

## RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

### On the Introduction of Guarded Lists in Bach

Barkallah, Manel; Jacquet, Jean Marie

*Published in:*

Electronic Proceedings in Theoretical Computer Science

*DOI:*

[10.4204/EPTCS.383.4](https://doi.org/10.4204/EPTCS.383.4)

*Publication date:*

2023

*Document Version*

Early version, also known as pre-print

[Link to publication](#)

*Citation for published version (HARVARD):*

Barkallah, M & Jacquet, JM 2023, 'On the Introduction of Guarded Lists in Bach: Expressiveness, Correctness, and Efficiency Issues', *Electronic Proceedings in Theoretical Computer Science*, vol. 383, pp. 55-72.  
<https://doi.org/10.4204/EPTCS.383.4>

#### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

#### Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

# On the Introduction of Guarded Lists in Bach: Expressiveness, Correctness, and Efficiency Issues

Manel Barkallah

Nadi Research Institute  
Faculty of Computer Science  
University of Namur  
Namur, Belgium

manel.barkallah@unamur.be

Jean-Marie Jacquet

Nadi Research Institute  
Faculty of Computer Science  
University of Namur  
Namur, Belgium

jean-marie.jacquet@unamur.be

Concurrency theory has received considerable attention, but mostly in the scope of synchronous process algebras such as CCS, CSP, and ACP. As another way of handling concurrency, data-based coordination languages aim to provide a clear separation between interaction and computation by synchronizing processes asynchronously by means of information being available or not on a shared space. Although these languages enjoy interesting properties, verifying program correctness remains challenging. Some works, such as Anemone, have introduced facilities, including animations and model checking of temporal logic formulae, to better grasp system modelling. However, model checking is known to raise performance issues due to the state space explosion problem. In this paper, we propose a guarded list construct as a solution to address this problem. We establish that the guarded list construct increases performance while strictly enriching the expressiveness of data-based coordination languages. Furthermore, we introduce a notion of refinement to introduce the guarded list construct in a correctness-preserving manner.

## 1 Introduction

Concurrency theory has been the attention of a considerable effort these last decades. However most of the effort has been devoted to algebra based on synchronous communication, such as CCS [31], CSP [20] and ACP [3]. Another path of research has been initiated by Gelernter and Carriero, who advocated in [17] that a clear separation between the interactional and the computational aspects of software components has to take place in order to build interactive distributed systems. Their claim has been supported by the design of a model, Linda [9], originally presented as a set of inter-agent communication primitives which may be added to almost any programming language. Besides process creation, this set includes primitives for adding, deleting, and testing the presence/absence of data in a shared dataspace. In doing so they proposed a new form of synchronization of processes, occurring asynchronously, through the availability or absence of pieces of information on a shared space.

A number of other models, now referred to as coordination models, have been proposed afterwards. However, although many pieces of work have been devoted to the proposal of new languages, semantics and implementations, few articles have addressed the concerns of practically constructing programs in coordination languages, in particular in checking that what is described by programs actually corresponds to what has to be modelled.

Based on previous results [6, 7, 11, 26, 12, 13, 23, 25, 27, 28, 29], we have introduced in [21] a workbench Scan to reason on programs written in Bach, a Linda-like dialect developed by the authors. It has been refined in [22] to cope with relations, processes and multiple scenes. The resulting workbench is named Anemone. In both cases, one of our goals was to allow the user to check properties by model



Figure 1: Rush Hour Problem. On the left part, the game as illustrated at <https://www.michaelfogleman.com/rush>. On the right part, the game modeled as a grid of  $6 \times 6$ , with cars and trucks depicted as rectangles of different colors.

checking temporal logic formulae and by producing traces that can be replayed as evidences of the establishment of the formulae. However, as well-known in model checking, this goal raises performance issues related to the state space explosion. In particular, letting animation-related primitives interleave in many ways duplicates research paths during model checking, with considerable performance problems to check that formulae are established. To address this problem, we introduce in this paper a guarded list construct and establish that it yields an increase in performance while strictly enriching the expressiveness of Bach.

The rest of the paper is organized as follows. Section 2 presents the reference Linda-like language Bach employed by Scan and Anemone. Section 3 introduces the guarded list construction as well as the refinement relation. It is proved to increase the expressiveness of the Bach language in Section 4 while the gain of efficiency in model-checking is established in Section 5. Finally, Section 6 compares our work with related work and Section 7 sums up the paper and sketches future work.

It is worth observing that, as duly compared in Section 6, introducing an atomic construct is not new. However, our contribution is (i) to introduce a construct tailored to coordination languages, (ii) to establish that it yields a gain of performance in model checking and also an increase of expressiveness, and finally (iii) to identify refinement-based criteria so as to guide the programmer to introduce the guarded list construct in a correctness-preserving manner.

To make the article more concrete, we shall use the running example of [22], namely a solution to the rush hour puzzle. This game, illustrated in Figure 1, consists in moving cars and trucks on a  $6 \times 6$  grid, according to their direction, such that the red car can exit. It can be formulated as a coordination problem by considering cars and trucks as autonomous agents which have to coordinate on the basis of free places.

## 2 The Anim-Bach language

### 2.1 Definition of data

Following Linda, the Bach language [13, 24] uses four primitives for manipulating pieces of information: *tell* to put a piece of information on a shared space, *ask* to check its presence, *nask* to check its absence and *get* to check its presence and remove one occurrence. In its simplest version, named BachT, pieces

of information consist of atomic tokens and the shared space, called the store, amounts to a multiset of tokens. Although in principle such a framework is sufficient to code many applications, it is however too elementary in practice to code them easily. To that end, we introduce more structured pieces of information which may employ sets defined as in

```
eset RCInt = { 1, 2, 3, 4, 5, 6}.
```

in which the set *RCInt* is defined as the set containing the elements 1 to 6. In addition to sets, maps can be defined between them as functions that take zero or more arguments. In practice, mapping equations are used as rewriting rules, from left to right in the aim of progressively reducing a complex map expression into a set element.

As an example of a map, assuming a grid of 6 by 6 featuring the rush hour problem as in [22] and assuming that trucks in this game take three cells and are identified by the upper and left-most cell they occupy, the operation *down\_truck* determines the cell to be taken by a truck moving down:

```
map down_truck : RCInt -> RCInt .
eqn down_truck(1) = 4. down_truck(2) = 5. down_truck(3) = 6.
```

Note from this example that mappings may be partially defined, with the responsibility put on the programmer to use them only when defined.

Structured pieces of information to be placed on the store consist of flat tokens as well as expressions of the form  $f(a_1, \dots, a_n)$  where  $f$  is a functor and  $a_1, \dots, a_n$  are set elements or structured pieces of information. As an example, in the rush hour example, it is convenient to represent the free places of the game as pieces of information of the form *free(i, j)* with  $i$  a row and  $j$  a column.

The set of structured pieces of information is subsequently denoted by  $\mathcal{S}$ . For short, si-term is used later to denote a structured piece of information. Mapping definitions induce a rewriting relation that we shall subsequently denote by  $\rightsquigarrow$ , that rewrites si-terms to final si-terms, namely si-terms that cannot be reduced further.

## 2.2 Primitives

The primitives consist of the *tell*, *ask*, *nask* and *get* primitives already introduced, which take as arguments elements of  $\mathcal{S}$ . A series of graphical primitives are added to them. They aim at animating the executions. They include *draw*, *move\_to*, *place\_at*, *hide*, *show* primitives, to cite only a few. The key point for this paper is that they always succeed and do not interfere with the shared space. For the rest of the paper, we shall assume a set  $GPrim$  of graphical primitives and will take primitives from it. The coordinated Bach language enriched by graphical primitives is subsequently referred to as Anim-Bach.

