Correct-by-construction asynchronous implementation of modular synchronous specifications

Benoît Caillaud  -  IRISA, Rennes, France
Dumitru Potop   -  INRIA, Rocquencourt, France
Outline

• Motivation: Asynchronous implementation of synchronous specifications
  – GALS architectures
  – Desired efficient implementation

• Formal model
  – Correctness

• Correctness criteria
  – Microstep weak endochrony
  – Microstep weak isochrony

• Conclusion
Synchrony, asynchrony, GALS

- Synchronous specification
  - Global clock $\Rightarrow$ ease of specification & verification
  - Popular, efficient tools for system design
    (digital circuits, safety-critical systems)

- Distributed implementation
  - Distributed software, complex digital circuits (SoC/NoC), heterogeneous systems
    - Loosely-connected components (asynchronous FIFOs...)

- GALS architectures = good implementation model
  - Synchronous components, asynchronous communication
  - Problem: preserve semantic consistency between synchronous specification and GALS implementation
What we want

1. Take a modular synchronous specification
What we want

1. Take a modular synchronous specification

2. Replace comm. with asynchronous FIFOs, wrappers

3. Preserve:
   • Functionality
   • Correctness
     • No “extra” traces
     • No deadlocks (Kahn processes)
   • Parallelism
Previous work

- **Latency-insensitive systems**
  - Carloni & Sangiovanni-Vincentelli (1999)
  - Goal: independence from communication delays
  - Global synchrony: system speed = slowest component speed

- **Endo/isochronous systems**
  - Benveniste, Caillaud, Le Guernic (1999)
    - Version: Generalized latency-insensitive circuits (Singh, Theobald, 2003)
  - Goals:
    - minimize communication
    - maximize concurrency, independence between system components
  - Not compositional!
Previous work

- Weakly endo/isochronous systems
  - Potop, Caillaud, Benveniste (2004)
  - Goals:
    - further minimize communication by exploiting intra-component concurrency
    - Compositionality!
  - Synchronous Mazurkiewicz traces
  - Does not handle causality and communication deadlocks

- This work: microstep weakly endo/iso systems
  - Goal: take into account causality and composition through read/write mechanisms
Our approach

• Define a model and criteria ensuring that:
  – Creating delay-insensitive wrappers that preserve the semantics is possible without adding new signals
  – Connecting through FIFOs the resulting components produces a semantics-preserving, deadlock-free GALS implementation

• Make given components satisfy the criteria:
  – Possible solutions
    • Encode (part of) the “absent” events (Carloni et al.)
    • Add new signals
    • Decide that none is necessary due to environment constraints

• Efficient sw/hw implementation
  – Sync./async. synthesis techniques, GALS-specific communication schemes, etc.
The model: basic definitions

- The basics: (incomplete) automata
  \[ \Sigma = (S, s_0, V, \rightarrow), \quad \rightarrow \subseteq S \times L(V) \times S, \quad L(V) = \prod_{v \in V} (D_v \cup \bot) \]
  
  - Composition by synchronized product:

  \[
  \begin{array}{c}
  0 \\
  A=1 \ B=\bot \ D=\bot \\
  \end{array} \quad \times \quad \begin{array}{c}
  0 \\
  A=1 \ B=7 \ C=3 \\
  \end{array} \quad = \quad \begin{array}{c}
  0,0 \\
  A=1 \ B=\bot \ C=3 \ D=\bot \\
  \end{array}
  \]

  - Renaming operator:

  \[
  \Sigma_1[D/C] : \quad \begin{array}{c}
  0 \\
  A=1 \ B=\bot \ C=\bot \\
  \end{array}
  \]

- Labels
  \[
  \begin{array}{c}
  A=1 \ B=\bot \ C=3 \equiv A=1 \ C=3 \\
  A=1 \ C=3 \leq A = 1 \ B=7 \ C=3 \\
  A=1 \ C=3 - A=1 = C=3 \\
  A=1 \ C=3 ; B=2 ; ; \\
  A=1 \ C=3 ; B=2 ; ; \preceq A=1 \ C=3 ; B=2 ; ; A=2;
  \end{array}
  \]

- Finite runs:
The model: basic definitions

- Generalized concurrent transition systems (GCTS)
  - Void transitions: 
  - Down closure: 

Example:
The model: I/O transition systems

- **Point-to-point communication:**
  - Broad/Multicast can be simulated...
  - Communication channels: $c = (!c, ?c)$ \[D_{!c} = D_{?c} = D_c\]
  - Dissociate emission from reception!

