Decidability Issues in Reduced Reachability Analysis

Leo CACCIARI and Omar RAFIQ

T.A.S.C., Université de Pau, Dpt. Informatique, Av. de l'Université, F-64000 France
e-mail: cacciari@infhp2.univ-pau.fr, rafiq@pauvx1.univ-pau.fr

Abstract

Reachability analysis, which is the most used technique in protocol validation, is based on the construction of a graph called reachability graph. However this technique has two serious drawbacks: the undecidability of the finiteness of the reachability graph and the state explosion when it is finite. To cope with the latter problem, reduction techniques are required. After a brief presentation of our reduced reachability graph we deal with related decidability issues and we show how our decidability results can be applied to the global reachability graph.

keywords: *protocol validation, reachability analysis, reduced validation, reachability graph finiteness.*

1. Introduction

Reachability analysis is the most popular technique in protocol validation. It consists in constructing a graph, called *reachability graph* and representing the complete behaviour of two finite state machines communcating through FIFO channels. However, this technique has two serious drawbacks: the undecidability of the finiteness of the reachability graph when the channels sizes are unbounded [BZ 81, BZ 83] and the state explosion when they are bounded.

In practice the sizes of channels are limited, and then the reachability graph is finite. However, the analyzed properties depend on the choosen sizes. Reachability analysis with unbounded channels is a basic technique to determine the maximum size of channels, if they are finite.

To cope with state explosion problem when the reachability graph is finite, reduction techniques are required. Several approaches have been proposed [RW 82, II 83, GY 84, ZB 86, CH 89]. The basic idea consists in constructing a smaller graph representing a partial behaviour of the protocol and allowing one to study properties of the communication.

After a brief presentation of our reduced reachability graph [CR 92], we deal with related decidability issues and we show how our decidability results can be applied to the global reachability graph. This work can be done, in almost the same way, for most of the existing reduction techniques [RW 82, II 83, ZB 86, CH 89].

Our main result is: *the finiteness of the reduced reachability graph is undecidable.* We prove this result by showing that if we have an *oracle* solving the problem, then we are able to decide the finiteness of the reachability graph.

As a consequence of our proof, we get that the finiteness of the reachability graph of a protocol is decidable if the finiteness of the reduced reachability graph of the same protocol is decidable.

By using this approach, we extend the result of Brand and Zafiropulo [BZ 81, BZ 83] stating that the finiteness of the reachability graph of a communicating system is decidable if one of the two channels is bounded.

This paper is made up of 6 sections. Section 2 gives basic definitions and results. Section 3 introduces our approach [CR 92] of reduced reachability analysis. Section 4 gives our decidability results. Section 5 presents some examples and Section 6 gives conclusion and orientation of our future work.

2. Basic definitions and results

This section gives some basic definitions and results related to reachability analysis in validating communication protocols.

Reachability analysis deals with *communicating systems* composed of *communicating finite state machines* exchanging messages through FIFO channels.

A *communicating finite state machine* (CFSM) is a 4-tuple $A = (Q,M,q^0,\sigma)$, where: Q is a finite set of *states*, M is a finite set of *messages* —which is the disjoint union of M^+, the set of *incoming messages* and M^-, the set of *outgoing messages*—, q^0 is a distinguished state which is

This work has been supported by CNET under grant 92 1B 178 on Formal Design of Cooperative Multimedia Network.

0-8186-3670-X/93 $03.00

the *initial state* of A and σ is a *transition function* which is a partial function $(M\cup\{\tau\})\times Q \rightarrow Q$, τ being a symbol not in M denoting *internal events* such as timeouts and service elements.

σ is extended to a partial function $(M\cup\{\tau\})^*\times Q \rightarrow Q$ by setting:

* $\sigma(\varepsilon,q) = q$ for all $q \in Q$,
* $\sigma(ax,q) = \sigma(x,\sigma(a,q))$ for $a\in (M\cup\{\tau\})$ and $x \in (M\cup\{\tau\})^*$.

A *communicating system* is a 4-tuple $S = (A_1,A_2,C_{1,2},C_{2,1})$ where $A_i = (Q_i,M_i,q^o_i,\sigma_i)$ is a CFSM for $i = 1, 2$, $M^-_1 = M^+_2 = M_{1,2}$ and $M^-_2 = M^+_1 = M_{2,1}$. $M_{i,j}$ is then the set of messages that can be sent by A_i to A_j.

The behaviour description of a communicating system is based on the notions of *global state* and *global transition.*

A *global state* is a 4-tuple $g = (q_1,q_2,c_{1,2},c_{2,1})$ where $q_i\in Q_i$ is a state of CFSM A_i, $i = 1, 2$ and $c_{i,j}\in M_{i,j}^*$ is the content of the FIFO channel from A_i to A_j, $i, j = 1, 2$, $i \neq j$.