The execution of primitives is formalized by the transition steps of Figure 2. Configurations are taken there as pairs of instructions, for the moment reduced to simple primitives, coupled to the contents of the shared space. Following the constraint-like setting of Bach in which the Linda primitives have been rephrased, the shared space is renamed as *store* and is formally defined as a multiset of si-terms. As a result, rule (T) states that the execution of the *tell(t)* primitive amounts to enriching the store by an occurrence of  $t$ . The  $E$  symbol is used in this rule as well as in other rules to denote a terminated computation. Similarly, rules (A) and (G) respectively state that the *ask(t)* and *get(t)* primitives check whether  $t$  is present on the store with the latter removing one occurrence. Dually, as expressed in rule (N), the primitive *nask(t)* tests whether  $t$  is absent from the store. Finally, rule (Gr) expresses that any graphical primitive succeeds without modifying the store.

$$\begin{array}{l}
\text{(T)} \quad \frac{t \rightsquigarrow u}{\langle \text{tell}(t) \mid \sigma \rangle \longrightarrow \langle E \mid \sigma \cup \{u\} \rangle} \\
\text{(A)} \quad \frac{t \rightsquigarrow u}{\langle \text{ask}(t) \mid \sigma \cup \{u\} \rangle \longrightarrow \langle E \mid \sigma \cup \{u\} \rangle} \\
\text{(G)} \quad \frac{t \rightsquigarrow u}{\langle \text{get}(t) \mid \sigma \cup \{u\} \rangle \longrightarrow \langle E \mid \sigma \rangle} \\
\text{(N)} \quad \frac{t \rightsquigarrow u, u \notin \sigma}{\langle \text{nask}(t) \mid \sigma \rangle \longrightarrow \langle E \mid \sigma \rangle} \\
\text{(Gr)} \quad \frac{p \in GPrim}{\langle p \mid \sigma \rangle \longrightarrow \langle E \mid \sigma \rangle}
\end{array}$$

Figure 2: Transition rules for the primitives

### 2.3 Agents

Primitives can be composed to form more complex agents by using traditional composition operators from concurrency theory: sequential composition, parallel composition and non-deterministic choice. Another mechanism is added in Anim-Bach: conditional statements of the form  $c \rightarrow s_1 \diamond s_2$ , which computes  $s_1$  if  $c$  evaluates to true or  $s_2$  otherwise. As a shorthand,  $c \rightarrow s_1$  is used to compute  $s_1$  when  $c$  evaluates to true. Conditions of type  $c$  are obtained from elementary ones, thanks to the classical and, or and negation operators, denoted respectively by  $\&$ ,  $|$  and  $!$ . Elementary conditions are obtained by relating set elements or mappings on them by equalities (denoted  $=$ ) or inequalities (denoted  $=, <, <=, >, >=$ ).

Procedures are defined similarly to mappings through the `proc` keyword by associating an agent with a procedure name. As in classical concurrency theory, it is assumed that the defining agents are guarded, in the sense that any call to a procedure is preceded by the execution of a primitive or can be rewritten in such a form.

As an example, the behavior of a vertical truck in the rush hour puzzle can be modelled by the following code:

```

proc VerticalTruck(r: RCInt, c: RCInt) =
  ( r>1 & r<5 -> ( get(free(pred(r),c)); tell(free(succ(succ(r)),c));
                  VerticalTruck(pred(r),c) )
  +
  ( r<4 -> ( get(free(down_truck(r),c)); tell(free(r,c));
            VerticalTruck(succ(r),c) ) ).

```

To understand it, remember that a truck is identified by the upper and left-most cell it occupies. The parameters of the `VerticalTruck` procedure are precisely the row number and the line number of this cell. Given that a vertical truck can move one cell up or one cell down, the procedure offers two alternatives through the "+" operator. The first one corresponds to a truck moving one cell up. To make this move realistic, the row  $r$  occupied by the truck should be strictly greater than one. Otherwise, the truck is already on the first row (like the yellow truck of Figure 1) and cannot move up. Moreover, as we shall see in a few seconds, the row  $r$  should also be strictly smaller than 5. Assuming the two conditions hold ( $r > 1 \& r < 5$ ) moving a truck one cell up proceeds in three steps. First we need to make sure that the cell up is free. This is obtained by getting the si-term  $free(pred(r),c)$  by means of the execution of the  $get(free(pred(r),c))$  primitive. Note that  $pred(r)$  is actually coded by a map as being  $r - 1$ . Second

$$\begin{array}{l}
\text{(S)} \quad \frac{\langle A \mid \sigma \rangle \longrightarrow \langle A' \mid \sigma' \rangle}{\langle A ; B \mid \sigma \rangle \longrightarrow \langle A' ; B \mid \sigma' \rangle} \\
\text{(P)} \quad \frac{\langle A \mid \sigma \rangle \longrightarrow \langle A' \mid \sigma' \rangle}{\langle A \parallel B \mid \sigma \rangle \longrightarrow \langle A' \parallel B \mid \sigma' \rangle} \\
\text{(C)} \quad \frac{\langle A \mid \sigma \rangle \longrightarrow \langle A' \mid \sigma' \rangle}{\langle A + B \mid \sigma \rangle \longrightarrow \langle A' \mid \sigma' \rangle} \\
\text{(Co)} \quad \frac{\models C, \langle A \mid \sigma \rangle \longrightarrow \langle A' \mid \sigma' \rangle}{\langle C \rightarrow A \diamond B \mid \sigma \rangle \longrightarrow \langle A' \mid \sigma' \rangle} \\
\text{(Pc)} \quad \frac{P(\bar{x}) = A, \langle A[\bar{x}/\bar{u}] \mid \sigma \rangle \longrightarrow \langle A' \mid \sigma' \rangle}{\langle P(\bar{u}) \mid \sigma \rangle \longrightarrow \langle A' \mid \sigma' \rangle}
\end{array}$$

Figure 3: Transition rules for the operators

the cell liberated by moving the truck one cell up is to be declared free. This is obtained by telling the corresponding *free* si-term on the store, namely by executing `tell(free(succ(succ(r))), c)`. Note that *succ*(*r*) is coded as *r* + 1 by a map, which is why *r* needs to be smaller than 5. Third the truck procedure has to be called recursively with *pred*(*r*) and *c* as new coordinates for the upper and left-most cell it occupies.

The behavior of the alternative movement in which the truck goes down by one cell is similar. As *r* is assumed to be in set  $RCInt = \{1, \dots, 6\}$  and we do not perform a *pred* operation there is no need to check that *r* is greater or equal to 1. However to get the cell down we need to check that *r* is strictly less than 4.

The operational semantics of complex agents is defined through the transition rules of Figure 3. They are quite classical. Rules (S), (P) and (C) provide the usual semantics for sequential, parallel and choice compositions. As expected, rule (Co) specifies that the conditional instruction  $C \rightarrow A \diamond B$  behaves as *A* if condition *C* can be evaluated to true and as *B* otherwise. Note that the notation  $\models C$  is used to denote the fact that *C* evaluates to true. Finally, rule (Pc) makes procedure call  $P(\bar{u})$  behave as the agent *A* defining procedure *P* with the formal arguments  $\bar{x}$  replaced by the actual ones  $\bar{u}$ .

In these rules, it is worth noting that we assume agents of the form  $(E;A)$ ,  $(E \parallel A)$  and  $(A \parallel E)$  to be rewritten as *A*.

## 2.4 A fragment of temporal logic

Linear temporal logic is widely used to reason on dynamic systems. The Scan and Anemone workbenches use a fragment of PLTL [15].

As usual, the logic employed relies on propositional state formulae. In the coordination context, these formulae are to be verified on the current contents of the store. Consequently, given a structured piece of information *t*, the notation  $\#t$  is introduced to denote the number of occurrences of *t* on the store and basic propositional formulae are defined as equalities or inequalities combining algebraic expressions involving integers and number of occurrences of structured pieces of information. An example of such a basic formulae is  $\#free(1, 1) = 1$  which states that the cell of coordinates (1, 1) is free.

Propositional state formulae are built from these basic formulae by using the classical propositional connectors. On the point of notations, given a store  $\sigma$  and a propositional state formulae *PF*, we shall write  $\sigma \models PF$  to indicate that *PF* is established on store  $\sigma$ .

