Generating Distributed Programs from Event-B Models

Horatiu Cirstea, Alexis Grall, Dominique Méry

Generating Distributed Programs from Event-B Models

Horatiu Cirstea
LORIA UMR 7503
Université de Lorraine
Vandœuvre-lès-Nancy, France
horatiu.cirstea@loria.fr

Alexis Grall
LORIA UMR 7503
Université de Lorraine
Vandœuvre-lès-Nancy, France
alexis.grall@loria.fr

Dominique Méry
LORIA UMR 7503
Telecom Nancy, Université de Lorraine
Vandœuvre-lès-Nancy, France
dominique.mery@loria.fr

Distributed algorithms offer challenges in checking that they meet their specifications. Verification techniques can be extended to deal with the verification of safety properties of distributed algorithms. In this paper, we present an approach for combining correct-by-construction approaches and transformations of formal models (EVENT-B) into programs (DISTALGO) to address the design of verified distributed programs. We define a subset LB (Local EVENT-B) of the EVENT-B modelling language restricted to events modelling the classical actions of distributed programs as internal or local computations, sending messages and receiving messages. We define then transformations of the various elements of the LB language into DISTALGO programs. The general methodology consists in starting from a statement of the problem to program and then progressively producing an LB model obtained after several refinement steps of the initial LB model. The derivation of the LB model is not described in the current paper and has already been addressed in other works. The transformation of LB models into DISTALGO programs is illustrated through a simple example. The refinement process and the soundness of the transformation allow one to produce correct-by-construction distributed programs.

1 Introduction

EVENT-B is a formal modelling language developed by Abrial [1] offering key features such as the use of set theory as a data modelling notation, the use of refinement to relate system models at different abstraction levels and the use of mathematical proofs to verify consistency between refinement levels. Moreover, the language is supported by the environment RODIN[2] which is extensible through the mechanism of plugin. Previous works [3, 13, 9, 10] illustrate the correct-by-construction design of distributed algorithms using EVENT-B models and refinements; those works show that at an adequate level of concretization of models, one can derive a distributed algorithm in a pseudo algorithmic notation. However, the derivation of concrete EVENT-B models requires to develop a methodology related to a given class of problems. For instance, we have produced a plugin EB2RC [11, 5] which automatically generates a recursive algorithm from an EVENT-B model derived by analysis of a problem such as Floyd's algorithm, or search algorithms, or sorting algorithms. The transformation of an EVENT-B model into a recursive algorithm was based on the definition of a class of (concrete) EVENT-B models satisfying constraints making the transformation automatic.

In the current paper, we study the systematic transformation of concrete EVENT-B models into the DISTALGO [7] programming language. In fact, the design of a distributed algorithm using the correct-by-construction approach starts by expressing the required computations in a very abstract EVENT-B model (AM) and then progressively refining the model into a final concrete model (CM) very close to an algorithmic expression of the distributed algorithm. The main advantage of such a refinement-based process is the preservation of safety properties of the different models: the refinement is checked by discharging a list of proof obligations. We do not describe the process for developing the model CM which is supposed to be a local EVENT-B model and which could be translated into an algorithmic

To appear in EPTCS.

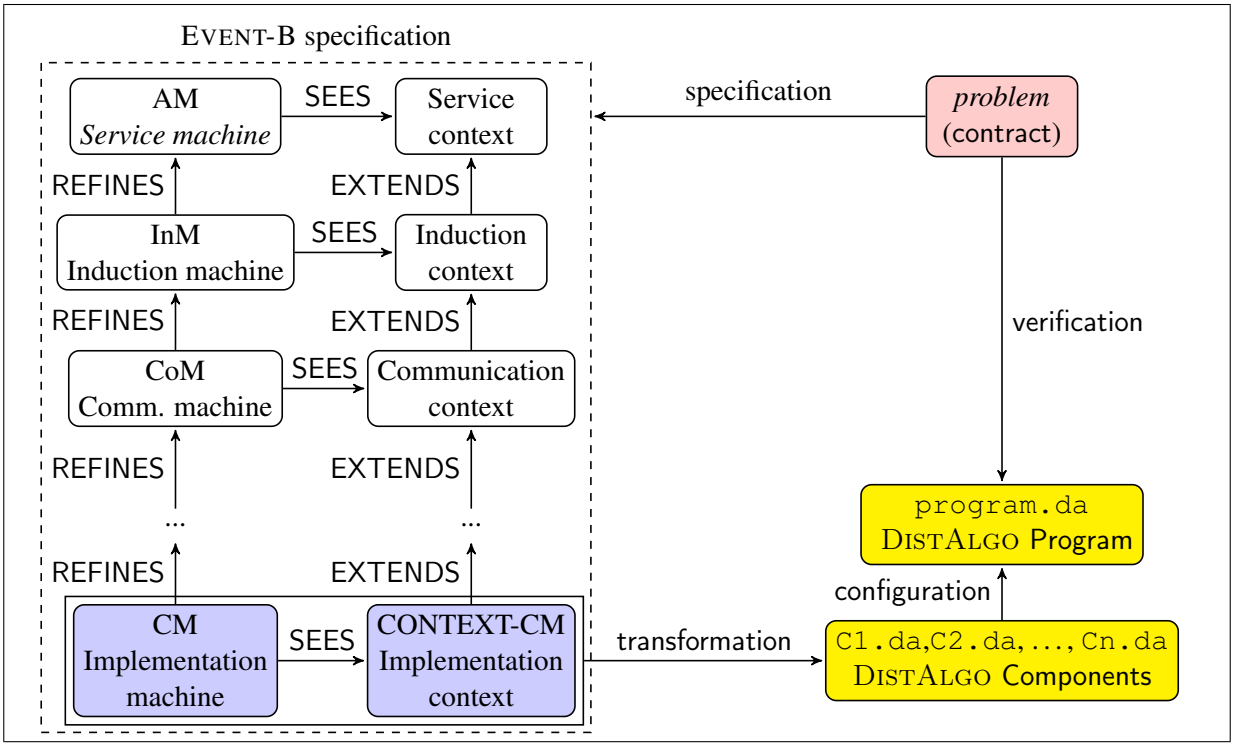


Figure 1: The global methodology for correct-by-construction distributed algorithms.

