A Process Algebra for Hybrid Systems

Jan Joris Vereijken

Department of Computing Science, Eindhoven University of Technology,
P.O. Box 513, NL-5600 MB Eindhoven, The Netherlands

http://www.win.tue.nl/win/cs/fm/janjoris/
janjoris@acm.org

May 10, 1995

1 Introduction

The work that is presented here was initiated by question of a colleague from the mechanical engineering department. He was analysing several industrial manufacturing processes (a tire production line, a cookie baking line, etc.). These processes were modeled in a procedural kind of programming language (called "χ" [AvdMR94]) extended with hybrid features such as continuous variables defined by differential equations. Having specified the process by such a program, analysis then proceeded by means of simulation.

Typically, they would design a production line, and then test it by building it on a small scale to see whether it worked. So a problem would first be found on the actual production line ("valve 4C gets clogged with coagulated cookie mix"). They would try to recreate that problematic situation in their simulation tool. Then an ad-hoc solution would be found in the simulator ("if we heat the cookie mix a bit more it will not coagulate"), and finally the physical production line would be modified to reflect the "improvement". This cycle was repeated over and over again, until confidence in the production line design had grown enough to justify substantial investments in a large scale production line.

This method (of course?) proved unsatisfactory for systems larger than some critical size: the "debugging cycle" for a production line needed to be repeated ad infinitum, with each "improvement" prompting more problems than it solved.

So although they were very precise and formal in specifying their processes, these specifications were then not used in any kind of formal analysis. This seemed very wasteful; so the idea arose to find a translation from the language χ to an (ACP-style) process algebra [BW90]. In that way the tedious simulation driven analysis could be replaced by, or at least augmented with, a hopefully less tedious formal analysis by process algebraic means.

With the purpose described above in mind, we created an ACP-style process algebra named $\mathrm{ACP}_{\mathrm{hs}}$ ("ACP for hybrid systems") that incorporates hybrid features. As our final goal is easy translation from the language χ to $\mathrm{ACP}_{\mathrm{hs}}$, we focused on the ease of specifying in an intuitive way, and power to specify in a way close to χ. Sometimes, this approach forced us to make compromises on the mathematical elegance of $\mathrm{ACP}_{\mathrm{hs}}$, and sometimes it resulted in some axioms and proofs being longer and messier than would have been necessary had we focused on theoretical beauty only. On the whole however, we believe we have created an process algebra that is both easy enough to specify in, and not too complicated to reason with.

2 Methodology

In this section we will delve a bit deeper in the technical details of $\mathrm{ACP}_{\mathrm{hs}}$. Historically speaking, $\mathrm{ACP}_{\mathrm{hs}}$ is very much a combination of two previously existing process algebras, namely

$ACP_{\rho\surd I}$ [BB95] and ACP_{ps} [BB94].

$ACP_{\rho\surd I}$ is a process algebra that provides real-time actions (for example "$a(7)$", meaning: perform action a at time 7), allowing specification in either absolute time, relative time, or both. Furthermore, it allows so called "urgent actions", which are actions that occur one after another without any time passing in between (for example "$a(7) \cdot b(7)$", meaning: perform action a at time 7, and then perform action b, also at time 7). Finally, it provides "integration", which denotes a sum over a continuum of alternatives (for example $\int_{v\in[1,2]} a(v)$, meaning: perform action a somewhere in the time interval $[1,2]$).

ACP_{ps} is a process algebra that provides "signals", where a signal describes a the visible part of the current state (for example "$(x = 3) \curvearrowright a$", meaning: in the state, $x = 3$ holds until the execution of a). Furthermore, it provides conditions (for example $(x = 3) :\rightarrow b$, meaning: execute b only if $x = 3$).