The fragment of temporal logic used in Scan and Anemone is then defined from these propositional state formulae by the following grammar :

$$TF ::= PF \mid \text{Next } TF \mid PF \text{ Until } TF$$

where  $PF$  is a propositional formula. A classical use, on which we shall focus in this paper, is to determine whether a propositional state formulae can be reached at some state. As an example, coming back to the rush hour problem, if the red car indicates that it leaves the grid by placing *out* on the store, a solution to the rush problem is obtained by verifying the formula

$$\text{true Until}(\#out = 1)$$

which we shall subsequently abbreviate as *Reach*(#out = 1).

The algorithm used in Scan and Anemone to establish reach properties basically consists of a breadth-first search on the state space engendered by an agent starting from the empty store. During this search, for each newly created state, a test is made to check whether the considered reach property holds.

Such an elementary algorithm works well for simple problems. However it becomes difficult to use when more complex problems are tackled. One of the reasons comes from the fact that states are duplicated many times by interleaving. Consider for instance the code for the `VerticalTruck` procedure introduced above. With primitives to animate its execution and colors introduced for visualization purposes, its more complete code is as follows:

```
proc VerticalTruck(r: RCInt, c: RCInt, p: Colors) =
  ( (r>1 & r<5) -> ( get(free(pred(r),c));
                    moveTruck(pred(r),c,p);
                    tell(free(succ(succ(r)),c));
                    VerticalTruck(pred(r),c,p) ))
  +
  ( (r<4) -> ( get(free(down_truck(r),c));
              moveTruck(succ(r),c,p);
              tell(free(r,c));
              VerticalTruck(succ(r),c,p) )).
```

Consider now two vertical trucks in parallel and for illustration the first three statements: `get(free(pred(r),c))`, `moveTruck(pred(r),c,p)` `tell(free(succ(succ(r)),c))`. Interleaving them in the two parallel instances of `VerticalTruck` is of no interest for checking whether *out* has been produced since what really matters is the state resulting after the three steps. Hence, provided the first `get` primitive succeeds, the two other primitives may be executed in a row. This observation leads us to introduce so-called guarded lists of primitives.

### 3 A guarded list construct

A *guarded list* of primitives is a construct of the form  $[p \rightarrow p_1, \dots, p_n]$  where  $p, p_1, \dots, p_n$  are primitives, with the list  $p_1, \dots, p_n$  being possibly empty. In that latter case, we shall write  $[p]$  for simplicity of the notations.

Basically, a guarded list of primitives is a list of primitives containing at least one primitive. The reason for writing guarded lists with an arrow and for calling it guarded comes from the fact that, provided the first primitive can be successfully executed, all the others are executed immediately after without rollback in case of failure. It is of course the responsibility of the programmers to guarantee that in

$$\begin{aligned}
(\mathbf{Le}) \quad & \langle [] \mid \sigma \rangle \longrightarrow \langle E \mid \sigma \rangle \\
(\mathbf{Ln}) \quad & \frac{\langle p \mid \sigma \rangle \longrightarrow \langle E \mid \tau \rangle, \langle L \mid \tau \rangle \longrightarrow^* \langle E \mid \phi \rangle}{\langle [p|L] \mid \sigma \rangle \longrightarrow \langle E \mid \phi \rangle} \\
(\mathbf{GL}) \quad & \frac{\langle p \mid \sigma \rangle \longrightarrow \langle E \mid \tau \rangle, \langle L \mid \tau \rangle \longrightarrow^* \langle E \mid \phi \rangle}{\langle [p \rightarrow L] \mid \sigma \rangle \longrightarrow \langle E \mid \phi \rangle}
\end{aligned}$$

Figure 4: Transition rules for guarded lists

case the first primitive can be successfully evaluated the remaining primitives can also be successfully executed. Note that this is obviously the case for tell primitives and the graphical primitives which always succeed regardless of the current content of the store. Note also that we shall subsequently identify criteria to introduce guarded lists while preserving correctness.

It is worth observing that guarded lists are atomic constructs which makes them different from conditional statements. In two words, the execution of  $[p \rightarrow p_1, \dots, p_n]$  is as follows. First the store is locked and the execution of  $p$  is tested. If it fails then no modification is performed on the store and the store is released. Otherwise not only  $p$  is executed but also after  $p_1, \dots, p_n$  in a row. After that the store is released. In contrast, the execution of the conditional statement  $c \rightarrow s_1 \diamond s_2$  amounts to check  $c$ , which does not require to lock the store since conditions are built on comparing si-terms and not their presence or absence on the store. If  $c$  is evaluated to true then  $s_1$  is executed, which means that one step of  $s_1$  is done if this is possible. If  $c$  is evaluated to false then one step of  $s_2$  is attempted.

The operational semantics of guarded lists is defined by rules (Le), (Ln) and (GL) of Figure 4. The first two rules define the semantics of lists of primitives, as being successively executed. Rule (Le) concerns the empty list of primitives  $[]$  while rule (Ln) inductively specifies that of a non-empty list  $[p|L]$  with  $p$  the first primitive and  $L$  is the list of the other primitives<sup>1</sup>. Rule (GL) then states that the guarded list  $[p \rightarrow L]$  can do a computation step from the store  $\sigma$  to  $\phi$  provided the primitive  $p$  can do a step changing the store  $\sigma$  to  $\tau$  and provided the list of primitives  $L$  can change  $\tau$  to  $\phi$ .

Of course, introducing guarded lists as an atomic construct reduces the interleaving possibilities between parallel processes. This is in fact what we want to achieve to get speed ups in the model checking phase. However from a programming point of view, one needs to guarantee that computations are kept in some way. This is the purpose of the introduction of the histories and of their contractions.

### Definition 1

1. Define the set of computational histories (or histories for short) *Shist* as the set  $Sstore^\omega \cup Sstore^* \cdot \{\delta^+, \delta^-\}$  where *Sstore* denotes the set of stores (namely of finite multisets of final si-terms), the  $*$  and  $\omega$  symbols are used to respectively denote finite and infinite repetitions and where  $\delta^+$  and  $\delta^-$  are used as ending marks respectively denoting successful and failing computations.
2. A history  $h_c$  is a contraction of an history  $h$  if it can be obtained from the latter by removing a finite number (possibly 0) elements of it, except the terminating marks  $\delta^+$  and  $\delta^-$ . This is subsequently denoted by  $h_c \preceq h$ .

<sup>1</sup>These list notations  $[]$  and  $[p|L]$  come from the logic programming way of handling lists.

3. Given a contraction  $h_c = \sigma_0 \cdot \dots \cdot \sigma_n \cdot \delta$  (resp.  $h_c = \sigma_0 \cdot \dots \cdot \sigma_n \cdot \dots$ ) of an history  $h$ , there are thus sequences of stores,  $\overline{\sigma}_0, \dots, \overline{\sigma}_n$  such that  $h = \overline{\sigma}_0 \cdot \sigma_0 \cdot \dots \cdot \overline{\sigma}_n \cdot \sigma_n \cdot \delta$  (resp.  $h = \overline{\sigma}_0 \cdot \sigma_0 \cdot \dots \cdot \overline{\sigma}_n \cdot \sigma_n \cdot \dots$ ). For any logic formula  $F$ , the history  $h_c$  is said to be  $F$ -preserving iff, for any  $i$  and for any store  $\tau$  of  $\overline{\sigma}_i$ , one has  $\tau \models F$  iff  $\sigma_i \models F$ . This is subsequently denoted as  $h_c \ll_F h$ .

Contractions and  $F$ -preserving contractions can be lifted in an obvious way to sets of histories.

**Definition 2** A set  $S_c$  of histories is a contraction (resp. a  $F$ -preserving contraction) of a set  $S$  of histories if any history of  $S_c$  is the contraction (resp. a  $F$ -preserving contraction) of a history of  $S$ . By lifting notations on histories, this is subsequently denoted by  $S_c \preceq S$  (resp.  $S_c \ll_F S$ ).

We can now define the history-based operational semantics as the one delivering all the computational histories. To make it general, we shall define it on any contents of the initial store.

