Modeling and Validation of Globally Asynchronous Design in Synchronous Frameworks

Mohammad Reza Mousavi, Paul Le Guernic, Jean-Pierre Talpin, Sandeep Kumar Shukla, Twan Basten

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Modeling and Validation of Globally Asynchronous Design in Synchronous Frameworks

Mohammad Reza Mousavi[1], Paul Le Guernic[2], Jean-Pierre Talpin[2],
Sandeep Kumar Shukla[3], Twan Basten[1]

[1] Eindhoven University of Technology
[2] INRIA/IRISA-Rennes

[3] Virginia Tech

N˚4935

Septembre 2003

THÈME 1

ISSN 0249-6399 ISRN INRIA/RR--4936--FR+ENG

Modeling and Validation of Globally Asynchronous Design in Synchronous Frameworks

Mohammad Reza Mousavi[1], Paul Le Guernic[2], Jean-Pierre Talpin[2], Sandeep Kumar Shukla[3], Twan Basten[1]

[1] Eindhoven University of Technology
[2] INRIA/IRISA-Rennes
[3] Virginia Tech

Thème 1 — Réseaux et systèmes
Projet ESPRESSO

Rapport de recherche n° 4935 — Septembre 2003 — 18 pages

Abstract: We lay a foundation for modeling and validation of asynchronous designs in a multi-clock synchronous programming model. This allows us to study properties of globally asynchronous systems using synchronous simulation and model-checking toolkits. Our approach can be summarized as automatic transformation of a design consisting of two asynchronously composed synchronous components into a fully synchronous multi-clock model preserving the flow equivalence. Since true asynchrony is not amenable to modeling in synchronous design frameworks, we seek to automatically insert desynchronizing protocol to 'match' the asynchronous model. Such protocol insertion brings about the possibility of formally investigating the behavior of globally asynchronous components in synchronous environments and hence leveraging the tools and techniques developed over decades for such environments. The ultimate goal of this research is to provide the possibility to model and build GALS systems in a way to preserve some proven properties when deployed on an asynchronous network.

Key-words: Formal methods, embedded systems design, globally asynchronous locally synchronous architectures

(Résumé : tsvp)

Unité de recherche INRIA Rennes
IRISA, Campus universitaire de Beaulieu, 35042 RENNES Cedex (France)
Téléphone : 02 99 84 71 00 - International : +33 2 99 84 71 00
Télécopie : 02 99 84 71 71 - International : +33 2 99 84 71 71

Conception de systèmes asynchrones fondée sur une approche polychrone

Résumé : Nous proposons une théorie pour la modélisation et la validation de systèmes asynchrones au moyen d'un modèle de programmation synchrone multi-horloge. Nous étudions les propriétés de systèmes globallement asynchrones en utilisant des techniques de simulations et de model-checking. Notre approche peut se résumer en la transformation automatique d'un système constitué de composants connectés de manière asynchrone en un système synchrone multi-horloge équivalent (en flôts) au premier. Comme l'asynchrone ne peut pas en général être modélisé dans un outil de conception synchrone, nous cherchons donc à insérer de manière automatique un protocole de désynchronisation capable de modéliser le comportement asynchrone de l'application considérée (lorsque cela est possible). Cette insertion de protocole offre la possibilité d'étudier formellement le comportement de systèmes asynchrones dans un outil de conception synchrone et donc d'utiliser les outils et les techniques (compilation, transformation, vérification) développées avec ces outils. Le but de notre travail est de permettre la modélisation et la construction d'architectures GALS (globallement asynchrones locallement synchrones) d'une manière préservant des propriétés formellement établies avant de les déployer sur un réseau asynchrone.

Mots-clé : Méthodes formelles, conception de systèmes enfouis, architectures globalement asynchrones locallement synchrones

1 Introduction

Synchronous languages have been extensively used in the (co-)design of software and hardware systems [4]. Applying synchronous languages to real-world designs revealed their strong and weak points over time. Abstract and easy to learn and use syntax, formal and succinct semantics (which paved the way for efficient simulation and verification tools) are among the strong points of such languages. However, the synchronous assumption turns out to be a limiting factor. On one side of the spectrum, in distributed real-time systems, providing a single, fully synchronized clock over distributed nodes may be very expensive or actually infeasible. On the other side of the spectrum, in nano-scale system design, the propagation delay of the clock over the chip size becomes a major obstacle in providing a single synchronized clock. Thus, all these domains call for a mix of synchronous and asynchronous design patterns.

Globally Asynchronous, Locally Synchronous (GALS) designs have emerged in the recent years in response to the above mentioned challenges and have received major attention from the system level design community. In GALS design, the system is composed of synchronous components that have their local synchronous clock structures and communicate using asynchronous schemes. There have been several attempts to formalize GALS design (see for example, [13, 3]).

Problem Statement In this paper, we address the problem of modeling and validating globally asynchronous composition of synchronous components in the multi-clock synchronous programming framework SIGNAL. The main goal of such an approach is to leverage the simulation and model checking toolkit existing for such frameworks [1]. Our solution can be seen as a formal methodology for composing existing IP blocks, designed with synchronous assumptions, in an asynchronous fashion to satisfy the demands of tomorrow's GALS designs.

Our approach can be summarized as transforming the design consisting of two synchronously composed components to a design that is *equal* to asynchronously composed components. Since true asynchrony does not exist in synchronous design frameworks, we seek for a desynchronizing protocol to match the asynchronous model. Finding such a protocol brings about the possibility of formally investigating the behavior of synchronous components in asynchronous environment.

In Section 2 we present some related work. Section 3, contains definitions of the SIGNAL language. Subsequently, we define an ideal desynchronizing protocol using unbounded fifo channels and prove it correct in Section 4. Since an unbounded fifo channel cannot be implemented in SIGNAL, this protocol is only an imaginary model but it can be used as a reference model for other non-perfect desynchronization protocols. Then, we provide the conditions under which this design can be refined to a network of bounded and thus implementable fifo channels. In Section 5, we propose an implementation by defining the fifo channels and the wrapping (the protocol) around components to prevent overwriting the

buffer data. Furthermore, we present a design to estimate the appropriate fifo channel size in practice. Finally, Section 6 summarizes the results and presents the concluding remarks.