When combining these two process algebras, one has to extend the signals and conditions with a capability to refer to time, and all the time operators need to be extended to the presence of signals and conditions. In this way, one can denote processes like:

$$(P(t) = 3 + t) \curvearrowright \int_{v\in[2,5]} (P(t) = 7) :\rightarrow a(v)$$

meaning: the pressure ("$P(t)$") in the system equals 3 plus the current time ("t"), now perform action a somewhere in the interval $[2,5]$, at a point where $P(t)$ equals 7. As this condition is only true at time point $t = 4$ the above expression simplifies to:

$$(P(t) = 3 + t) \curvearrowright a(4)$$

In our full article we provide axioms for ACP_{hs} that algebraically define which expressions can be rewritten into each other. The purpose of this is to allow one to specify the expected behavior of a process ("the line produces cookies") and the actual implementation of a process ("the cookie production line works as follows...") both in ACP_{hs}. If one then can show, by algebraic means, that both specifications denote the same process, one has proven that the given implementation satisfies the intended behavior.

Furthermore, we give a Plotkin-style structured operational semantics for all operators of ACP_{hs}, and define a notion of (strong) bisimulation.

We also give some theorems (for example an expansion theorem) that we have found convenient when tackling problems of some size. The full article concludes by applying the described techniques to a few problems of varying size.

3 Small example

To give an global impression of how such a analysis proceeds, we show a small example. The system we chose is a simple, almost trivial, heater and thermostat system that controls the temperature in a certain room.

We have a heater, which when turned on heats the room by 1 °C per hour. When it is off, the room cools down by 1 °C per hour (through warmth leakage to the outside). There is a thermostat that turns the heater off if the temperature reaches 22 °C and turns the heater back on when the temperature reaches 18 °C. The system is started with a room temperature of 0 °C and the heater on.

We will analyze this system using both absolute time (syntactically recognizable by the round parentheses) and relative time (recognizable by the square brackets).

3.1 Specification (absolute time)

We first specify our heater-thermostat system (HT) using absolute time, i.e. all time stamps refer to the absolute time, the time that has elapsed since the system was started. This leads to the specification of Table 1 on the following page, which we will now explain step by step.

$$
\begin{aligned}
\text{Heater} &= H_{\text{on}}(0) \\
H_{\text{on}}(u) &= \int_{v=u}^{\infty} r_{\text{off}}(v) \cdot \text{off}_1(v) \cdot H_{\text{off}}(v) \\
H_{\text{off}}(u) &= \int_{v=u}^{\infty} r_{\text{on}}(v) \cdot \text{on}_1(v) \cdot H_{\text{on}}(v)
\end{aligned}
$$

$$
\begin{aligned}
\text{Thermostat} &= T_{\text{cold}}(0) \\
T_{\text{cold}}(u) &= \int_{v=u}^{\infty} (T(t) = 22) :\!\rightarrow s_{\text{off}}(v) \cdot T_{\text{warm}}(v) \\
T_{\text{warm}}(u) &= \int_{v=u}^{\infty} (T(t) = 18) :\!\rightarrow s_{\text{on}}(v) \cdot T_{\text{cold}}(v)
\end{aligned}
$$

$$
\begin{aligned}
S &= S'(0) \\
S'(u) &= \int_{v=u}^{\infty} \text{off}_2(v) \cdot \left(\frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright S''(v) \\
S''(u) &= \int_{v=u}^{\infty} \text{on}_2(v) \cdot \left(\frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright S'(v)
\end{aligned}
$$

$$
\begin{aligned}
H &= \{r_{\text{off}}, s_{\text{off}}, r_{\text{on}}, r_{\text{off}}, \text{on}_1, \text{on}_2, \text{off}_1, \text{off}_2\} \\
C &= \{r_{\text{off}} \mid s_{\text{off}} = c_{\text{off}}, r_{\text{on}} \mid s_{\text{on}} = c_{\text{on}}, \text{off}_1 \mid \text{off}_2 = \text{off}, \text{on}_1 \mid \text{on}_2 = \text{on}\}
\end{aligned}
$$

$$
\text{HT} = \left(T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright \partial_H(\text{Heater} \parallel \text{Thermostat} \parallel S)
$$

Table 1: Heater and Thermostat, absolute time version.

