Zélus: A Synchronous Language with ODEs

Tool Paper

Timothy Bourke
NICTA
Sydney, Australia
Timothy.Bourke@nicta.com.au

Marc Pouzet
Univ. Pierre et Marie Curie
DI, Ecole normale supérieure
INRIA Paris, France
Marc.Pouzet@ens.fr

ABSTRACT
Zélus is a new programming language for modeling systems that mix discrete logical time and continuous time behaviors. From a user’s perspective, its main originality is to extend an existing Lustre-like synchronous language with Ordinary Differential Equations (ODEs). The extension is conservative: any synchronous program expressed as data-flow equations and hierarchical automata can be composed arbitrarily with ODEs in the same source code.

A dedicated type system and causality analysis ensure that all discrete changes are aligned with zero-crossing events so that no side effects or discontinuities occur during integration. Programs are statically scheduled and translated into sequential code which, by construction, runs in bounded time and space. Compilation is effected by source-to-source translation into a small synchronous subset which is processed by a standard synchronous compiler architecture. The resulting code is paired with an off-the-shelf numeric solver.

We show that it is possible to build a modeler for explicit hybrid systems à la Simulink/Stateflow on top of an existing synchronous language, using it both as a semantic basis and as a target for code generation.

Categories and Subject Descriptors
C.3 [Special-Purpose and Application-Based Systems]; Real-time and embedded systems; D.3.2 [Programming Languages]: Language Classifications—Data-flow languages; I.6.8 [Simulation and Modeling]: Types of Simulation—Continuous, Discrete Event; D.3.4 [Programming Languages]: Processors—Code generation, Compilers

General Terms
Algorithms, Languages

Keywords
Hybrid systems; Hybrid automata; Synchronous languages; Block diagrams; Type systems;

1. INTRODUCTION
Hybrid systems modelers are used not only in the high-level design and simulation of complex embedded systems, but also as development platforms in which the same source is used for formal verification, testing, simulation, and the generation of target executables. The quintessential example is the Simulink/Stateflow suite,1 but there are also LabVIEW,2 Modelica,3 and several others [6].

These tools are distinguished from the formal model of hybrid automata [14] by their focus on modular programming and simulation of both physical models and their controllers. In this context, reproducible, efficient simulations and the ability to generate statically scheduled code are essential features. As a major consequence, programming constructs are typically deterministic whereas hybrid automata are essentially non-deterministic and oriented toward specification and formal verification through the over-approximation of piece-wise continuous behaviors.

The underlying mathematical model of hybrid modelers is the synchronous parallel composition of stream equations, differential equations, and hierarchical automata. But even with a carefully chosen numeric solver, actual simulations only ever approximate the ideal behaviors of such models. A formal semantics exists for discrete subsets [20, 13], but mixes of discrete and continuous-time signals often have unpredictable and mathematically weird behaviors [3, 2]. For instance, a continuous STATEFLOW state may be triggered repeatedly if a transition guard remains true, and, although transitions are instantaneous, the amount of simulation time that elapses between triggerings is non-zero and depends on when the solver decides to stop, which in turn is influenced by simulation parameters, global numerical error, and the occurrence of other zero-crossings. The behavior of a model may even change if it is placed in parallel with an independent block, for example one that tests the zero-crossings of a sinusoid signal. In this case, changing the sinusoid frequency may radically change the output of the other model. This time leak is not due to numerical artifacts but to a more fundamental reason: discrete time is not logical but global, it exposes the internal steps of the simulation engine.

Synchronous languages [5] differ from this approach by providing a logical notion of time, independent of a physical implementation. For example, the LUSTRE equations

\[ x = 0 \rightarrow \text{pre } y \quad \text{and} \quad y = \text{if } c \text{ then } x + 1 \text{ else } z \]

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
Copyright 20XX ACM X-XXXX-XX-X/XX ...$15.00.

