Modeling Hybrid Systems in Hy-*tccp*

Damián Adalid María del Mar Gallardo Laura Titolo
[damian,gallardo,laura.titolo]@lcc.uma.es

Dept. Lenguajes y Ciencias de la Computación
E.T.S.I. Informática University of Málaga*

Abstract. Concurrent, reactive and hybrid systems require quality modeling languages to be described and analyzed. The Timed Concurrent Constraint Language (*tccp*) was introduced as a simple but powerful model for reactive systems. In this paper, we present *hybrid tccp* (Hy-*tccp*), an extension of *tccp* over continuous time which includes new constructs to model the continuous dynamics of hybrid systems.

1 Introduction

Concurrent, reactive and hybrid systems have had a wide diffusion and they have become essential to an increasingly large number of applications. Often, systems of these kinds are safety critical, i.e., an error in the software can have tragic consequences. In the case of hybrid systems, the modeling and the analysis phases are particularly hard due to the combination of discrete and continuous dynamics and the presence of real variables. Many formalisms have been developed to describe concurrent systems. One of these is the *Concurrent Constraint paradigm* (*ccp*) [8]. It differs from other paradigms mainly due to the notion of store-as-constraint that replaces the classical store-as-valuation model. In this paradigm, the agents running in parallel communicate by means of a global constraint store. The *Timed Concurrent Constraint Language* [2] (*tccp* in short) is a concurrent logic language obtained by extending *ccp* with the notion of time and a suitable mechanism to model time-outs and preemptions.

In this paper, we present Hy-*tccp* an extension of *tccp* over continuous time. The declarative nature of Hy-*tccp* facilitates a high level description of hybrid systems in the style of hybrid automata [7]. Furthermore, its logical nature eases the development of semantics based program manipulation tools for hybrid systems (verifiers, analyzers, debuggers...). Parallel composition of hybrid automata is naturally supported in Hy-*tccp* due to the existence of a global shared store and to the synchronization mechanism.

The paper is organized as follows. In Section 2, we briefly introduce the language *tccp* and we show how we have extended it to obtain Hy-*tccp*. Section 3 contains an example to highlight the expressive power of our language. Finally, Section 4 concludes the paper and presents some related work.

* This work has been supported by the Andalusian Excellence Project P11-TIC7659 and the Spanish Ministry of Economy and Competitiveness project TIN2012-35669

2 Hy-*tccp*: a hybrid extension of *tccp*

The *Timed Concurrent Constraint Language* (*tccp*, [2]) is a time extension of *ccp* suitable for describing concurrent and reactive systems. The computation in *tccp* proceeds as the concurrent execution of several agents that can monotonically add information in a global constraint *store*, or query information from it. *tccp* is parametric w.r.t. a *cylindric constraint system* which handles the information on system variables. Briefly, a cylindric constraint system is a structure $\mathbf{C} = \langle \mathcal{C}, \vdash, \wedge, \mathit{false}, \mathit{true}, \mathit{Var}, \exists \rangle$ composed by a set of constraints $\mathcal{C}$ ordered by the entailment relation $\vdash$ (intuitively, $c \vdash d$ if c contains more information than d) where $\wedge$ is a binary operator that merges the information from two constraints; *false* and *true* are, respectively, the greatest and the least element of $\mathcal{C}$; *Var* is a denumerable set of variables and $\exists$ existentially quantifies variables over constraints. The syntax of agents is given by the grammar:

$$A ::= \mathsf{stop} \mid \mathsf{tell}(c) \mid A \parallel A \mid \exists x\, A \mid \textstyle\sum_{i=1}^{n} \mathsf{ask}(c_i) \rightarrow A \mid \mathsf{now}\ c\ \mathsf{then}\ A\ \mathsf{else}\ A \mid p(\bar{x})$$