A *transition* of S called *global transition* is a pair (i,α), where $i = 1, 2$ and α is one of $+a$ for $a\in M^+_i$ (reception transition), $-a$ for $a\in M^-_i$ (emission transition) or τ (internal transition).

A global transition (i,α) is said to be *fireable* in global state $g = (q_1,q_2,c_{1,2},c_{2,1})$ if and only if one of the following conditions is satisfied:

i) $t = (i,\tau)$ and $\sigma_i(\tau,q_i)$ is defined,
ii) $t = (i,+a)$ for $a\in M_{j,i}$, $c_{j,i} = aw$ for $w\in M_{j,i}^*$ and $\sigma_i(a,q_i)$ is defined,
iii) $t = (i,-a)$ for $a\in M_{i,j}$ and $\sigma_i(a,q_i)$ is defined.

When the global transition $t = (i,\alpha)$ is fireable in a global state $g = (q_1,q_2,c_{1,2},c_{2,1})$, the firing of t leads S to a global state $g' = (q'_1,q'_2,c'_{1,2},c'_{2,1})$ where:

i) if $t = (i,\tau)$, then $q'_i = \sigma_i(\tau,q_i)$, $c'_{i,j} = c_{i,j}$ and $c'_{j,i} = c_{j,i}$,
ii) if $t = (i,+a)$, then $q'_i = \sigma_i(a,q_i)$, $c'_{i,j} = c_{i,j}$ and $c'_{j,i} = w$,
iii) if $t = (i,-a)$, then $q'_i = \sigma_i(a,q_i)$, $c'_{i,j} = c_{i,j}a$ and $c'_{j,i} = c_{j,i}$.

We say that the global state $g' = (q'_1,q'_2,c'_{1,2},c'_{2,1})$ is *reached* from g *by the transition* t, and we write $g\rightarrow_t g'$.

We define the relation $\rightarrow$ between global states of S by:

$$f\rightarrow g \equiv \exists\ (i,\alpha) \text{ s.t. } f\rightarrow_{(i,\alpha)} g.$$

The relation $\rightarrow$ is seen as the union of two relations, namely $\rightarrow_1$ and $\rightarrow_2$, where:

$$f\rightarrow_i g \equiv \exists\ \alpha \text{ s.t. } f\rightarrow_{(i,\alpha)} g.$$

As usual, $\rightarrow^*$ is the transitive and reflexive closure of $\rightarrow$. If $f\rightarrow^* g$, we said that g is *reachable* from f. A global state is said to be *reachable* if it is reachable from the initial state of the system, i. e. the state $g^o=(q^o_1,q^o_2,\varepsilon,\varepsilon)$ in which both machines are in their initial state and the channels are empty.

The behaviour of S can be represented by a graph $\mathbf{R_S}$, called *reachability graph.*

$\mathbf{R_S}$ is the directed and arc-labelled graph whose verticies are the reachable states of S and where there is an arc labelled (i,α) between states f and g if and only if $f\rightarrow_{(i,\alpha)} g$.

$\mathbf{R_S}$ is mainly used to examine communication properties of S [BZ 81, BZ 83, WE 78]. However, this approach has two serious drawbacks: the undecidability of the finiteness of the reachability graph [BZ 81, BZ 83] and the state explosion when it is finite, even in the case of small CFSM. Some condition under which the finiteness of $\mathbf{R_S}$ can be decided have been pointed out in [FI 88, GG 87, KM 69, RG 84, RY 86].

3. Reduced reachability analysis

To deal with the state explosion problem of rechability analysis, several approaches have been proposed to reduce the size of $\mathbf{R_S}$. The basic idea consists in constructing a smaller graph representing a partial behaviour of S and allowing one to study properties of the communication.

In this section, we present the principles of our reduced reachability technique [CR 92]. It is more powerfull than the existing ones in terms of events taken into account and analyzed properties.

3.1. Preliminaries

Let g be a global state of a system S; unless otherwise stated, we have $g = (q_1^{(g)},q_2^{(g)},c_{1,2}^{(g)},c_{2,1}^{(g)})$ and we denote by δ_g the quantity $|c_{1,2}^{(g)}| - |c_{2,1}^{(g)}|$; i. e. δ_g is the difference between the sizes of the channels in the global state g. Firing a non internal transition in CFSM A_1 (resp. A_2) makes this difference increase (resp. decrease) by one, while firing an internal transition in whatever CFSM lets this difference unchanged. This is formally stated in the following Lemma.