1http://www.mathworks.com/products/simulink/
2http://www.ni.com/labview/
3http://www.modelica.org/
define the two sequences \((x_n)_{n \in \mathbb{N}}\) and \((y_n)_{n \in \mathbb{N}}\) which are computed sequentially with \(x_0 = 0, x_n = y_{n-1}\), and for all \(n \in \mathbb{N}, y_n = \text{if } c_0 \text{ then } x_n + 1 \text{ else } x_n.\) Time is logical, that is, nothing can be inferred about the actual time that passes between instants \(i\) and \(i + 1\). Synchronous programs see the environment as a source of input and output sequences and ignore intervening gaps. They are thus only suitable for the design of discrete controllers. In contrast, a model expressed with Ordinary Differential Equations (ODEs) or Differential Algebraic Equations (DAEs) continues to evolve during such gaps and a variable-step numeric solver is necessary to approximate continuous trajectories efficiently and faithfully.

So, what is the best way to combine the precision of synchronous languages for programming discrete components with the extra expressiveness afforded by ODEs approximated by numeric algorithms? Any combination must be conservative: the behavior of a synchronous program should not change if ODEs are placed in parallel, it should have the same logical-time semantics and compile to the same code, in particular to avoid inconsistencies between simulation and execution. Furthermore, discrete computations and side effects should not occur during numerical approximation.

In order to avoid the aforementioned time leak and to have a clear separation between discrete and continuous-time signals, we proposed the following convention, quoting [3]:

“A signal is discrete if it is activated on a discrete clock. A clock is termed discrete if it has been declared so or if it is the result of a zero-crossing or a sub-sampling of a discrete clock. Otherwise, it is termed continuous.”

This means that any synchronous program can be paired with ODEs as long as it is activated on a discrete clock. The definition is sufficiently general to model, for example, a discrete controller activated on a timer (periodic or not) or a deterministic hybrid automata with dynamic conditions.

In previous work, we proposed the basis of a Lustre-like language extended with ODEs and following the above discipline. We defined the semantics of a minimal language using non-standard analysis [4], and proposed a type system that ensures the absence of time leaks, and a compilation method [3]. We later added hierarchical automata [2]. These techniques have been implemented in a new language, called Zélus, which allows arbitrary combinations of dataflow equations, hierarchical automata, and ODEs. It is equipped with a type system and causality analysis to statically ensure that all discrete computations are aligned with zero-crossings. It is compiled by a source-to-source translation into synchronous code which is then itself compiled to sequential code paired with an off-the-shelf numeric solver. This paper describes the key aspects of the language, and its design and implementation. We use synchronous programming as both a semantic foundation, where we are strongly influenced by the work of Lee et al. [17] and Mosterman et al. [11, 19], and as a target for code generation.

2. AN OVERVIEW OF ZÉLUS

Zélus\(^4\) is a first-order synchronous dataflow programming language extended with resettable ODEs and hierarchical

\footnote{The unit delay initialized to 0, \(0 \rightarrow \text{pre}\), is \(\frac{1}{2}\) in Simulink.}

\footnote{The compiler, runtime, and examples are available at: http://www.di.ens.fr/~pouzet/zelusreview.}

automata. Rather than define the abstract syntax (available in [2, §3.1]), we show its main features through examples.

A Zélus program is a sequence of definitions. The following declares a discrete function which counts the number of occurrences of \(t\) and detects when there have been \(n\):

\[
\text{let node after} (n, t) = (c = n) \text{ where rec } c = 0 \rightarrow \text{pre(min(tick, n))} \text{ and tick } = \text{ if } t \text{ then } c + 1 \text{ else } c,
\]

where \(\text{pre}\) is the non-initialized unit delay, \(- \rightarrow\), is the initialization operator of Lustre, \(\text{min}\) computes the minimum of its arguments and if/then/else is the mux operator. The semantics in terms of infinite sequences is

\[
\forall i \in \mathbb{N}^+, c_i = \text{min}(\text{tick}_{i-1}, n_{i-1}) \text{ and } c_0 = 0
\]

\[
\forall i \in \mathbb{N}, \text{tick}_i = \text{if } t_i \text{ then } c_i + 1 \text{ else } c_i,
\]

and the compiler infers the signature:

\[
\text{val after : int } \times \text{ int } \Rightarrow \text{bool}
\]