As can be seen, HT consists of three components, running in parallel: the component "Heater", which models the heater, the component "Thermostat" which models the thermostat, and the component "S", which models the "characteristics of the heater and the room" (namely the facts that with the heater on, the temperature rises by 1 °C per hour, and with the heater off, it falls by 1 °C per hour).

The component "Heater" works as follows. The initial state of the heater is "on" at time 0 ("Heater = $H_{\text{on}}(0)$"). When the heater is in the state "on" at time u ("$H_{\text{on}}(u)$"), it first tries to execute the action r_{off} between time 0 and ∞ (implemented by the integral from 0 to ∞). As this action r_{off} synchronizes with s_{off}, it can only be done when the "Thermostat" component is willing to do s_{off}. Intuitively: the heater can only execute r_{off} when the thermostat measures the room temperature to be 22 °C. When the heater eventually executes this synchronizing action r_{off} at time v, it knows that the temperature is 22 °C, and stop heating at the same moment v ("$\text{off}_1(v)$", note that this is an urgent action). The heater then continues in the state "off", at time current time v ("$H_{\text{off}}(v)$"). This subcomponent H_{off} works in a similar way as H_{on}, with the roles of "off" and "on" interchanged.

Then the component "Thermostat". It has two main states: "T_{cold}" and "T_{warm}". In the state "T_{cold}", the thermostat is measuring the temperature until it becomes 22°C ("$(T(t) = 22) :\!\rightarrow$"). When that happens, the thermostat (immediately) performs the action s_{off}, which synchronizes with the r_{off} action of the heater, as described above. After that, the thermostat is in the state "T_{warm}", which is similar to "T_{cold}", albeit that it now waits for the temperature to drop to 18°C.

This leaves us with component "S". As said, this component models the "characteristics of the heater and the room", namely the facts that with the heater on, the temperature rises by 1 °C per hour, and with the heater off, it falls by 1 °C per hour. It does this by trying to

execute "off_2" and "on_2" actions, which synchronize with the "off_1" and "on_1" actions of the heater, as described above. As a result the "S" component knows exactly when the heater is being turned on and off. When the heater turns off, S' emits the signal "$\frac{\mathrm{d}T}{\mathrm{d}t} = -1$" into the system, signifying that the temperature is now dropping by 1°C per hour. Mutatis mutandis, S'' emits the signal "$\frac{\mathrm{d}T}{\mathrm{d}t} = 1$" to signify that the temperature is rising when the heater turns on.

The complete system now consists of the components "Heater", "Thermostat", and "S" running in parallel:

$$\mathrm{HT} = \left(T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright \partial_H(\text{Heater} \parallel \text{Thermostat} \parallel S)$$

As can be seen, the system starts in an initial state where the temperature is 0°C ("$T(0) = 0$"), rising by 1°C per hour ("$\frac{\mathrm{d}T}{\mathrm{d}t} = 1$").

3.2 Analysis (absolute time)

We will now analyze the specification given in Table 1 by linearizing it. By means of an expansion theorem (not given in this abstract, see the full paper) we determine for every state we reach the enabled actions. As it turns out, in every state there is exactly one enabled action, so we can algebraically rewrite our specification (by the expansion theorem, which follows from the axioms) into an equivalent one that just contains sequential composition (this is much stronger than "merely" linear). The calculation is given below:

