CS:5810 Formal Methods in Software Engineering

Reactive Systems and the Lustre Language

Adrien Champion  Cesare Tinelli

---

Copyright 20015-17, Adrien Champion and Cesare Tinelli, the University of Iowa. These notes are copyrighted materials and may not be used in other course settings outside of the University of Iowa in their current form or modified form without the express written permission of one of the copyright holders. During this course, students are prohibited from selling notes to or being paid for taking notes by any person or commercial firm without the express written permission of one of the copyright holder.
Embedded systems development

Pivot language between design and code should have clear and precise semantics, and be consistent with design / prototype formats and target platforms.
Embedded systems development

Pivot language between design and code should

- have clear and precise semantics, and
Embedded systems development

Pivot language between design and code should

- have clear and precise semantics, and
- be consistent with design / prototype formats and target platforms
Lustre: a synchronous dataflow language

- **Synchronous:**
  - a base clock regulates computations;
  - computations are inherently parallel

- **Dataflow:**
  - inputs, outputs, variables, constants . . . are endless streams of values
Lustre: a synchronous dataflow language

- **Synchronous:**
  
a base clock regulates computations;
  computations are inherently parallel

- **Dataflow:**
  
inputs, outputs, variables, constants . . . are endless streams of values

- **Declarative:**
  
set of equations, no statements
Lustre: a synchronous dataflow language

- **Synchronous:**
  
  a base clock regulates computations;
  computations are inherently parallel

- **Dataflow:**
  
  inputs, outputs, variables, constants . . . are endless streams of values

- **Declarative:**
  
  set of equations, no statements

- **Reactive systems:**
  
  Lustre programs run forever
  At each clock tick they
  - compute outputs from their inputs
  - before the next clock tick
A simple example

```plaintext
node average (x, y: real) returns (out: real);
let
    out = (x + y) / 2.0;
```

A simple example

```plaintext
node average (x, y: real) returns (out: real);
let
    out = (x + y) / 2.0;
tel
```

Circuit view:

```
x + y

/ 2.0

out
```
A simple example

\[
\text{node average (x, y: real) returns (out: real);} \\
\text{let} \\
\qquad \text{out} = (x + y) / 2.0; \\
\text{tel}
\]

Mathematical view:

\[
\forall i \in \mathbb{N}, \quad \text{out}_i = \frac{x_i + y_i}{2}
\]
A simple example

```plaintext
node average (x, y: real) returns (out: real);
let
    out = (x + y) / 2.0;
tel
```

Transition system unrolled view:

clock ticks  0  1  2  3  ...
A simple example

```
node average (x, y: real) returns (out: real);
let
  out = (x + y) / 2.0;
tel
```

Transition system unrolled view:

Clock ticks

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_0$</td>
<td>$x_0$</td>
<td>$x_1$</td>
<td>$x_2$</td>
<td>$x_3$</td>
<td>...</td>
</tr>
<tr>
<td>$y_0$</td>
<td>$y_0$</td>
<td>$y_1$</td>
<td>$y_2$</td>
<td>$y_3$</td>
<td>...</td>
</tr>
<tr>
<td>$\frac{x_0+y_0}{2.0}$</td>
<td>$\frac{x_1+y_1}{2.0}$</td>
<td>$\frac{x_2+y_2}{2.0}$</td>
<td>$\frac{x_3+y_3}{2.0}$</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>$out_0$</td>
<td>$out_1$</td>
<td>$out_2$</td>
<td>$out_3$</td>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>
A simple example

**node average (x, y: real) returns (out: real);**

**let**

\[
\text{out } = \frac{x + y}{2.0};
\]

**tel**


Transition system unrolled view:

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>6.0</td>
<td>0.0</td>
<td>7.0</td>
</tr>
<tr>
<td>4.0+6.0</td>
<td>0.0+7.0</td>
<td>1.0+1.0</td>
<td>7.0+1.0</td>
</tr>
<tr>
<td>2.0</td>
<td>2.0</td>
<td>2.0</td>
<td>2.0</td>
</tr>
<tr>
<td>5.0</td>
<td>3.5</td>
<td>1.0</td>
<td>4.0</td>
</tr>
</tbody>
</table>

clock ticks: 0, 1, 2, 3, …
Combinational programs

- Basic types: bool, int, real

- Constants (i.e., constant streams):

<table>
<thead>
<tr>
<th></th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>...</td>
</tr>
</tbody>
</table>

All classical operators are provided
Combinational programs

- Basic types: bool, int, real

- Constants (i.e., constant streams):
  
  \[
  \begin{array}{ccccccc}
  2 & 2 & 2 & 2 & 2 & 2 & 2 \\
  \text{true} & \text{true} & \text{true} & \text{true} & \text{true} & \text{true} & \text{true} & \ldots
  \end{array}
  \]