The counter can be instantiated in a two state automaton,

\[
\text{let node blink} (n, m, t) = x \text{ where automaton}
\]

\[
\text{On } \rightarrow \text{do } x = \text{true until } (\text{after} (n, t)) \text{ then Off}
\]

\[
\text{Off } \rightarrow \text{do } x = \text{false until } (\text{after} (m, t)) \text{ then On}
\]

which returns a value for \(x\) that alternates between true for \(n\) occurrences of \(t\) and false for \(m\) occurrences of \(t\). The keyword until stands for a weak preemption, that is, \(x\) equals true when \(\text{after}(n, t)\) is true and becomes false the following instant. The semantics and compilation of automata, defined in [8], is that of SCADE 6\(^6\) and Lucid Synchrone.\(^7\) The blinking behavior can be reset on a boolean condition \(r\) by nesting it inside a one state automaton that tests \(r\), which we write using the reset/every syntactic sugar:

\[
\text{let node blink_reset} (r, n, m, t) = x \text{ where reset automaton}
\]

\[
\text{On } \rightarrow \text{do } x = \text{true until } (\text{after} (n, t)) \text{ then Off}
\]

\[
\text{Off } \rightarrow \text{do } x = \text{false until } (\text{after} (m, t)) \text{ then On}
\]

every \(r\)

The type signatures inferred by the compiler are:

\[
\text{val blink : int } \times \text{ int } \times \text{ int } \Rightarrow \text{bool}
\]

\[
\text{val blink_reset : int } \times \text{ int } \times \text{ int } \times \text{ int } \Rightarrow \text{bool}
\]

Up to syntactic details, these Zélus programs could have been written as is in SCADE 6 or Lucid Synchrone.

But Zélus goes beyond discrete dataflow programming and allows the definition of continuous-time variables. For instance, consider a boom turning on a fixed pivot. The boom’s angle can be expressed as a differential equation with initial value \(i\) and derivative \(v\) using the der keyword:

\[
\text{der angle } = v \text{ init } i
\]

Its (ideal) value at model time \(t\) is:

\[
\text{angle}(t) = i(0) + \int_0^t v(x) \, dx.
\]

It is compiled into a continuous state variable whose value is approximated by a numeric solver as described in §3.2.

\(^4\)http://www.esterel-technologies.com

\(^6\)http://www.di.ens.fr/~pouzet/zelusreview

\(^7\)http://www.di.ens.fr/~pouzet/lucid-synchrone
Now, if we wanted to achieve a reference velocity $v_r$ using Proportional-Integral (PI) control, we need only add three equations in parallel:\footnote{\texttt{-}, \texttt{*}, \texttt{+}. are floating-point arithmetic operators.}
\begin{align*}
\cdots \text{and } \text{error} & = v_r - v \\
\text{and } \text{der } v & = 0.7 \times \text{error} + 0.3 \times z \text{ init } 0.0 \\
\text{and } \text{der } z & = \text{error init } 0.0
\end{align*}

It could be that we also want to reset the controller state $z$ when the angle reaches or exceeds a limit $\max$. Two new constructs are needed: a way of detecting such interesting events and a way of directly setting the value of a continuous state. The standard way to detect events in a numeric solver is via zero-crossings where a solver monitors expressions for changes in sign and then, if they are detected, searches for a more precise instant of crossing. We introduce an \texttt{up()} operator to monitor an expression for a (rising) zero-crossing; with this, the definition of $z$ becomes:
\begin{align*}
\text{der } z & = v_r - v \text{ init } 0.0 \text{ reset up(angle } - , \max) \rightarrow 0.0
\end{align*}
which says to reset the value of $z$ to 0.0 the instant when angle $- \max$ becomes zero or positive. A \text{der} definition defines two values: a state ($z$) initially and in response to discrete events, and its derivative ($\dot{z}$) during continuous phases.