2 Related Work

In [2], distributing SIGNAL programs is studied under synchronous conditions. Since all components are assumed to work with a single master clock, there, the size of the buffer is naturally restricted to one. In [14], the problem of decomposing SIGNAL programs into components is studied and a handshaking mechanism is proposed for the asynchronous communication of components. Our work extends the results of [2, 14] to asynchronous settings were handshaking is removed or reduced to some extent.

In [13], the issue of communication-based design is addressed. It introduces the idea of *Behavior Adapters* in order to interface two (possibly mismatching) input and output signals. Fifo queues are then proposed as primitive communication channels. It is claimed there that unbounded fifo channels are ideal communication mechanisms for asynchronous designs (expressed as Abstract Co-Design Finite State Machines or ACFSMs for short). Then ACFSMs are refined into ECFSMs which contain a network of bounded fifo channels and a blocking mechanism or a lossy channel to overcome the rate mismatch problem.

Our contribution to the work of [13] can be summarized in the following two issues: First, we formalize the concepts of asynchronous design in the SIGNAL model. This formalization provides us the possibility to prove the claim of ideal asynchrony with unbounded buffer and the conditions for refining it to bounded buffer. Moreover, it provides the reference theoretical model for implementations of asynchrony. Secondly, we propose a practical design to estimate the size of buffer in the refined design so that we can decrease the amount of blocking for normal system behavior.

The work of Berry and Sentovich in [5] studies the issue of asynchronous interaction between synchronous Esterel programs. There, the authors solve the problem of overwriting messages due to asynchrony by proposing a protocol that blocks the sender processor until the receiver process consumes the data value in the buffer. Although in this way the buffer size is restricted to 1, the parallelism and pipelining is decreased.

In [7], distribution of synchronous sequential programs (in style of Esterel programs) is discussed. In this approach, the asynchronous interaction between the components is encapsulated in *send* and *recieve* commands and the main effort is invested in exploring the appropriate places for send and receives in order to minimize communication and maximize parallelism. However, the issue of buffer size is left implicit and remains to be addressed by investigating the semantics of (asynchronous) send and receive commands which in one way or the other involves this issue.

Implementing asynchronous systems using synchronous languages is also studied in [8]. After defining a generic semantic model for synchronous and asynchronous computation, the attention is focused on implementing communication mechanisms such as mutual exclusion mechanisms and rendez-vous. Although these mechanisms can be very handy in asynchronous system design, the paper does not suggest any process starting from syn-

chronous designs and arriving in components instrumented with these structures. This is one of the goals of the present paper (with respect to fifo channels).

The work of [9] models asynchrony (interleaving semantics) in I/O Automata model using a synchronous communication mechanism. However, due to differences between the models of computation (such as input enabling assumption in I/O Automata), the notion of buffer is internalized inside the semantics of [9] and is not addressed explicitly.

3 System Design in SIGNAL

The abstract syntax of core-SIGNAL is given in Figure 1. In this syntax, a SIGNAL program is decomposed into several components. Components are assumed to work synchronously and in parallel. Decomposition of a SIGNAL program can be as a result of re-use a number of COTS (Commercial Off The Shelf) components or using decomposition techniques based on graph partitioning (see for example [12, 14]). A single component consists of a number of signal definitions. The set of all signal names is denoted by X with typical members $x, y, z, \ldots$. There are a few primitive operators in SIGNAL allowing for definition of basic processes. The expression $x = \texttt{pre}\ val\ y$ defines that the signal named x holds the previous value of signal y, and it is initially set to val (thus, x and y are synchronous). The equation $x = y\ \texttt{when}\ z$ defines x to have the value of y when z is present and *true*. The equation $x = y\ \texttt{default}\ z$ defines x by y when it is present and otherwise by z.

$$
\begin{array}{lcll}
\mathit{Program} & ::= & \mathit{PName} = & \mathit{Component} \mid \\
 & & & \mathit{Component} \mid\mid_s \mathit{Program} \\
\mathit{Component} & ::= & \mathit{CName} = \mathit{Expressions} & \\
\mathit{Expressions} & ::= & \mathit{Expression} \mid \mathit{Expression}, \mathit{Expressions} & \\
\mathit{Expression} & ::= & x = \texttt{pre}\ val\ y \mid & \\
 & & x = y\ \texttt{when}\ z \mid & \\
 & & x = y\ \texttt{default}\ z \mid & \\
 & & x = f(y, z, \ldots) &
\end{array}
$$

Figure 1: Abstract Syntax of SIGNAL

Apart from primitive operators, we assume existence of a number of arithmetic operators (and in particular, equality, denoted by $==$) that make computation on synchronously available arguments. In our examples of SIGNAL programs, we use $\hat{}x$ as a shorthand for $true\ \texttt{when}\ (x == x)$ which intuitively means "the clock of x".

Example 1 (One-Place Buffer) To specify a single place buffer, first we give specification of a single cell memory, as follows:

$$
\begin{array}{lcl}
data & = & msgIn\ \texttt{default}\ (\texttt{pre}\ 0\ data) \\
msgOut & = & data\ \texttt{when}\ \hat{}msgOut
\end{array}
$$

The above program allows for independent read and write accesses (denoted by $msgIn$ and $msgOut$) and the memory cell keeps the last written value and is initialized to 0. The

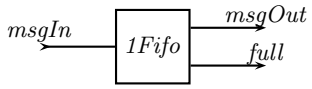
$$
\begin{array}{lcl}
[[x = \texttt{pre}\ \ val\ y]] & = & \{b_{|\{x,y\}} | tags(b(x)) = tags(b(y)), b(x)(t(b(y)_1)) = val, \\
& & \forall i \in I\!N, b(x)(t(b(y)_{i+1})) = b(y)(t(b(y)_i))\} \\
[[x = y\ \texttt{when}\ z]] & = & \{b_{|\{x,y,z\}} | tags(b(x)) = tags(b(y)) \cap \{t | t \in tags(b(z)) \wedge b(z)(t) = true\}, \\
& & \forall t \in tags(b(x)), b(x)(t) = b(y)(t)\} \\
[[x = y\ \texttt{default}\ z]] & = & \{b_{|\{x,y,z\}} | tags(b(x)) = tags(b(y)) \cup tags(b(z)), \\
& & \forall t \in tags(b(x)), (b(x)(t) = (b(y)(t)\ \wedge\ t \in tags(b)(y))) \vee \\
& & (b(x)(t) = b(z)(t)\ \wedge\ t \notin tags(b(y))\ \wedge\ t \in tags(b)(z)))\}
\end{array}
$$