distributed notation. We focus on the transformations required for obtaining a DISTALGO program from a local EVENT-B model as indicated in Figure 1: the program `program.da` is generated from CM and CONTEXT-CM. We will not provide the proof of correctness of the translation but we will give enough details for trusting it. The proof will be given in a future work.

An overview of the integrated development framework Figure 1 provides an overview of our integrated development framework for refinement-based program verification of distributed algorithms. The general methodology starts by stating the *problem* to solve by listing the requirements (*i.e.* the contract) attached to the problem; the requirements can be either expressed in a formal language or in an informal textual language. One has then to specify the EVENT-B machine AM translating the main requirements for the given problem. Then a list of formal EVENT-B refined machines are produced to obtain a final EVENT-B machine and context, CM and CM-CONTEXT. Finally, the translations of these final context and machine into DISTALGO components and programs are generated in two main steps: the automatic compilation of CM and CM-CONTEXT into a DISTALGO program, and the manual tuning of the obtained DISTALGO components (if some configurations were not specified in the model).

The refinement block (with nodes AM, CONTEXT-AM, CM and CONTEXT-CM) in Figure 1, illustrates the mechanism for deriving machines via refinement. It can be explained briefly as follows:

- The machine AM defines events having the same contract as that expressed in the requirements. This machine SEES the SERVICE CONTEXT, which expresses static information about the machine.

- The machines INM and COM are introducing respectively the description of the computing process and the corresponding communications.
- The machine CM refines COM generating a concrete specification that satisfies the requirements. This machine SEES the context CONTEXT-CM, which introduces control information for the new machine.
- The labelled actions REFINES, SEES and EXTENDS, are supported by the RODIN platform and are verified *completely* using the proof assistant provided by RODIN.

The result of the refinement is the EVENT-B machine CM, which contains the refined events and the proof obligations that must be discharged in order to prove that the refinement is correct.

Transformations of this EVENT-B machine CM into a DISTALGO program is based on the extraction of information concerning the network and the process classes from the context CONTEXT-CM, and on the analysis of the localization of the different variables. The events of CM are supposed to be local which means that they are using only local instances of variables. For instance, *pc* will be a local variable with an instance $pc(p)$ for the process p. We will define precisely the localization process from the code of EVENT-B models. Finally, some constants whose values are not defined in the context are instantiated during the configuration phase.

Related work From previous experience, we illustrate how the refinement can improve and facilitate the verification process by relating state-based models.

We described a simple extension of the *call-as-event* paradigm [8, 11] to handle the design of concurrent programs in the *coordination*-based approach but we do not target a specific programming language as DISTALGO. The EB2ALL (http://eb2all.loria.fr) framework provides a list of transformations of EVENT-B models into classical programming languages (C, C++, Java, ...) but it does not consider distributed algorithms. The current work can be considered as adding a new target programming language but with the target of a distributed program like it was proposed in Visidia (http://visidia.labri.fr) together with EVENT-B with the plugin B2VISIDIA relating the local EVENT-B model and a VISIDIA program. However, the VISIDIA approach addresses distributed programs defined as set of rewriting rules of graphs, which is less concrete and effective than DISTALGO programs. Code generation from classical B models are supported by the Atelier B (http://www.atelierb.eu) tools but those transformations do not consider distributed programming model. Atelier B supports code generation into Ada, C, C++. Moreover, it is defined over Classical B software models restricted to the B0 language which is a computable subset of the B language but without communications features. An EventB2Java [4] tool for RODIN has been developed for translating any EVENT-B specification into (sequential) JML or Java code. Finally, a Tasking EVENT-B [6] for RODIN extends the EVENT-B language to provide features for specifying concurrent multi-tasking systems. A model is decomposed into several tasking machines which schedule and perform tasks involving shared machines which correspond to protected resources accessed by tasking machines. The plugin provides a tool support for translating a tasking specification into ADA code. The generated programs are not distributed ones and consider only a subclass of the ADA language. Our work focuses on generating DISTALGOprograms from local EVENT-B models and provides a way to preserve powerfull safety properties from the local models.

Overview of the paper In the next section, we briefly present the two languages EVENT-B and DISTALGO. We introduce also the modelling technique of G. Tel [12] for expressing distributed algorithms at the abstract level where a distributed algorithm is a set of local algorithms and each local algorithm

is able to do either an internal action, or sending a message, or receiving a message. Section 3 shows how distributed programs can be modelled in the sub-language called LB for Local EVENT-B. Finally, in Section 4 we define the transformation of LB models into DISTALGO programs. Our paper then concludes with the results and future work. A more detailed description of the translation is given in Appendix A. The complete definition of the machine CM and of context CM-CONTEXT used for the example translated in the paper is given in Appendix B; the complete development of the model is given in Appendix D.The complete translation of the final context and machine into DISTALGO components and programs is given in Appendix C.

2 Modelling Distributed Programs

We consider here the specification of distributed programs based on a model of computation due to G. Tel [12]. We describe briefly in this section this model as well the EVENT-B modelling language and the DISTALGO programming language. We will show later on how the corresponding specifications are implemented following the methodology described in Figure 1.

