathsf{Set}$ defined for every $U \in \Omega(\mathsf{InSys})$ by $\mathsf{B}_T(U) = \{h : T \to \mathsf{St}(U) \times \mathsf{Pa}(U) \mid K(h, T)\}$ and for every $U_1 \overset{\iota}{\subseteq} U_2$ by $\mathsf{B}_T(\iota) : \mathsf{B}_T(U_2) \to \mathsf{B}_T(U_1)$, where for every $h \in \mathsf{B}_T(U_2)$, $\mathsf{B}_T(\iota)(h) = (\mathsf{St}(\iota) \times \mathsf{Pa}(\iota)) \circ h : T \xrightarrow{h} \mathsf{St}(U_2) \times \mathsf{Pa}(U_2) \xrightarrow{\mathsf{St}(\iota)\times\mathsf{Pa}(\iota)} \mathsf{St}(U_1) \times \mathsf{Pa}(U_1)$. 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 $(f, s, s') \in Tr(U)$.*

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 $(s, s') \in Tr_S(f)$.

Theorem 4. *For any $T \in \mathcal{T}$, $\mathsf{B}_T : \Omega(\mathsf{InSys})^{op} \to \mathsf{Set}$ 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 either (**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.*

Proof: *(Idea)* The fact that B_T is a sheaf follows from the definition of B_T and the fact that St, Pa, and Tr are sheaves. The existence of a bijection between $\mathsf{B}_T(U)$ and $B_T(S_U)$ follows from results used in Theorems 2 and 3 when proving that $F(S_U)$ is in bijection with $\mathsf{F}(U)$ for $F \in \{St, Pa, Tr\}$. $\square$

In order to reason about the evolution of systems in time, it may be useful to express time internally in the category $\mathsf{Sh}(\mathsf{InSys})$.

Definition 9 (Time). *Time is modeled by the sheafification of the constant presheaf $\mathcal{N} : \Omega(\mathsf{InSys})^{op} \to \mathsf{Set}$ (defined for every U by $\mathcal{N}(U) = \mathbb{N}$), which by abuse of notation we denote $\mathbb{N}$ as well.*[2]

We can also define functors $\mathsf{B^{St}}_T$ and $\mathsf{B^{Pa}}_T$ which only encode information about states (resp. actions). 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 $S_i \in U$, $h(n_i) = ((s_j^i)_{S_j \in U}, (f_j^i)_{S_j \in U})$.

Theorem 5. *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 $\mathsf{a}_{S_i}(h, n) = h(n)$.*

Proof: *(Sketch)* Follows immediately from the way the stalk functors are defined on morphisms, and from the fact that, by Theorems 2 and 4, $F_{S_i} \simeq F(\downarrow S_i) \simeq F(S_i)$ for $F \in \{\mathsf{St}, \mathsf{Pa}, \mathsf{B}_T\}$, and from the fact that $\mathbb{N}_{S_i} \simeq \mathbb{N}(\downarrow S_i) \simeq \mathbb{N}$. $\square$

An alternative way to describe behavior is by traces of execution. We obtained results which extend those given in [MP86], and which give a sheaf-theoretic formalization to results of Diekert [Die90]. Due to space limitations we cannot present these results here; for details cf. [SS97].

[2] It is denoted $(\mathcal{N}^+)^+$ in [MLM92], p. 130; it can be shown that for every $U \in \Omega(\mathsf{InSys})$, $(\mathcal{N}^+)^+(U) = \{i : U \to \mathbb{N} \mid i \text{ locally constant}\}$. $\mathbb{N} = (\mathcal{N}^+)^+$ is the natural number object in $\mathsf{Sh}(\mathsf{InSys})$; maps $1 \xrightarrow{0} \mathbb{N} \xrightarrow{s} \mathbb{N}$ and a subobject $\leq \subseteq \mathbb{N} \times \mathbb{N}$ can be defined.

4.1 Using geometric logic to express properties of 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.

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 $f_i^* : \mathsf{Sh}(\mathsf{InSys}) \to \mathsf{Set}$ are collectively faithful, so they reflect the validity of geometric axioms.

Global section functor. Consider the unique map $g : \mathsf{InSys} \to \{*\}$. The corresponding 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.

Theorem 6. $\mathsf{Sh}(\mathsf{InSys})$ *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 2, 3, and 4 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 5, $f_i^*(\mathsf{appl}) = \mathsf{a}_{S_i} : B_{\mathbb{N}}(S_i) \times \mathbb{N} \to St(S_i) \times Pa(S_i)$. 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 examples. We consider classes of properties of systems (adapted from [Krö87]) and express them in the language $\mathcal{L}$. For instance, if h is a possible behavior and j a moment of 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 $\mathsf{s} = \mathsf{p}_1 \circ \mathsf{appl} : \mathsf{b} \times \mathsf{t} \stackrel{\mathsf{appl}}{\to} \mathsf{st} \times \mathsf{pa} \stackrel{\mathsf{p}_1}{\to} \mathsf{st}$.

