Towards a verified Lustre compiler with modular reset
Timothy Bourke, Lélio Brun, Marc Pouzet

To cite this version:
Timothy Bourke, Lélio Brun, Marc Pouzet. Towards a verified Lustre compiler with modular reset. 21st International Workshop on Software and Compilers for Embedded Systems (SCOPES 2018), May 2018, Sankt Goar, Germany. pp.4, 10.1145/3207719.3207732. hal-01817949

HAL Id: hal-01817949
https://inria.hal.science/hal-01817949
Submitted on 18 Jun 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Towards a verified Lustre compiler with modular reset

Extended Abstract

Timothy Bourke
Inria Paris
École normale supérieure,
PSL University
timothy.bourke@inria.fr

Lélio Brun
INRIA Paris
École normale supérieure,
PSL University
lelio.brun@ens.fr

Marc Pouzet
UPMC, Sorbonne Universités
École normale supérieure,
PSL University
marc.pouzet@ens.fr

ABSTRACT
This paper presents ongoing work to add a modular reset construct to a verified Lustre compiler. We present a novel formal specification for the construct and sketch our plans to integrate it into the compiler and its correctness proof.

CCS CONCEPTS
- Software and its engineering → Semantics; Formal software verification; Compilers;

KEYWORDS
Synchronous Languages (Lustre), Verified Compilation

1 INTRODUCTION
Lustre is a programming language for embedded control and signal processing systems [4]. Synchronous languages like Lustre allow engineers to design and validate systems at the level of abstract block diagrams and to automatically generate executable code.

Compilation transforms sets of equations defining streams of values into imperative code. We are developing a formally verified Lustre compiler called Vélus [3] in the Coq [8] interactive theorem prover. It integrates the CompCert C compiler [2, 7] and formally guarantees that repeated execution of the generated assembly code reproduces the successive values of the dataflow streams.

In this paper, we present ongoing work to add a modular reset construct [6] to Vélus. In particular we show a novel extension of the dataflow semantics to include this imperative construct and describe the challenges remaining to generate efficient and provably correct code.

Figure 1: A graphical representation of a state machine for a simple navigation system

2 LUSTRE AND ITS VERIFIED COMPILER
The example in Figure 1 shows the logic of a simple navigation system, such as could be specified, for instance, in graphical tools like SCADE Suite1 or Simulink.2 The system takes three inputs: g, data from a GPS unit, dx, a local odometric estimate, and s, a boolean input that triggers mode changes. It produces an output x giving the current position. The system has two modes: GPS uses the external data directly and INS (Inertial Navigation System) is a fallback mode where the position is estimated by adding successive dx values to the external value at mode entry.

The state machine shown in the figure can be compiled into a purely dataflow program that uses a modular reset [5]. To show why the modular reset is necessary, we start by reprogramming the example in Lustre without it:

```lustre
node INS(g, dx: int; rst: bool) returns (x: int);
let
x = if (true fby false) or rst then g else (0 fby (x + dx));
tel

node NAV(g, dx: int; s: bool) returns (x: int);
var r, c: bool;
let
x = merge c (g when c) (INS((g, dx, r) when not c));
c = true fby (merge c (not s when c) (s when not c));
r = false fby (s and c);
tel
```

This program contains two nodes. A node is a function, between a list of input streams and a list of output streams, defined by a set of equations. A program associates each expression with an (infinite) stream of values. Consider, for example, the execution shown below. Variable names are given at left and their successive values are lined up alongside in columns. We fix arbitrary values for the input variables (above the line).

1 http://www.ansys.com/products/embedded-software/ansys-scade-suite
2 http://www.mathworks.com/products/simulink/
The \( c \) variable encodes the active mode, true for GPS and false for INS. The \texttt{when} operator expresses the conditional activations implied by the state machine. In the table, the value of the expression \( g \) \texttt{when} \( c \) is labeled \( x_{\text{GPS}} \) and only has a value when \( c \) is true. The value of the expression \( \text{INS}((g, dx, r) \text{ when not c}) \) is labeled \( x_{\text{INS}} \) and only has a value when \( c \) is false. These complementary streams are combined with the \texttt{merge} operator to give a value for \( x \).