2.1 General Definitions for Distributed Programs

Distributed algorithms and programs can be expressed in many programming languages (CSP, ADA, Java, LINDA, ...) and in many modelling languages (I/O automata, CCS, TLA$^+$, UNITY,...). In our approach, we intend to relate one modelling language EVENT-B and one programming language DISTALGO through the model of distributed computation due to G. Tel [12] used often for describing basic and advanced distributed algorithms.

Definition 1. *(local and distributed algorithms [12]) Given a set $\mathscr{LC}$ of configurations, a set $\mathscr{LI} \subseteq \mathscr{LC}$ of initial configurations, and a set $\mathscr{M}$ of messages, a local algorithm $\mathscr{LA}$ is a structure $(\mathscr{LC}, \mathscr{LI}, \longrightarrow_i, \longrightarrow_s, \longrightarrow_r, \mathscr{M})$ with:*

- $\longrightarrow_i \subseteq \mathscr{LC} \times \mathscr{LC}$ *modelling internal computation steps,*
- $\longrightarrow_s \subseteq \mathscr{LC} \times \mathscr{M} \times \mathscr{LC}$ *modelling sending steps,*
- $\longrightarrow_r \subseteq \mathscr{LC} \times \mathscr{M} \times \mathscr{LC}$ *modelling receiving steps.*

A distributed algorithm for a collection of processes is a collection $\{\mathscr{LA}_1, \ldots, \mathscr{LA}_n\}$ of local algorithms, one algorithm $\mathscr{LA}_k = (\mathscr{LC}_k, \mathscr{LI}_k, \longrightarrow_i^k, \longrightarrow_s^k, \longrightarrow_r^k, \mathscr{M})$ for each process P_k, with a transition relation $\longrightarrow$ defined over the set $\mathscr{C} = \mathscr{LC}_1 \times \ldots \times \mathscr{LC}_n \times (\mathscr{M} \to \mathbb{N})$ of configurations. Given two configurations $C = (C_1, \ldots, C_n, M)$ and $C' = (C'_1, \ldots, C'_n, M')$, we have $C \longrightarrow C'$ iff
$\exists k \in \{1, \ldots, n\} : (\forall j \in 1..n : j \neq k : C_j = C'_j)$ *and*

- *(internal transition)* $C_k \longrightarrow_i^k C'_k \wedge M' = M$
- *(send transition)* $\exists m \in \mathscr{M} : \left\{ \begin{array}{l} \forall o \in \mathscr{M} \setminus \{m\} : M'(o) = M(o) \\ \wedge\, M'(m) = M(m) + 1 \wedge\ (C_k, m, C'_k) \in \longrightarrow_s^k \end{array} \right.$
- *(receive transition)* $\exists m \in \mathscr{M} : M(m) \neq 0 : \left\{ \begin{array}{l} \forall o \in \mathscr{M} \setminus \{m\} : M'(o) = M(o) \\ \wedge\, M(m) = M'(m) + 1 \wedge\ (C_k, m, C'_k) \in \longrightarrow_r^k \end{array} \right.$

Following this approach for specifying distributed algorithms we have thus to define a collection of processes $P_1, \ldots, P_n$ with a local algorithm attached to each process. We first briefly introduce EVENT-B and DISTALGO and then define the local algorithms using these formalisms.

2.2 The Modelling Framework: EVENT-B

This section describes the modelling components of the EVENT-B language [1]. The EVENT-B language [1] contains two main components, the *context* which describes the static properties of a system using *carrier sets* s, *constants* c, *axioms* $A(s,c)$ and *theorems* $T_c(s,c)$, and the *machine* which describes behavioural properties of a system using *variables* v, *invariants* $I(s,c,v)$, *theorems* $T_m(s,c,v)$, *variants* $V(s,c,v)$ and *events* evt. A context can be extended by another context, a machine can be refined by another machine and a machine can use the *sees* relation to include other contexts.

An EVENT-B machine defines a set of *state variables* Var, taking their values in a set Val, and possibly modified by a set of *events* $Events$. A set of invariants $I_i(s,c,v)$ contains typing information and required safety properties that must be satisfied by the defined system. Each event $evt =$ ANY x WHERE $G_{evt}(s,c,v,x)$ THEN $v : |P_{evt}(s,c,v,x,v')$ END is composed of parameter(s) x, guard(s) $G_{evt}(s,c,v,x)$ and action(s) $v : |P_{evt}(s,c,v,x,v')$. Unprimed variables refer to the state variables before the event occurs and primed variables refer to the state variables after observation of the event. The *before-after* predicate $BA(evt)(s,c,v,v')$ for evt is defined by $(\exists\ x \cdot G_{evt}(s,c,v,x) \wedge P_{evt}(s,c,v,x,v'))$. A state st of a machine is an element of the set $St_{EB} = Var \to Val$. The value of a variable $u \in Var$ in the state st is $st(u)$ and is denoted $st[\![u]\!]$. The notation $[\![.]\!]$ is extended to the list of variables $v = (v_1,\ldots,v_n)$ by stating $st[\![(v_1,\ldots,v_n)]\!] = (st(v_1),\ldots,st(v_n))$. Finally, $[\![.]\!]$ is extended to handle (arithmetical, boolean) expressions by inductive definition: $st[\![exp(v)]\!] = exp(st[\![v]\!]/v)$. Since events are defined by expressions with free occurrence of unprimed and primed variables for v as v and v', we have to extend $[\![.]\!]$ as follows. For two states st_1, st_2 and an expression $exp(v,v')$ on primed variables v' and unprimed variables v, $st_1[\![exp(v,v')]\!]st_2$ is defined by $exp(st_1[\![v]\!]/v, st_2[\![v]\!]/v')$ the value of expression exp where unprimed variables are evaluated in state st_1 and primed variables are evaluated in state st_2. When an event evt is observed between two states st_1 and st_2, then $st_1[\![BA(evt)(s,c,v,v')]\!]st_2$ holds and we write $st_1 \xrightarrow{evt} st_2$. We assume that only one event can be observed at any transition and a transition between two states is written as $st_1 \to st_2$ which is equivalent to $\exists\ evt \in Event \cdot\ st_1 \xrightarrow{evt} st_2$. In this paper, we write deterministic *actions* of the form $v := E(s,c,v,x)$ that are equivalent to $v : |v' = E(s,c,v,x)$. Using the transition relation over set of states, we can define state properties as safety or invariance and traces properties.