More complicated behaviors are better described as automata where defining equations and events being monitored change depending on mode. For instance, if the direction of the boom’s motion changes in response to the input signals \texttt{push} and \texttt{pull}, and if the boom becomes stuck when it reaches a limit of motion, we may define $v_r$ as follows:
\begin{align*}
\text{autonomaton} & \text{ \texttt{Pushing} } \rightarrow \text{ do } v_r = \maxf \\
& \text{ until up(angle } - , \max) \text{ then Stuck} \\
& \text{ } \text{ | pull() then Pulling} \\
\text{autonomaton} & \text{ \texttt{Pulling} } \rightarrow \text{ do } v_r = - \maxf \\
& \text{ until up(min } - , \text{ angle) then Stuck} \\
& \text{ } \text{ | push() then Pulling} \\
\text{autonomaton} & \text{ \texttt{Stuck} } \rightarrow \text{ do } v_r = 0.0 \text{ done}
\end{align*}
The \text{autonomaton} construct is like an equation and each mode contains a set of definitions which, naturally, may themselves include derivatives and automata. Here, the value of $v_r$ is defined as either $\maxf$, $-\maxf$, or 0.

Transitions are ordered by priority and their guards have type \texttt{signal}. Events of type \texttt{signal} are emitted by discrete components or introduced by \texttt{up()} : \texttt{float } \sim \texttt{unit signal}. As a consequence of this typing rule, boolean expressions cannot serve directly as guards in continuous automata. While it

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{idealized_backhoe_loader.png}
\caption{Idealized Backhoe Loader model}
\end{figure}

would be possible to compile an expression $\text{up}(e: \texttt{bool})$ into $\text{up}(\texttt{if } e \texttt{ then } 1.0 \texttt{ else } -1.0.)$, as effectively occurs in Statetwo, the search for zero-crossings then degenerates into binary search, and, more unsatisfying still, boolean complement, like signal absence, is not closed on discrete signals. Ultimately, we think we can better analyze and execute hybrid programs by restricting the form of triggering expressions.

One of Zélu’s strengths is the way that larger models can be constructed using abstraction and instantiation. For example, the various fragments discussed so far are readily combined into a more interesting model: that of the idealized backhoe loader that we use to teach discrete reactive programming. A labeled screen capture from its graphical simulator is shown in Figure 1. Using input signals from buttons and \texttt{*in/*out} sensors, and the outputs listed at right, students must write a discrete controller to operate the three backhoe segments. The simulator must, of course, approximate the movement of the segments.
The node declaration for a single segment is shown in Figure 2. It declares a hybrid node called `segment` taking three inputs: a triple of movement parameters (min, max, i), the maximum force, maxf, the control signals (push, pull, go); and giving as output the sensor values (segin, segout) and the segment position, angle.

The body of `segment` combines the elements already discussed with some minor modifications. For one, the reference velocity v_r is 0 when go is false and rate otherwise. The value of rate depends on the direction of motion, which in reality is determined by a hydraulic valve but which we model as a hybrid automaton. The automaton differs in its initial state, but also because of the self-loop transitions that model bouncing at the limits of motion:

```
until (atlimit() on (last v > 0.3 * . maxf)) then do ...
```

The operator on : α signal × bool ¬→ α signal filters signals through boolean expressions. When atlim occurs and the expression is satisfied, the transition resets the value of v and emits the signal hit. We are obliged to write last v in the guard and do/in equations to respect causality: the value of v cannot be tested before it is defined! Semantically last v is the left-limit of v. The hit signal resets the controller integrator, z, so that the sudden spikes on v are ignored.

A complete simulation is constructed as the parallel composition of instantiations of the `segment` node (three times: boom, stick, and bucket), a similar node that moves the legs, a function for updating the visualization, and a node implementing a discrete controller. Whereas a hybrid node like `segment` may be executed repeatedly to approximate continuous states, activations of the visualization function and controller node must be triggered more conservatively: the former because it has side-effects (it draws in a window); the latter because it may update internal discrete states. For instance, we call the update function with

```
let x = up(s) in
let y = e1 in e2 in e3 is transformed into
```

Figure 3: Compiler architecture

Table 1: ZÉLUS in numbers
12. Simple optimizations are performed: dead-code removal, elimination of copy variables and common sub-expressions.

13. Equations are statically scheduled according to data-flow dependencies.

14. The code is modularly translated into sequential code.

The architecture is mainly that of the LUCID SYNCHRONE compiler\textsuperscript{10} and only the highlighted boxes are really novel. We detail them in the following sections.