Table 1: Semantics of elementary SIGNAL equations

independence between the rate of input and output signals shows the essence of polychrony in SIGNAL design. This provides us the possibility for desynchronizing the designs. To change this initial specification to a single place buffer where the causality between reads and writes are forced and the first in first out principle is observed, we have to make the following changes to the program:

$$
\begin{array}{ll}
data & = (msgIn\ \texttt{when}\ (\texttt{not}\ full))\ \texttt{default} \\
& \quad (\texttt{pre}\ 0\ data) \\
full & = (false\ \texttt{when}\ {}^\wedge msgOut)\ \texttt{default} \\
& \quad ((true\ \texttt{when}\ {}^\wedge msgIn)\ \texttt{default} \\
& \quad (\texttt{pre}\ false\ full)) \\
msgOut & = data\ \texttt{when}\ ({}^\wedge msgIn\ \texttt{default}\ full) \\
{}^\wedge data & = ({}^\wedge msgIn\ \texttt{default}\ {}^\wedge msgOut)\ \texttt{default}\ {}^\wedge full
\end{array}
$$

This program only writes the value of input into the buffer, if the buffer is not full and only allows to take the data from the output, if the buffer contains some data. The buffer is initially set to be empty and becomes full when a data item is written to it provided that it is not taken out at the same moment.



msgIn		1		2		3
full	*false*	*true*		*true*	*true*	*false*
data	0	1	1	1	1	3
msgOut					1	3

Figure 2: Sample behavior of a 1-place buffer

In this paper, we use the tagged model [11] of SIGNAL language defined in [10]. Tagged model of [10] defines behavior of a SIGNAL process (program) in terms of independent signals that

may have different time scales. Thus, in this *polychronous* model, time is not necessarily linear. Denotation of a SIGNAL process is defined as follows.

Definition 1 (Denotation of a Process) Time is taken from a dense set T (called *tags*) with a partial order $\preceq$. This notion of time allows for specification of distributed processes with local clocks (possibly with different rates) and synchronization points. Events are values of signal at points of time. The set of events $\varepsilon = T \times V$ is a relation between tags and values (V). We denote the time of event e by $t(e)$. A signal $s \in S : T \rightarrow V$ is a partial function defining the value of a signal over a discrete chain of tags (thus, events in a signal are internally ordered and their tags are assumed to be well-founded). For a signal s, we denote its i'th event ($i \in \mathbb{N}$) by s_i and the sub-chain of length $n+1$ starting from i'th event by $s_{i...i+n}$. The set of events of signal s up to the point t is denoted by $[s]_t$ and the length of the chain of signal s is denoted by $|s| \in \mathbb{N} \cup \{\infty\}$. In this paper, we are concerned with processes containing infinite (reactive) behavior. However, our results can be easily generalized to cover finite behavior, as well.

A behavior $b \in B : X \rightarrow S$ is a partial function defining signal values for different signal names from the set X. Domain of a behavior b is denoted by $vars(b)$ and represents signal names taking part in this behavior. A process $P \subseteq B$ is a set of behaviors over a common set of signal names defining different possible behaviors of a program (a component). Two processes P and Q are equal ($P = Q$) if they contain the same set of behaviors. Projection of a behavior b on a set of variables $var \subseteq X$ (denoted by $b_{|var}$) is defined by restricting the domain of the behavior to var. Projection of a process P on var (denoted by denoted by $P_{|var}$) is defined by projection of all its member behaviors. Its dual, denoted by $b_{\backslash var}$ (similarly, $P_{\backslash var}$), is a short-hand for $b_{|vars(b)\backslash var}$.

Semantics of basic equations in SIGNAL is defined in Table 1, in terms of denotation of the basic processes.

Definition 2 (Stretching and Stretch-Equivalence) A behavior b is a stretching of behavior c denoted by $b \leq c$ if and only if $vars(b) = vars(c)$ and there exists a bijection $f : T \rightarrow T$ such that

1. $\forall t, u \in T, t \preceq u \Leftrightarrow f(t) \preceq f(u)$
2. $\forall t \in T, t \preceq f(t)$
3. $\forall x \in vars(b) dom(c(x)) = f(dom(b(x)))$
4. $\forall x \in vars(b) \forall t \in T, b(x)(t) = c(x)(f(t))$

Intuitively, stretching changes the time scale of behaviors while preserving the causal orderings. Two behaviors b and c are stretch equivalent, denoted by $b \lesseqgtr c$, if and only if there exists a behavior d such that $d \leq b$ and $d \leq c$. The definition of stretching and stretch equivalence is extended to processes using element-wise comparison of member behaviors. Stretch closure of a processor is denoted by P^* and is defined as $\{b | \exists c \in P, b \lesseqgtr c\}$. A process P is stretch-closed if and only if $P^* = P$.

Definition 3 (Synchronous Parallel Composition) Semantics of synchronous parallel composition (denoted by $||_s$), is defined as follows:

$$P \,||_s\, Q = \{d_{|X\cup Y} | \exists (b,c) \in P \times Q, d_{|X} = b_{|X} \wedge d_{|Y} = c_{|Y}\}$$

where $X = vars(P)$ and $Y = vars(Q)$.

Lemma 1 All SIGNAL programs are stretch-closed.