The EVENT-B modelling language supports the *correct-by-construction* approach to design an abstract model and a series of refined models for developing any large and complex system. Refinements, introduced by the REFINES clause, transform an abstract model into a more concrete version by modifying the state description. A refinement allows modelling a system gradually by introducing safety properties at various refinement levels. New variables and new events may be introduced in a new refinement level. These refinements preserve the relation between the refining model and its corresponding refined concrete model, while introducing new events and variables to specify more concrete behavior of a system. The defined abstract and concrete state variables are linked by introducing the *gluing invariants*. The generated proof obligations ensure that each abstract event is correctly refined by its concrete version. RODIN [2] is an integrated development environment for the EVENT-B modelling language based on Eclipse. It includes project management, stepwise model development, proof assistance, model checking, animation and automatic code generation. Once an EVENT-B model is modelled and syntactically checked on the RODIN platform then a set of proof obligations (POs) is generated using the RODIN proof engine. EVENT-B supports different kinds of proof obligations, such as invariant preservation, non-deterministic action feasibility, guard strengthening in refinements, simulation, variant, well-definedness etc. More details related to the modelling language and proof obligations can be found in [1].

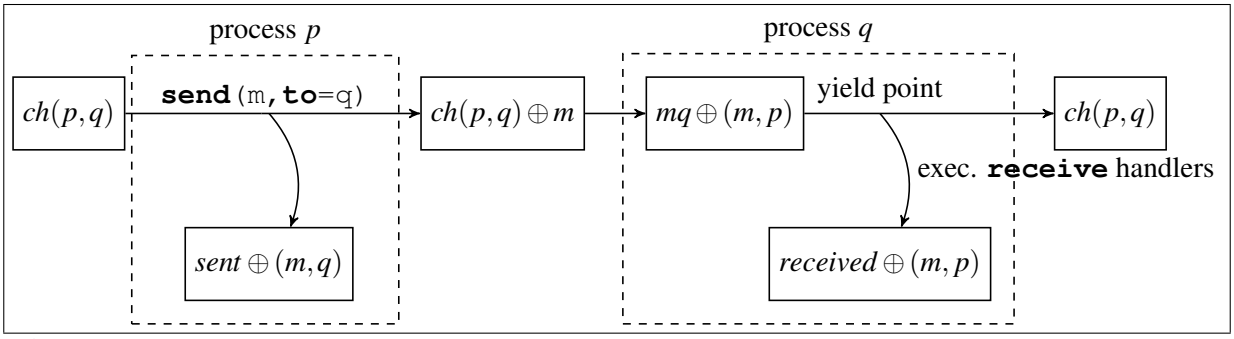


Figure 2: Communications in DISTALGO: the communication channels *ch*, as well as the message queues *mq* cannot be accessed explicitly in DISTALGO; only the sent and received messages can be accessed using the **sent** and **received** primitives.

2.3 The DISTALGO Distributed Programming Language

DISTALGO [7] is a programming language used to develop distributed algorithms by providing high level programming mechanisms such as communication primitives for the exchange of messages between a set of processes.

A DISTALGO program is composed of several process classes managed by a `main` module (see Example 4.1). A process class is made of a **setup** method which initializes the class attributes, a **run** method for carrying out the main execution flow, several **receive** methods for handling the reception of messages and other user defined methods that may be called by the **run** method. For each process class `PC`, the `main` module uses a statement of the form `pset=new(PC,num=n)` to build the set `pset` of `n` processes running the algorithm specified for `PC`. The **setup** method is called for the processes in each class and the **start** directive is eventually used to trigger the **run** method of all processes.

A process can send a `message` to another process `q` with a statement **send**`(message,to=q)`. When a message arrives at the receiving process, it is put in a message queue waiting to be received by the process. To receive messages, the process control flow must be at a yield point and this enables the receiving of every message in the message queue. When a message is received, the **receive** message handlers matching the message are executed. A yield point is a labeled statement `--l` **if await** `b1:s1` **elif** `b2:s2` **elif** ... **elif** `bn:sn` waiting for one of the conditions `bi` to hold in order to execute the corresponding branch `si`. The history of sent and received messages can be accessed in DISTALGO using the **sent** and **received** primitives. The idea is that conditions on the history of sent and received messages can be used in the different methods of a local algorithm to determine the value of any variable. A graphical representation of the message exchanges is given in Figure 2. Since DISTALGO is implemented as a PYTHON module all the data structures and primitives of the latter can be used. In our translation we use, in particular, **list**s, sometimes built using the function **range** which creates a list interval of integers, and **set**s, which can be built from a list or using the function **setof**$(expr(x_1,\ldots,x_n),\ x_1$ **in** $S_1,\ldots,x_n$ **in** $S_n,\ pred(x_1,\ldots,x_n))$ which is a set comprehension with *expr*essions built out of elements in the sets $S_1,\ldots,S_n$ and satisfying a *pred*icate. PYTHON dictionaries are also used; these can be updated with the elements of another dictionary using the method **update** and cloned with the function **deepcopy** which copies an object and the objects it contains recursively. The DISTALGO boolean functions **each** and **some** acting as a universal quantifier and an existential quantifier respectively, are also used.