**Definition 3** Define the language  $\mathcal{L}_g$  as the Anim-Bach language with the guard list construct.

**Definition 4** Define the operational semantics  $\mathcal{O}_h : \mathcal{L}_g \rightarrow \mathcal{P}(\text{Shist})$  as the following function. For any agent  $A$  and any store  $\tau$

$$\begin{aligned} \mathcal{O}_h(A)(\tau) = & \\ & \{ \sigma_0 \cdot \dots \cdot \sigma_n \cdot \delta^+ : \langle A \mid \sigma_0 \rangle \longrightarrow \dots \longrightarrow \langle E \mid \sigma_n \rangle, \sigma_0 = \tau, n \geq 0 \} \\ & \cup \{ \sigma_0 \cdot \dots \cdot \sigma_n \cdot \delta^- : \langle A \mid \sigma_0 \rangle \longrightarrow \dots \longrightarrow \langle A_n \mid \sigma_n \rangle \not\rightarrow, \sigma_0 = \tau, A_n \neq E, n \geq 0 \} \\ & \cup \{ \sigma_0 \cdot \dots \cdot \sigma_n \cdot \dots : \langle A \mid \sigma_0 \rangle \longrightarrow \dots \longrightarrow \langle A_n \mid \sigma_n \rangle \longrightarrow \dots, \sigma_0 = \tau, \forall n \geq 0 : A_n \neq E \} \end{aligned}$$

We are now in a position to define the refinement of agents.

**Definition 5** Agent  $A$  is said to refine agent  $B$  iff  $\mathcal{O}_h(A)(\tau) \preceq \mathcal{O}_h(B)(\tau)$ , for any store  $\tau$ .

The following proposition is a direct consequence of the above definitions. Its interest is to establish contractions and  $F$ -preserving properties from a syntactic characterization.

### Proposition 1

1. If  $p_1, \dots, p_n$  are tell primitives or graphical primitives then for any primitive  $p$ , the guarded list  $GL = [p \rightarrow p_1, \dots, p_n]$  refines the sequential composition  $SC = p; p_1; \dots; p_n$ . As a result, any reachable property proved on the stores generated by the execution of  $GL$  from a given store  $\tau$  is also established on the stores generated by the execution of  $SC$  from  $\tau$ .
2. Assuming additionally that the arguments of the tell primitives of  $p_1, \dots, p_n$  are distinct from the si-terms appearing in the reachable formulae  $F$ , then  $GL$  is also a  $F$ -preserving contraction of  $SC$ . It results that  $F$  is established on the stores resulting from the execution of  $SC$  from any store  $\tau$  iff it is established on the stores resulting from the execution of  $GL$  from  $\tau$ .

For the study of expressiveness, it will be useful to turn to a simpler semantics focusing on the resulting stores of finite computations. Such a semantics is defined as follows.

**Definition 6** Define the operational semantics  $\mathcal{O}_f : \mathcal{L}_g \rightarrow \mathcal{P}(\text{Sstore} \times \{\delta^+, \delta^-\})$  as the following function: for any agent  $A \in \mathcal{L}_g$

$$\begin{aligned} \mathcal{O}_f(A) = & \{ (\sigma, \delta^+) : \langle A \mid \emptyset \rangle \rightarrow^* \langle E \mid \sigma \rangle \} \\ & \cup \\ & \{ (\sigma, \delta^-) : \langle A \mid \emptyset \rangle \rightarrow^* \langle B \mid \sigma \rangle \not\rightarrow, B \neq E \} \end{aligned}$$

It is immediate to verify that, for any agent  $A$ , the semantics  $\mathcal{O}_f(A)$  is obtained by considering the final stores of the finite histories of  $\mathcal{O}_h(A)(\emptyset)$ .

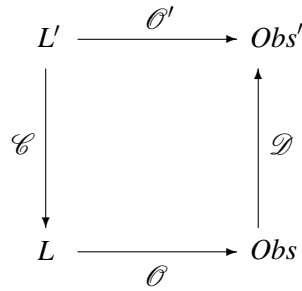


Figure 5: Basic embedding.

## 4 Expressiveness

Although it is interesting to bring efficiency during model checking, the guarded list construct also brings an increase of expressiveness. This is evidenced in this section by using the notion of modular embedding introduced in [5]. As pointed out there, from a computational point of view, all “reasonable” sequential programming languages are equivalent, as they express the same class of functions. Still it is common practice to speak about the “power” of a language on the basis of the expressibility or non-expressibility of programming constructs. In general, a sequential language  $L$  is considered to be more expressive than another sequential language  $L'$  if the constructs of  $L'$  can be translated in  $L$  without requiring a “global reorganization of the program” [16], that is, in a compositional way. Of course the translation must preserve the meaning, at least in the weak sense of preserving termination.

When considering concurrent languages, the notion of termination must be reconsidered as each possible computation represents a possible different evolution of a system of interacting processes. Moreover *deadlock* represents an additional case of termination. We shall consequently rely on the operational semantics  $\mathcal{O}_f$  of Definition 6, focused on the final store of finite computations together with the termination mark.

The basic definition of embedding, given by Shapiro [34] is the following. Consider two languages  $L$  and  $L'$ . Moreover assume we are given the semantics mappings  $\mathcal{O} : L \rightarrow Obs$  and  $\mathcal{O}' : L' \rightarrow Obs'$ , where  $Obs$  and  $Obs'$  are some suitable domains. Then  $L$  can *embed*  $L'$  if there exists a mapping  $\mathcal{C}$  (*coder*) from the statements of  $L'$  to the statements of  $L$ , and a mapping  $\mathcal{D}$  (*decoder*) from  $Obs$  to  $Obs'$ , such that the diagram of Figure 5 commutes, namely such that for every statement  $A \in L'$ :  $\mathcal{D}(\mathcal{O}(\mathcal{C}(A))) = \mathcal{O}'(A)$ .

The basic notion of embedding is too weak since, for instance, the above equation is satisfied by any pair of Turing-complete languages. De Boer and Palamidessi hence proposed in [5] to add three constraints on the coder  $\mathcal{C}$  and on the decoder  $\mathcal{D}$  in order to obtain a notion of *modular* embedding usable for concurrent languages:

1.  $\mathcal{D}$  should be defined in an element-wise way with respect to  $\mathcal{O}$ :

$$\forall X \in Obs : \mathcal{D}(X) = \{\mathcal{D}_{el}(x) \mid x \in X\} \tag{P1}$$

for some appropriate mapping  $\mathcal{D}_{el}$ ;

2. the coder  $\mathcal{C}$  should be defined in a compositional way with respect to the sequential, parallel and

choice operators<sup>2</sup>:

$$\begin{aligned}\mathcal{C}(A ; B) &= \mathcal{C}(A) ; \mathcal{C}(B) \\ \mathcal{C}(A \parallel B) &= \mathcal{C}(A) \parallel \mathcal{C}(B) \\ \mathcal{C}(A + B) &= \mathcal{C}(A) + \mathcal{C}(B)\end{aligned}\tag{P_2}$$

3. the embedding should preserve the behavior of the original processes with respect to deadlock, failure and success (*termination invariance*):

$$\forall X \in Obs, \forall x \in X : tm'(\mathcal{D}_{el}(x)) = tm(x)\tag{P_3}$$

where  $tm$  and  $tm'$  extract the information on termination from the observables of  $L$  and  $L'$ , respectively.

An embedding is then called *modular* if it satisfies properties  $P_1$ ,  $P_2$ , and  $P_3$ .

The existence of a modular embedding from  $L'$  into  $L$  is denoted as  $L' \leq L$ . It is easy to see that  $\leq$  is a pre-order relation. Moreover if  $L' \subseteq L$  then  $L' \leq L$  that is, any language embeds all its sublanguages. This property descends immediately from the definition of embedding, by setting  $\mathcal{C}$  and  $\mathcal{D}$  equal to the identity function.