- **Clocks:** $\tau \tau_1 \ldots$ of domain $D_{clk} = \{T\}$

- **I/O transition system:**
  - GCTS where all variables are channels or clocks
  - Example:
The model: synchronous systems

- **Synchronous system:** $\Sigma = (S, s_0, V, \tau, \rightarrow)$

I/O transition system, one clock, and satisfying:

1. Clock transitions:

   \[
   s \xrightarrow{r} s' \quad \Rightarrow \quad r\text{ equals } \bot \text{ over } V
   \]

3. Stuttering invariance:

   \[
   s_0 \xrightarrow{\tau} s_0 \quad \text{and} \quad s \xrightarrow{\tau} s' \Rightarrow s' \xrightarrow{\tau}
   \]

5. Single assignment:

   \[
   s_0 \xrightarrow{r_1} s_1 \xrightarrow{r_2} \ldots \xrightarrow{r_n} s_n \quad \Rightarrow \quad \text{supp}(r_i) \cap \text{supp}(r_j) = \emptyset \text{ for all } i \neq j
   \]

- **Example:**

   ![Example Diagram]
The model: composition

- Synchronous 1-place register:

\[
\text{SFIFO}(c, \tau): \quad \sigma^0 \xrightarrow{!c=x} \sigma_x \xrightarrow{?c=x} \sigma^1 \quad \text{for all } x \in D_c
\]

- Synchronous composition (on clock \(\tau\)):

\[
\Sigma_1|\Sigma_2 = \Sigma_1[\tau_1/\tau] \times \Sigma_2[\tau_2/\tau] \times \text{SFIFO}(c_1, \tau) \times \ldots \times \text{SFIFO}(c_n, \tau)
\]

- Asynchronous FIFO:

\[
\text{AFIFO}(c): \quad x_1 \ldots x_n \xrightarrow{!c=x_{n+1}} x_1 \ldots x_{n+1} \xrightarrow{?c=x_1} x_2 \ldots x_n
\]

\[
\text{for all } x_1, \ldots, x_n, x_{n+1} \in D_c
\]

- Asynchronous composition:

\[
\Sigma_1||\Sigma_2 = \Sigma_1 \times \Sigma_2 \times \text{AFIFO}(c_1) \times \ldots \times \text{AFIFO}(c_n)
\]
The model: composition
Example

$\Sigma_1: \tau_1$

$\Sigma_2: \tau_2$

$\Sigma_1|\Sigma_2:$

$\Sigma_1||\Sigma_2:$
Example

\[\Sigma_1: \tau_1 \quad \Sigma_2: \tau_2\]

\[\tau_1, \tau_2, \tau_1 \tau_2\]

\[\tau_2, \tau_2, \tau_1 \tau_2\]

\[\Sigma_1 \| \Sigma_2:\]

\[\tau_1, \tau_2, \tau_1 \tau_2\]

\[\tau_1, \tau_2, \tau_1 \tau_2\]

\[\tau_1, \tau_2, \tau_1 \tau_2\]
Correctness

• Some notations:

\[ \begin{align*}
!A=1 \; ; \; \tau_1 ; \; ?A=1 \; ; \; \tau_2 ; \; !C=3 \; ; \; \sim \; !A=1 \; ?A=1 \; ; \; \tau_1 \tau_2 ; \; !C=3 \; ; \; \tau_2 ; \\
!A=1 \; ; \; \tau_1 ; \; \tau_2 ; \; !C=3 \; ; \leq !A=1 \; ?A=1 \; ; \; \tau_1 \tau_2 ; \; !C=3 \; ; \; \tau_2 ;
\end{align*} \]