We denote by D^* the set of finite sequences with elements in D. A state of a DISTALGO program is an

element of the set $St_{DA} = (Process \to Statement) \times (Process \to LocalState) \times (Process \to MsgQueue) \times ChannelStates$. $Process$ is the set of processes and $Process \to Statement$ is a function which associates to each process the next statement to execute. The local state of a process is an element of $Var \nrightarrow Val$ associating Values to the Variables. $MsgQueue = (Val \times Process)^*$ is the set of message queues and $ChannelStates = Process \times Process \nrightarrow Val^*$ is the set of possible states of the channels between each pair of processes.

The operational semantics of DISTALGO is defined as a transition relation $\to$ between program states. Given a function f, we write $f[x \to y]$ to specify that $f(x) = y$ and we denote by $f[x := y]$ the function f where y is mapped to x. We present the transitions significant for this paper; a complete definition can be found in [7]. Given a process p, the assignment of a value val to a variable v results in a change of the local state of p:

$$(P[p \to v := val; s], ls[p \to ls_p], mq, ch) \to (P[p := s], ls[p := ls_p[v := val]], mq, ch)$$

When sending a message to a process q, we memorise it as sent and add it to the corresponding channel:

$$(P[p \to send(m, to = q); s], ls[p \to ls_p], mq, ch[(p,q) \to ch_{p,q}])$$
$$\to (P[p := s], ls[p := ls_p[sent := ls_p(sent) @ \langle (m,q) \rangle]], mq, ch[(p,q) := ch_{p,q} @ \langle m \rangle], mq)$$

The arrival of a message to a process q consists in adding it to the local message queue:

$$(P, ls, mq[q \to mq_q], ch[(p,q) \to m.mt]) \to (P, ls, mq[q := mq_q @ \langle (m,p) \rangle], ch[(p,q) := mt])$$

For the reception of a message at a label l with a statement s' corresponding to the receive handler bodies we have:

$$(P[p \to l\ if\ await(b_1) : s_1\ elif\ \ldots\ elif\ b_n : s_n; s], ls[p \to ls_p], mq[p \to m.mt], ch)$$
$$\to (P[p := s'; l\ if\ await(b_1) : s_1\ elif\ \ldots\ elif\ b_n : s_n; s], ls[p := ls_p[received := ls_p(received) @ \langle m \rangle]],$$
$$mq[p := mt], ch)$$

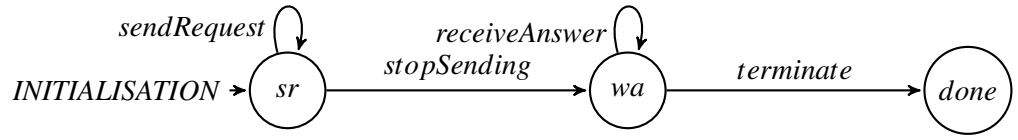
When all messages are received, *i.e.* the queue is empty, and a condition b_i of the await statement is satisfied we have:

$$(P[p \to l\ if\ await(b_1) : s_1\ elif\ \ldots\ elif\ b_n : s_n; s], ls, mq[p \to \langle\rangle], ch) \to (P[p := s_i; s], ls, mq, ch)$$

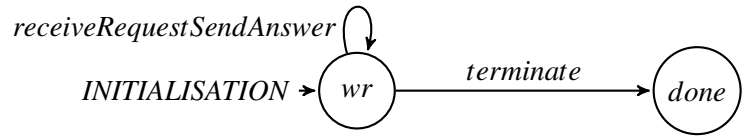
3 Modelling Distributed Algorithms in EVENT-B

We use the modelling technique of G. Tel [12] and express a distributed algorithm as a set of local algorithms, each local algorithm being able to do an internal action, or to send a message, or to receive a message. The final context CONTEXT-CM and machine CM in Figure 1 model such a distributed algorithm using a subset of the modelling language EVENT-B, denoted LB (Local EVENT-B). We use the simple distributed algorithm introduced in Example 3.1 to explain the methodology for modelling algorithms following Tel's technique and the restrictions imposed on LB (to facilitate the translation towards DISTALGO).

Example 3.1. *We consider a distributed algorithm where each process q in a set of processes Q sends its stored value to a central process p who previously made the corresponding requests. The communication channels between the requester and the other processes are reliable, i.e. messages are neither lost nor modified, but the order in which messages are sent in a channel may change. The local algorithm of the requester process p has three states:*



While in state sr, p sends a request to each of the processes in Q and moves to state wa, when all requests have been sent. In the state wa, it awaits for answers from the processes in Q.



When all answers are received, process p has terminated its local algorithm and moves to state done*. Each process in Q is initially in a state wr in which it waits for a request from p and moves to state* done *after receiving the request and sending its stored value.*

The general architecture of the distributed algorithm (processes, topology, channels, communications) is specified in the EVENT-B context CONTEXT-CM while the list of events of the machine CM induces the specifications of the local algorithms as labelled transition systems. In the sequel, the pair CM and CONTEXT-CM defining the LB distributed model is called simply CM.