Let us now compare the Anim-Bach language with guarded lists with the Anim-Bach language without guarded lists. As introduced before, the former is denoted by  $\mathcal{L}_g$ . The latter will be denoted by  $\mathcal{L}_r$ . Following [7], we shall also test three sublanguages composed (i) of the ask, tell primitives, (ii) of the ask, tell, get primitives and (iii) of the ask, tell, get, nask primitives. These sublanguages will be denoted by specifying the primitives between parentheses, as in  $\mathcal{L}_g(\text{ask}, \text{tell})$ . Moreover, to focus on the core features, we shall discard conditional statements and procedures, which are essentially introduced for the ease of coding applications.

By language inclusion, a first obvious result is that the Anim-Bach sublanguages with guarded lists embed their counterparts without guarded lists.

**Proposition 2** *For any subset  $\mathcal{X}$  of primitives, one has  $\mathcal{L}_r(\mathcal{X}) \leq \mathcal{L}_g(\mathcal{X})$ .*

The converse relations do not hold. Intuitively, this is due to the fact that, in contrast to  $\mathcal{L}_r$ , the languages  $\mathcal{L}_g$  have the possibility of *atomically* testing the simultaneous presence of two si-terms on the store. The formal proof requires of course a deeper treatment. It turns out however that the techniques employed in [7] can be adapted to guarded lists. One of them, which results from classical concurrency theory, is that any agent can be reformulated in a so-called normal form.

**Definition 7** *Agents (of  $\mathcal{L}_g$ ) in normal forms are agents of  $\mathcal{L}_g$  which obey the following grammar, where  $N$  is an agent in normal form,  $p$  is a primitive (either graphical or store-related) or a guarded list of primitives and  $A$  denotes an arbitrary (non restricted) agent*

$$N ::= p \mid p ; A \mid N + N.$$

**Proposition 3** *For any agent  $A$  of  $\mathcal{L}_g$ , there is an agent  $N$  of  $\mathcal{L}_g$  in normal form which has the same derivation sequences as  $A$ .*

<sup>2</sup>Actually, this is not required for the sequential operator in [5] since it does not occur in that work.

**Proof.** Indeed, it is possible to associate to any agent  $A$  an agent  $\tau(A)$  in normal form by using the following translation defined inductively on the structure of  $A$ :

$$\begin{aligned}\tau(p) &= p \\ \tau(X;Y) &= \tau(X);Y \\ \tau(X+Y) &= \tau(X) + \tau(Y) \\ \tau(X \parallel Y) &= \tau(X) \parallel Y + \tau(Y) \parallel X\end{aligned}$$

$$\begin{aligned}p \parallel Z &= p;Z \\ (p;A) \parallel Z &= p;(A \parallel Z) \\ (N_1 + N_2) \parallel Z &= N_1 \parallel Z + N_2 \parallel Z\end{aligned}$$

It is easy to verify that, for any agent  $A$ , the agent  $\tau(A)$  is in normal form. Moreover, it is straightforward to verify that  $A$  and  $\tau(A)$  share the same derivation sequences.  $\square$

We are now in a position to establish that  $\mathcal{L}_g(ask, tell)$  cannot be embedded in  $\mathcal{L}_r(ask, tell)$ .

**Proposition 4**  $\mathcal{L}_g(ask, tell) \not\leq \mathcal{L}_r(ask, tell)$

**Proof.** Let us proceed by contradiction and assume the existence of a coder  $\mathcal{C}$  and a decoder  $\mathcal{D}$ . The proof is composed of three main steps.

STEP 1: on the coding of  $tell(a)$  and  $tell(b)$ . Let  $a, b$  be two distinct si-terms. Since  $\mathcal{O}_f([tell(a)]) = \{(\{a\}, \delta^+)\}$ , any computation of  $\mathcal{C}([tell(a)])$  starting in the empty store succeeds by property  $P_3$ . Let

$$\langle \mathcal{C}([tell(a)]) \mid \emptyset \rangle \longrightarrow \dots \longrightarrow \langle E \mid \{a_1, \dots, a_m\} \rangle$$

be one computation of  $\mathcal{C}([tell(a)])$ . Similarly, any computation of  $\mathcal{C}([tell(b)])$  starting on the empty store succeeds. Let

$$\langle \mathcal{C}([tell(b)]) \mid \emptyset \rangle \longrightarrow \dots \longrightarrow \langle E \mid \{b_1, \dots, b_n\} \rangle$$

be one computation of  $\mathcal{C}([tell(b)])$ . Note that, as we only consider ask and tell primitives, this computations can be reproduced on any store  $\tau$ . We thus have also that

$$\langle \mathcal{C}([tell(b)]) \mid \tau \rangle \longrightarrow \dots \longrightarrow \langle E \mid \tau \cup \{b_1, \dots, b_n\} \rangle$$

In particular, as  $\mathcal{C}([tell(a)]; [tell(b)]) = \mathcal{C}([tell(a)]; \mathcal{C}([tell(b)])$ , we have that

$$\begin{aligned}\langle \mathcal{C}([tell(a)]; [tell(b)]) \mid \emptyset \rangle &\longrightarrow \dots \\ &\longrightarrow \langle \mathcal{C}([tell(b)]) \mid \{a_1, \dots, a_m\} \rangle \longrightarrow \dots \\ &\longrightarrow \langle E \mid \{a_1, \dots, a_m, b_1, \dots, b_n\} \rangle\end{aligned}$$

STEP 2: coding of an auxiliary statement  $AB$ . Consider now  $AB = [ask(a) \rightarrow ask(b)]$ . Obviously, as it requires  $a$  to be present, the execution of  $AB$  on the empty store cannot do any step and thus  $\mathcal{O}_f(AB) = \{(\emptyset, \delta^-)\}$ . Let us now turn to its coding  $\mathcal{C}(AB)$ . By Proposition 3, it can be regarded in its normal form. As it is in  $\mathcal{L}_r(tell, ask)$ , its more general form is as follows

$$tell(t_1); A_1 + \dots + tell(t_p); A_p + ask(u_1); B_1 + \dots + ask(u_q); B_q + gp_1; C_1 + \dots + gp_r; C_r$$

where  $gp_1, \dots, gp_r$  are graphical primitives. Let us first establish that there is no alternative guarded by a  $tell(t_i)$  operation. Indeed, if this was the case, then

$$D = \langle \mathcal{C}(AB) \mid \emptyset \rangle \longrightarrow \langle A_i \mid \{t_i\} \rangle$$

would be a valid computation prefix of  $\mathcal{C}(AB)$ . As  $\mathcal{O}_f(AB) = \{(\emptyset, \delta^-)\}$ , this prefix should deadlock afterwards. However, as  $\mathcal{C}(AB + [tell(a)]) = \mathcal{C}(AB) + \mathcal{C}([tell(a)])$ , the computation step  $D$  is also a valid computation prefix of  $\mathcal{C}(AB + [tell(a)])$ . Hence,  $\mathcal{C}(AB + [tell(a)])$  admits a failing computation which, by property  $P_3$ , contradicts the fact that  $\mathcal{O}_f(AB + [tell(a)]) = \{(\{a\}, \delta^+)\}$ . The proof of the absence of an alternative guarded by a graphical primitive  $gp_i$  proceeds similarly.