Proof. Inspecting (in Table 1), we see that basic statements preserve stretch-closedness. Synchronous parallel composition also preserves stretch-closedness (see Lemma 4 in the Appendix). Thus, the lemma follows by an structural induction on the structure of the programs. ⊠

Definition 4 (Relaxation and Flow Equivalence) Behavior b is a relaxation of c, denoted by $c \sqsubseteq b$ if and only if $vars(b) = vars(c)$ and for all $x \in vars(b), b_{|\{x\}} \leq c_{|\{x\}}$. Intuitively, relaxation stretches different signal with possibly different rates (which may not preserve causal ordering). Two behaviors b and c are flow equivalent, denoted by $b \approx c$, if and only if $\exists d, b \sqsubseteq d \wedge c \sqsubseteq d$. Relaxation of processes is defined similarly by an element-wise comparison of behaviors.

Definition 5 (Renaming Signals) Behavior $b[y/x]$ (similarly, process $P[y/x]$) is the result of renaming signal name x by the fresh signal name y ($y \notin vars(P)$) in b (similarly, in all behaviors in P).

4 Desynchronizing

The aim of this section is to give an implementation (a concrete way of modelling) of asynchronous parallel composition in SIGNAL language using synchronous (polychronous) constructs. We start with defining the notion of asynchronous parallel composition and restrict it to a causally ordered distributed setting. Then, we show that replacing explicit data dependencies of two components with an unbounded fifo buffer (defined semantically in the remainder) is a correct implementation of asynchronous causal parallel composition. Then, we set out to replace the unbounded fifo with fifo channels of a bounded size. To do this, we investigate the conditions under which this leads to a correct implementation. This section sets the theoretical ground on desynchonization for empirical design in the following section.

4.1 Desynchronizing with Unbounded Fifo

The main idea behind desynchronizing is implementing the asynchronous parallel composition in SIGNAL designs using fifo channels. Figure 3 depicts a schematic view of desynchronization. In this process, by introducing a fifo channel for each data dependency on

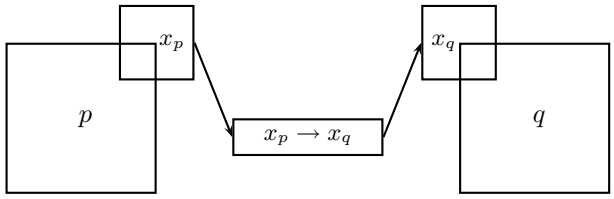


Figure 3: Desynchronization: Schematic View

a shared variable, we relax the synchrony between the two components. To prove correctness of this approach, we start with proving the fact that if this replacement is done by an unbounded fifo channels, it is indeed a correct implementation of a asynchronous-causal parallel composition:

Definition 6 (Asynchronous Parallel Composition) Asynchronous parallel composition of two processes P and Q is defined as follows [10]:

$$\begin{aligned} P \mid\mid_a Q = \{ & d_{|X \cup Y} | \exists (b,c) \in P \times Q, \\ & d_{\backslash Y} \lesseqgtr b_{\backslash Y} \wedge d_{\backslash X} \lesseqgtr c_{\backslash X} \\ & \wedge b_{|X \cap Y} \sqsubseteq d_{|X \cap Y} \wedge c_{|X \cap Y} \sqsubseteq d_{|X \cap Y} \} \end{aligned}$$

where $X = vars(P)$ and $Y = vars(Q)$. This definition defines that when two processes are put in asynchronous parallel composition, their internal actions may be stretched (due to different relative time scales of their local platforms) and their common variables (their communication media) may be stretched with different rate (denoted by relaxation notation, due to different characteristics of communication channels).

Corollary 1 For two processes P^* and Q^* such that $vars(P) \cap vars(Q) = \emptyset$, it holds that:

$$P^* \mid\mid_s Q^* = P^* \mid\mid_a Q^*$$

Note that for the above corollary to hold, the assumption of being stretch-closed for both P^* and Q^* is essential.

Definition 7 (Asynchronous-Causal Parallel Composition) If two processes P and Q share a variable x ($x \in vars(P) \cap vars(Q)$), then there is an *explicit data-dependency* between P and Q. If there is a causal ordering between P and Q (or vice-versa) on data-dependency x, it is shown by $P \leq_x Q$ ($Q <_x P$, respectively). This means that P is the producer of x and Q is its consumer (x appears only in the right-hand-side of the assignments in P and in the left-hand-side in Q). Note that in a general SIGNAL program, for a data dependency x, it is not necessarily true that $P \leq_x Q$ or $Q \leq_x P$. However, we conjecture that any reasonable SIGNAL program (that does not have cyclic data dependencies at any point of time) can be transformed to a program that has the above property (by decomposing all two way channel variables into two one way channels).

We define asynchronous causal parallel composition of two processes (denoted by $||_{\leq,a}$) as follows:

$$\begin{aligned} P \,||_{\leq,a}\, Q = \{ & d_{|X\cup Y} | \exists (b,c) \in P \times Q, \\ & d_{\backslash Y} \lesseqgtr b_{\backslash Y} \wedge d_{\backslash X} \lesseqgtr c_{\backslash X} \\ & \wedge b_{|X\cap Y} \sqsubseteq d_{|X\cap Y} \wedge c_{|X\cap Y} \sqsubseteq d_{|X\cap Y} \\ & \wedge \forall x \in X \cap Y, P \leq_x Q \Rightarrow b_{|\{x\}} \leq c_{|\{x\}} \\ & \wedge \forall y \in X \cap Y, Q \leq_y P \Rightarrow c_{|\{y\}} \leq b_{|\{y\}} \} \end{aligned}$$

The above definition common to asynchronous parallel composition allows for asynchronous communication and stretching internal behavior of processes. Furthermore, it asserts that if P depends on x for Q, it cannot read x before it is written by Q and vice versa.

Corollary 2 For two processes P and Q such that $vars(P) \cap vars(Q) = \emptyset$, it holds that:

$$P \,||_a\, Q = P \,||_{\leq,a}\, Q$$

Definition 8 (Asynchronous Fifo Channel) An (unbounded) asynchronous fifo channel $AFifo_{x\to y}$ with input port x and output port y is the smallest stretch-closed process P satisfying $vars(P) = \{x, y\}$ and $P_{|x}[y/x] \leq P_{|y}$.