where c, $c_1, \ldots, c_n$ are finite constraints in $\mathcal{C}$, $\bar{x} \in \mathit{Var} \times \cdots \times \mathit{Var}$ and p is a predicate symbol. A *tccp* program is a pair $D.A$, where A is the initial agent and D is a set of *process declarations* of the form $p(\bar{x}) :- A$. The notion of time is introduced by defining a *discrete* global clock. The *operational semantics* of *tccp* [2] is described by a transition system $T = (\mathit{Conf}, \rightarrow)$. Configurations in *Conf* are pairs $\langle A, c \rangle$ representing the agent A to be executed in the current global store c. The transition relation $\rightarrow \subseteq \mathit{Conf} \times \mathit{Conf}$ is the least relation satisfying the rules in Figure 1. As can be seen from the rules, the stop agent represents the successful termination of the computation. The $\mathsf{tell}(c)$ agent adds the constraint c to the current store. The choice agent $\sum_{i=1}^{n} \mathsf{ask}(c_i) \rightarrow A_i$ non-deterministically executes one of the agents A_i whose corresponding guard c_i is entailed by the store; otherwise, if no guard is entailed by the store, the agent suspends. The conditional agent now c then A else B behaves like A (respectively B) if c is (respectively is not) entailed by the store. $A \parallel B$ models the parallel composition of A and B in terms of maximal parallelism, i.e., all the enabled agents of A and B are executed at the same time. The agent $\exists x\, A$ makes variable x local to A. Finally, the agent $p(\bar{x})$ takes from D a declaration of the form $p(\bar{x}) :- A$ and then executes A.

We introduce the language Hy-*tccp*, which subsumes *tccp* and includes new agents to model hybrid systems in the style of hybrid automata. Hybrid automata [7] are an extension of finite-state automata. Intuitively, their discrete behavior is defined by means of a finite set of discrete states (called *locations*) and a set of (instantaneous) *discrete transitions* from one location to another. The continuous behavior of hybrid automata is described at each location by some Ordinary Differential Equations (ODEs) which describe how continuous variables evolve over time (*continuous transitions*). Each location is associated

[1] The auxiliary agent $\exists^{l} x\, A$ makes explicit the local store l of A. This auxiliary agent is linked to the principal hiding construct by setting the initial local store to *true*, thus $\exists x\, A := \exists^{\mathit{true}} x\, A$.

$$\frac{}{\langle \mathsf{tell}(c),\, d\rangle \to \langle \mathsf{stop},\, c \wedge d\rangle} \qquad \frac{\exists\, 1 \le j \le n,\, d \vdash c_j}{\langle \sum_{i=1}^{n} \mathsf{ask}(c_i) \to A_i,\, d\rangle \to \langle A_j,\, d\rangle}$$

$$\frac{\langle A,\, d\rangle \to \langle A',\, d'\rangle,\; d \vdash c}{\langle \mathsf{now}\ c\ \mathsf{then}\ A\ \mathsf{else}\ B,\, d\rangle \to \langle A',\, d'\rangle} \qquad \frac{\langle A,\, d\rangle \not\to,\; d \vdash c}{\langle \mathsf{now}\ c\ \mathsf{then}\ A\ \mathsf{else}\ B,\, d\rangle \to \langle A,\, d\rangle}$$

$$\frac{\langle B,\, d\rangle \to \langle B',\, d'\rangle,\; d \nvdash c}{\langle \mathsf{now}\ c\ \mathsf{then}\ A\ \mathsf{else}\ B,\, d\rangle \to \langle B',\, d'\rangle} \qquad \frac{\langle B,\, d\rangle \not\to,\; d \nvdash c}{\langle \mathsf{now}\ c\ \mathsf{then}\ A\ \mathsf{else}\ B,\, d\rangle \to \langle B,\, d\rangle}$$

$$\frac{\langle A,\, d\rangle \to \langle A',\, d'\rangle \quad \langle B,\, d\rangle \to \langle B',\, c'\rangle}{\langle A \parallel B,\, d\rangle \to \langle A' \parallel B',\, d' \wedge c'\rangle} \qquad \frac{\langle A,\, d\rangle \to \langle A',\, d'\rangle \quad \langle B,\, d\rangle \not\to}{\langle A \parallel B,\, d\rangle \to \langle A' \parallel B,\, d'\rangle}$$

$$\frac{\langle A,\, l \wedge \exists_x\, d\rangle \to \langle B,\, l'\rangle}{\langle \exists^{l} x\, A,\, d\rangle \to \langle \exists^{l'} x\, B,\, d \wedge \exists_x\, l'\rangle} \qquad \frac{p(\bar{x}) \coloneq A \in D}{\langle p(\bar{x}),\, d\rangle \to \langle A,\, d\rangle}$$