$$\begin{aligned}
\mathrm{HT} &= \left(T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright \partial_H(\text{Heater} \parallel \text{Thermostat} \parallel S) \\
&= \left(T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright \partial_H(H_{\text{on}}(0) \parallel T_{\text{cold}}(0) \parallel S'(0)) \\
&= \left(T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright c_{\text{off}}(22) \cdot (T(22) = 22) \curvearrowright \\
&\quad \partial_H(\text{off}_1(22) \cdot H_{\text{off}}(22) \parallel T_{\text{warm}}(22) \parallel S'(22)) \\
&= \left(T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright c_{\text{off}}(22) \cdot (T(22) = 22) \curvearrowright \text{off}(22) \cdot \\
&\quad (T(22) = 22) \curvearrowright \partial_H\left(H_{\text{off}}(22) \parallel T_{\text{warm}}(22) \parallel \left(\frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright S''(22)\right) \\
&= \left(T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright c_{\text{off}}(22) \cdot (T(22) = 22) \curvearrowright \text{off}(22) \cdot \\
&\quad \left(T(22) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright \\
&\quad \partial_H\left(H_{\text{off}}(22) \cdot T_{\text{warm}}(22) \parallel \left(\frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright S''(22)\right) \\
&= \left(T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright c_{\text{off}}(22) \cdot (T(22) = 22) \curvearrowright \text{off}(22) \cdot \mathrm{HT}_{\text{warm}}(22) \\
\mathrm{HT}_{\text{warm}}(u) &= \left(T(u) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright \partial_H\left(H_{\text{off}}(u) \parallel T_{\text{warm}}(u) \parallel \left(\frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright S''(u)\right) \\
&= \left(T(u) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright c_{\text{on}}(u+4) \cdot (T(u+4) = 18) \curvearrowright \\
&\quad \partial_H\left(\text{on}_1(u+4) \cdot H_{\text{on}}(u+4) \parallel T_{\text{cold}}(u+4) \parallel \left(\frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright S''(u+4)\right) \\
&= \left(T(u) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright c_{\text{on}}(u+4) \cdot (T(u+4) = 18) \curvearrowright \\
&\quad \text{on}(u+4) \cdot (T(u+4) = 18) \curvearrowright \\
&\quad \partial_H\left(H_{\text{on}}(u+4) \parallel T_{\text{cold}}(u+4) \parallel \left(\frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright S'(u+4)\right)
\end{aligned}$$

$$
\begin{aligned}
&= \left(T(u) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright c_{\mathrm{on}}(u+4) \cdot (T(u+4) = 18) \curvearrowright \\
&\quad \mathrm{on}(u+4) \cdot \left(T(u+4) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright \\
&\quad \partial_H \left(H_{\mathrm{on}}(u+4) \parallel T_{\mathrm{cold}}(u+4) \parallel \left(\frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright S'(u+4)\right) \\
&= \left(T(u) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright c_{\mathrm{on}}(u+4) \cdot (T(u+4) = 18) \curvearrowright \\
&\quad \mathrm{on}(u+4) \cdot \mathrm{HT}_{\mathrm{cold}}(u+4) \\
\mathrm{HT}_{\mathrm{cold}}(u) &= \left(T(u) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright \partial_H \left(H_{\mathrm{on}}(u) \parallel T_{\mathrm{cold}}(u) \parallel \left(\frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright S''(u)\right) \\
&= \left(T(u) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright c_{\mathrm{off}}(u+4) \cdot (T(u+4) = 22) \curvearrowright \\
&\quad \partial_H \left(\mathrm{off}_1(u+4) \cdot H_{\mathrm{off}}(u+4) \parallel T_{\mathrm{warm}}(u+4) \parallel \left(\frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright S'(u+4)\right) \\
&= \left(T(u) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright c_{\mathrm{off}}(u+4) \cdot (T(u+4) = 22) \curvearrowright \\
&\quad \mathrm{off}(u+4) \cdot (T(u+4) = 22) \curvearrowright \\
&\quad \partial_H \left(H_{\mathrm{off}}(u+4) \parallel T_{\mathrm{warm}}(u+4) \parallel \left(\frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright S''(u+4)\right) \\
&= \left(T(u) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright c_{\mathrm{off}}(u+4) \cdot (T(u+4) = 22) \curvearrowright \\
&\quad \mathrm{off}(u+4) \cdot \left(T(u+4) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright \\
&\quad \partial_H \left(H_{\mathrm{off}}(u+4) \parallel T_{\mathrm{warm}}(u+4) \parallel \left(\frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright S''(u+4)\right) \\
&= \left(T(u) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright c_{\mathrm{off}}(u+4) \cdot (T(u+4) = 22) \curvearrowright \\
&\quad \mathrm{off}(u+4) \cdot \mathrm{HT}_{\mathrm{warm}}(u+4)
\end{aligned}
$$