### 3.1 Typing and Causality

As the backhoe example demonstrates, ZÉLUS allows liberal combinations of combinational, discrete, and continuous elements. Nevertheless, discontinuities and side-effects must only occur on discrete clocks; programs that violate this rule are rejected. The principles and formal rules underlying the type system of ZÉLUS are presented elsewhere [3, 2]; here we focus on the pragmatic motivations and implementation.

Every function definition, equation or expression is associated to a kind \( k \in \{A, D, C\} \): A if combinatorial, D if discrete-time, and C if continuous-time. Kinds are related by the minimal subtyping relation such that \( A \subseteq D \) and \( A \subseteq C \). They are ascribed to entire ‘blocks’ rather than to individual ‘wires’—each node or set of equations has a single kind which is inherited by individual inputs and outputs.

The system extends naturally to automata: all the states of a ‘continuous’ automaton are also of kind C and may thus contain ODEs. The signature of a function \( f \) with input type \( t_1 \) and output type \( t_2 \) is thus of the form:

\[
f : \forall \beta_1, ..., \beta_n.t_1 \xrightarrow{} t_2 \quad \text{(where the } \beta_i \text{ are type variables)}
\]

(We write \( \xrightarrow{} \) as \( \rightarrow \), \( \xrightarrow{\subseteq} \) as \( \Rightarrow \), and \( \xrightarrow{\subseteq} \) as \( \rightarrow \)). This block-based scheme greatly simplifies the formal rules, implementation, and type-related messages (interface files and errors) and so far we have not found it hinders writing programs.

A combinational function is defined by writing:

\[
\text{let } \text{square}(x) = x \cdot x.
\]

It's inferred type is \( \text{float} \rightarrow \text{float} \). A declaration with the keyword node gives a function that executes in discrete time and which may thus contain unit delays, and the keyword hybrid gives a function that executes in continuous time.

As an example of the typing analysis, consider a program that tries to place an ODE in parallel with a discrete counter:

\[
\text{let hybrid wrong}(x) = o \text{ where rec der o = } 1.0 \text{ init } -1.0 \text{ and cpt = } 0.0 \text{ fby cpt + } . o
\]

The compiler rejects it with the message:

File "ex. Is", line 3, characters 12–25: > and cpt = 0 fby cpt +. o

\textsuperscript{10}Through it has been rewritten entirely.

---

**Type error**: this is a discrete expression and is expected to be continuous.

As wrong is defined with keyword hybrid, it must not contain a discrete-time computation which is not triggered on a discrete clock. It could be made valid by writing, for example,

\[
\begin{align*}
\text{let hybrid good}(x) = o \text{ where } \\
\text{rec der o = } 1.0 \text{ init } -1.0 \text{ reset z() } \rightarrow \text{ -1.0 } \\
\text{and cpt = } \text{present z() } \rightarrow \text{ (0 fby cpt + o) init 0 } \\
\text{and z = } \text{up(last o)}
\end{align*}
\]

After typing, a causality analysis is performed to ensure the absence of instantaneous loops. It follows two simple principles: every loop on a discrete signal must be broken by a unit delay and every loop on a continuous-time signal must be broken by an integrator. This is essentially what existing tools like SIMULINK do.

### 3.2 Compilation of ODEs and Runtime

The typing and causality analyzes help fulfill three fundamental requirements: (a) to simulate continuous processes with state-of-the-art numeric solvers, (b) to import existing synchronous code without modification, and, (c) to use existing tools to compile everything.