Lemma 1

Let $f\rightarrow g$.

i) If $f\rightarrow_{(i,\tau)} g$, then $\delta_g = \delta_f$.
ii) If $f\rightarrow_{(1,\alpha)} g$, $\alpha\neq\tau$, then $\delta_g = \delta_f+1$.
iii) If $f\rightarrow_{(2,\alpha)} g$, $\alpha\neq\tau$, then $\delta_g = \delta_f-1$ ◇.

Let $A = (Q,M,q^o,\sigma)$ be a CFSM. We say that A is *well-behaved* if and only if, for every $q\in Q$ there is no integer n, $n>0$, such that $\sigma(\tau^n,q) = q$, i. e. if there is no cycle composed only of internal events. A communicating

system is well-behaved if and only if both its CFSMs are well-behaved. In the following we make the hypothesis that all systems under consideration are well-behaved.

3.2. Parallel transitions

Let f, g, h and k be global states such that there exist global transitions t = (1,α) and p = (2,β) such that:

$$f \rightarrow_t h \rightarrow_p g$$

and

$$f \rightarrow_p k \rightarrow_t g$$

g is said to be *reachable from* f *by parallel transitions* t *and* p and this is indifferentely written either

$$f \rightarrow_{t||p} g$$

or

$$f \rightarrow_{p||t} g$$

t and p are said to be *parallelwise applicable* in f.

The following Lemma [CR 92] gives a sufficent condition so that two transitions be parallelwise applicable.

Lemma 2

Let f, g and h be three global states such that:

$$f \rightarrow_{(i,\alpha)} h \rightarrow_{(j,\beta)} g,\ i \neq j.$$

If $|c_{i,j}^{(f)}| > 0$, *then the transitions* (i,α) *and* (j,β) *are parallelwise applicable in f* ◇.

3.3. Reduced transitions

Let f and g be two global states, we say that g comes from f by a *reduced transition* r if one of the following conditions holds:

i) $r = (i,\tau)$ and $f \rightarrow_{(i,\tau)} g$, some $i \in \{1,2\}$,

ii) $r = (i,\alpha)$, $c_{i,j}^{(f)} = \varepsilon$ and $f \rightarrow_{(i,\alpha)} g$, some $i \in \{1,2\}$,

iii) $r = (i,+a)$, $c_{j,i}^{(f)} = a$ and $f \rightarrow_{(i,+a)} g$, some $i \in \{1,2\}$, $a \in M_{j,i}$,

iv) $r = t||p$ where $p = (1,-a)$ and $t = (2,-b)$ are emission transitions, $|c_{1,2}^{(f)}| = |c_{2,1}^{(f)}| = 1$ and $f \rightarrow_{p||t} q$, or

v) $r = t||p$ where $p = (1,\alpha)$ and $t = (2,\beta)$ are non internal transitions, $|c_{1,2}^{(f)}|, |c_{2,1}^{(f)}| > 1$ and $f \rightarrow_{p||t} q$.

If g comes from f by a reduced transition r we write $f \Rightarrow_r g$. We define a *reduced reachability* relation $\Rightarrow$ by:

$$f \Rightarrow g \equiv \exists\ r \text{ such that } f \Rightarrow_r g.$$

The relation $\Rightarrow^*$ is defined as the reflexive and transitive closure of $\Rightarrow$. If $f \Rightarrow^* g$, we say that g is *reducely reachable from* f. A global state is said *reducely reachable* if it is reducely reachable from the initial state.

As shown in [CR 92], reducely reachable states are exactly the reachable R-state, where a R-state is a global state g such that either $\delta_g = 0$ or one channel is empty while the other holds exactly one message.

We can define the *reduced graph* of system $S = (A_1,A_2,C_{1,2},C_{2,1})$ as the directed and arc-labelled graph $\mathbf{RG_S}$ whose verticies are the reachable R-states and where there is an arc labeled by the reduced transition r between states f and g if and only if $f \Rightarrow_r g$.

3.4. Reduced validation

In our reduced reachability analysis [CR 92] one can examine four communications properties: deadlocks, unspecified receptions, blocking unspecified receptions and blocking cycles.

A *deadlock* is a global state $g = (q_1,q_2,c_{1,2},c_{2,1})$ where $c_{1,2} = c_{2,1} = \varepsilon$ and, for i = 1, 2 $\sigma_i(\alpha,q_i)$ is undefined for every α in $M^-_i \cup \{\tau\}$.

An *unspecified reception* exists for CFSM A_i in the global state $g = (q_1,q_2,c_{1,2},c_{2,1})$ if $c_{i,j} = aw$ and $\sigma_i(a,q_i)$ is undefined.