Let us now establish that none of the  $u_i$ 's belong to  $\{a_1, \dots, a_m\} \cup \{b_1, \dots, b_n\}$ . Indeed, if  $u_j \in \{a_1, \dots, a_m\}$  for some  $j \in \{1, \dots, q\}$ , then, as  $\mathcal{C}([tell(a)]; AB) = \mathcal{C}([tell(a)]) ; \mathcal{C}(AB)$ , the derivation

$$\begin{aligned} D' &= \langle \mathcal{C}([tell(a)]; AB) \mid \emptyset \rangle \longrightarrow \dots \longrightarrow \langle \mathcal{C}(AB) \mid \{a_1, \dots, a_m\} \rangle \\ &\quad \longrightarrow \langle B_j \mid \{a_1, \dots, a_m\} \rangle \end{aligned}$$

is a valid computation prefix of  $\mathcal{C}([tell(a)]; AB)$ . However, by applying rule (T),

$$\langle [tell(a)]; AB \mid \emptyset \rangle \longrightarrow \langle AB \mid \{a\} \rangle \not\rightarrow$$

By Property  $P_3$ , it follows that  $D'$  can only be continued by failing suffixes. However, thanks to the fact that  $\mathcal{C}([tell(a)]; (AB + [ask(a)])) = \mathcal{C}([tell(a)]) ; (\mathcal{C}(AB) + \mathcal{C}([ask(a)]))$  the prefix  $D'$  induces the following computation prefix  $D''$  for  $\mathcal{C}([tell(a)]; (AB + [ask(a)]))$

$$\begin{aligned} D'' &= \langle \mathcal{C}([tell(a)]; (AB + [ask(a)])) \mid \emptyset \rangle \longrightarrow \dots \\ &\quad \longrightarrow \langle \mathcal{C}(AB) + \mathcal{C}([ask(a)]) \mid \{a_1, \dots, a_m\} \rangle \\ &\quad \longrightarrow \langle B_j \mid \{a_1, \dots, a_m\} \rangle. \end{aligned}$$

which can only be continued by failing suffixes whereas  $[tell(a)]; (AB + [ask(a)])$  only admits a successful computation.

The proof proceeds similarly in the case  $u_j \in \{b_1, \dots, b_n\}$  for some  $j \in \{1, \dots, q\}$  by then considering  $[tell(b)]; AB$  and  $[tell(b)]; (AB + [ask(b)])$ .

STEP 3: combining the first two steps to produce a contradiction. The  $u_i$ 's are thus forced not to belong to  $\{a_1, \dots, a_m\} \cup \{b_1, \dots, b_n\}$ . However, this induces a contradiction. To that end, let us first observe that  $\mathcal{C}(AB)$  cannot do any step on the store  $\{a_1, \dots, a_m, b_1, \dots, b_n\}$  since none of the  $ask(u_i)$  primitives can do a step. As a result,

$$\langle AB \mid \{a_1, \dots, a_m, b_1, \dots, b_n\} \rangle \not\rightarrow$$

Now, by compositionality of the coder with respect to the sequential composition (property  $P_2$ ),  $\mathcal{C}([tell(a)]; [tell(b)]; AB) = \mathcal{C}([tell(a)]) ; \mathcal{C}([tell(b)]) ; \mathcal{C}(AB)$ , and consequently the following derivation is valid:

$$\langle \mathcal{C}([tell(a)]; [tell(b)]; AB) \mid \emptyset \rangle \longrightarrow \dots \longrightarrow \langle AB \mid \{a_1, \dots, a_m, b_1, \dots, b_n\} \rangle$$

and yields a failing computation for  $\mathcal{C}([tell(a)]; [tell(b)]; AB)$ . However, as easily checked,  $[tell(a)]; [tell(b)]; AB$  has only one successful computation.  $\square$

Using similar arguments as in [7], it is possible to extend the previous proof so as to establish the following results.

**Proposition 5**

1.  $\mathcal{L}_g(\text{get}, \text{tell}) \not\leq \mathcal{L}_r(\text{get}, \text{tell})$
2.  $\mathcal{L}_g(\text{ask}, \text{get}, \text{tell}) \not\leq \mathcal{L}_r(\text{ask}, \text{get}, \text{tell})$
3.  $\mathcal{L}_g(\text{ask}, \text{nask}, \text{get}, \text{tell}) \not\leq \mathcal{L}_r(\text{ask}, \text{nask}, \text{get}, \text{tell})$

Case	Nb's cars/trucks	Game
1	2	VPurpleTruck(2,4), HRedCar(3,2)
2	3	VPurpleTruck(2,1), HRedCar(3,2), HGreenCar(1,1)
3	4	VPurpleTruck(2,1), HRedCar(3,2), HGreenCar(1,1), VOrangeCar(5,1)
4	5	VPurpleTruck(2,1), HRedCar(3,2), HGreenCar(1,1), VOrangeCar(5,1), VBlueTruck(2,4)
5	6	VPurpleTruck(2,1), HRedCar(3,2), HGreenCar(1,1), VOrangeCar(5,1), VBlueTruck(2,4), HGreenTruck(6,3)
6	7	VPurpleTruck(2,1), HRedCar(3,2), HGreenCar(1,1), VOrangeCar(5,1), VBlueTruck(2,4), HGreenTruck(6,3), VYellowTruck(1,6)

Table 1: Test cases

## 5 Performance

Let us now illustrate the gain of efficiency during model-checking obtained by the guarded list construct. To that end, we shall subsequently compare the performance of the Scan and Anemone breath-first search model checker on various examples of the rush hour puzzle coded, on the one hand, without the guarded list construct, and, on the other hand, with the guarded list construct.

As described in the previous sections, the rush hour puzzle can be formulated as a coordination problem by considering cars and trucks as autonomous agents which have to coordinate on the basis of free places. The complete code is available at [4]. Besides sets, maps and widget definitions, it is basically composed of generic procedures for coding horizontal cars and trucks as well as vertical cars and trucks. Specific cars and trucks are then obtained by instantiating colors and places and are put in parallel.

The code for the cars and trucks follows the pattern of the code presented in page 60. Basically, under some conditions, each car and truck amounts to (i) obtaining a free place to move through the execution of a `get` primitive, (ii) then to operating the movement graphically through the execution of a `move` primitive and (iii) finally to freeing the place previously occupied by means of the execution of a `tell` primitive. As an example, the following code is a snippet refining the code of page 60.

```
get ( free ( pred ( r ) , c ) );
move ( truck_img ( c ) , pred ( r ) , c );
tell ( free ( succ ( succ ( r ) ) , c ) )
```

The problem is solved when the *out* si-term is put on the store, which leads to checking that the property  $\#out = 1$  can be reached. As easily checked, the hypotheses of Proposition 1 are verified so that we can replace the above code snippet by the following:

```
[ get ( free ( pred ( r ) , c ) ) ->
  move ( truck_img ( c ) , pred ( r ) , c ) ,
  tell ( free ( succ ( succ ( r ) ) , c ) ) ]
```

This code is indeed an  $F$ -preserving contraction for the formulae  $F = (\#out = 1)$ .

By performing this transformation, one gains per vehicle the computation of two stores on four, which induces the hope of a gain of performance of  $2^n$  if  $n$  is the number of vehicles in parallel. To verify the actual gain of performance, we have model checked the two codes (one with guarded list and the other without guarded list) on the examples of Table 1. They are inspired by cards of the real game

Case	Without GL	With GL	Gain	Expected gain
1	2630 ms (2s)	298 ms (0s)	8.82	4
2	64341 ms (64s   1m)	355 ms (0s)	181	8
3	60339 ms (60s   1m)	770 ms (1s)	78	16
4	495578 ms (496s   8m)	1032 ms (1s)	480	32
5	3271343 ms (3271s   55m)	4100 ms (4s)	797	64
6	$\geq 10h$	4862322 (1h35m)	$\geq 6$	128

Table 2: Performance results

and, in view of the above hope, are taken by progressively adding vehicles. The last column in Table 1 gives a brief description of the considered game. The V and H prefixes refer to a vehicle put vertically or horizontally, while the coordinates are those of the rows (counted from top to bottom) and columns (counted from left to right).

Table 2 reports on the data obtained on a portable computer Lenovo x64 bits, running Windows 10 with 16 GB of memory. The first column refers to the test case, the second and the third columns give the time in milliseconds necessary for model checking, the fourth column the time ratio and the last column the hoped gain according to  $2^n$  where  $n$  is the number of vehicles in the game. As can be seen from this table, guarded lists lead to a real performance gain and even a greater performance than expected<sup>3</sup>. This can be explained by the fact that the Scan and Anemone model checker relies on non-optimized structures like sequential lists and basically evaluates dynamically the transition system during the model-checking phase. It is also interesting to observe that the exponential behavior resulting from the interleaving of behaviors is kept to a reasonable cost for the first five cases with guarded lists, while it starts exploding from the fourth case without guarded lists. The interested reader may redo the campaign of tests by using the material available at [4].