- Pointwise operators:
  
  \[
  \begin{array}{cccccccc}
  x & x_0 & x_1 & x_2 & x_3 & x_4 & \ldots \\
  y & y_0 & y_1 & y_2 & y_3 & y_4 & \ldots \\
  x + y & x_0 + y_0 & x_1 + y_1 & x_2 + y_2 & x_3 + y_3 & x_4 + y_4 & \ldots
  \end{array}
  \]

- All classical operators are provided
Conditional expressions:

```plaintext
node max (n1, n2: real) returns (out: real);
let
  out = if (n1 >= n2) then n1 else n2;
tel
```

- Functional “if ... then ... else ...”
- It is an expression, **not a statement**
Combinational programs

Conditional expressions:

node max (n1, n2: real) returns (out: real);
let

     out = if (n1 >= n2) then n1 else n2;

let

- Functional “if ... then ... else ...”
- It is an expression, **not a statement**

     -- This does not compile
     if (a >= b) then m = a else m = b;
Local variables:

```plaintext
node max (a,b: real) returns (out: real);
var
  condition: bool;
let
  out = if condition then a else b;
  condition = a >= b;
tel
```
Combinational programs

Local variables:

```plaintext
code node max (a, b: real) returns (out: real);
var
  condition: bool;
let
  out = if condition then a else b;
  condition = a >= b;
endlet
```

- Order does not matter
- Set of equations not sequence of statements
Combinational programs

Local variables:

```plaintext
node max (a, b: real) returns (out: real);
var
  condition: bool;
let
  out = if condition then a else b;
  condition = a >= b;
tel
```

- Order does not matter
- Set of equations not sequence of statements
- Causality is resolved syntactically
Combinational programs

Combinational recursion is forbidden:

\[ x = 1 / (2 - x); \]
Combinational programs

Combinational recursion is forbidden:

\[ x = 1 / (2 - x); \]

- has a unique integer solution: \( x = 1 \),
- but is not computable step by step
Combinational programs

Combinational recursion is forbidden:

\[ x = 1 / (2 - x); \]

- has a unique integer solution: \( x = 1 \),
- but is not computable step by step

Syntactic loop:

\[ x = \text{if } c \text{ then } y \text{ else } 0; \]
\[ y = \text{if } c \text{ then } 1 \text{ else } x; \]
Combinational programs

Combinational recursion is forbidden:

\[ x = 1 / (2 - x); \]

- has a unique integer solution: \( x = 1 \),
- but is not computable step by step

Syntactic loop:

\[
\begin{align*}
    x &= \text{if } c \text{ then } y \text{ else } 0; \\
    y &= \text{if } c \text{ then } 1 \text{ else } x;
\end{align*}
\]

- not a real (semantic) loop:
  \[
  \begin{align*}
    x &= \text{if } c \text{ then } 1 \text{ else } 0; \\
    y &= x;
  \end{align*}
  \]
- but still forbidden by Lustre
Memory programs

Previous operator $\text{pre}$:

$(\text{pre } x)_0$ is undefined ($\text{nil}$)

$(\text{pre } x)_i = x_{i-1}$ for $i > 0$
Memory programs

Previous operator \( \text{pre} : \)

\[
\begin{align*}
\text{(pre } x)_0 & \quad \text{is undefined (nil)} \\
\text{(pre } x)_i &= x_{i-1} \quad \text{for } i > 0
\end{align*}
\]

Initialization \( \rightarrow : \)

\[
\begin{align*}
\text{(x } \rightarrow y)_0 &= x_0 \\
\text{(x } \rightarrow y)_i &= y_i \quad \text{for } i > 0
\end{align*}
\]
## Memory programs

**Previous operator** \( \text{pre} \):  
\[
(\text{pre } x)_0 \text{ is undefined ( \textit{nil} )} \\
(\text{pre } x)_i = x_{i-1} \text{ for } i > 0
\]

**Initialization** \( \rightarrow \):  
\[
(x \rightarrow y)_0 = x_0 \\
(x \rightarrow y)_i = y_i \text{ for } i > 0
\]

**Examples:**

<table>
<thead>
<tr>
<th>( x )</th>
<th>( x_0 )</th>
<th>( x_1 )</th>
<th>( x_2 )</th>
<th>( x_3 )</th>
<th>( x_4 )</th>
<th>( x_5 )</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{pre } x )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Memory programs

Previous operator \( \text{pre} \):
\[
(\text{pre } x)_0 \quad \text{is undefined (nil)}
\]
\[
(\text{pre } x)_i = x_{i-1} \quad \text{for } i > 0
\]

Initialization \( \rightarrow \):
\[
(x \rightarrow y)_0 = x_0
\]
\[
(x \rightarrow y)_i = y_i \quad \text{for } i > 0
\]