A *blocking unspecified reception* exists for CFSM A_i in the global state $g = (q_1,q_2,c_{1,2},c_{2,1})$ if $\sigma_i(\alpha,q_i)$ is undefined for every α in $M^-_i \cup \{\tau\}$, $c_{i,j} = aw$ and $\sigma_i(a,q_i)$ is undefined.

In the system S a *blocking cycle* is a set $B = \{g_1, g_2, \ldots, g_n, \ldots\}$ (finite or infinite) of reachable global states such that:

* $|B| > 1$,
* g^o, the initial state of S, is not in B,
* if g, g'∈ B, then g' is reachable from g,
* if g∈ B and g'∉ B, then g' is not reachable from g.

Theorem 1

Let $S = (A_1,A_2,C_{1,2},C_{2,1})$ *be a communicating system and* $\mathbf{RG_S}$ *be its reduced graph, then*

i) if S has deadlocks, then $\mathbf{RG_S}$ *contains all of them;*

ii) if S has unspecified receptions, then $\mathbf{RG_S}$ *contains at least one of them;*

iii) if S has blocking unspecified receptions, then $\mathbf{RG_S}$ *contains at least one of them;*

iv) if S has blocking cycles, then each of them is represented by one blocking cycle of $\mathbf{RG_S}$ *and conversely* ◇.

3.5. Examples

Now let's examine two examples of communicating systems showing features of this approach.

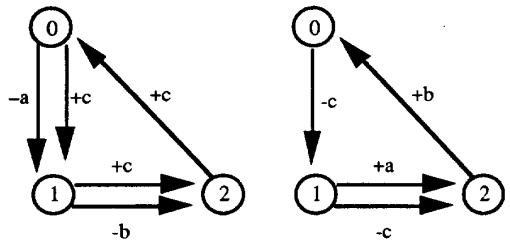

Figure 1

The first communicating system is shown in Figure 1, while its reduced graph is shown in Figure 2. It has 15 states, while its related reachability graph has 37 states. The graph of Figure 2 shows the existence of an unique deadlock, of at least six unspecified receptions, four of which at least are blocking unspecified receptions.

For readability of Figure 2 we have simplified the labels of arcs writing α instead of (i,α).

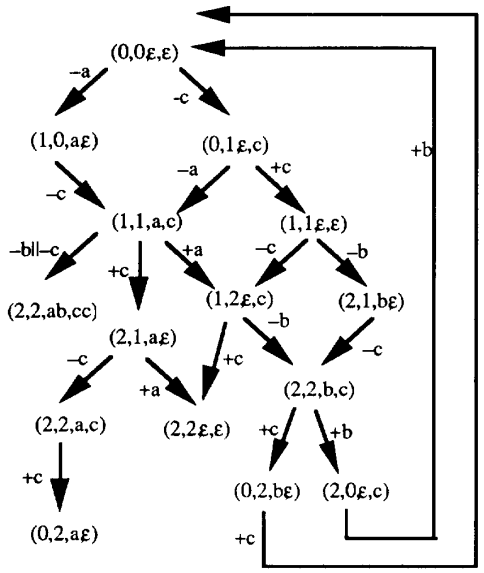

Figure 2

The second example of communicating system is shown in Figure 3, while its reduced graph is shown in Figure 4. It has 6 states while its related reachability graph is infinite (see below). The reduced graph shows that there exists, for the given system, at least one blocking unspecified reception. However, there is no blocking cycle and no deadlock.

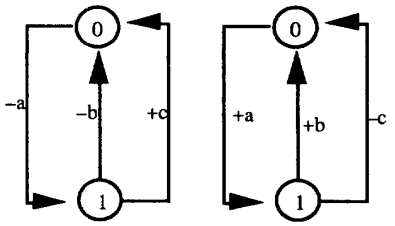

Figure 3

This example leads naturally to ask if it is possible to decide about the finiteness of the reduced reachability graph of a given communicating system. The next section is devoted to this problem.

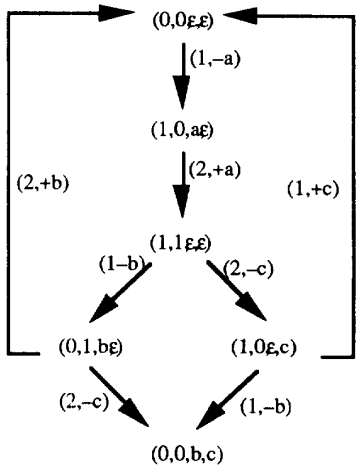

Figure 4

4. Decidability issues

In this section $S = (A_1, A_2, C_{1,2}, C_{2,1})$ is a communicating system, **R** is the set of reachable states of S —i. e. the vertex set of $\mathbf{RG}_S$—, **RR** is the set of reachable R-states —i. e. the vertex set of $\mathbf{RG}_S$— and Δ is the set of *diagonal states*:

$$\Delta = \{g \in \mathbf{R} \mid \delta_g = 0\}.$$

If g is a reachable global state, then $\Gamma_i(g)$, for i = 1, 2, denotes the set of global states that are reachable from g by a sequence of transitions only composed by transitions of A_i:

$$\Gamma_i(g) = \{h \in \mathbf{R} \mid g \rightarrow_i^* h\}.$$

Let's generalize a Lemma proved by Chabbar [CH 89] in the case of CFSMs without internal events, to CFSMs with internal events.