## 6 Related work

Although, to the best of our knowledge, it has not been exploited by coordination languages, the idea of forcing statements to be executed without interruption is not new. In [14] Dijkstra has introduced guarded commands, which are statements of the form  $G \rightarrow S$  that atomically executes statement  $S$  provided the condition  $G$  is evaluated to true. They are mostly combined in repetitive constructs of the form

$$\begin{array}{l}
 \mathbf{do} \quad G_0 \rightarrow S_0 \\
 \quad \square \quad G_1 \rightarrow S_1 \\
 \quad \dots \\
 \quad \square \quad G_n \rightarrow S_n \\
 \mathbf{od}
 \end{array}$$

which repetitively selects one of the executable guarded commands until none of them are executable. A non-deterministic choice is operated in the selection of the guarded commands in case several of them can be executed. Later Abrial has used guarded commands in the Event-B method [1]. Such a construct is also at the core of the guarded Horn clause framework proposed by Ueda in [35] to introduce parallelism

<sup>3</sup>In the last case, we stopped the model-checker after 10 hours of run

in logic programming. There Horn clauses are rewritten in the following form

$$H \leftarrow G_1, \dots, G_m | B_1, \dots, B_n$$

with  $H, G_1, \dots, G_m, B_1, \dots, B_n$  being atoms. The classical SLD-resolution used to reduce an atom is modified as follows. Assume  $A$  is the atom to be reduced. All the clauses whose head  $H$  is unifiable with  $A$  have their guard  $G_1, \dots, G_m$  evaluated. The first one which succeeds determines the clause that is used, the other being simply discarded. To avoid mismatching instantiations of variables, the evaluation of any  $G_i$  is suspended if it can only succeed by binding variables. Finally, several pieces of work have tried to incorporate transactions and atomic constructs in “classical” process algebras, like CCS. For instance, A2CCS [19] proposes to refine complex actions into sequences of elementary ones by modelling atomic behaviors at two levels, with so-called high-level actions being decomposed into atomic sequences of low-level actions. To enforce isolation, atomic sequences are required to go into a special invisible state during all their execution. In fact, sequences of elementary actions are executed sequentially, without interleaving with other actions, as though in a critical section. RCCS [10] is another process algebra incorporating distributed backtracking to handle transactions inside CCS. The main idea is that, in RCCS, each process has access to a log of its synchronization history and may always wind back to a previous state. A similar idea of log is used in AtCCS [2]. There, during the evaluation of an atomic block, actions are recorded in a private log and have no effects outside the scope of the transaction until it is committed. An explicit termination action “end” is used to signal that a transaction is finished and should be committed. States are used in addition to model the evaluation of expressions and can be viewed as tuples put or retrieved from shared spaces in coordination languages. When a transaction has reached commitment and if the local state meets the global one, then all actions present in the log are performed at the same time and the transaction is closed. Otherwise the transaction is aborted.

Our guarded list construct share similarities with these pieces of work. A major difference is however that we restrict the guard to a single primitive to be evaluated. This eases the implementation since, once the primitive has been successfully evaluated, the remaining primitives can be executed in a row without using distributed backtracking as in RCCS, private spaces as in AtCCS for speculative computations and checks for compatibility between local and global environments. Intricate suspensions inherent in guarded Horn clauses are also avoided. Nevertheless, under this restriction, the combination with the non deterministic choice operator  $+$  allows to achieve computations similar to the repetitive statements of guarded commands. With respect to these pieces of work, our contribution is also to focus on model checking and to propose a refinement strategy that allows to transform programs by introducing the guarded list construct. An expressiveness study is also proposed in this paper and not in these pieces of work.

Limiting the state explosion problem in model checking by limiting interleaving is similar in spirit with the partial-order reduction introduced in [18, 30, 32, 36]. Realizing that  $n$  independent parallel transitions result in  $n!$  different orderings and  $2^n$  different states, the idea is to select a representative composed of  $n + 1$  states. Indeed, as the transitions are independent, properties need only to be verified on a possible ordering. This technique has been employed in many research efforts for model checking asynchronous systems. However, these efforts aim at designing more efficient algorithms on optimized automata. The approach taken here is different. We do not change our algorithm for model checking, but rather introduce a new construct as well as considerations on refinements to transform programs into more efficient programs.

## 7 Conclusion

In the aim of improving the performance of the model checking tool introduced in the workbenches Scan [21] and Anemone[22], this article has introduced a new construct, named guarded list. It has been proved to yield an increase of expressiveness to Linda-like languages, while indeed bringing an increase of efficiency during the model checking phase. In order to pave the way to transform programs by safely introducing the guarded list construct, we have also proposed a notion of refinement and have characterized situations in which one can safely replace a sequence of primitives by a guarded list of primitives.

Our work opens several paths for future research. As regards the expressiveness study, we have used the approach proposed in [6] for a few sublanguages. This naturally leads to deepen the study to include all the sublanguages and to compare them with the  $L_{MR}$  and  $L_{CS}$  families of languages studied in [6]. Moreover this approach is only one of the possible approaches to compare languages. It would be for instance interesting to verify whether the absolute approach promoted by Zavattaro et al in [8] would change the expressiveness hierarchy of languages. Moreover, expressiveness studies based on bisimulations and fully abstract semantics such as reported in [33] are also worth exploring. As regards model-checking, the algorithm embodied in the Scan and Anemone workbenches is quite elementary and calls for improvements. In that line of research, it would be interesting to study how state collapsing and pruning techniques used for checking large distributed systems may improve the performance of the model checker. Finally, future work will aim at developing further the theory of refinement and in investigating correctness preserving transformation techniques.

## 8 Acknowledgment

The authors thank the University of Namur for its support. They also thank the Walloon Region for partial support through the Ariac project (convention 210235) and the CyberExcellence project (convention 2110186). Moreover they are grateful to the anonymous reviewers for their comments on earlier versions of this work.

## References

- [1] J.-R. Abrial (2010): *Modeling in Event-B - System and Software Engineering*. Cambridge University Press, doi:10.1017/CBO9781139195881.
- [2] L. Acciai, M. Boreale & S. Dal-Zilio (2007): *A Concurrent Calculus with Atomic Transactions*. In R. De Nicola, editor: *Proceedings of the 16th European Symposium on Programming Languages and Systems (ESOP), Lecture Notes in Computer Science 4421*, Springer, pp. 48–63, doi:10.1007/978-3-540-71316-6\_5.
- [3] J.C.M. Baeten & W.P. Weijland (1990): *Process Algebra*. Cambridge tracts in Theoretical Computer Science 18, Cambridge University Press, doi:10.1017/CBO9780511624193.
- [4] M. Barkallah & J.-M. Jacquet (2020): *Model-checking the Rush Hour Bach Program*. Available at [https://staff.info.unamur.be/mbarkall/ICE\\_2023](https://staff.info.unamur.be/mbarkall/ICE_2023) or [https://staff.info.unamur.be/jmj/ICE\\_2023](https://staff.info.unamur.be/jmj/ICE_2023). Created on May 30th 2023.
- [5] F.S. de Boer & C. Palamidessi (1994): *Embedding as a Tool for Language Comparison*. *Information and Computation* 108(1), pp. 128–157, doi:10.1006/inco.1994.1004.
- [6] A. Brogi & J.-M. Jacquet (1998): *On the Expressiveness of Linda-like Concurrent Languages*. *Electronical Notes in Theoretical Computer Science* 16(2), pp. 61–82.