Theorem 1 Suppose that P and Q are stretch-closed processes and x is a shared signal produced by P and consumed by Q ($P \leq_x Q$), then

$$\begin{aligned} & (P \,||_{\leq,a}\, Q)_{\backslash\{x\}} = \\ & \quad ((P[x/x_P] \,||_{\leq,a}\, Q[x/x_Q]) \,||_s\, AFifo_{x_P\to x_Q})_{\backslash\{x_P,x_Q\}} \end{aligned}$$

Note that using asynchronous parallel composition, we are only able to prove the refinement of the ideal asynchronous design with respect to flow inclusion (see Corollary 4 in Appendix). This is because of the fifo behavior of the channel that introduces an ordering between the messages sent and received on a single variable (channel).

Due to Theorem 1, if we continue the process of desynchronization, we get a network of fifo channels (named R) such that: $(P \,||_{\leq,a}\, Q)_{\backslash I} = ((P' \,||_{\leq,a}\, Q') \,||_s\, R)_{\backslash I'}$, where $I = vars(P) \cap vars(Q)$, P' and Q' are results of iterative replacements of explicit data dependencies with fresh variables and I' is the set of such fresh variables. Since all explicit data dependencies between P and Q are resolved ($vars(P') \cap vars(Q') = \emptyset$), with the help of Corollaries 1 and 2, we achieve complete desynchronization as follows:

$$\begin{aligned} (P \,||_{\leq,a}\, Q)_{\backslash I} &= ((P' \,||_{\leq,a}\, Q') \,||_s\, R)_{\backslash I'} \\ &= (P' \,||_s\, Q' \,||_s\, R)_{\backslash I'} \end{aligned}$$

However, an unbounded fifo channel is only a semantical object and does not have a corresponding SIGNAL component, neither it is implementable in most embedded system designs. Thus, we would like to replace the unbounded channel with a bounded one. This is certainly not possible in all designs, however, we investigate this possibility in the next section.

4.2 Desynchronizing Using Bounded Fifo

To restrict the desynchronizing protocol to a network of bounded fifos, we first specify the semantics of bounded network. Then, we give a semantic characterization of processes that can show the asynchronous behavior if they are composed using bounded fifos.

Definition 9 (Bounded N-Fifo) A bounded n-fifo, denoted by $nFifo_{x\to y}$ is the largest process P with $vars(P) = \{x, y\}$, satisfying the following condition:

$$P \subseteq AFifo_{x\to y} \wedge \forall b \in P, \forall t \in T, |[b(y)]_t| \leq n + |[a(x)]_t|$$

The above definition specifies that a bounded n-fifo should first, satisfy the fifo characteristics and second, at each point of time the number of writes can deviate from the number of reads so far by at most n. Next, we give the characterization of processes that share only a single variable and this explicit data dependency can be replaced by a bounded fifo buffer.

Lemma 2 If $vars(P) \cap vars(Q) = \{x\}$ then $(P \mid\mid_{\leq,a} Q)_{\setminus\{x\}} = (P[x_P/x] \mid\mid_s Q[x_Q/x] \mid\mid_s nFifo_{x_P\to x_Q})_{\setminus\{x_P,x_Q\}}$, if:

1. $P \leq_x Q \wedge$
2. $\forall (a,b) \in P \times Q, a_{|\{x\}} \leq b_{|\{x\}} \Rightarrow$
   $\exists (a',b') \in P \times Q, a'_{\setminus\{x\}} = a_{\setminus\{x\}} \wedge b'_{\setminus\{x\}} = b_{\setminus\{x\}} \wedge$
   $\forall i \in I\!N, t(b'(x)_i) \preceq t(a'(x)_{i+n})$

The above Lemma defines necessary and sufficient conditions for two components P and Q so that if they are connected by an $nFifo$, they can perform the same behavior as when they are put in an arbitrary asynchronous network. That is, all read actions of component Q from x can at most be delayed after n more write actions of P on the same variable (thus, preventing the buffer overflow).

Next, we generalize Lemma 2 to a network of fifo channels in both directions:

Theorem 2 Consider the two process P and Q, let I and O be the subsets (partitions) of $vars(P) \cap vars(Q)$ such that $\forall x \in I, Q \leq_x P$ and $\forall y \in O, P \leq_y Q$. If for all $x \in vars(P) \cap vars(Q)$:
$\forall (a,b) \in P \times Q,$
$(\forall x' \in I, a_{|\{x'\}} < b_{|\{x'\}} \wedge \forall y' \in O, a_{|\{y'\}} < b_{|\{y'\}}) \Rightarrow$
$\exists (a',b') \in P \times Q,$
$a_{\setminus(I\cup O)} = a'_{\setminus(I\cup O)} \wedge b_{\setminus(I\cup O)} = b'_{\setminus(I\cup O)} \wedge$
$\forall x \in I, t(b'(x)_i) \preceq t(a'(x)_{i+n_x}) \wedge$
$\forall y \in O, t(a'(y)_i) \preceq t(b'(y)_{i+n_y})$
then $(P \mid\mid_{\leq,a} Q)_{\setminus(I\cup O)} = (P' \mid\mid_s Q' \mid\mid_s R)_{\setminus(I'\cup O')}$, where P' and Q' are result of replacing all variables $x \in I \cup O$ with fresh variables x_P and x_Q, respectively, R is the network of $n_x Fifo_{x_P\to y_Q}$ (or $n_y Fifo_{y_Q\to y_P}$) channels and I' and O' are sets of such fresh variables.

Note that the proposed approach and in particular the above theorem holds for channels with single-producer and single-consumer components. In other words, it is assumed that a shared variable can only be shared by two components. This is not a very restrictive assumptions since form multiple-producer, multiple-consumer shared variables, one can make use of standard copy (fork) and merge (join) components to copy the shared channel for several components and join several write attempts of different components into one channel.

5 Approximating the Buffer Size

In this section we are aiming at implementing the desynchronization ideas inside the SIGNAL model. To do this, first we have to define the implementation of the network of fifo processes. Although the characterization we gave in the previous section can be formally checked on semantics of components, it does not give a constructive way of determining the buffer size. Thus, we propose a practical approach in this section, using which we are able to estimate the buffer size (for a given environment).