Lemma 3

For a system S the set of reachable global states is given by

$$R = \cup_{d\in\Delta}(\Gamma_1(d)\cup\Gamma_2(d))$$

Proof: Let g be any reachable global state. To prove Lemma 3 we show that:

(1) if $\delta_g \geq 0$, then there exists $d\in\Delta$ such that $d\rightarrow_1{}^* g$ (i. e. $g\in\Gamma_1(d)$),

(2) if $\delta_g \leq 0$, then there exists $d\in\Delta$ such that $d\rightarrow_2{}^* g$ (i. e. $g\in\Gamma_2(d)$).

Clearly, conditions (1) and (2) are symmetrical and therefore we have only to prove one of them, say (1).

if $\delta_g=0$, i. e. if $g\in\Delta$, then there is nothing to prove. We can then suppose, without loss of generality, that $\delta_g>0$. As g is reachable we have $g^o\rightarrow^* g$, i. e.:

$$g^o=g_0\rightarrow_{t_1} g_1\rightarrow_{t_2}\cdots g_{n-1}\rightarrow_{t_n} g_n=g.$$

We distinguish two cases according to the CFSM firing t_n.

I. If $t_n = (1,\alpha)$, then $\delta_{g_{n-1}}\geq\delta_g-1\geq 0$ and the Lemma is proved by induction on n.

II. If $t_n = (2,\alpha)$, let k, $1\leq k<n$, be such that $t_k=(1,\alpha_k)$ and $t_h=(2,\alpha_h)$ for all $h>k$ — remark that, as $\delta_g > 0$, such a k exists by Lemma 1. By Lemma 1, $\delta_{g_k}\geq\delta_g>0$; it then follows that $|c_{1,2}{}^{(g_k)}|>0$. By repeatedly applying Lemma 2 we go back to case I above◇.

It was proved in [CR 92] that the set **RR** of reducely reachable states is obtained as the union of Δ and the set of reachable states having one channel empty while the other holds exactly one message. Obviously the latter set is finite, and so $\mathbf{RG_S}$ is finite if and only if Δ is. By this remark and Lemma 3 above we obtain the following Lemma, whose straightforward proof is omitted.

Lemma 4

If S is such that RG_S is finite, then R_S is infinite if and only if there exists $d\in\Delta$ such that either $\Gamma_1(d)$ or $\Gamma_2(d)$ is infinite ◇.

Definition 1

Let $A = (Q,M,\sigma,q^o)$ be a communicating finite state machine. A state $q\in Q$ is said infinitely emetting state (IE-state) *if there exists $x\in(M\cup\{\tau\})^*$ such that $\sigma(x,q) = q$.*

A IE-state is then a state in which a CFSM can make infinitely many transitions independentely of the environement, i. e. of its input channel. Obviously if $g = (q_1,q_2,c_{1,2},c_{2,1})$ is a reachable global state such that q_1 is an IE-state of A_1 (resp. q_2 is an IE-state of A_2), then all global states $(q_1,q_2,c_{1,2}x^n,c_{2,1})$ (resp. $(q_1,q_2,c_{1,2},c_{2,1}x^n)$) are reachable for $n\geq 0$. It then follows that $\mathbf{R_S}$ is infinite. Remark that the converse statement — i. e. that if $\mathbf{R_S}$ is infinite, then there exists a reachable global state $g = (q_1,q_2,c_{1,2},c_{2,1})$ such that either q_1 is an IE-state of A_1 or q_2 is an IE-state of A_2— is false as it is shown by the following example. Neither of the two CFSM composing the system of Figure 5 has IE-states, nevertheless the reachability graph of this system is infinite. However the reduced reachability graph of this system is also infinite.