3.1 Defining the General Architecture of the Distributed Program

Sets, constants and corresponding axioms defined in the context of a distributed model are of two categories: the general ones present in the context of any algorithm and those which are specific to the modeled algorithms. The most important elements of the context corresponding to the algorithm described in Example 3.1 is given in Figure 3:

For every distributed algorithm, the set Nodes of processes is defined axiomatically as a partition into process classes, the processes of each class featuring a similar local algorithm:

$$\texttt{Nodes} : \mathit{partition}(\mathsf{Nodes}, \mathit{PCl}_1, \ldots, \mathit{PCl}_n)$$

For each process class PCl_i one can enumerate explicitly its processes using an axiom

$$\texttt{PCl}_i : \mathit{partition}(\mathit{PCl}_i, \{\mathit{proc}_1\}, \ldots, \{\mathit{proc}_m\})$$

These partitions depend of course on the specific algorithm modeled and, in general, the processes are not explicitly enumerated. For our example, we have the class P of requester processes consisting of only one process p, and the class Q of processes with stored values. The number and identities of these latter processes is not specified, keeping thus the model the most general possible at this stage.

The topology, denoted network, is specified by a function associating to each process its neighbours: $\mathsf{network} \in \mathsf{Nodes} \to \mathbb{P}(\mathsf{Nodes})$. The concrete definition of the topology specific to the distributed algorithm under consideration is specified using an axiom whose general form should be

$$\texttt{network\_value} : \mathsf{network} = \{\mathit{proc} \cdot \mathit{proc} \in \mathit{PCl}_1 | \mathit{proc} \mapsto \mathit{expr}_1\} \cup \cdots \cup \{\mathit{proc} \cdot \mathit{proc} \in \mathit{PCl}_n | \mathit{proc} \mapsto \mathit{expr}_n\}$$

In the example, the topology is defined as a star with the process p in the center.

As we will see later on, the *control states* in States are used for structuring the observation of events in the local algorithms. The set of all possible control states of all processes is defined as a partition by an axiom `States`. The particular state done denotes the final state of any local algorithm. The explicit definition of the control states is used here to guide the translation of the local algorithms by grouping events that are enabled in the same state. Explicit control states also enable the generation of state machines for visualizing the distributed algorithm.

CONTEXT CONTEXT-CM
EXTENDS C00
SETS
Nodes States Messages // General sets
$MessagePrefixes$ // Algorithm specific sets
CONSTANTS
network // The topology (general)
Channels emptyChannel sent received inChannel // Communication channels (general)
send receive lose // Communication primitives (general)
P p Q // Process classes and processes (specific to the algorithm)
$request$ $answer$ // Algorithm specific constants
$availableResources$ // Algorithm specific constant
sr wa wr done // Process states (specific to the algorithm except for done, general)
AXIOMS
Nodes: $partition(\text{Nodes}, P, Q)$ // Partition of the set of processes
P: $partition(P, \{p\})$ // Partition of the classes of processes
network_typing: $\text{network} \in \text{Nodes} \rightarrow \mathbb{P}(\text{Nodes})$ // Network specification
network_value: $\text{network} = \{proc \cdot proc \in P | proc \mapsto Q\} \cup \{proc \cdot proc \in Q | proc \mapsto \{p\}\}$
// States of the processes
States: $partition(\text{States}, \{sr\}, \{wa\}, \{wr\}, \{done\})$
// Communication channels
Channels: $\text{Channels} = \text{Nodes} \times \text{Nodes} \rightarrow (\text{Messages} \rightarrow \mathbb{N} \times \mathbb{N} \times \mathbb{N})$
// Algorithm specific constants (types of exchanged messages, process resources)
MessagePrefixes: $partition(MessagePrefixes, \{request\}, \{answer\})$ //@P@Q
availableResources_typing: $availableResources \in Q \rightarrow \mathbb{N}$
// Communication axioms (general to all algorithms)
END

Figure 3: Sets and constants for the Example 3.1

The context should also define a constant Channels modelling the set of all possible values of communication channels between processes and the set Messages of messages exchanged through these channels. The current state of a channel between two processes is defined as a multiset, corresponding to the messages that were sent, received and in transition, *i.e.* sent but not yet received or lost. For instance, sent(channel,p,q,mes) is returning how many times the message mes has been sent by p to q. Hence, for each channel we can retrieve the exchanged messages using the functions sent, received and inChannel of type $\text{Channels} \times (\text{Nodes} \times \text{Nodes}) \times \text{Messages} \rightarrow \mathbb{N}$. The functions send, receive and lose of type $\text{Channels} \times (\text{Nodes} \times \text{Nodes}) \times \text{Messages} \rightarrow \text{Channels}$ describe the transformation of a channel between two processes (*i.e.* adding or removing a message) when one operation (send, receive or lose) is observed. More precisely, we consider that the channels do not preserve the order in which messages are sent, and sending a message consists in incrementing the inChannel part and the sent part of a channel between two processes. Checking if a message is ready to be received by a process from another for a value of the channels consists in checking that the message is in the inChannel part of the channel between the two processes. The axioms specifying the behaviour and the characteristics of the communication channels (*e.g.* order preserving) as well as the corresponding primitives are general, *i.e.* do not depend on the modeled distributed algorithm. The evolution of the channel between two processes p and q concerning a message m is modeled in LB by the variable $channels(p \mapsto q)(m)$, as depicted in Figure 4. This variable models the channel ch and the message queues mq as well as the **`sent`** and **`received`**

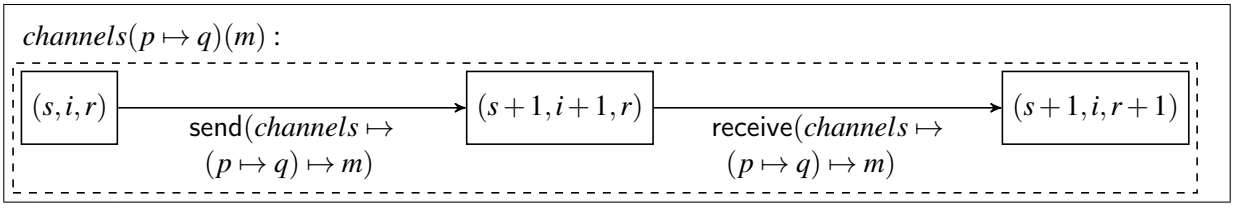


Figure 4: We suppose that m has been already sent, resp. received, s, resp r times, and that i copies are in the channel: $channels(p \mapsto q)(m) = (s,i,r)$. When we *send* the message m we increment the sent counter and the number of messages in the channel; when we *receive* it we increment the received counter and decrement the number of messages in the channel.