Fig. 1. The transition system for *tccp*.[1]

with an *invariant* predicate which constrains the value of the continuous variables at that location and with an *initial* predicate that establishes their possible initial values. Discrete transitions are associated with a *jump* predicate that may include a *guard* and a *reset* predicate which updates the value and/or the flow of continuous variables.

Hy-*tccp* uses a *tccp* monotonic store (called *discrete store*) to model the information about the current location and the associated invariants. Discrete transitions of hybrid automata are modeled as instantaneous transitions in Hy-*tccp* and they are used to synchronize parallel agents. We distinguish the set of discrete variables Var, whose information is accumulated monotonically, and the set of continuous variables $\widetilde{Var}$, whose values change continuously over time ($Var \cap \widetilde{Var} = \varnothing$). Constraints in $\mathcal{C}$ are now defined over $Var \cup \widetilde{Var}$. The *tccp* store is extended by adding a component called *continuous store*. The continuous store is not monotonic, instead it records the dynamical evolution of the continuous variables. Thus, a Hy-*tccp* store is a pair $\langle c, \tilde{c}\rangle$ where c (discrete store) is a monotonic constraint store as in *tccp* and $\tilde{c}$ (continuous store) is a function that associates a continuous variable with its current value and its flow[2], which indicates how its value changes over time by means of an ODE. Given a continuous store $\tilde{c}$ and a continuous variable x, $\tilde{c}(x) = \langle v, f\rangle$ means that x has value v and flow f. Given $\tau \in \mathbb{R}_{>0}$ and $inv \in \mathcal{C}$ we denote as $\langle c, \tilde{c}\rangle \rightsquigarrow_{\tau}^{inv} \langle c, \tilde{c}_{\tau}\rangle$ the projection of the store $\langle c, \tilde{c}\rangle$ at time τ satisfying inv. The value of the variables are updated at time τ, while the flows are unchanged. In order to model behaviors typical of hybrid systems we introduce two new agents w.r.t. *tccp*: change and $\widetilde{\mathsf{ask}}$. The agent change updates the value and/or the flow of a given continuous variable (*reset* predicate of hybrid automata). The *tccp* choice agent is extended by allowing the non-deterministic choice between discrete and continuous transitions in the following way: $\sum_{i=1}^{n} \mathsf{ask}(c_i) \to A_i + \sum_{j=1}^{m} \widetilde{\mathsf{ask}}(inv_j)$ where

[2] In this paper, we assume that continuous variables evolve independently from each other. Given $x \in \widetilde{Var}$, its flow is defined as a predicate on set $\{x, \dot{x}\}$ where $\dot{x}$ denotes the first order derivative of x (e.g. $\dot{x} = 2$ or $\dot{x} = 2x$).

$$\frac{}{\langle \mathsf{change}(x, v, f),\ d,\ \tilde{d}\rangle \rightarrow_\sigma \langle \mathsf{stop},\ d,\ \tilde{d} \lhd (x \mapsto (v, f))\rangle} \quad (\mathbf{R1})$$

$$\frac{\exists\, 1 \leq k \leq m,\ \tau \in \mathbb{R}^+ .\ \langle d,\ \tilde{d}\rangle \rightsquigarrow_\tau^{inv_j} \langle d,\ \tilde{d}_\tau\rangle}{\langle \sum_{i=1}^{n} \mathsf{ask}(c_i) \rightarrow A_i + \sum_{j=1}^{m} \widetilde{\mathsf{ask}}(inv_j),\ d,\ \tilde{d}\rangle \rightarrow_\tau \langle \sum_{i=1}^{n} \mathsf{ask}(c_i) \rightarrow A_i + \sum_{j=1}^{m} \widetilde{\mathsf{ask}}(inv_j),\ d,\ \tilde{d}_\tau\rangle} \quad (\mathbf{R2})$$