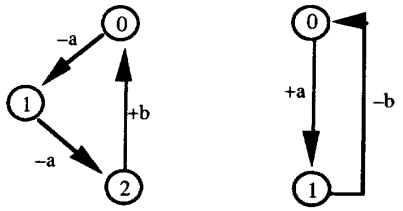

Figure 5

Even in the case of a finite reduced reachability graph, however, we cannot guarantee that, if $\mathbf{R_S}$ is infinite, then there exists a reducely reachable global state $g = (q_1,q_2,c_{1,2},c_{2,1})$ such that either q_1 is an IE-state of A_1 or q_2 is an IE-state of A_2. As an example of this fact, take the system of Figure 6, whose (finite) reduced reachability graph is shown in Figure 7. The only IE-state of this system is state 3 of the CFSM on the left side. looking at the reduced reachability graph of the system one can convince himself that there is no R-state in the form $(3,q_2,c_{1,2},c_{2,1})$. However it is not hard to see that the global states $(3,2,aac^n,b)$ are reachable for all $n\geq 0$, proving that the reachability graph of this system is infinite.

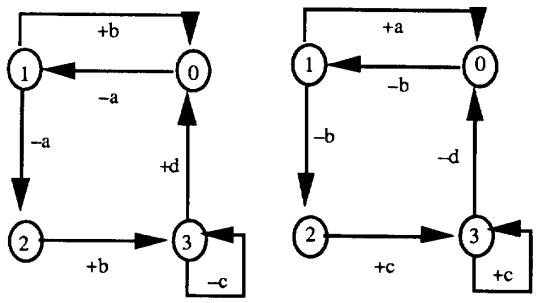

Figure 6

What exactly can be proved (see Theorem 2 below) is that if $\mathbf{RG_S}$ is finite while $\mathbf{R_S}$ is infinite then $\mathbf{R_S}$ must contain a global state $(q_1,q_2,c_{1,2},c_{2,1})$ such that either q_1 is an IE-state of A_1 or q_2 is an IE-state of A_2. Moreover it is possible to detect the presence of such a state by looking at only the diagonal states (which, the reduced

graph being finite, are finitely many). To achieve this goal we need some more work.

Definition 2

Let $A = (Q,M,q^0,\sigma)$ be a communicating finite state machine and q a state of A. The language IEP(q) of the infinetely emetting prefix for *q is the set of words x of $(M^+)^*$ such that there exists a word $y \in (M^- \cup \{\tau\})^*$ such that $\sigma(z,q)$ is an IE-state of A, z being a word of the shuffle product $x \omega y$ of x and y.*

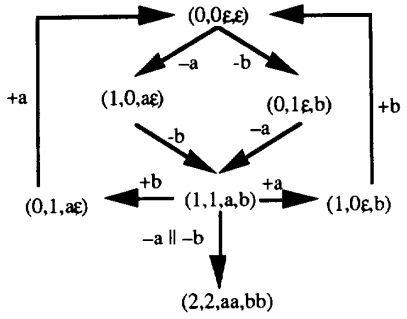

Figure 7

The set IEP(q) is then the set of words that should be supplied by the environement of A in order to bring A from q to an IE-state. It is easy to show, by constructing a finite state automaton accepting it, that the set IEP(q) is a regular langage. It then follows that the langage

$$PIEP(q) \equiv IEP(q)(M^+)^*$$

is also regular. If the input channel of A contains a word in PIEP(q) while A is in state q, then A can reach a IE-state without its peer machine fires any transition. This has an important consequence which is pointed out in Lemma below.

Lemma 6

If $g = (q_1,q_2,c_{1,2},c_{2,1})$ is a reachable global state such that $c_{2,1} \in PIEP(q_1)$ (resp. $c_{1,2} \in PIEP(q_2)$), then $\Gamma_1(g)$ (resp. $\Gamma_2(g)$) is infinite.

Proof: Let $c_{2,1} = xu$ where $x \in$ IEP(q) and let y be a word of $(M^- \cup \{\tau\})^*$ and $z \in x\omega y$ be such that $q'_1 = \sigma_1(z,q_1)$ is an IE-state of A_1. We have $g \rightarrow_1{}^* h$ where $h = (q'_1,q_2,c_{1,2}y',u)$, y' being the projection of y over $(M^-)^*$. By the remark following Definition 1 the set $\Gamma_1(h)$ is infinite. As $g \rightarrow_1{}^* h$, $\Gamma_1(h)$ is a subset of $\Gamma_1(g)$. It follows that $\Gamma_1(g)$ is also infinite ◇.

We can now prove a Theorem giving a characterisation of those cases in which RG_S is finite and R_S is finite.

Theorem 2

If RG_S is finite, then R_S is finite if and only if there exists a reachable diagonal state $d = (q_1,q_2,c_{1,2},c_{2,1})$ such that one at least of the following conditions is fulfilled

(1) $c_{2,1} \in PIEP(q_1)$,

(2) $c_{1,2} \in PIEP(q_2)$.