• Formal correctness criterion

\[ \Sigma_1 \parallel \ldots \parallel \Sigma_n \text{ is correct w.r.t. } \Sigma_1 \parallel \ldots \parallel \Sigma_n \text{ if} \]

for all \( s \in \text{RSS}(\Sigma_1 \parallel \ldots \parallel \Sigma_n) \) and all \( \phi \in \text{Traces}_{\Sigma_1 \parallel \ldots \parallel \Sigma_n}(s) \)

there exist \( \alpha \in \text{Traces}_{\Sigma_1 \parallel \ldots \parallel \Sigma_n}(s) \) and \( \beta \in \text{Traces}_{\Sigma_1 \parallel \ldots \parallel \Sigma_n}(s) \)

such that \( \phi \leq \alpha \) and \( \alpha \sim \beta \)

• Intuition: every trace of \( \Sigma_1 \parallel \ldots \parallel \Sigma_n \) can be completed to one that is equivalent to a synchronous trace
Microstep weak endochrony

- **Compositional delay-insensitivity criterion** (signal absence information is not needed)
- **Axioms (part 1):**
  
  A1: Determinism

  A2: In every state, non-clock transitions sharing no common variable are independent
Microstep weak endochrony

- **Axioms (continued):**
  
  A1: Determinism
  
  A2: In every state, non-clock transitions sharing no common variable are independent
  
  A3: Non-contradictory reactions can be united

  ![Graph 1](image1)
  
  ![Graph 2](image2)

  A4: Conflict does not change with time

  ![Graph 3](image3)
Example

\[ \Sigma_1: \quad \tau_1 \quad 0 \quad !A \quad 1 \quad 2 \quad \tau_1 \quad \tau_1 \quad ?R \quad 3 \quad \tau_1 \]
Example

$\Sigma'_1: \tau_1$

0 \rightarrow 1: !A, ?D=0

1 \rightarrow 2: \tau_1, ?B

1 \rightarrow 3: ?D=1, ?R

2 \rightarrow 3: \tau_1, ?R

3 \rightarrow 2: \tau_1, ?B
Example

$\Sigma_1^\prime$: $\tau_1$ $!A$ $?D=0$ $2'$ $?B$ $2$ $\tau_1$

$?D=1$ $3'$ $?R$ $3$ $\tau_1$

$\Sigma_3$: $\tau_1$ $!A$ $?B$ $2$ $\tau_1$

$?R$ $3$ $\tau_1$

$4$ $\tau_1$
Weak non-blocking property

- **Weak non-blocking**

  $\Sigma_1, \ldots, \Sigma_n$ are weakly non-blocking iff

  for all $s \in \text{RSS}(\Sigma_1|\ldots|\Sigma_n)$ and all $\phi \in \text{Traces}_{\Sigma_1|\ldots|\Sigma_n}(s)$ maximal and containing no clock transition, there exists $\alpha \in \text{Traces}_{\Sigma_1|\ldots|\Sigma_n}(s)$ non-void such that $\alpha \preceq \phi$ and $\alpha;\tau \in \text{Traces}_{\Sigma_1|\ldots|\Sigma_n}(s)$

- **Semantics preservation criterion**

  If $\Sigma_1, \ldots, \Sigma_n$ are weak non-blocking and weak endochronous, then $\Sigma_1||\ldots||\Sigma_n$ is correct w.r.t. $\Sigma_1|\ldots|\Sigma_n$
Example

$\Sigma_1': \tau_1$

$\Sigma_4: \tau_2$

Diagram of a system with transitions and states labeled with symbols and labels indicating inputs and outputs.
Example

$\Sigma_1': \tau_1$

$\Sigma_4': \tau_2$
Conclusion

• Decidable criteria for GALS implementation of synchronous specifications
  – Covers causality and read/write communication
  – Compositionality, concurrency

• Future: Synthesis
  – Heuristics for actual synchronous languages and specifications. Scaling issues (large specifications).
  – GALS circuits using asynchronous logic
  – Deal with mode changing latency

• What about timed models?