$$\frac{\langle A,\ d,\ \tilde{d}\rangle \rightarrow_\tau \langle A,\ d,\ \tilde{d}'\rangle \quad \langle B,\ d,\ \tilde{d}\rangle \rightarrow_\tau \langle B,\ d,\ \tilde{d}'\rangle}{\langle A \parallel B,\ d,\ \tilde{d}\rangle \rightarrow_\tau \langle A \parallel B,\ d,\ \tilde{d}'\rangle} \quad (\mathbf{R3})$$

$$\frac{\langle A,\ d,\ \tilde{d}\rangle \rightarrow_\sigma \langle A',\ d',\ \tilde{d}'\rangle \quad \langle B,\ d,\ \tilde{d}\rangle \rightarrow_\tau \langle B,\ d,\ \tilde{d}''\rangle}{\langle A \parallel B,\ d,\ \tilde{d}\rangle \rightarrow_\sigma \langle A' \parallel B,\ d',\ \tilde{d}'\rangle} \quad (\mathbf{R4})$$

Fig. 2. The transition system for Hy-*tccp*.

$n \geq 0$ and $m \geq 0$. Here, the $\widetilde{\mathsf{ask}}$ branches can be non-deterministically selected in case the invariant inv_j is entailed in the current store. This corresponds to the passage of continuous time in a hybrid automaton location. The continuous variables evolve over *continuous* time while inv_j holds and until another ask branch is selected. The *operational semantics* of Hy-*tccp* is described by a transition system $T = (\widetilde{Conf}, \rightarrow_\sigma, \rightarrow_\tau)$. Configurations in $\widetilde{Conf}$ are triple $\langle A, c, \tilde{c}\rangle$ representing the agent A to be executed in the current extended store $\langle c, \tilde{c}\rangle$. The transition relation $\rightarrow_\sigma \subseteq \widetilde{Conf} \times \widetilde{Conf}$ represents a *tccp* discrete transition whose execution is instantaneous, while $\rightarrow_\tau \subseteq \widetilde{Conf} \times \widetilde{Conf}$ models a continuous transition of duration τ. In Figure 2 we describe the rules that we have added to the operational semantics of *tccp* in order to deal with continuous time and variables. In Rule **R1** the agent `change` uses the operator $\lhd$ that, given a continuous store $\tilde{c}$ and a triple (x, v, f), updates $\tilde{c}$ with a new initial value v and a new flow f for the variable x. In Rule **R2** time passes continuously while one of the $\widetilde{\mathsf{ask}}$ invariants holds in the store and the values of the continuous variables change over time following their flow. Rule **R3** represents the parallel execution of two continuous transitions, note that their duration must coincide. Rule **R4** expresses the parallel composition of a discrete and a continuous transition. In this case, the discrete transition is executed before the continuous one.

3 Example: a dam management system

In this section we model a dam management system with Hy-*tccp* (Figure 3). Our experience in this area [4] has shown us that this is a realistic and significant example to demonstrate the expressive power and usability of our language. Due to the monotonicity of the discrete constraint store, streams (written in a list-fashion way) are used to model *imperative-style* variables [2]. Our dam controller system is modeled as the parallel composition of a controller, a supplier and two gate processes[3]. *Vol* represents the total amount of water, it has initial value *INITVOL* and flow 0 (i.e., its value is constant over time). T represents a timer used by the `supplier`, it has initial value 0 and flow 1, thus it evolves

[3] The code of `gate` is omitted due to space limitations.