Proof: By Lemma 4 to prove this Theorem it is sufficent to prove that (1) (resp. (2)) holds if and only if $\Gamma_1(g)$ (resp. $\Gamma_2(g)$) is infinite.

If $c_{2,1} \in$ PIEP(q_1), then ,by Lemma 6, the set $\Gamma_1(g)$ is infinite and so its R_S.

Suppose now that $\Gamma_1(g)$ is infinite. By the hypothesis of well-behaveness of S, the subgraph T of R_S spanned by $\Gamma_1(g)$ is a tree. Moreover, T is locally finite. By the Köning's Lemma, there exists an infinite path in T. This means that there exists global states g_i, i = 1, 2,... such that:

$$g=g_1 \rightarrow_{t_1} g_2 \rightarrow_{t_2} g_2 \ldots \rightarrow_{t_{n-1}} g_n \rightarrow_{t_n} \cdots$$

where $t_i = (1,\alpha_i)$. As $c_{2,1}$ is finite, only finitely many of the t_i are receptions. It follows that there exists $n \geq 1$ such that for $i \geq n$ t_i is either an internal transition or an emission. As Q_1 is finite there exists $h > k \geq n$ such that A_1 is in the same state, say q, both in g_h and in g_k. Let z be the word of $(M^-_1 \cup \{\tau\})^*$ corresponding to transitions t_k to t_h, then $q=\sigma_1(z,q)$, i. e. q is an IE-state of A_1. On the other side if x is the word of $(M^+)^*$ correspondig to the messages received by A_1 in firing transition t_1 to t_{k-1}, then it is clear that $x \in$ IEP(q) and that x is a prefix of $c_{2,1}$. This means that $c_{2,1} \in$ PIEP(q), as required.

Exactly in the same way, one can prove that $c_{1,2} \in$ PIEP(q_2) if and only if $\Gamma_2(g)$ is infinite ◇.

```
function RS_finite?(S:system):boolean;
begin
  if not RGS_finite?(S) then
    return false
  else
    construct the set Δ;
    for (q1,q2,c1,2,c2,1)∈Δ do
      if c2,1∈PIEP(q1) then
        return false
      else
        if c2,1∈PIEP(q1) then
          return false
        fi
      fi
    od
  fi
end
```

Figure 8

We are now ready to prove the main result of this paper.

Theoreme 3

The finiteness of RG_S is undecidable.

Proof: This Theorem is proved by showing that, if there exists an algorithm RG_S_finite? deciding about the finiteness of RG_S, then we can construct an algorithm R_S_finite? deciding about the finiteness of R_S. If RG_S is infinite the algorithm returns **false** otherwise it exhaustively examines the diagonal states looking for a state fulfilling conditions of Theorem 2. If one such state is found the algorithm returns **false** otherwise it returns **true**. As the finiteness of R_S is undecidable [BZ 81, BZ 83] we have a contradiction and Theorem 3 is proved. The algorithm R_S_finite? is shown in Figure 8 ◇.

Now let's notice that in fact, we have proved a more general result than that stated in Theorem 3. This result follows.

Theorem 4

Let Σ be a class of communicating systems such that the finiteness of RG_S is decidable for those systems S belonging to Σ, then the finiteness of R_S is decidable for every S belonging to Σ ◇.

Remark that if the system **S** is such that one of its channels is bounded, then RG_S is finite. We get then the following Corollary of Theorem 4.

Corollary

If a system S is such that one of its channels is bounded then the finiteness of R_S is decidable ◇.

This corollary is proved in [BZ 81, BZ 83]. However, the proof of Brand and Zafiropulo uses an algorithm which requires the knowledge of which channel is bounded and the value of the bound. In this respect our result is an extension of the result of Brand and Zafiropulo. Let's give another extension of this result through Theorem 5.

Definition 3

Let $S = (A_1,A_2,C_{1,2},C_{2,1})$ be a communicating system. We say that the channels of S are relatively bounded *if there exist constants n_1 and n_2 such that for every reachable global state $(q_1,q_2,c_{1,2},c_{2,1})$ such that $|c_{1,2}| > n_1$ (resp. $|c_{2,1}| > n_2$) we have $|c_{2,1}| \leq n_2$ (resp. $|c_{1,2}| \leq n_1$).*

Let Σ be the class of these communicating systems whose channels are relatively bounded. The following Lemma is straightforward.

Lemma 7

If $S \in \Sigma$, then RG_S is finite ◇.

Combining Lemma 7 and the previous Corollary we get the following Theorem.

Theorem 5

The finiteness of R_S is decidable for those systems belonging to Σ ◇.

