A categorical view of process refinement

P. Degano\textsuperscript{1,2}  
R. Gorrieri\textsuperscript{3}  
G. Rosolini\textsuperscript{2}

\textsuperscript{1} Dipartimento di Informatica  
Corso Italia 40  
56100 Pisa, Italy

\textsuperscript{2} Dipartimento di Matematica  
via D'Azeglio 85A  
43100 Parma, Italy

\textsuperscript{3} Dipartimento di Matematica  
Porta S. Donato 5  
40127 Bologna, Italy

ABSTRACT: A very general notion of refinement of event structures is presented that refines both the events and the relations of causality and conflict. It is based on a purely semantic construction based on sections of a functor between domain-like categories. The present construction is compared to others in the literature.

Keywords: Hierarchical specifications, concurrent programs, categories, true concurrency, event structures.

Contents

1 Domains and event structures

2 The category-theoretic construction

3 Event refinement as a functor

4 Refinement in the general case

5 A characterization of disciplined refinement
Introduction

The idea of considering modular representations of concurrent processes has the obvious intention of reducing the complexity of specific programs. Indeed refinement of concurrent processes has already appeared in the literature, cf. [8]. There are now two main lines of approach to set up a discipline for the specification, the design and the verification of concurrent processes: one takes the algebraic, linguistic point of view where a new operator of action refinement is added to the usual operators of Process Description Languages, e.g. extensions of CCS-like languages as in [1, 10, 9, 15], enrichment of event structures and causal trees as in [6, 18, 19]. The other considers processes as collections of (guarded) actions with no additional structure, and actions are freely transformed into more detailed processes, e.g. refinement of action systems [4, 2], communication closed layers [12, 13, 17], and concurrent database transactions [3].

A first synthesis of the approaches mentioned above is in [14] where the collections of actions are endowed with an algebraic structure by means of a process description language. Essentially its (linear time, truly concurrent) denotational semantics maps a process to a set of partial orderings of events. These represent process activities, and they are partially ordered by relative causality. The language has also a non-standard operator of sequentialization and the semantics of sequentialization between two actions states that (part of) the refinement of the second action may occur before the execution of the first is completed.

The present paper continues the investigation on those lines, starting with branching time, truly concurrent models for Process Description Languages—the event structures of [20]. A set of events comes equipped with two binary relations of causality (an order usually denoted as ≤) and of conflict (an irreflexive symmetric relation persistent w.r.t. the order, usually written as †). The intuition is that when α < β at most one of the two can occur in the same execution, and that two events are concurrent if they are neither in the causal relation nor in conflict. On these structures we propose a notion of refinement where an event structure $E'$ is substituted for an event $a$ of another structure $E$. It is more liberal than similar proposals as in [6, 18, 9], in that we allow also the relations of causality and conflict that involve $a$ to be refined.

It is worth noting that, while the operations of refinement presented in [1, 6, 10, 9, 18, 15] preserve, in some algebraic sense, the two basic relations, the notion presented in this paper does not distribute in general over ≤ or †. In fact it is a more general construction than the others; but the basic construction from category theory involved in building the semantic domains is rather simple, and we believe it deserves further attention.

The basic construction considers the data of a refinement as a domain $D$ (of configurations of an event structure) and a functor $F: D \rightarrow \text{Dom}$ from the order category $D$ into some category of domains (to be specified later). The values of $F$ on the elements (= objects) of $D$ are the replacement domains and the values of $F$ on arrows $x \leq y$ in $D$ describe how to refine the relations of causality and conflict. With these data one can consider a fibration $\sum F \rightarrow D$; the category of sections turns out to be a poset, actually a domain under mild assumption on $F$.

The construction proposed in the paper implements a purely semantic notion of refinement. As mentioned above, it is a conservative extension of analogous proposals in [6, 9, 18], as these notions correspond to the case when the relations of causality and conflict are preserved under refinement (in a sense specified in section 3). Beside the notion