lineary over time. When T reaches the value 3600, the `supplier` sends to the `controller` the value of the new inflow of water through the input channel In. At this point, the `controller` checks to which interval the current volume of water (Vol) belongs. Intervals are defined by using several sub-indexed constants $THRESHOLD_i$. According to the current value of Vol, the `controller` sends a signal to each gate through the output channels $ToG1$ and $ToG2$ in order to set their status. At the same time, the continuous store is updated. We use the symbol _ in the second argument of agent `change` to indicate that only the flow of Vol is updated, while its value is unchanged. The new flow of Vol depends on the new inflow received from the `supplier` ($NewIn$) and on a value representing the water discharged through the gates. This value is computed by the function Out according to the current state of the gates. It is worth noting that the $\widetilde{\mathsf{ask}}$ construct in `supplier` is used to make time pass. Its invariant ensures that T never exceeds the value 3600.

$$
\begin{array}{l}
\texttt{init}\text{:-}\ \exists\ In,\ ToG1,\ ToG2,\ Vol, T\big(\mathsf{change}(\,T, 0, \dot{T}{=}1)\ \|\ \texttt{supplier}(T,\ In)\ \|\ \mathsf{tell}(\,Vol{\leq}THRESHOLD_3)\ \| \\
\quad \mathsf{change}(\,Vol, INITVOL, \dot{Vol}{=}0)\ \|\ \texttt{controller}(\,Vol, In,\ ToG1,\ ToG2)\ \|\ \texttt{gate}(\,ToG1)\ \|\ \texttt{gate}(\,ToG2)\big) \\
\\
\texttt{controller}(\,Vol, In,\ ToG1,\ ToG2) :\text{-}\ \exists NewIn,\ ToG1',\ ToG2',\ In'\big(\\
\quad \mathsf{ask}(\,In{=}[\,NewIn|\_\,]) \rightarrow \big(\,\mathsf{tell}(\,In{=}[\,NewIn|In'\,])\ \| \\
\qquad \mathsf{ask}(\,Vol{\leq}THRESHOLD_1) \rightarrow (\mathsf{tell}(\,ToG1{=}[\,close|\,ToG1'\,])\ \|\ \mathsf{tell}(ToG2{=}[\,close|ToG2'\,])\ \| \\
\qquad\quad \mathsf{change}(\,Vol, \_, \dot{Vol}{=}NewIn{-}Out(close, close))\ \|\ \texttt{controller}(\,Vol, In',\ ToG1',\ ToG2')) \\
\qquad +\mathsf{ask}(\,Vol{>}THRESHOLD_1 \wedge Vol{\leq}THRESHOLD_2) \rightarrow (\mathsf{tell}(ToG1{=}[halfOpen|ToG1'\,])\ \| \\
\qquad\quad \mathsf{tell}(\,ToG2{=}[halfOpen|ToG2'\,])\ \|\ \mathsf{change}(\,Vol, \_, \dot{Vol}{=}NewIn{-}Out(halfOpen, halfOpen))\ \| \\
\qquad\quad \texttt{controller}(\,Vol, In',\ ToG1',\ ToG2')) \\
\qquad +\mathsf{ask}(\,Vol{>}THRESHOLD_2 \wedge Vol{<}THRESHOLD_3) \rightarrow (\mathsf{tell}(\,ToG1{=}[halfOpen|\,ToG1'\,])\ \| \\
\qquad\quad \mathsf{tell}(\,ToG2{=}[\,open|\,ToG2'\,])\ \|\ \mathsf{change}(\,Vol, \_, \dot{Vol}{=}NewIn{-}Out(halfOpen, open))\ \| \\
\qquad\quad \texttt{controller}(\,Vol, In',\ ToG1',\ ToG2'))\big) \\
\quad +\mathsf{ask}(\,Vol{=}THRESHOLD_3) \rightarrow \big(\,\mathsf{tell}(\,ToG1{=}[\,open|\,ToG1'\,])\ \|\ \mathsf{tell}(\,ToG2{=}[\,open|\,ToG2'\,])\ \| \\
\qquad\quad \mathsf{change}(\,Vol, \_, \dot{Vol}{=}{-}Out(open, open))\ \|\ \texttt{controller}(\,Vol, In,\ ToG1',\ ToG2'))\big)\big) \\
\\
\texttt{supplier}(T,\ In) :\text{-}\ \exists In'\big(\,\widetilde{\mathsf{ask}}(T{\leq}3600) \\
\quad +\mathsf{ask}(T{=}3600) \rightarrow (\mathsf{tell}(In{=}[Random(0, 350)|In'\,])\ \|\ \mathsf{change}(T, 0, \dot{T}{=}1)\ \|\ \texttt{supplier}(T,\ In'))\big)
\end{array}
$$