DISTALGO primitives in Figure 2; the transfer of the message from the channel to the message queue which is builtin in DISTALGO is not explicitly modeled in LB.

Sets and constants mentioned above should be present in the context of any distributed algorithm modeled in LB. Other enumerated sets defined necessarily as the disjoint union of singletons using the *partition* construct as well as constants specific to the modeled algorithm can be defined in the context. The type of a constant *cst* is defined by an axiom of name `cst_typing` while its value may be defined by an axiom of name `cst_value`. For instance, in our example we require that each process of Q has a non-negative integer *availableResources*. For the purpose of our example, we also define an enumerated set $MessagePrefixes$ consisting of *request* and *answer* which correspond to the two kinds of messages exchanged between the processes. For simplicity we consider here that any of these types is a sub-type of Messages and hide the injections we use in the real model.

Annotations of the form $@PCl_1 \dots @PCl_n$ are used to specify that the annotated elements are *local* to the processes in the corresponding class. This is done either in the axiom `cst_typing` to indicate the process classes concerned by the constant *cst*, or in the axiom `S` specifying the *partition* of an enumerated set S to indicate the process classes concerned by the elements of the set; the latter applies for the axiom `MessagePrefixes` in our example.

Definition 2 (Local constants)**.** *Given a process $proc \in PCl$ and a constant cst, we say that cst is* local *to proc when it is a function whose evaluation depends on proc (i.e. of type $PCl \to cstType$ or $Nodes \to cstType$) or when it is (an element of an enumerated set whose partition is) annotated by $@PCl$. By abuse of language we might sometimes say that cst is local to PCl. We denote $LC(PCl)$ the set of local constants for (the processes of) PCl.*

In our example, the elements of $MessagePrefixes$ are local to both p and $q \in Q$, $\mathsf{network}(r)$ is local to any $r \in P \cup Q$ and $availableResources(q)$ is local to any $q \in Q$.

3.2 Producing Local Algorithms as State Machines

We specify now the algorithms for the set of processes. Recall that all processes in a process class run the same algorithm, the one associated to the class.

The machine CM in Figure 1 declares the types and initializes the local variables of each process class of the distributed algorithm; we use the same naming conventions for the corresponding axioms as for the constants in the context. The variable *pc* identifying the current state of each local algorithm and the communication variable *channels* of type Channels are defined for any algorithm, the definition of other variables depends on the modeled algorithm. The variables together with their initialization and the corresponding invariants in the machine CM modelling the algorithm described in Example 3.1 is given in Figure 5.

MACHINE CM
SEES CONTEXT-CM
VARIABLES
channels pc result requestFrom
INVARIANTS
channels_typing: $channels \in \mathsf{Channels}$
pc_typing: $pc \in \mathsf{Nodes} \rightarrow STATES$
result_typing: $result \in P \rightarrow (\mathsf{Nodes} \nrightarrow \mathbb{N})$
requestFrom_typing: $requestFrom \in Q \rightarrow \mathsf{Nodes}$
channels_respect_network: $\forall x,y,m \cdot (x \in \mathsf{Nodes} \wedge y \in \mathsf{Nodes} \wedge m \in \mathsf{Messages} \wedge \mathsf{sent}(channels \mapsto (x \mapsto y) \mapsto m) > 0 \Rightarrow y \in \mathsf{network}(x))$
requestFrom_correctness: $\forall q \cdot (q \in Q \wedge pc(q) = \mathsf{done} \Rightarrow requestFrom(q) = \{p\})$
partial_correctness: $pc(p) = done \Rightarrow result(p) = availableResources$
EVENTS
Initialisation $\widehat{=}$
begin
act1: $channels := \mathsf{emptyChannel}$
act2: $pc := \{proc \cdot proc \in P | proc \mapsto sr\} \cup \{q \cdot q \in Q | q \mapsto wr\}$
act3: $result := \{proc \cdot proc \in P | proc \mapsto \varnothing\}$
act4: $requestFrom := \{q \cdot q \in Q | q \mapsto \varnothing\}$
end
END

Figure 5: Variables, invariants and initialisation for the Example 3.1

Definition 3 (Local variables)**.** *Given a process $proc \in PCl$ and a variable var, we say that var is* local *to proc when it is a function whose evaluation depends on proc (i.e. of type $PCl \rightarrow varType$ or $\mathsf{Nodes} \rightarrow varType$). By abuse of language we might sometimes say that var is local to PCl. We denote $LV(PCl)$ the set of local variables for (the processes of) PCl and $LV(proc) = LV(PCl)$ the set of local variables for a process $proc \in PCl$.*

Every variable *var* (except *channels*) is local to one (or all) class(es) of processes as specified by a typing invariant $var \in PCl \rightarrow varType$ (or $var \in \mathsf{Nodes} \rightarrow varType$). Every variable is initialised as usual by a deterministic assignment which specifies the value of the variable for the processes of each concerned class using statements of the form $\{proc \cdot proc \in PCl | proc \mapsto expr\}$ with the expression *expr* using *only local constants and variables of the process proc*. One can easily check that the initialisation expressions used in our example satisfy all the locality constraints. For example, the algorithm specific variable *result* concerns only the process $p \in P$ with the expression $result(p)$ corresponding to the values received from the processes of Q.