Throwing away the intermediate steps, this brings us to the following system of three equations:

$$
\begin{aligned}
\mathrm{HT} &= \left(T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright c_{\mathrm{off}}(22) \cdot (T(22) = 22) \curvearrowright \mathrm{off}(22) \cdot \mathrm{HT}_{\mathrm{warm}}(22) \\
\mathrm{HT}_{\mathrm{warm}}(u) &= \left(T(u) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright c_{\mathrm{on}}(u+4) \cdot (T(u+4) = 18) \curvearrowright \\
&\quad \mathrm{on}(u+4) \cdot \mathrm{HT}_{\mathrm{cold}}(u+4) \\
\mathrm{HT}_{\mathrm{cold}}(u) &= \left(T(u) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright c_{\mathrm{off}}(u+4) \cdot (T(u+4) = 22) \curvearrowright \\
&\quad \mathrm{off}(u+4) \cdot \mathrm{HT}_{\mathrm{warm}}(u+4)
\end{aligned}
$$

Abstracting from the synchronization actions we get the system HT′:

$$
\begin{aligned}
\mathrm{HT}' &= \left(T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright \mathrm{off}(22) \cdot \mathrm{HT}'_{\mathrm{warm}}(22) \\
\mathrm{HT}'_{\mathrm{warm}}(u) &= \left(T(u) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right) \curvearrowright \mathrm{on}(u+4) \cdot \mathrm{HT}'_{\mathrm{cold}}(u+4) \\
\mathrm{HT}'_{\mathrm{cold}}(u) &= \left(T(u) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right) \curvearrowright \mathrm{off}(u+4) \cdot \mathrm{HT}'_{\mathrm{warm}}(u+4)
\end{aligned}
$$

So HT starts in a state where the temperature is 0°C, rising by 1°C per hour. After 22 hours (when it is 22°C), the heater turns off, after which the temperature starts to fall. Four hours

later, (when it is 18°C), the heater turns on, the temperature starts to rise, and another four hours later the temperature is 22°C again. This cycle repeats ad infinitum.

This completes the absolute time version of our small example. Note that we have not given any correctness criterion. One such criterion could for example be "eventually the temperature stays within the interval $18 \leq T(t) \leq 22$".

This is not necessarily a bad thing; we are more focused on transforming large, concurrent, specifications in equivalent small, linear ones to get an insight in the functioning of a hybrid system, than we are interested in verifying a specific property. Nevertheless, it would be nice to be able to verify formal properties. More on this in the conclusions of this abstract, and the full paper.

3.3 Specification (relative time)

We will now analyze the same heater and thermostat again, this time using relative time (note the square brackets).

When inspecting the above analysis in absolute time, one notices that it is needlessly cluttered with variables ("u" and "v") that only serve to express the concept of "now". It would be far easier to avoid this dragging along of variables by using relative time.

This leads to the specification of Table 2. This specification intuitively works just like its absolute time counterpart, and is much easier to read.

$$
\begin{aligned}
\text{Heater} &= H_{\text{on}} \\
H_{\text{on}} &= \int_{v=0}^{\infty} r_{\text{off}}[v] \cdot \text{off}_1[0] \cdot H_{\text{off}} \\
H_{\text{off}} &= \int_{v=0}^{\infty} r_{\text{on}}[v] \cdot \text{on}_1[0] \cdot H_{\text{on}}
\end{aligned}
$$

$$
\begin{aligned}
\text{Thermostat} &= T_{\text{cold}} \\
T_{\text{cold}} &= \int_{v=0}^{\infty} [T(t) = 22] :\rightarrow s_{\text{off}}[v] \cdot T_{\text{warm}} \\
T_{\text{warm}} &= \int_{v=0}^{\infty} [T(t) = 18] :\rightarrow s_{\text{on}}[v] \cdot T_{\text{cold}}
\end{aligned}
$$