The local variable \( r \) is defined with the initialized delay operator \texttt{fby} ("followed by")—the \( z^{-1} \) of Digital Signal Processing. The subexpression \texttt{true fby false} defines the stream \( T \cdot F \cdot F \cdot F \cdot \cdots \); for \( r \), we have \( r(0) = F \) and \( \forall i > 0, r(i) = s(i-1) \land c(i-1) \). The initial value of \( c \) is \( T \) (GPS mode) and its next value depends on the current values of \( c \) and \( s \). That is, (weak) transitions fire at one instant to determine the mode at the next instant; each time that \( s \) is \( T \) in the table above, the active mode alternates a column later.

The node \texttt{INS} implements a discrete integrator: it calculates the cumulative sum of values on \( dx \), (re)starting from \( g \) initially and whenever \( rst \) is true. The instance of \texttt{INS} is thus reset using GPS data whenever \( r \) is true, that is, whenever the state machine enters the inertial mode.

In this translation of the state machine, we added an explicit reset signal to the \texttt{INS} interface and around the enclosed \texttt{fby} expression. In general, though, this is impractical and inefficient, as modes may contain arbitrarily many and arbitrarily nested node instantiations. The modular reset primitive solves this problem. We first describe, however, the compilation and semantics of basic Lustre programs before showing how to extend them in Section 3.

### 2.1 Compiler Architecture

The Vélus compiler [3] turns Lustre programs into imperative code. It implements \textit{clock-directed modular compilation} [1] in which each node is compiled into a distinct sequential function and each equation is assigned a static clock expression that becomes a nesting of conditional statements in the generated code.

The successive source-to-source transformations of the Vélus compiler are outlined in Figure 2.

\textit{Parsing} turns a source file into an abstract syntax tree with no type or clock annotations. \textit{Elaboration} adds type and clock annotations to a program and checks that they are consistent.

\textit{Normalization} rewrites a program into an abstract syntax that has two forms of expressions: \textit{control expressions} that may contain \texttt{merges} and \texttt{ifs} (at top level) and \textit{simple expressions} that may not. Neither form may contains \texttt{fby}s or node instantiations. Instead there are three forms of equations: those that equate a variable with a control expression, those that equate a variable with a \texttt{fby} over a simple expression, and those that equate one or more variables with a node instantiation over simple expressions.

\textit{Scheduling} sorts equations by variable dependencies: variables must be written before they are read, except those defined by \texttt{fby}s which must be read before they are overwritten with a value for use in a subsequent cycle. Normalizing and scheduling the example gives the following program.

```plaintext
node INS(g, dx: int; rst: bool) returns (x: int)
  var t: bool; y: int;
  let
    x = if t or rst then g else y;
    t = true fby false;
    y = 0 fby (x + dx);
  tel

node NAV(g, dx: int; s: bool) returns (x: int)
  var r, c, k: bool; x_INS: int when not c;
  let
    x_INS = INS((g, dx, r) when not c);
    k = merge c (not s when c) (s when not c);
    x = merge c (g when c) x_INS;
    r = false fby (s and c);
    c = true fby k;
  tel
```

\textit{Translation} transforms dataflow programs into an imperative intermediate language called \texttt{Obc}. Each equation in the original program becomes a conditionally executed assignment so that repeated execution of the imperative program generates the successive values of the streams in the dataflow program. Translation naively introduces \textit{if} statements for each individual equation. A subsequent \textit{fusion optimization} merges adjacent conditionals whenever possible to reduce branching.

\textit{Generation} transforms \texttt{Obc} into \texttt{Clight}. \texttt{Clight} [2] is an input language of the CompCert verified C compiler, which Vélus exploits for the \textit{compilation} to and \textit{printing} of assembly code.

Most of the compiler passes are specified and proved correct in Coq. Coq ‘extracts’ them into OCaml code which can be executed. Our correctness proofs compose with those of CompCert to give the end-to-end correctness theorem presented elsewhere [3].

### 2.2 Dataflow Semantic Model

Defining the semantics of Lustre programs in Coq essentially means representing their executions—that is, the ‘grid’ shown above for the example—in formal logic. The execution of a node is encoded as an \textit{environment} \( H \) that maps each variable to a stream of values and a \textit{base clock} \( bk \), a boolean stream that marks the instants when the node is active.
The semantics is centered around a pair of mutually recursive predicates, one for nodes and the other for individual equations. The formal rule for nodes is:

\[
\begin{align*}
\text{node } f & (i) \text{ returns } \overline{\vartheta} \\
& \text{var } \overline{\varphi} \text{ let } \overline{\varphi} \text{ tel} \\
\text{same_clock}^k (\overline{x} \leftrightarrow \overline{y}) & \quad bk = \text{clock}^k \overline{x} \\
H_{\text{var} \overline{\varphi}} & \varnothing \overline{x} \quad H_{\text{var} \overline{\varphi} \overline{\varphi}} \overline{y} \\
G & \quad H_{\text{eqp} \overline{\varphi}} \overline{\overline{\varphi}} \\
G_{1\text{node}} & f(\overline{x}, \overline{y})
\end{align*}
\]