Examples:

\[
\begin{array}{c|cccccccc}
\text{x} & x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & \ldots \\
\text{pre x} & // & x_0 & x_1 & x_2 & x_3 & x_4 & \ldots \\
\end{array}
\]
Memory programs

Previous operator \( \text{pre} \):
\[
\begin{align*}
(\text{pre} \ x)_0 & \text{ is undefined (nil)} \\
(\text{pre} \ x)_i &= x_{i-1} \text{ for } i > 0
\end{align*}
\]

Initialization \( \rightarrow \):
\[
\begin{align*}
(x \rightarrow y)_0 &= x_0 \\
(x \rightarrow y)_i &= y_i \text{ for } i > 0
\end{align*}
\]

Examples:
\[
\begin{array}{c|ccccccc}
   x & x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & \ldots \\
\hline
\text{pre} \ x & // & x_0 & x_1 & x_2 & x_3 & x_4 & \ldots \\
   y & y_0 & y_1 & y_2 & y_3 & y_4 & y_5 & \ldots \\
   x \rightarrow y & & & & & & &
\end{array}
\]

11 / 17
Memory programs

Previous operator  \texttt{pre}:
\[
(\texttt{pre } x)_0 \quad \text{is undefined (nil)}
\]
\[
(\texttt{pre } x)_i = x_{i-1} \quad \text{for } i > 0
\]

Initialization  \texttt{->}:
\[
(x \rightarrow y)_0 = x_0
\]
\[
(x \rightarrow y)_i = y_i \quad \text{for } i > 0
\]

Examples:

\[
\begin{array}{l|cccccc}
  x & x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & \ldots \\
  \texttt{pre } x & // & x_0 & x_1 & x_2 & x_3 & x_4 & \ldots \\
  y & y_0 & y_1 & y_2 & y_3 & y_4 & y_5 & \ldots \\
  x \rightarrow y & x_0 & y_1 & y_2 & y_3 & y_4 & y_5 & \ldots \\
\end{array}
\]
Memory programs

Previous operator $\text{pre}$:

$(\text{pre } x)_0$ is undefined (nil)

$(\text{pre } x)_i = x_{i-1}$ for $i > 0$

Initialization $\rightarrow$:

$(x \rightarrow y)_0 = x_0$

$(x \rightarrow y)_i = y_i$ for $i > 0$

Examples:

<table>
<thead>
<tr>
<th>$x$</th>
<th>$x_0$</th>
<th>$x_1$</th>
<th>$x_2$</th>
<th>$x_3$</th>
<th>$x_4$</th>
<th>$x_5$</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{pre } x$</td>
<td>$// x_0$</td>
<td>$x_1$</td>
<td>$x_2$</td>
<td>$x_3$</td>
<td>$x_4$</td>
<td>$x_5$</td>
<td>...</td>
</tr>
<tr>
<td>$y$</td>
<td>$y_0$</td>
<td>$y_1$</td>
<td>$y_2$</td>
<td>$y_3$</td>
<td>$y_4$</td>
<td>$y_5$</td>
<td>...</td>
</tr>
<tr>
<td>$x \rightarrow y$</td>
<td>$x_0$</td>
<td>$y_1$</td>
<td>$y_2$</td>
<td>$y_3$</td>
<td>$y_4$</td>
<td>$y_5$</td>
<td>...</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>...</td>
</tr>
<tr>
<td>2 $\rightarrow (\text{pre } x)$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Memory programs

Previous operator \texttt{pre}:
\begin{align*}
(\texttt{pre }x)_0 & \text{ is undefined (nil)} \\
(\texttt{pre }x)_i & = x_{i-1} \quad \text{for } i > 0
\end{align*}

Initialization \texttt{-}\texttt{->}:
\begin{align*}
(x \rightarrow y)_0 & = x_0 \\
(x \rightarrow y)_i & = y_i \quad \text{for } i > 0
\end{align*}

Examples:
\begin{align*}
\begin{array}{c|cccccccc}
    x & x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & \ldots \\
\texttt{pre }x & // & x_0 & x_1 & x_2 & x_3 & x_4 & \ldots \\
    y & y_0 & y_1 & y_2 & y_3 & y_4 & y_5 & \ldots \\
    x \rightarrow y & x_0 & y_1 & y_2 & y_3 & y_4 & y_5 & \ldots \\
    2 & 2 & 2 & 2 & 2 & 2 & 2 & \ldots \\
    2 \rightarrow (\texttt{pre }x) & 2 & x_0 & x_1 & x_2 & x_3 & x_4 & \ldots 
\end{array}
\end{align*}
Recursive definition using \texttt{pre}:

\begin{align*}
n &= 0 \rightarrow 1 + \texttt{pre } n; \\
a &= \texttt{false} \rightarrow \texttt{not pre } a;
\end{align*}

\begin{tabular}{c|c}
\text{n} & 0 \\
\text{a} & \text{false}
\end{tabular}
Memory programs