$$
\begin{aligned}
S &= S' \\
S' &= \int_{v=0}^{\infty} \text{off}_2[v] \cdot \left[\frac{\mathrm{d}T}{\mathrm{d}t} = -1\right] \curvearrowright S'' \\
S'' &= \int_{v=0}^{\infty} \text{on}_2[v] \cdot \left[\frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright S'
\end{aligned}
$$

$$
\begin{aligned}
H &= \{r_{\text{off}}, s_{\text{off}}, r_{\text{on}}, r_{\text{off}}, \text{on}_1, \text{on}_2, \text{off}_1, \text{off}_2\} \\
C &= \{r_{\text{off}} \mid s_{\text{off}} = c_{\text{off}}, r_{\text{on}} \mid s_{\text{on}} = c_{\text{on}}, \text{off}_1 \mid \text{off}_2 = \text{off}, \text{on}_1 \mid \text{on}_2 = \text{on}\}
\end{aligned}
$$

$$
\text{HT} = \left[T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright \partial_H(\text{Heater} \parallel \text{Thermostat} \parallel S)
$$

Table 2: Heater and Thermostat, relative time version.

3.4 Analysis (relative time)

Again we linearize. The calculation is given below. Note that it is significantly cleaner and shorter than in the absolute time case.

$$
\begin{aligned}
\mathrm{HT} &= \left[T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright \partial_H(\text{Heater} \parallel \text{Thermostat} \parallel S) \\
&= \left[T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright \partial_H(H_{\mathrm{on}} \parallel T_{\mathrm{cold}} \parallel S') \\
&= \left[T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright c_{\mathrm{off}}[22] \cdot [T(0) = 22] \curvearrowright \partial_H(\mathrm{off}_1[0] \cdot H_{\mathrm{off}} \cdot T_{\mathrm{warm}} \parallel S') \\
&= \left[T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright c_{\mathrm{off}}[22] \cdot [T(0) = 22] \curvearrowright \mathrm{off}[0] \cdot \\
&\quad [T(0) = 22] \curvearrowright \partial_H\left(H_{\mathrm{off}} \cdot T_{\mathrm{warm}} \parallel \left[\frac{\mathrm{d}T}{\mathrm{d}t} = -1\right] \curvearrowright S''\right) \\
&= \left[T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright c_{\mathrm{off}}[22] \cdot [T(0) = 22] \curvearrowright \mathrm{off}[0] \cdot \\
&\quad \left[T(0) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right] \curvearrowright \partial_H\left(H_{\mathrm{off}} \cdot T_{\mathrm{warm}} \parallel \left[\frac{\mathrm{d}T}{\mathrm{d}t} = -1\right] \curvearrowright S''\right) \\
&= \left[T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright c_{\mathrm{off}}[22] \cdot [T(0) = 22] \curvearrowright \mathrm{off}[0] \cdot \mathrm{HT}_{\mathrm{warm}} \\
\mathrm{HT}_{\mathrm{warm}} &= \left[T(0) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right] \curvearrowright \partial_H\left(H_{\mathrm{off}} \parallel T_{\mathrm{warm}} \parallel \left[\frac{\mathrm{d}T}{\mathrm{d}t} = -1\right] \curvearrowright S''\right) \\
&= \left[T(0) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right] \curvearrowright c_{\mathrm{on}}[4] \cdot [T(0) = 18] \curvearrowright \\
&\quad \partial_H\left(\mathrm{on}_1[0] \cdot H_{\mathrm{on}} \parallel T_{\mathrm{cold}} \parallel \left[\frac{\mathrm{d}T}{\mathrm{d}t} = -1\right] \curvearrowright S''\right) \\
&= \left[T(0) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right] \curvearrowright c_{\mathrm{on}}[4] \cdot [T(0) = 18] \curvearrowright \mathrm{on}[0] \cdot \\
&\quad [T(0) = 18] \curvearrowright \partial_H\left(H_{\mathrm{on}} \parallel T_{\mathrm{cold}} \parallel \left[\frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright S'\right) \\
&= \left[T(0) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right] \curvearrowright c_{\mathrm{on}}[4] \cdot [T(0) = 18] \curvearrowright \mathrm{on}[0] \cdot \\
&\quad \left[T(0) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright \partial_H\left(H_{\mathrm{on}} \parallel T_{\mathrm{cold}} \parallel \left[\frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright S'\right) \\
&= \left[T(0) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right] \curvearrowright c_{\mathrm{on}}[4] \cdot [T(0) = 18] \curvearrowright \mathrm{on}[0] \cdot \mathrm{HT}_{\mathrm{cold}} \\
\mathrm{HT}_{\mathrm{cold}} &= \left[T(0) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright \partial_H\left(H_{\mathrm{on}} \parallel T_{\mathrm{cold}} \parallel \left[\frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright S''\right) \\
&= \left[T(0) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright c_{\mathrm{off}}[4] \cdot [T(0) = 22] \curvearrowright \\
&\quad \partial_H\left(\mathrm{off}_1[0] \cdot H_{\mathrm{off}} \parallel T_{\mathrm{warm}} \parallel \left[\frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright S'\right) \\
&= \left[T(0) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright c_{\mathrm{off}}[4] \cdot [T(0) = 22] \curvearrowright \mathrm{off}[0] \cdot \\
&\quad [T(0) = 22] \curvearrowright \partial_H\left(H_{\mathrm{off}} \parallel T_{\mathrm{warm}} \parallel \left[\frac{\mathrm{d}T}{\mathrm{d}t} = -1\right] \curvearrowright S''\right) \\
&= \left[T(0) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1\right] \curvearrowright c_{\mathrm{off}}[4] \cdot [T(0) = 22] \curvearrowright \mathrm{off}[0] \cdot \\
&\quad \left[T(0) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1\right] \curvearrowright \partial_H\left(H_{\mathrm{off}} \parallel T_{\mathrm{warm}} \parallel \left[\frac{\mathrm{d}T}{\mathrm{d}t} = -1\right] \curvearrowright S''\right)
\end{aligned}
$$