It declares (below the line) that in a program \( G \), a node \( f \) relates a list of input streams \( \overline{x} \) to a list of output streams \( \overline{y} \) if (above the line), (i) \( f \) is declared in \( G \) with input variables \( \overline{i} \), output variables \( \overline{\vartheta} \), local variables \( \overline{\varphi} \), and equations \( \overline{\varphi} \); (ii) the input and output streams are all present or absent simultaneously; (iii) a base clock \( bk \) is true only when the inputs are present; (iv) there exists an environment \( H \) that associates the input variables to the input streams; (v) it associates the output variables to the output streams, and; (vi) it also satisfies all the equations.

The predicate for individual equations has three cases, one for each of the equation forms.

\[
G'_{\text{node}} f(\overline{x}, \overline{y})
\]

It declares that in a program \( G \), an environment \( H \) satisfies a clocked equation \( \overline{x} =_c f(\overline{e}) \), if (i) the argument expressions \( \overline{e} \), with clock \( ck \), evaluate in \( H \) to the list of streams \( \overline{e} \); (ii) the node \( f \) relates the input streams \( \overline{e} \) to a list of output streams \( \overline{x} \); and, (iii) \( H \) associates the variables \( x \) to these output streams.


techicalities aside, the predicates express two important principles: externally, a node relates input streams to output streams; internally, the input and output streams are projected from an environment (the grid representing an execution) that must satisfy all the constraints imposed by the node equations.

3 THE MODULAR RESET CONSTRUCT

The modular reset was introduced \([6]\) as a basic primitive for specifying dynamically reconfigurable systems and is used notably in the compilation of state machines \([5]\). A node instantiation \( f(\overline{e}) \) reset by a boolean expression \( r \) is written \( f(\overline{e}) \text{ every } r \). Using this construct, the state machine of Figure 1 can be expressed as the following dataflow program.

\[
\begin{align*}
node \ INS(g, dx: \text{int}) & \text{ returns } (x: \text{int}) \\
& \text{let} \ x = \text{if} (\text{true fby false}) \text{ then } g \text{ else } (\emptyset \text{ fby } (x + dx)) \text{; tel} \\
node NAV(g, dx: \text{int}; s: \text{bool}) & \text{ returns } (x: \text{int}) \\
& \text{var } r, c: \text{bool} \text{; let} \\
& x = \text{merge } c \ (g \text{ when } c) \ (\text{INS}(g, dx) \text{ when not } c) \text{ every } r \text{;} \ c = \text{true fby } (\text{merge } c \ (\text{not } s \text{ when } c) \ (s \text{ when not } c)) \text{;} \\
& r = \text{false fby } (s \text{ and } c) \text{; tel} \\
\end{align*}
\]

Compared to the previous translation, it is not necessary to pass an additional argument to INS nor to consider resets in the definition of \( x \). The modular reset is an imperative construct: it effectively 'restarts' a dataflow node by recursively resetting all fby's to their initial values—and this is exactly how it is implemented.

3.1 Dataflow with Reset Semantic Model

Hamon and Pouzet \([6]\) present a recursive intuition of the modular reset. If Lustre allowed recursion, an equation \( y = f(x) \text{ every } r \) could be translated into the following program.

\[
\begin{align*}
node \ true\text{-until}(r: \text{bool}) & \text{ returns } (c: \text{bool}) \\
& \text{let} \ c = \text{if } r \text{ then false else } (\text{true fby } c) \text{; tel} \\
node reset\_f(x: \text{int}; r: \text{bool}) & \text{ returns } (y: \text{int}) \\
& \text{var } c: \text{bool} \text{; let} \\
& c = \text{true\_until}(r) \text{;} \ y = \text{merge } c \ (f(x \text{ when } c)) \ (\text{reset\_f}(x, r) \text{ when not } c) \text{; tel}
\end{align*}
\]

In any instance of \( reset\_f \), the \( c \) variable is true until the next reset and then it is always false. While \( c \) is true, an instance of \( f(x \text{ when } c) \) defines the values of \( y \). When \( c \) becomes false, this instance is never reactivated and the values of \( y \) are defined by a fresh, recursive instantiation of \( reset\_f \).