(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 are of the form $(\forall h : \mathsf{b})(\forall j : \mathsf{t})[(P(\mathsf{s}(h,0)) \wedge A(\mathsf{s}(h,j))) \Rightarrow Q(\mathsf{s}(h,j))]$.

Theorem 7. *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 4.1), and can be interpreted in both* $\mathsf{Sh}(\mathsf{InSys})$ *and* Set *(to express, for every* S_i *in* InSys*, the corresponding property of* S_i*, or* S*).*

Then, all formulae considered above (safety, liveness and precedence properties) are preserved under inverse image functors if in the definitions of the property P *(c.q.* Q, A*) only conjunction, disjunction and existential quantification occur. They are additionally preserved by direct image functors if only conjunction and unique existential quantification occur.*

Proof: *(Sketch)* Assume that (1) holds, and $\mathsf{st_f}$ is a subsort of st. Let $i : \mathsf{st_f} \to \mathsf{st}$ be the inclusion. Then $\mathsf{Final}(s)$ is expressed in $\mathcal{L}$ by $(\exists s' : \mathsf{st_f})(i(s') = s)$, and if s' exists, it is unique. If (1) and (2) hold, the formulae above can be expressed in the language $\mathcal{L}$. Therefore, the conclusion follows, since all given formulae are geometric if P, Q, A are (resp. cartesian if P, Q, A are, and only unique existential quantification occurs). □

Examples.

1. Let $\phi_1 = (\forall s, s', s'' : \mathsf{st})(\forall a : \mathsf{pa})[(\mathsf{tr}(a,s,s') \wedge \mathsf{tr}(a,s,s'')) \Rightarrow s' = s'']$ express *determinism.* Since ϕ_1 is a cartesian axiom, if all systems in InSys satisfy ϕ_1, then ϕ_1 is true (internally) in $\mathsf{Sh}(\mathsf{InSys})$. Moreover, it follows that ϕ_1 is true in the system obtained by interconnecting the systems in InSys.
2. Let $\phi_2 = (\forall h : \mathsf{b})(\forall a : \mathsf{pa})(\forall i : \mathsf{t})[(\exists s : \mathsf{st})(\mathsf{tr}(a, \mathsf{p_1}(\mathsf{appl}(h,i)), s)) \Rightarrow (\exists j : \mathsf{t})(j \geq i \wedge \mathsf{p_2}(\mathsf{appl}(h,j)) = a)]$ express *fairness of execution.* Since ϕ_2 is a geometric axiom, it is preserved and reflected by the stalk functors. Since an existential quantifier occurs, ϕ_2 may not be preserved by the global section functor. If ϕ_2 is part of a cartesian theory $\mathbb{T}$ (i.e. the existence of s and j is $\mathbb{T}$-provably unique), then its validity (as part of $\mathbb{T}$) is preserved by g_*. The validity of ϕ_2 is also preserved by g_* if all systems in InSys are independent, i.e. $S_i \wedge S_j = \emptyset$ if $S_i \neq S_j$ (If InSys is finite, $(\mathsf{InSys}\backslash\emptyset, \Omega(\mathsf{InSys}\backslash\emptyset))$ is then a Stone space, cf. also *Remark 1*).
3. Let $\phi_3 = (\forall s : \mathsf{st})(\exists a : \mathsf{pa})(\exists s' : \mathsf{st})(\mathsf{tr}(a,s,s') \wedge (s \neq s'))$ express *deadlock freedom.* Since ϕ_3 contains the negation sign, it is not geometric and may not be preserved by direct and inverse geometric morphisms; in particular neither by the global section nor by the stalk functors.

Remark 1. The empty system $\emptyset$ can be excluded from consideration, as follows. Let $\Omega_1(\mathsf{InSys})$ be the family of all subsets of $\mathsf{InSys}\backslash\emptyset$ closed under t.c. subsystems. (If no element in InSys is the colimit of other elements in InSys, then $\Omega_1(\mathsf{InSys})$ is the free frame freely generated by InSys together with the constraint that the empty family of systems covers the empty system.) All the considerations above remain valid when $\Omega(\mathsf{InSys})$ is replaced by $\Omega_1(\mathsf{InSys})$. The space $(\mathsf{InSys}\backslash\emptyset, \Omega_1(\mathsf{InSys}))$ is totally disconnected if for every $S_1, S_2 \in \mathsf{InSys}$, their largest common t.c. subsystem $S_1 \wedge S_2$ is empty; the space is compact if additionally InSys is finite. In this situation a larger class of axioms is preserved by the global section functor (uniqueness in existential quantification is not required, cf. e.g. [Joh82], Ch. V.1.12). Then, the definition of time as a sheaf $\mathbb{N}$ expresses the fact that independent systems may have independent clocks.