Fig. 3. HY-*tccp* model for a dam management system

4 Conclusions and Related Work

In this paper we have presented HY-*tccp*, an extension of *tccp* over continuous time, with the aim of modeling hybrid systems in a simple and declarative way. The language is parametric to both, the cylindric constraint system used to manage the discrete behavior, and the class of differential equation solvers that models the continuous behavior. Although we are aware that the decidability limits of hybrid systems [7] lie on the class of initialized rectangular systems, in this paper we have only restricted the class of differential equations used by assuming that the dynamics of a continuous variable does not depend on the others. In this way we obtain a more general framework.

In [6], *hcc* was introduced as the first extension over continuous time of the concurrent constraint paradigm. Although both Hy-*tccp* and *hcc* are declarative languages with a logical nature, they have some important differences. Hy-*tccp* has been defined as a modeling language for hybrid systems in the style of hybrid automata. Unlike *hcc*, which is deterministic, Hy-*tccp* provides the non-deterministic choice agent which allows the transitions of hybrid automata to be expressed as a list of ask and $\widetilde{\text{ask}}$ branches. Furthermore, in *hcc*, the information on the value and flow of continuous variables is modeled as a constraint of the underlying continuous constraint system. On the contrary, in Hy-*tccp*, there is a clear distinction between discrete and continuous variables. The process algebra *Hybrid Chi* [1] shares with Hy-*tccp* the separation between discrete and continuous variables, the synchronous nature and the concept of delayable guard (corresponding to the suspension of the non-deterministic choice). In [3], *HyPa* is introduced as an extension of the process algebra *ACP*. It differs from *Hybrid Chi* mainly in the way time-determinism is treated, and in the modeling of time passing.

In the future we plan to develop a framework for the description and simulation of Hy-*tccp* programs. We are also interested in defining a translation rules system from Hy-*tccp* to hybrid automata and viceversa. Furthermore, we plan to use model checking and abstract interpretation to verify temporal properties of hybrid systems written in Hy-*tccp* (as done in [5] for SPIN).

References

1. van Beek, D.A., Man, K.L., Reniers, M.A., Rooda, J.E., Schiffelers, R.R.H.: Syntax and consistent equation semantics of hybrid chi. Journal of Logic and Algebraic Programming 68(1-2), 129–210 (2006)
2. de Boer, F.S., Gabbrielli, M., Meo, M.C.: A Timed Concurrent Constraint Language. Information and Computation 161(1), 45–83 (2000)
3. Cuijpers, P.J.L., Reniers, M.A.: Hybrid process algebra. Journal of Logic and Algebraic Programming 62(2), 191–245 (2005)
4. Gallardo, M.M., Merino, P., Panizo, L., Linares, A.: A practical use of model checking for synthesis: generating a dam controller for flood management. Software: Practice and Experience 41, 1329–1347 (2011)
5. Gallardo, M.M., Panizo, L.: Extending Model Checkers for Hybrid System Verification: the case study of SPIN. Software Testing, Verification and Reliability (2013)
6. Gupta, V., Jagadeesan, R., Saraswat, V.A., Bobrow, D.: Programming in hybrid constraint languages. In: Antsaklis, P., Kohn, W., Nerode, A., Sastry, S. (eds.) Hybrid Systems II. Lecture Notes in Computer Science, vol. 999, pp. 226–251. Springer (1994)
7. Henzinger, T.A.: The theory of hybrid automata. In: Proceedings of the 11th Annual IEEE Symposium on Logic in Computer Science. pp. 278–292. LICS '96, IEEE Computer Society, Washington, DC, USA (1996)
8. Saraswat, V.A.: Concurrent Constraint Programming Languages. Ph.D. thesis, Pittsburgh, PA, USA (1989)