Although such recursive programs are not accepted in Lustre, since compiling them for execution in bounded memory is difficult or impossible, this approach could be used to encode the modular reset semantics in Coq. But doing so engenders technicalities—like the need to mix mutually recursive inductive and coinductive predicates—that we prefer to avoid.

Another approach, derived from the original formalization \([6, \S 4.3]\) and mimicking the translation presented in Section 2, is to augment the semantics of nodes with a 'reset stream'. The new 'wire' is passed from node to node, combined by disjunction with local reset signals, and included in the semantics of the fby construct. Ideally though, the modular reset could be added without having to complicate the existing semantic definitions.

Our solution builds on key ideas from the recursive intuition.

1. There is an instance of \( f \) for every true value in \( r \).
2. Each instance constrains the overall execution starting from its true value up to, but not including, the next true value.

We define an operator \( k \times r \times dx \) that takes the value of \( dx \) from the instant of the \( k \)th true value of \( r \) to the instant just before the \((k + 1)\)th true value of \( r \) and is otherwise absent. The table below shows the effect of this operator—here abbreviated to \( x_{dx} \)—on the INS node for arbitrary values of \( r, g, \) and \( dx \).

<table>
<thead>
<tr>
<th>( r )</th>
<th>( g )</th>
<th>( dx )</th>
<th>( g_0 )</th>
<th>( dx_0 )</th>
<th>( INS(g_0, dx_0) )</th>
<th>( g_1 )</th>
<th>( dx_1 )</th>
<th>( INS(g_1, dx_1) )</th>
<th>( g_2 )</th>
<th>( dx_2 )</th>
<th>( INS(g_2, dx_2) )</th>
<th>( g_3 )</th>
<th>( dx_3 )</th>
<th>( INS(g_3, dx_3) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>9</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>11</td>
<td>15</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>15</td>
<td>16</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

\[
\begin{align*}
\text{INS}(g, dx) & \text{ every } r \\
& 3 4 6 8 9 15 18 20
\end{align*}
\]
The table shows a sequence of distinct instances of the \( \text{INS} \) node, with each applied to successiveclippings of the input streams to give successive clippings of the overall output stream. This gives an
infinite unrolling of the recursive intuition. Each instance constrains a different part of the output stream. Since the streams within a
node are absent whenever the inputs are, any \texttt{fbys} can only take its
initial value after its enclosing instance becomes active.

This idea is formalized by simply using a universal quantifier to denote the unrolling of node instances:

\[
\forall k. \ G \node \ f(mask \ k \ rk \ \overline{x}, \ mask \ k \ rk \ \overline{y}) 
\]

This predicate declares that in a program \( G \) and subject to a \texttt{reset}
clock \( \text{rk} \), a node \( f \) relates a list of input streams \( \overline{x} \) to a list of output
streams \( \overline{y} \) if a sequence of node instances relates suitably clipped
subsequences of the input streams to corresponding subsequences of the output streams. There is no need to explicitly ‘merge’ the
subsequences: the relational semantics simply requires that for a
given \( \overline{x} \) there exist a \( \overline{y} \) that satisfies all the constraints. The
masking of inputs ensures that a node instance is ‘fresh’ when it
becomes active. The masking of outputs ensures that an inactive
node instance does not constrain \( \overline{y} \).

We can now formally state the rule for equations defined by
node instantiation with \texttt{reset}:

\[
\begin{aligned}
H_{\forall \var r} & \var rs & \var rk & = \text{boolmask}^k \var rs \\
& \var e : \var ck \var e \var x & \var G, \var rk \var reset \ f(\var x, \var x) & \var H_{\forall \var r} \var x \var x & \var y & = \var f(\var e) \forall \var r \\
& \var G, \var H \var bk \var eck \var x & = \var ck & \var f(\var e) & \forall \var x & \var x \\
\end{aligned}
\]

It is essentially the same as the earlier rule for node instantiations
without \texttt{reset}, except that the variable \( \var r \) must be
associated with a stream \( \var rs \) and the mutual induction goes through the
new predicate rather than directly through the one for nodes.

### 3.2 Compiling the modular reset

In clock-directed modular compilation [1], a Lustre node is translated
into an Obc class with two methods: \texttt{reset} initializes the
instance variables for \texttt{fbys} and \texttt{step} calculates a transition. Methods
are recursively invoked for node instances. Our current prototype
translates (without proof) a reset equation \( \var x = \var ck \ var f(\var e) \forall \var r \) into
a conditional call to \texttt{reset} followed directly by a call to \texttt{step}. Each
call is wrapped in conditionals according to its static clock.

