On the Composition of Hybrid Systems

Sébastien Bornot and Joseph Sifakis
Sebastien.Bornot@imag.fr Joseph.Sifakis@imag.fr

VERIMAG, 2 rue Vignate, 38610 Gières, France

1 Introduction

Concurrent systems can be usually specified as systems of communicating processes obtained by composing sequential processes by means of binary parallel composition operators. The latter express process interaction in terms of action composition. Their semantics is usually defined by two types of rules.

- Synchronization rules that specify how an action of the product process is defined as the result of the (simultaneous) occurrence of two actions in two component processes.
- Interleaving rules, that specify how an action of a component process is an action of the product process. These rules allow some component processes to be idle while the others progress.

Combining synchronization and interleaving rules is essential for the specification of systems as process coordination requires both synchronization and waiting. However, their adequate combination must satisfy two conflicting requirements:

Deadlock-freedom: Deadlocks may appear in the product process as a result of enforcing synchronization, for instance, when two processes are at states from which only non matching synchronization actions can be performed. Such deadlocks can be avoided by using "escape" transitions generated by application of interleaving rules. However, the presence of both synchronization and interleaving actions may imply non maximal progress.

Maximal progress: When synchronization of two actions is possible, interleaving rules, used precisely to avoid deadlocks, may be applicable. Maximal progress means that synchronization is preferred to interleaving when both are possible. This is sometimes achieved by using restriction or hiding operators that prune out interleaving actions.

The above problems are amplified for timed or hybrid systems where time progress is synchronous and waiting times are bounded. This can be easily observed when hybrid specifications are obtained by adding timing constraints to untimed communicating systems specifications, as it has been pointed out in [SY96].

In [SY96,BS97b] it is claimed that specifying time progress conditions independently from discrete transitions may be source of inconsistencies in specifications. We propose a model where time progress constraints are associated with
actions and thus time progress is directly related with the ability of a system to
perform actions. This model satisfies the property of time reactivity in the sense
that if no action is enabled at a state, time can progress.

Following the process algebra approach, we consider discrete (untimed) sys-
tems represented as terms generated from a set of abstract actions by using
operators such as prefixing, non deterministic choice and parallel composition.
We extend the semantics of these operators to hybrid actions.

For a given abstract action \( a \), a hybrid action extension of \( a \), is defined as a
triple \( (g_a, d_a, f_a) \) where \( g_a \) and \( d_a \) are unary predicates and \( f_a \) is a total function
on a continuous set of states. The predicate \( g_a \) is a guard characterizing the states
from which \( a \) is enabled while \( d_a \) is a deadline satisfied by all the enabling states
at which the action \( a \) becomes urgent (time progress is stopped). The function
\( f_a \) represents the effect of the action when it is executed.

As usually, for a given n-ary operator \( op \), the hybrid actions of the term
\( op(t_1, \ldots, t_n) \) are obtained by composing the hybrid actions of the arguments \( t_i \).

We show that the semantics of operators on abstract actions can be extended to
hybrid actions in different manners. The extensions have the same semantics for
discrete transitions but may differ in urgency (ability to perform actions within
a given delay).

We assume that parallel composition of two discrete systems can be expressed
as the non-deterministic choice of terms starting with interleaving or synchro-
nization actions (by means of some expansion theorem [BK85]). The expansion
theorem is extended to hybrid actions in the following manner :

- To guarantee maximal progress, non-deterministic choice is replaced by pri-
ority choice that gives higher priority to synchronization actions over inter-
leaving actions.
- Synchronization operators between abstract actions are extended to hybrid
actions. The guard and the deadline resulting from the synchronization of
two hybrid actions depend on the guards and deadlines of the synchronizing
hybrid actions. We show that for hybrid actions different synchronization
operations of practical interest can be defined by taking as synchronization
guards and deadlines modal formulas. In particular, we identify three im-
portant synchronization modes : AND-synchronization where the guards of
the synchronization action is the conjunction of the guards of the contribut-
ing actions. MAX-synchronization used to model synchronization with wait-
ing and for which the synchronization action occurs as soon as all of the
contributing actions have been completed. MIN-synchronization where the
synchronization action occurs as soon as one of the contributing actions is
completed.

The paper is organized as follows. In section 2, we define hybrid extensions of
discrete systems as a labeling homomorphism that extends prefixing and choice
operators. Section 3 presents a framework for parallel composition of hybrid
systems as an extension of parallel composition of untimed systems. For the