5.1 Implementing Fifo Channels

An $nFifo$ channel can be implemented using composition of n $1Fifo$'s defined in Example 1, as follows:

$$\begin{array}{lcl} nFifo_{x_P \to x_Q} & = & 1Fifo_{x_P \to x_1}[full_1/full] \\ & ||_s & \ldots \\ & ||_s & 1Fifo_{x_{n-1} \to x_Q}[full_{n-1}/full] \\ alarm & = & (full_1 \wedge \ldots \wedge full_n) \texttt{ when } x_P \\ ok & = & \texttt{not } (alarm) \end{array}$$

Note that the *alarm* signals is synchronized with *write* attempts. Thus, when an unsuccessful attempt to write to the buffer the *alarm* signal is raised. Its negation describes a successful write attempt.

5.2 Instrumenting the Fifo Channels

Using the implementation of $nFifo$ channel, given in the previous subsection, we are able to design the circuitry around the fifo channels as shown in Figure 4. In this figure, every time a write signal is received by the channel, if the channel is full and the data cannot be inserted to the channel, an *alarm* signal is raised by the channel which in turn results in an *inc* event of the corresponding buffer. An *ok* signal from the fifo results in resetting the counter. We keep the maximum value of the counter in a register which represents the number of times we consecutively missed a write to the buffer (for sake of brevity, we do not give detailed SIGNAL implementation of counter and register components here). Designers can start with a set of behavior and a rough guess of the needed buffer size and use the instrumented fifo network (replacing explicit data dependencies) to find the right estimation of the buffer size. This is done by simulating the behavior of the design for a

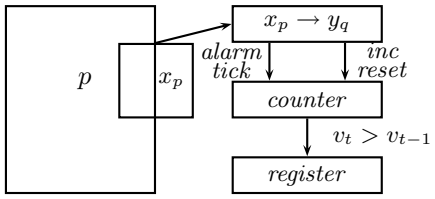


Figure 4: Instrumented Fifo

given environment, observing the values in the counters, incrementing the buffer size by these values, and iterating the simulation till no alarm is raised. This process guarantees that for a set of (normal) behaviors, no buffer overflow will happen. However, since the designer does not necessarily feed all possible behaviors into the design, we need a feedback loop to prevent lossing data in exceptional cases of buffer overflow.

To do this, we can use the *alarm* signal to mask the clock of the producer component. Masking the clock of the producer may be too naive for some critical designs. In such cases, different service levels should be implemented in which the rate of production and consumption of data items can be tuned. The necessity to change the service level can then be indicated by observing the status of communication between components using the fifo buffers between them. If a fifo buffer continuously gets an overflow, this means that we have to either speed up the consumer side (by decreasing service level in consumer side) or slow down the producer side. Similarly, if we continuously notice consumer is attempting to access an empty fifo buffer this is an indication of inappropriate service level which should be fixed by hibernating the consumer side or activating the producer side.

Verification of the desynchronized consists of checking that no *alarm* signal is raised. In case of failing to prove this, the error trace may help us finding the input sequence resulting in *alarm*. This input can be added to our simulation data. Then, we can re-iterate the process by simulating with the new test-data, estimating the sufficient buffer size and coming back to verification phase.

Lemma 3 If no alarm is raised then the design is correct in the sense of Theorem 2.

6 Conclusion

In this paper, we established the theoretical model of asynchronous composition in SIGNAL model and its implementation using fifo buffers. In addition to that, we proposed a practical design template to estimate the buffer size. The proposed approach allows for efficient analysis and implementation of asynchronous designs. Furthermore, it brings about the possibility of specifying GALS systems in the synchronous framework and benefitting from the tooling around it.

Studying compositionality and stability issues in the buffer size proof and estimation remains as one of our future research topics. We are also looking at constructive algorithms

based on the clock dependency graph to make the buffer size estimation and proof automatic. Using program morphism approach (similar to the approach taken in [6]) is another possibility for simulating the program behavior and estimating the buffer size.

References

[1] The polychrony toolset. `http://www.irisa.fr/espresso/Polychrony`.

[2] P. Aubry, P. Le Guernic, and S. Machard. Synchronous distribution of SIGNAL programs. In *Proceedings of HICSS-29*, pages 656–665. IEEE Computer Society, 1996.

[3] A. Benveniste, B. Caillaud, and P. Le Guernic. From synchrony to asynchrony. In J. C. M. Baeten and S. Mauw, editors, *Proceedings of CONCUR'99*, volume 1664 of *LNCS*, pages 162–177. Springer, 1999.

[4] A. Benveniste, P. Caspi, P. Le Guernic, H. Marchand, J.-P. Talpin, and S. Tripakis. A protocol for loosely time-triggered architectures. In A. Sangiovanni-Vincentelli and J. Sifakis, editors, *Proceedings of EMSOFT'02*, volume 2491 of *LNCS*, pages 252–266. Springer, 2002.

[5] G. Berry and E. M. Sentovich. An implementation of constructive synchronous programs in POLIS. *Formal Methods in System Design*, 17(2):135–161, 2000.

[6] A. Gamatié, T. Gautier, and L. Besnard. Modeling of avionics applications and performance evaluation techniques using the synchronous language signal. In *To Appear in Proceedings of SLAP'03*, volume 88 of *ENTCS*. Elsevier, 2003.

[7] A. Girault and C. Ménier. Automatic production of globally asynchronous locally synchronous systems. In A. Sangiovanni-Vincentelli and J. Sifakis, editors, *Proceedings of EMSOFT'02*, volume 2491 of *LNCS*, pages 266–281. Springer, 2002.

[8] N. Halbwachs and S. Baghdadi. Synchronous modelling of asynchronous systems. In A. Sangiovanni-Vincentelli and J. Sifakis, editors, *Proceedings of EMSOFT'02*, volume 2491 of *LNCS*, pages 240–251. Springer, 2002.

[9] R. Kurshan, M. Merritt, A. Orda, S. Sachs. Modelling Asynchrony with a Synchronous Model. *Formal Methods in System Design*, 15(3): 175–199, 1999.

[10] P. Le Guernic, J.-P. Talpin, and J.-C. Le Lann. Polychrony for system design. *Journal for Circuits, Systems and Computers*, Apr. 2003.