5. Examples

Let's start by the system shown in Figure 1. It is easy to see that neither of the two CFSM has an IE-state. Since the reduced graph of this system is finite (see Figure 2) it follows from Theorem 2 that the reachability graph of this system is also finite. This result is to be compared with what we said about the system shown in Figure 5. As we said above neither of the two CFSM composing this system has an IE-state. Nevertheless the reduced graph of this system is infinite, which obviously implies that its reachability graph is also infinite.

In the system of Figure 3, the states of the CFSM on the left side are all IE-states. On the other hand none of the states of the CFSM on the right side is an IE-state. One can notice that:

$$PIEP(0) = c^*$$

and that:

$$PIEP(1) = c^+.$$

Examining the reduced graph of Figure 4, one can see that:

$$\Delta = \{(0,0,\varepsilon,\varepsilon), (1,1,\varepsilon,\varepsilon), (0,0,b,c)\}.$$

Since the global states of Δ satisfies condition (1) of Theorem 2, it follows that the reachability graph of the communicating system of Figure 3 is infinite.

Finally for the system shown in Figure 6 we have pointed out that the only IE-state is state 3 of the left side CFSM. It is also easy to see that:

$$PIEP(0)=PIEP(1)=PIEP(2) = b\{b,d\}^*$$

and

$$PIEP(3) = \{b,d\}^*.$$

The set of reachable diagonal states of this system is given by:

$$\Delta=\{(0,0,\varepsilon,\varepsilon), (1,1,a,b), (2,2,aa,bb)\},$$

and it is easy to see that both states (1,1,a,b) and (2,2,aa,bb) satisfy condition (1) of Theorem 2. It then follows that the rechability graph of this system is infinite.

6. Conclusion and future work

We have proved that the finiteness problem for the reduced reachability graph of a communicating system is undecidable. We have also extended a well known result about the decidability of the finiteness of the reachability graph.

Naturally our current work is oriented to determine sufficent conditions allowing one to decide if the reduced reachability graph is finite.

7. References

[BZ 81] D. Brand and P. Zafiropulo, *On Communicating Finite-State Machines*, IBM Research report RZ 1053 (#37725), Zurich 1981.

[BZ 83] D. Brand and P. Zafiropulo, *On Communicating Finite-State Machines*, J. Ass. Comput. Mach., **30**(1983) 361-371.

[CH 89] E. Chabbar, *Etude et Analyse de la Communication des Processus*, LaBRI, Université de Bordeaux I, internal report # I-8918, 1989, Bordeaux, France.

[CR 92] L. Cacciari and O. Rafiq, *On Improving Reduced Reachability Analysis*, FORTE'92, M. Diaz and R. Groz Ed., Elsevier, September 1992,137-152.

[FI 88] A. Finkel, *A New Class of Analyzable CFSM With Unbounded FIFO Channels*, PSTV VIII, Elsevier, 1988, 263-294.

[GY 84] M. G. Gouda and Y. T. Yu, *Protocol Validation by Maximal Progressive Exploration*, IEEE Tans. on Com. **COM-32**(1984).

[GG 87] M. G. Gouda, E. Gurari, T. Lai and L. Rosier, *On Deadlock Detection in Systems of Communicating Finite State Machines*, Computers and Artificial Inteligence, **6**(1987) 209-228.

[HO 87] G. J. Holtzmann, *On Limits and Possibilities of Automated Protocol Analysis*, PSTV VII, Elsevier, June 1987, 339-344.

[II 83] M. Itoh and H. Ichikawa, *Protocol Verification Algorithm Using Reduced Reachability Analysis*, IECE Trans. Japan **E66**(1983) 88-93.

[KM 69] R. M. Karp and R. E. Miller, *Parallel Program Schemata*, JCSS **3**(1969) 147-195.

[RG 84] L. Rosier and M. G. Gouda, *On Deciding Progress for a Class of Communicating Protocols*, Proced. of the 8th Ann. Conf. on Inf. Sci. and Syst., Princeton Univ. Press, 1984, 663-667.

[RW 82] J. Rubin and C. H. West, *An Improved Protocol Validation Technique*, Comp. Networks, **6**(1982) 65-73.

[RY 86] L. Rosier and H. Yen, *Boundness, Empty Channel Detection, and Synchronisation for Communicating Finite Automata*, TCS **44**(1986) 66-105.

[WE 78] C. H. West, An Automated Technque of Communication Protocol Validation, IEEE Trans. Com. **COM-26**(1978) 1271-1275.

[ZB 86] J. Zhao and G. v. Bochmann, *Reduced Reachability Analysis of Communication Protocols: a New Approach*, PSTV VI, Elsevier, June 1986, 243-254.