Recursive definition using \texttt{pre}:

\begin{align*}
\text{n} &= 0 \rightarrow 1 + \texttt{pre n}; \\
\text{a} &= \texttt{false} \rightarrow \texttt{not pre a};
\end{align*}

\begin{tabular}{|c|c|c|c|c|c|}
\hline
\text{n} & 0 & 1 & 2 & 3 & \ldots \\
\text{a} & \texttt{false} \\
\hline
\end{tabular}
Memory programs

Recursive definition using \textit{pre}:

\begin{align*}
n &= 0 \rightarrow 1 + \text{pre } n; \\
a &= \text{false} \rightarrow \text{not pre } a;
\end{align*}

\begin{tabular}{l|cccccc}
  n & 0 & 1 & 2 & 3 & \ldots \\
  a & false & true & false & true & \ldots \\
\end{tabular}
node guess (signal: bool) returns (e: bool);
let
  e = false -> signal and not pre signal;
tel

<table>
<thead>
<tr>
<th>signal</th>
<th>0 1 1 0 1 0 ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td></td>
</tr>
</tbody>
</table>
node guess (signal: bool) returns (e: bool);
let
e = false -> signal and not pre signal;
tel

<table>
<thead>
<tr>
<th>signal</th>
<th>0 1 1 0 1 0 ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>0</td>
</tr>
</tbody>
</table>
node guess (signal: bool) returns (e: bool);
let
e = false -> signal and not pre signal;
tel

<table>
<thead>
<tr>
<th>signal</th>
<th>0 1 1 0 1 0 0 ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>0 1 0 0 1 0 0 ...</td>
</tr>
</tbody>
</table>
Raising edge:

```plaintext
node guess (signal: bool) returns (e: bool);
let
    e = false -> signal and not pre signal;
```

tel

<table>
<thead>
<tr>
<th>signal</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>...</td>
</tr>
</tbody>
</table>
Memory programs: examples

```
node guess (n: int) returns (out1, out2: int);
let
  out1 = n -> if (n < pre out1) then n else pre out1;
  out2 = n -> if (n > pre out2) then n else pre out2;
  tel
```

```
<table>
<thead>
<tr>
<th>n</th>
<th>4</th>
<th>2</th>
<th>3</th>
<th>0</th>
<th>3</th>
<th>7</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>out1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
node guess (n: int) returns (out1, out2: int);
let
  out1 = n -> if (n < pre out1) then n else pre out1;
  out2 = n -> if (n > pre out2) then n else pre out2;
  tel

| n  | 4 2 3 0 3 7 ...
|----|------------------|
| out1 | 4 4 4 4 4 7 ...

node guess (n: int) returns (out1, out2: int);
let
  out1 = n -> if (n < pre out1) then n else pre out1;
  out2 = n -> if (n > pre out2) then n else pre out2;
let
node guess (n: int) returns (out1, out2: int);
let
  out1 = n -> if (n < pre out1) then n else pre out1;
  out2 = n -> if (n > pre out2) then n else pre out2;
end
Memory programs: examples

Min and max of a sequence:

```plaintext
node guess (n: int) returns (out1, out2: int);
let
    out1 = n -> if (n < pre out1) then n else pre out1;
    out2 = n -> if (n > pre out2) then n else pre out2;
```

<table>
<thead>
<tr>
<th>n</th>
<th>4 2 3 0 3 7 ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>out1</td>
<td>4 2 2 0 0 0 0 ...</td>
</tr>
<tr>
<td>out2</td>
<td>4 4 4 4 4 7 ...</td>
</tr>
</tbody>
</table>
Design a node

```plaintext
node switch (on, off: bool) returns (state: bool);
```

such that:

- state raises (false to true) if on;
- state falls (true to false) if off;
Design a node

```plaintext
node switch (on, off: bool) returns (state: bool);
```

such that:

- state raises (false to true) if on;
- state falls (true to false) if off;
- everything behaves as if state was false at the origin;
- switch must work properly even if on and off are the same.
Compute the sequence 1, 1, 2, 3, 5, 8 ...
Compute the sequence 1, 1, 2, 3, 5, 8, 13, 21 …

Fibonacci sequence:

\[ u_0 = u_1 = 1 \]
\[ u_n = u_{n-1} + u_{n-2} \quad \text{for} \ n \geq 2 \]
These notes are based on the following lectures notes:

The Lustre Language — Synchronous Programming
by Pascal Raymond and Nicolas Halbwachs
Verimag-CNRS