- [7] A. Brogi & J.-M. Jacquet (2003): *On the Expressiveness of Coordination via Shared Dataspaces*. *Science of Computer Programming* 46(1-2), pp. 71–98, doi:10.1016/S0167-6423(02)00087-4.
- [8] N. Busi, R. Gorrieri & G. Zavattaro (2000): *On the Expressiveness of Linda Coordination Primitives*. *Information and Computation* 156(1-2), pp. 90–121, doi:10.1006/inco.1999.2823.
- [9] N. Carriero & D. Gelernter (1989): *Linda in Context*. *Communications of the ACM* 32(4), pp. 444–458, doi:10.1145/63334.63337.
- [10] V. Danos & J. Krivine (2005): *Transactions in RCCS*. In M. Abadi & L. de Alfaro, editors: *Proceedings of the 16th International Conference on Concurrency Theory, Lecture Notes in Computer Science* 3653, Springer, pp. 398–412, doi:10.1007/11539452\_31.
- [11] D. Darquennes, J.-M. Jacquet & I. Linden (2013): *On Density in Coordination Languages*. In C. Canal & M. Villari, editors: *CCIS 393, Advances in Service-Oriented and Cloud Computing, ESOC 2013, Proceedings of Foclasa Workshop*, Springer, Malaga, Spain, pp. 189–203.
- [12] D. Darquennes, J.-M. Jacquet & I. Linden (2015): *On Distributed Density in Tuple-based Coordination Languages*. In J. Cámara & J. Proença, editors: *Proceedings 13th International Workshop on Foundations of Coordination Languages and Self-Adaptive Systems, EPTCS* 175, Springer, Rome, Italy, pp. 36–53.
- [13] D. Darquennes, J.-M. Jacquet & I. Linden (2018): *On Multiplicities in Tuple-Based Coordination Languages: The Bach Family of Languages and Its Expressiveness Study*. In G. Di Marzo Serugendo & M. Loreti, editors: *Proceedings of the 20th International Conference on Coordination Models and Languages, Lecture Notes in Computer Science* 10852, Springer, pp. 81–109, doi:10.1007/978-3-319-92408-3\_4.
- [14] E.W. Dijkstra (1975): *Guarded Commands, Nondeterminacy and Formal Derivation of Programs*. *Communication of the ACM* 18(8), pp. 453–457, doi:10.1145/360933.360975.
- [15] E. Allen Emerson (1990): *Temporal and Modal Logic*. In: *Handbook of Theoretical Computer Science, Volume B: Formal Models and Semantics (B)*, Elsevier, pp. 995–1072.
- [16] M. Felleisen (1990): *On the Expressive Power of Programming Languages*. In N. Jones, editor: *Proceedings European Symposium on Programming, Lecture Notes in Computer Science* 432, Springer-Verlag, pp. 134–151, doi:10.1007/3-540-52592-0\_60.
- [17] D. Gelernter & N. Carriero (1992): *Coordination Languages and Their Significance*. *Communications of the ACM* 35(2), pp. 97–107, doi:10.1145/129630.376083.
- [18] P. Godefroid & P. Wolper (1991): *Using Partial Orders for the Efficient Verification of Deadlock Freedom and Safety Properties*. In K.G. Larsen & A. Skou, editors: *Proceedings of the 3rd International Workshop on Computer Aided Verification, Lecture Notes in Computer Science* 575, Springer, pp. 332–342, doi:10.1007/3-540-55179-4\_32.
- [19] R. Gorrieri, S. Marchetti & U. Montanari (1990): *A2CCS: Atomic Actions for CCS*. *Theoretical Computer Science* 72(2&3), pp. 203–223, doi:10.1016/0304-3975(90)90035-G.
- [20] C.A.R. Hoare (1985): *Communicating Sequential Processes*. Prentice-Hall.
- [21] J.-M. Jacquet & M. Barkallah (2019): *Scan: A Simple Coordination Workbench*. In H. Riis Nielson & E. Tuosto, editors: *Proceedings of the 21st International Conference on Coordination Models and Languages, Lecture Notes in Computer Science* 11533, Springer, pp. 75–91, doi:10.1007/978-3-030-22397-7\_5.
- [22] J.-M. Jacquet & M. Barkallah (2021): *Anemone: A workbench for the Multi-Bach Coordination Language*. *Science of Computer Programming* 202, p. 102579, doi:10.1016/j.scico.2020.102579.
- [23] J.-M. Jacquet, K. De Bosschere & A. Brogi (2000): *On Timed Coordination Languages*. In A. Porto & G.-C. Roman, editors: *Proc. 4th International Conference on Coordination Languages and Models, Lecture Notes in Computer Science* 1906, Springer, pp. 81–98, doi:10.1007/3-540-45263-X\_6.
- [24] J.-M. Jacquet & I. Linden (2007): *Coordinating Context-aware Applications in Mobile Ad-hoc Networks*. In T. Braun, D. Konstantas, S. Mascolo & M. Wulff, editors: *Proceedings of the first ERCIM workshop on eMobility*, The University of Bern, pp. 107–118.

- [25] J.-M. Jacquet & I. Linden (2009): *Fully Abstract Models and Refinements as Tools to Compare Agents in Timed Coordination Languages*. *Theoretical Computer Science* 410(2-3), pp. 221–253, doi:10.1016/j.tcs.2008.09.020.
- [26] Jean-Marie Jacquet, Isabelle Linden & Denis Darquennes (2016): *On the introduction of density in tuple-space coordination languages*. *Science of Computer Programming* 115-116, pp. 149–176, doi:10.1016/j.scico.2015.10.011.
- [27] I. Linden & J.-M. Jacquet (2004): *On the Expressiveness of Absolute-Time Coordination Languages*. In R. De Nicola, G.L. Ferrari & G. Meredith, editors: *Proc. 6th International Conference on Coordination Models and Languages, Lecture Notes in Computer Science* 2949, Springer, pp. 232–247, doi:10.1007/978-3-540-24634-3\_18.
- [28] I. Linden & J.-M. Jacquet (2007): *On the Expressiveness of Timed Coordination via Shared Dataspace*. *Electronical Notes in Theoretical Computer Science* 180(2), pp. 71–89, doi:10.1016/j.entcs.2006.10.047.
- [29] I. Linden, J.-M. Jacquet, K. De Bosschere & A. Brogi (2004): *On the Expressiveness of Relative-Timed Coordination Models*. *Electronical Notes in Theoretical Computer Science* 97, pp. 125–153, doi:10.1016/j.entcs.2004.04.034.
- [30] K.L. McMillan (1992): *Using Unfoldings to Avoid the State Explosion Problem in the Verification of Asynchronous Circuits*. In G. von Bochmann & D.K. Probst, editors: *Proceedings of the Fourth International Workshop on Computer Aided Verification, Lecture Notes in Computer Science* 663, Springer, pp. 164–177, doi:10.1007/3-540-56496-9\_14.
- [31] R. Milner (1989): *Communication and Concurrency*. PHI Series in computer science, Prentice Hall.
- [32] D.A. Peled (1993): *All from One, One for All: on Model Checking Using Representatives*. In C. Courcoubetis, editor: *Proceedings of the 5th International Conference on Computer Aided Verification, Lecture Notes in Computer Science* 697, Springer, pp. 409–423, doi:10.1007/3-540-56922-7\_34.
- [33] K. Peters (2019): *Comparing Process Calculi Using Encodings*. In J. Pérez & J. Rot, editors: *Proceedings of the Combined Workshops on Expressiveness in Concurrency and Structural Operational Semantics, (EXPRESS/SOS), EPTCS* 300, pp. 19–38.
- [34] E.Y. Shapiro (1992): *Embeddings among Concurrent Programming Languages*. In W.R. Cleaveland, editor: *Proceedings of CONCUR'92*, Springer-Verlag, pp. 486–503, doi:10.1007/BFb0084811.
- [35] K. Ueda (1985): *Guarded Horn Clauses*. In E. Wada, editor: *Proceedings of the 4th Conference on Logic Programming, Lecture Notes in Computer Science* 221, Springer, pp. 168–179, doi:10.1007/3-540-16479-0\_17.
- [36] A. Valmari (1996): *The State Explosion Problem*. In W. Reisig & G. Rozenberg, editors: *Lectures on Petri Nets I: Basic Models, Lecture Notes in Computer Science* 1491, Springer, pp. 429–528, doi:10.1007/3-540-65306-6\_21.