$$= \left[T(0) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1 \right] \curvearrowright c_{\mathrm{off}}[4] \cdot [T(0) = 22] \curvearrowright \mathrm{off}[0] \cdot \mathrm{HT}_{\mathrm{warm}}$$

Throwing away the intermediate steps, this brings us to the following system of three equations:

$$\mathrm{HT} = \left[T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1 \right] \curvearrowright c_{\mathrm{off}}[22] \cdot [T(0) = 22] \curvearrowright \mathrm{off}[0] \cdot \mathrm{HT}_{\mathrm{warm}}$$

$$\mathrm{HT}_{\mathrm{warm}} = \left[T(0) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1 \right] \curvearrowright c_{\mathrm{on}}[4] \cdot [T(0) = 18] \curvearrowright \mathrm{on}[0] \cdot \mathrm{HT}_{\mathrm{cold}}$$

$$\mathrm{HT}_{\mathrm{cold}} = \left[T(0) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1 \right] \curvearrowright c_{\mathrm{off}}[4] \cdot [T(0) = 22] \curvearrowright \mathrm{off}[0] \cdot \mathrm{HT}_{\mathrm{warm}}$$

Abstracting from the synchronization actions we get the system HT′:

$$\mathrm{HT}' = \left[T(0) = 0 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1 \right] \curvearrowright \mathrm{off}[22] \cdot \mathrm{HT}'_{\mathrm{warm}}$$

$$\mathrm{HT}'_{\mathrm{warm}} = \left[T(0) = 22 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = -1 \right] \curvearrowright \mathrm{on}[4] \cdot \mathrm{HT}'_{\mathrm{cold}}$$

$$\mathrm{HT}'_{\mathrm{cold}} = \left[T(0) = 18 \wedge \frac{\mathrm{d}T}{\mathrm{d}t} = 1 \right] \curvearrowright \mathrm{off}[4] \cdot \mathrm{HT}'_{\mathrm{warm}}$$

From these equations the behavior of the heater and thermostat system can be even easier understood than in the absolute time case.