[11] E. A. Lee and A. Sangiovanni-Vincentelli. A framework for comparing models of computation. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 17, Dec. 1998.

[12] O. Maffeiïs and P. Le Guernic. Distributed implementation of SIGNAL: Scheduling & graph clustering. In H. Langmaack, W. P. de Roever, and J. Vytopil, editors, *Proceedings of FTRTFT'94*, volume 863 of *LNCS*, pages 547–566. Springer, 1994.

[13] A. Sangiovanni-Vincentelli, M. Sgroi, and L. Lavagno. Formal models for communication-based design. In C. Palamidessi, editor, *Proceedings of CONCUR'00*, volume 1877 of *LNCS*, pages 29–47. Springer, 2000.

[14] K. Wolinski and M. Belhadj. High level synthesis of globally asynchronous locally synchronous circuits. In *Proceedings NATW'94*, 1994.

A Proofs and Formal Results

Note: Proofs are available only for the review process. They will be removed from the paper in the proceedings and will be available on-line in form of a technical report.

Lemma 4 For all general processes P and Q the following properties hold:

1. $P = Q \Rightarrow P^* = Q^*$
2. $P^* = Q^* \Leftrightarrow P \leqslant Q$.
3. $P = (P \mid\mid_s Q)_{|X} \Leftrightarrow P_{|X\cap Y} = Q_{|X\cap Y}$, where $X = vars(P)$ and $Y = vars(Q)$
4. $P \mid\mid_s P = P$
5. $P \mid\mid_s Q = Q \mid\mid_s P$
6. $P^* \mid\mid_s Q^* = (P^* \mid\mid_s Q^*)^*$

Proof. Items 1, 4, and 5 hold trivially (4 is immediate consequence of 3). For the proof of item 2, we prove that $P^* = Q^* \Rightarrow \forall b \in P \exists c \in Q, b \leqslant c$: $\forall b \in P, b \in P^* \Rightarrow \forall b \in P, b \in Q^* \Rightarrow \forall b \in P, \exists c \in Q, b \leqslant c$. Similarly (due to symmetry), we have $P^* = Q^* \Rightarrow \forall b \in Q \exists c \in P, b \leqslant c$. For the other implication of this item, we have

$\forall b, b \in P^* \Rightarrow$
$\exists b' \in P, b \leqslant b' \Rightarrow$
$\exists (b', c) \in P \times Q, b \leqslant b' \wedge b' \leqslant c \Rightarrow$
$\exists c \in Q, c \leqslant b \Rightarrow b \in Q^*$

Again, due to symmetry, we have $P \leqslant Q \Rightarrow (\forall b, b \in Q^* \Rightarrow b \in P^*)$.

For the right implication of item 3, consider an arbitrary $a \in P$, then $a_{|X\cap Y} \in Q_{|X\cap Y}$ and hence $\exists b \in Q, b_{X\cap Y} = a_{X\cap Y}$. Now, consider the behavior c constructed from merging a and b, according to Definition 3 it holds that $c \in P \mid\mid_s Q$ and $c_{|X} = a$, and thus $a \in (P \mid\mid_s Q)_{|X}$. Similarly for the left implication, consider the behavior $a \in P_{|X\cap Y}$ then $\exists b \in P, a_{X\cap Y} = a_{X\cap Y}$ and according to the assumption $b \in (P \mid\mid_s Q)_{|X}$. Then, there exists a $c \in P \mid\mid_S Q, b_{|X} = c_{|X}$. It follows from Definition 3 that $c \in Q$ and thus $c_{|X\cap Y} \in Q_{|X\cap Y}$ and thus $a_{X\cap Y} \in Q_{|X\cap Y}$.

For the proof of item 6, it trivially holds that $P^* \mid\mid_s Q^* \subseteq (P^* \mid\mid_s Q^*)^*$. Thus, it remains to prove that $(P^* \mid\mid_s Q^*)^* \subseteq P^* \mid\mid_s Q^*$. Let $X = vars(P)$, $Y = vars(Q)$ and $I = X \cap Y$, then we have:

$a \in (P^* \mid\mid_s Q^*)^* \Rightarrow \exists a', a' \in P^* \mid\mid_s Q^* \wedge a' \lesseqgtr a \Rightarrow$
$\exists (b', c') \in P^* \times Q^*,$
$\quad b'_{|X} = a'_{|X} \wedge c'_{|Y} = a'_{|Y} \wedge a' \lesseqgtr a \Rightarrow$
$\exists (b', c') \in P^* \times Q^*,$
$\quad b'_{|X} = a'_{|X} \wedge c'_{|Y} = a'_{|Y}, \wedge \exists a'', a'' \leq a' \wedge a'' \leq a \Rightarrow$
$\exists (b'', c'') \in P^* \times Q^*,$
$\quad b''_{|X} = a''_{|X} \wedge c'_{|Y} = a''_{|Y}, \wedge a'' \leq a' \wedge a'' \leq a \Rightarrow$
$\exists (b, c) \in P^* \times Q^*,$
$\quad b_{|X} = a_{|X} \wedge c_{|Y} = a_{|Y}, \wedge a'' \leq a' \wedge a'' \leq a \Rightarrow$
$a \in P^* \mid\mid_s Q^*$

$\boxtimes$

Lemma 5 For arbitrary general processes P and Q:

1. $P \sqsubseteq P \mid\mid_a P$
2. $P \mid\mid_a Q = Q \mid\mid_a P$

Corollary 3

1. $b \leq c \Leftrightarrow b \sqsubseteq c$
2. $b \leq c \Leftrightarrow b[y/x] \leq c[y/x]$ [1]

Proof of theorem 1 *Proof.* Suppose that $vars(P) = X$ and $vars(Q) = Y$ (it clearly holds that $x \in X \cap Y$). First, we prove the containment of the behavior of $((P[x/x_P] \mid\mid_{\leq,a} Q[x/x_Q])|AFifo_{x_P \to x_Q})_{\setminus\{x_P, x_Q\}}$ in $(P \mid\mid_{\leq,a} Q)_{\setminus\{x\}}$:

$\forall a, a \in ((P[x/x_P] \mid\mid_{\leq,a} Q[x/x_Q])\mid$ $AFifo_{x_P \to x_Q})_{\setminus\{x_P, x_Q\}} \Rightarrow$	Def. 3
$\exists b, b_{\setminus\{x_P, x_Q\}} = a \wedge$ $b \in P[x/x_P] \mid\mid_{\leq,a} Q[x/x_Q] \wedge$ $b_{\mid\{x_P, x_Q\}} \in AFifo_{x_P \to x_Q}) \Rightarrow$	Def. 8
$b_{\setminus\{x_P, x_Q\}} = a \wedge$ $b \in P[x/x_P] \mid\mid_{\leq,a} Q[x/x_Q] \wedge$ $b_{\mid\{x_P\}} \leq b_{\mid\{x_Q\}} \Rightarrow$	Def. 7
$b_{\setminus\{x_P, x_Q\}} = a \wedge$ $b_{\setminus\{x_P, x_Q\}}(P \mid\mid_{\leq,a} Q)_{\setminus\{x\}} \Rightarrow$	
$a \in (P \mid\mid_{\leq,a} Q)_{\setminus\{x\}}$	

[1] similarly, for relaxation and for the stretch and flow equivalence relations

The inclusion of the left-hand-side follows from the following proof:

$a \in (P \mid\mid_{\leq,a} Q)_{\setminus\{x\}} \Rightarrow$	
$\exists b, b_{\setminus\{x\}} = a \wedge b \in (P \mid\mid_{\leq,a} Q)$	Def. 7
$\exists (c,d) \in P \times Q,$ $c_{\setminus Y} \lesssim b_{\setminus Y} \wedge d_{\setminus X} \lesssim b_{\setminus X} \wedge$ $c_{\mid X\cap Y} \sqsubseteq b_{\mid X\cap Y} \wedge d_{\mid X\cap Y} \sqsubseteq b_{\mid X\cap Y} \wedge$ $P \leq_x Q \wedge \forall y, P \leq_y Q \Rightarrow$ $\forall z, Q \leq_z P \Rightarrow d_{\mid\{z\}} \leq c_{\mid\{z\}}$	$c_{\mid\{y\}} \leq d_{\mid\{y\}}$ $\wedge x \in X \cap Y$
$c_{\setminus Y}[x_P/x] \lesssim b_{\setminus Y}[x_P/x] \wedge$ $d_{\setminus X}[x_Q/x] \lesssim b_{\setminus X}[x_Q/x] \wedge$ $c_{\mid X\cap Y}[x_P/x] \sqsubseteq b_{\mid X\cap Y}[x_P/x] \wedge$ $d_{\mid X\cap Y}[x_Q/x] \sqsubseteq b_{\mid X\cap Y}[x_Q/x] \wedge$ $c[x_P/x]_{\mid\{x_P\}}[x_Q/x_P] \leq d[x_Q/x]_{\mid\{x_Q\}} \wedge$ $\forall y \in (X \cap Y) \setminus \{x\},$ $P[x_P/x] \leq_y Q[x_Q/x] \Rightarrow$ $c_{\mid\{y\}}[x_P/x] \leq d_{\mid\{y\}}[x_P/x] \wedge$ $\forall z \in X \cap Y,$ $Q[x_P/x] \leq_z P \Rightarrow$ $d_{\mid\{z\}} \leq c_{\mid\{z\}}$	Def. 7 & 3
$b_{\setminus\{x\}} \in ((P[x/x_P] \mid\mid_{\leq,a} Q[x/x_Q])$ $\mid AFifo_{x_P \to x_Q})_{\setminus\{x_P,x_Q\}} \Rightarrow$	
$a \in ((P[x/x_P] \mid\mid_{\leq,a} Q[x/x_Q])\mid$ $AFifo_{x_P \to x_Q})_{\setminus\{x_P,x_Q\}}$	

⊠

Corollary 4 For stretch-closed P and Q with explicit data dependency on x, we have:

$$(P \mid\mid_a Q)_{\setminus\{x\}} \sqsupseteq ((P[x/x_P] \mid\mid_a Q[x/x_Q]) \mid\mid_s AFifo_{x_P \to x_Q})_{\setminus x_P, x_Q}$$

Lemma 6 Consider two behaviors a and b such that $vars(a) = vars(b) = \{x\}$, if $\forall i \in \mathbb{N}, t(a(x)_i) \preceq t(b(x)_{i+n})$, then $\forall t \in T, |[b(x)]_t| \leq n + |[a(x)]_t|$.

Proof. Suppose that the lemma does not hold, then there exists a time t in which $|[b(x)]_t| > |[a(x)]_t| + n$. Let j be the index of the last events of $b(x)$ before t. If such events exist, then

according to the lemma hypothesis, we have $t(a(x)_{j-n}) \preceq t(b(x)_j)$. Thus, the size of $[a(x)]_t$ is at least $j-n$ and this contradicts our assumption ($|[b(x)]_t| = j \not> n+(j-n) \leq n+|[a(x)]_t|$). So, such an event should not exist. This means that t is not related to the time of any event in b and hence $|[b(x)]_t| = |b(x)|$. But since we assume infinite behavior, $|b(x)| = |a(x)| = \infty$ (contradiction with the assumption). ⊠

The Proof of lemma 2 follows the same line as of Lemma 1 using Lemma 6.

Unité de recherche INRIA Lorraine, Technopôle de Nancy-Brabois, Campus scientifique,
615 rue du Jardin Botanique, BP 101, 54600 VILLERS LÈS NANCY
Unité de recherche INRIA Rennes, Irisa, Campus universitaire de Beaulieu, 35042 RENNES Cedex
Unité de recherche INRIA Rhône-Alpes, 655, avenue de l'Europe, 38330 MONTBONNOT ST MARTIN
Unité de recherche INRIA Rocquencourt, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex
Unité de recherche INRIA Sophia-Antipolis, 2004 route des Lucioles, BP 93, 06902 SOPHIA-ANTIPOLIS Cedex

Éditeur
INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex (France)
http://www.inria.fr
ISSN 0249-6399