5 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. Our results are influenced by the results of Goguen in [Gog92], where a sheaf-theoretic framework for modeling concurrent interaction is presented. There, objects are taken to be sheaves, and then the behavior of systems (diagrams in the framework) corresponds to constructing a limit, while interconnecting systems amounts to taking colimits. At the end, Goguen suggests to look at the more elaborate framework of topos theory and see what kind of reasoning can be achieved using the internal logic of a topos of sheaves. This is the direction we have explored in this paper. The main advantage of our approach is that it opens the possibility to verify properties of complex systems in a modular way.

In recent papers on model checking, decomposition of systems was used to avoid the state explosion problem. We refer for instance to [CGL96], where systems are modeled by finite Kripke structures. In that context, it is shown that formulae in universal computation tree logics ($ACTL^*$) can be checked in a modular way; for this (i) certain fairness assumptions are made; and (ii) it may be necessary to make additional assumptions about the environment when verifying properties of individual components. Both in formulae in $ACTL^*$ and in geometric and cartesian formulae, as defined in this paper, restrictions are imposed in the use of existential quantification and negation. We would like to gain a better understanding about the possible links between the results presented in this paper and the methods from model checking mentioned above.

We plan to continue our research in several directions. First, we can consider categories with more special morphisms (e.g. conservative extensions, definitional extensions). Second, we can consider more general morphisms expressing "translations" between languages of different systems. For this, the theory of institutions may be a suitable theoretical framework. Third, since we showed that transitions define subsheaves $\mathsf{Tr} \subseteq \mathsf{Pa} \times \mathsf{St} \times \mathsf{St}$, we can associate a "generic transition system" to a given category of systems, where both states and actions are sheaves. The results of Adámek and Trnková [AT90] on defining automata in a category could then be applied to the concrete category $\mathsf{Sh}(\mathsf{InSys})$; this would allow us to carry over general constructions like minimal realization.

References

[AT90] J. Adámek and V. Trnková. *Automata and Algebras in Categories.* Kluwer Academic Publishers, 1990.

[CGL96] E.M. Clarke, O. Grumberg, and D.E. Long. Model checking. In *Nato ASI Series F*, volume 152, New York, Heidelberg, Berlin, 1996. Springer-Verlag.

[CK90] C.C. Chang and H.J. Keisler. *Model Theory.* North-Holland, Amsterdam, 3rd edition, 1990.

[CW96] G.L. Cattani and G. Winskel. Presheaf models for concurrency. In D. van Dalen and M. Bezem, editors, *Proceedings of Computer Science Logic '96*, LNCS 1258, pages 58–75. Springer Verlag, Berlin, 1996.

[Die90] V. Diekert. Combinatorics on Traces. In *LNCS 454*. Springer Verlag, 1990.

[Gog92] J.A. Goguen. Sheaf semantics for concurrent interacting objects. *Mathematical Structures in Computer Science*, 11:159–191, 1992.

[Joh82] P. Johnstone. *Stone Spaces.* Cambridge Studies in Advanced Mathematics 3. Cambridge University Press, 1982.

[Krö87] F. Kröger. *Temporal Logic of Programs*, volume 8 of *EATCS Monographs on Theoretical Computer Science.* Springer Verlag, 1987.

[Lil93] J. Lilius. A sheaf semantics for Petri nets. Technical Report A23, Dept. of Computer Science, Helsinki University of Technology, 1993.

[Mal94] G. Malcolm. Interconnections of object specifications. In R. Wieringa and R. Feenstra, editors, *Working Papers of the International Workshop on Information Systems – Correctness and Reusability*, 1994. Appeared as internal report IR-357 of the Vrije Universiteit Amsterdam.

[MLM92] S. Mac Lane and I. Moerdijk. *Sheaves in Geometry and Logic.* Universitext. Springer Verlag, 1992.

[MP86] L. Monteiro and F. Pereira. A sheaf theoretic model for concurrency. *Proc. Logic in Computer Science (LICS'86)*, 1986.

[Pfa91] J. Pfalzgraf. Logical fiberings and polycontextural systems. In P. Jorrand and J. Kelemen, editors, *Proc. Fundamentals of Artificial Intelligence Research*, volume 535 of *LNCS (subseries LNAI)*, pages 170–184. Springer Verlag, 1991.

[Sof96] V. Sofronie. Towards a sheaf theoretic approach to cooperating agents scenarios. In J. Calmet, J.A. Campbell, and J. Pfalzgraf, editors, *Proceedings of Artificial Intelligence and Symbolic Mathematical Computation, International Conference, AISMC-3, Steyr*, LNCS 1138, pages 289–304. Springer-Verlag, 1996.

[SS97] 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.

[Win96] G. Winskel. A presheaf semantics of value-passing proceses. In Montanari and Sassone, editors, *Concurrency Theory: 7th International Conference, CONCUR '96 Proceedings*, LNCS 1119, pages 98–114, 1996.