Consider, for example, this simple program that instantiates the
\texttt{INS} node and a \texttt{filter} node, whose definition is irrelevant:

\[
\begin{aligned}
\text{node main}(x, \text{dx}: \text{int}; \text{ck}, \text{r}: \text{bool}) \ & \text{returns} \ (y: \text{int}) \\
\var v, \ w: \text{int} \ & \text{when} \ \text{ck}; \\
\text{let} \\
\ & \var v = \text{filter}(\text{w when} \ \text{ck}); \\
\ & \var w = \text{INS}(\var v, \ \text{dx when} \ \text{ck}) \ & \text{every} \ \text{r}; \\
\ & \var y = \text{merge} \ \var ck \ \text{w} \ \var e; \\
\text{tel} \\
\end{aligned}
\]

Translation to Obc obeys the following step method.

\[
\begin{aligned}
\text{step}(x, \text{dx}: \text{int}; \text{ck}, \text{r}: \text{bool}) \ & \text{returns} \ (y: \text{int}) \ & \var v, \ w: \text{int} \ & \text{[if (ck)} \ \\
\ & \var v = \text{filter}(\var w).\var step(\var x)); \\
\ & \text{if (r)} \ \\
\ & \var w = \text{INS}(\var w).\var step(\var v, \ \text{dx}); \\
\ & \text{if (ck)} \ \\
\ & \var y = \var w \ & \text{else} \ \\
\ & \var y = 0 \} \\
\end{aligned}
\]

In this case, the fusion optimization will optimize the third and
fourth conditionals, but the interceding \texttt{reset} call prevents coa-
seling the first and third statements. This is a shame, since the
following manually optimized code calculates the same result but
with less branching.

\[
\begin{aligned}
\text{step}(x, \text{dx}: \text{int}; \text{ck}, \text{r}: \text{bool}) \ & \text{returns} \ (y: \text{int}) \ & \var v, \ w: \text{int} \ & \text{[if (r)} \ \\
\ & \{ \text{INS}(\var w).\var reset() \}; \\
\ & \text{if (ck)} \ \\
\ & \var v = \text{filter}(\var v).\var step(\var x); \\
\ & \var w = \text{INS}(\var w).\var step(\var v, \ \text{dx}); \\
\ & \var y = \var w \ & \text{else} \ \\
\ & \var y = 0 \} \\
\end{aligned}
\]

The problem is that scheduling occurs before method calls are in-
trouded, and to respect data dependencies the equation for \( \var w \) must
come between those for \( \var v \) and \( \var y \). Translating equations one-by-
one facilitates the correctness proof, but inevitably places the
reset and \texttt{step} calls together. Scheduling equations is easy to justify as
the dataflow semantics is independent of their order; justifying
reorderings of sequential programs requires more effort. Compiling
hierarchical state machines produces Lustre programs with poten-
tially many clocks and modular resets and excessive branching
gives longer execution times and pessimistic worst-case estimates.
Our future work thus aims to more effectively optimize this case.

## 4 SUMMARY AND FUTURE WORK

We have presented a novel formalization in Coq of the semantics of
the modular reset construct. Our future work will focus on develop-
ing an intermediate dataflow language that exposes the details of
node instances and methods. This will allow more precise sched-
ung and make the fusion optimization more effective. We are also
working to complete the correctness proof for the compilation of
the modular reset.

### REFERENCES

Clock-directed modular code generation for synchronous data-flow languages.
In Proceedings of the 9th ACM SIGPLAN Conference on Languages, Compilers,
121–130.

a C Compiler Front-End. In Proceedings of the 14th International Symposium on
Springer, Hamilton, Canada, 460–475.

[3] Timothy Bourke, Lélio Brun, Pierre-Evariste Dagand, Xavier Leroy, Marc Pouzet,
of the 38th ACM SIGPLAN Conference on Programming Language Design and

language for programming synchronous systems. In Proceedings of the 14th ACM
SIGPLAN-SIGACT Symposium on Principles Of Programming Languages (POPL

sion of Synchronous Data-flow with State Machines. In Proceedings of the 5th ACM
ACM Press, Jersey City, USA, 173–182.

Flow Programs. In Proceedings of the 2nd ACM SIGPLAN International Conference
on Principles and Practice of Declarative Programming (PPDP 2000). Frank Flem-
ing (Ed.). ACM Press, Montréal, Canada, 289–300.

7 (2009), 107–115.

Version 8.5.