A hybrid simulation alternates between two phases as depicted in Figure 4. In state \( D \), some code next is executed, \( y', go' = \text{next}(y, x) \), to compute the next value of the discrete state variables \( y \) and \( go \) from the current value of \( y \) and a continuous state \( x \). This computation occurs when any of the zero-crossings \( z_1, ..., z_n \) or \( go \) are true. Side effects and changes of state variables (continuous or discrete) may occur at such instants. A simulation keeps iterating in this state, in which physical time does not progress, until \( go \) becomes false. Then, integration in a numeric solver begins. A solver takes functions \( f_y \) and \( g_y \) parameterized by \( y \) and a horizon \( h \) with:

\[
\begin{align*}
x(t + h) \text{ and approximates } & \tilde{x}(t + h) \text{ from the current time } t \text{ while } \\
\text{monitoring the elements of } & \tilde{z} \text{ for changes of sign. The solver } \\
\text{stops when it reaches time } t_i + h \text{ or when one or more zero-crossings has been detected. State } & D \text{ is then entered and the code is executed and may respond to detected events.}
\end{align*}
\]

It is up to the compiler to construct next, \( f \), \( g \), the discrete state \( y \), and the continuous state \( x \). This is done by the source-to-source transformations which turn hybrid functions into discrete nodes with additional inputs and outputs as shown in this extract from the compilation of der \( z = \ldots \) and up(angle -- . -- max) in segment:

\[
\begin{align*}
\text{let node segment}((i z_1, i z_2), (i z, i v, i l a n g e), d, (i m i n, i m a x, i), i m a x, (i p u s h, i p u l l, i g o)) = \\
((i u p z_1, i u p z_2), (n z, n v, i n a n g e), \\
g o_1 \text{ or } g o_2 \text{ or } g o_3, ((i s e g i n, i s e g o u t), \text{angle})) \\
\ldots \\
\text{and at limit } = i z_1 \text{ and up z } = \text{angle } -- \cdot \cdot \cdot \\
\end{align*}
\]

---
Each up(c) is replaced with a boolean input izi to signal detection of the corresponding zero-crossing and a floating-point output upzi to transmit the value of the expression e. The equation der z = error init 0.0 reset hit() → 0.0 is translated into dz = error, z = if hit then 0.0 else iz, and equation nz = if d then z else dz, where d is a boolean flag that is true in D and false in C. Iz is an input that contains the value of the state variable z estimated by the solver (an element of z), and nz is an output. Finally, a last z variable replaces all occurrences of last z within the other definitions. The present statement has been transformed into a switch statement match/with over the concrete representation of the signal hit. When hit is present, z is (re)set directly to 0.0. The synchronous function is then compiled to sequential code.

Once the source program has been compiled into an executable, it is possible to choose the numeric solver and zero-crossing detection algorithm, and to set their parameters from the command-line. We have implemented a modular framework based on Ocaml functors and first-class modules to integrate solvers. In addition to an interface to the SUNDIALS CVODE solver [15], we have implemented several numeric solvers and the ‘Illinois’ false position method for zero-crossing detection using standard techniques [10] (Butcher tables, Hermite interpolation, and error estimation).

We have experimented with various examples from the literature, including the sticky masses [16, Example 6.8] and air traffic control [21], and from SIMULINK, including the bang-bang temperature controller and clutch model.

4. COMPARISON WITH OTHER TOOLS

The ZÉLUS language is most distinguished from SIMULINK by the type system that regulates compositions of discrete and continuous elements and the compilation by source-to-source transformation. While the basic semantics of a SIMULINK model follow simple principles, the behavior of important corner-cases can really only be understood by careful operational reasoning, and such intricacies must be faithfully reproduced by compilers and analysis tools. Users intending to compile their models into controllers are advised to avoid certain features, or to favor others; for instance, to use function call triggers to explicitly determine the execution order of blocks. In contrast, ZÉLUS has a consistent and simple semantics, the same source-to-source translations generate code for simulation and for embedded targets. Only the last step, that turns basic dataflow assignments into imperative code, requires customization for specific targets.

ZÉLUS shares the same basic model of executions, that alternate between continuous phases and sequences of ‘run-to-completion’ discrete actions, as specification frameworks like CHARON [1], SpaceEx [12], and Hybrid I/O Automata [18], and like them, concerns itself with modular composition. The biggest difference is the use of synchronous, rather than interleaved, parallelism, which enforces a strong discipline on communication through shared variables, which we consider as clocked streams, and on causality, since the language ensures a single value per variable per instant. Furthermore, we insist on externalizing all non-determinism from models.

Acknowledgments

We warmly thank Cyprien Lecourt for his work on solver modules and the development of various examples.

5. REFERENCES