So, one could ask, why bother with absolute time at all? As we will argue in the full article, specifications and calculations are indeed more naturally expressed using relative time constructs. Paradoxically, however, axiomizing relative time constructs is very painful, whereas it is quite easy for absolute time.

Therefore, the approach we have taken is to have all axioms in absolute time, then define relative time constructs in terms of absolute time constructs[1]. The equalities needed to rewrite systems then become theorems, that can be proven from expanding the definitions of the relative time constructs, and proving the resulting absolute time theorem using the axioms.

4 Conclusions

We have found a way to successfully apply (ACP-style) algebraic techniques to hybrid systems. Because of ACP's modular nature, this opens up the whole spectrum of ACP techniques (past, present, and future). On several points this will save us the trouble of reinventing the wheel.

As we put emphasis on practical applicability rather than theoretical beauty, the theory is quite a bit larger than most algebraic theories. But we strongly feel that this disadvantage is more than made up for by the advantage of being able to specify close to the way the mechanical engineering language χ does.

Although we do not provide a formal translation from χ to $\mathrm{ACP}_{\mathrm{hs}}$, it is our experience that $\mathrm{ACP}_{\mathrm{hs}}$ provides enough expressibility to easily express all χ specifications we have encountered so far.

Where we do have some difficulties is with the notion of correctness. (Strong) bisimulation is probably too much to demand between a high level specification and a very low level implementation of a production line. It would be nice the have a notion of refinement or abstraction in the setting of $\mathrm{ACP}_{\mathrm{hs}}$, but there has not been done much research on this as of yet.

An other alternative for a notion of correctness might be by specifying the desired behavior by means of a temporal logic formula. This formula could then be checked against the process graph of an $\mathrm{ACP}_{\mathrm{hs}}$ implementation.

[1] The basic idea behind this is not ours; it appears in several places in the literature, e.g. [BB95].

For future research we plan to look into the two above mentioned alternative notions of correctness. It is our hope that while doing so we will be able to tackle ever larger and larger examples, finally arriving at the point where we can provide a serious alternative to the simulation driven design method described above.

Honesty dictates us to state we still quite far from formally analysing the 1000-odd line χ programs that can quite satisfactorily be simulated. To reach that point, it will probably be necessary to integrate our approach with computer aided process algebra tools, for example the PSF toolkit currently under development at Eindhoven University of Technology and the University of Amsterdam. It is our firm belief that a solid theoretical understanding of hybrid systems in an algebraic framework, combined with sophisticated computer tools to perform the tedious algebraic manipulations sometimes necessary, will yield powerful techniques for assuring hybrid systems correct.

5 Acknowledgments

We like to thank Norbert Arends, Jos Baeten, Roland Bol, Jozef Hooman, Sjouke Mauw, and Hans Mulder for their various suggestions and comments.

Bibliography

[AvdMR94] N.W.A. Arends, J.M. van de Mortel, and J.E. Rooda. Specification language for continuous systems. In *Proceedings of the IASTED International Conference on Applied Modeling and Simulation*, 1994.

[BB94] J.C.M. Baeten and J.A. Bergstra. Process algebra with propositional signals. Technical Report CSR 94/49, Eindhoven University of Technology, Computing Science Department, 1994.

[BB95] J.C.M. Baeten and J.A. Bergstra. Real time process algebra with infinitesimals. In [PVvV95], pages 148–187, 1995.

[BW90] J.C.M. Baeten and W.P. Weijland. *Process Algebra*. Number 18 in Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 1990.

[PVvV95] A. Ponse, C. Verhoef, and S.F.M. van Vlijmen, editors. *Algebra of Communicating Processes*. Workshops in Computing. Springer-Verlag, 1995. Proceedings of ACP94, the First Workshop on the Algebra of Communicating Processes.