Note that a variable can be local to a process class or to all process classes; in the former category we have, in our example, the variable *result* local to (processes of) P and the variable *requestFrom* local to (processes of) Q while in the latter we have the variable *pc* which is local both to (processes of) P and (processes of) Q. The machine CM should contain a variable modelling communications, $channels \in \mathsf{Channels}$, which traces the state of communication channels.

Note that the invariant `partial_correctness` expresses that, if process p terminates, then the result of the algorithm is correct. This invariant was verified in our EVENT-B model.

With respect to Tel's model (Section 2.1) a local configuration is an element of the set $LS = Var \nrightarrow Val$ and if we denote by ls_{proc} the local configuration of (the algorithm of) the process *proc*, then the domain

of ls_{proc} is exactly $\mathsf{LV}(proc)$. Moreover, the set of configurations of (the distributed algorithm of) the LB model is then $\mathscr{C} = (\mathsf{Nodes} \to LS) \times \mathsf{Channels}$. Note also that a configuration defines the values of all variables of an LB specification and is therefore equivalent to an EVENT-B state as defined in Section 2.2.

Every local variable *var* is defined in the clause INVARIANTS of the machine. In fact, $var(p)$ is the effective local variable of p and it is sometimes written as var_p (see for instance, G. Tel [12]).

Events of the machine CM correspond to state transitions of the local algorithms of the processes. Process events are observed for a specific process of a process class.

Definition 4 (LB events, states)**.** *An* event *evt in LB is such that*

- *it features one parameter proc typed by a guard* $proc \in PCl$ *with* $PCl \in \mathsf{Nodes}$*;*
- *all actions are assignments* $x(proc) := pExpr$ *or* $channels := cExpr$ *with cExpr of the form*
  - $send(channels \mapsto (proc \mapsto pExpr) \mapsto mExpr)$
  - $receive(channels \mapsto (pExpr \mapsto proc) \mapsto mExpr)$

  If the event contains an action send*, resp.* receive*, then it is called a* send event*, resp* receive event*; it is called* internal *otherwise.*
- *it features a guard* $pc(proc) = st$ *which specifies the event is enabled in state* $st \in \mathsf{States}$*;*
- *it features a typing guard* $t \in tExpr$ *for each parameter;*
- *if it is an internal or a send event, it can feature general guards gExpr or guards of the form*
  - $\mathsf{sent}(channels \mapsto (proc \mapsto pExpr) \mapsto mExpr) = nExpr$
  - $\mathsf{received}(channels \mapsto (pExpr \mapsto proc) \mapsto mExpr) = nExpr$
- *if it is a receive event, it can feature matching guards for the parameters source and message which should be always present for such an event;*

with all expressions $tExpr, gExpr, pExpr, mExpr, nExpr$ *built over local constants, local variables, parameters of the event, literal integers and booleans.*

We say that the event is observed for a process proc and moreover, that is observable *in state st. We denote by* $\mathsf{Events}(PCl)$ *and* $\mathsf{Events}(proc)$ *the set of local events for the set of processes PCl and for the process proc respectively and by* $\mathsf{Events}(PCl, st)$ *and* $\mathsf{Events}(proc, st)$ *the events in* $\mathsf{Events}(PCl)$ *and* $\mathsf{Events}(proc)$ *respectively, that are observable in state st.*

Given a process class PCl, the set of states of processes *of PCl, denoted by* $\mathsf{StatesSet}(PCl)$*, consists of the states st such that there exists a parameter proc and a guard* $pc(proc) = st$ *for some event* $evt \in \mathsf{Events}(PCl)$.

The *send* and *receive* events are modifying the variable channel which is in fact a shared variable. Comparing to the classification proposed by Gerard Tel [12] we also add for convenience a *receive-and-send* event to allow more flexible models; one can split such an event into two separate *receive* and *send* events. The loss of a message can be modelled by an event modifying only the communication channels.

When considering a send event, one must verify that the destination of the message is a neighbour of the emitter. As we can see in the invariants of our machine CM an invariant property `channels_respect_network` expresses that every sent messages has been sent to a neighbour of the sender.

The events of the EVENT-B machine CM corresponding to the algorithm for the process p introduced in Example 3.1 are presented in Figure 6. Note that *sendRequest* is a *send* event and does not modify $pc(p)$, *stopSending* is an internal event with a guard verifying if p has sent a request to all its neighbours, *receiveAnswer* is a receive event for answers to the requests (the internal event *terminate* not presented here verifies that an answer has been received from every neighbour and terminates the local algorithm of

Event *sendRequest* $\widehat{=}$
  any *proc q*
  where
    grd1: $proc \in P$
    grd2: $q \in \mathsf{network}(proc)$
    grd3: $pc(proc) = sr$
    grd4: $\mathsf{sent}(channels \mapsto (proc \mapsto q) \mapsto request) = 0$
  then
    act1: $channels := \mathsf{send}(channels \mapsto (proc \mapsto q) \mapsto request)$
  end
Event *stopSending* $\widehat{=}$
  any *proc*
  where
    grd1: $proc \in P$
    grd2: $pc(proc) = sr$
    grd3: $\forall q \cdot (q \in \mathsf{network}(proc) \Rightarrow \mathsf{sent}(channels \mapsto (proc \mapsto q) \mapsto request) > 0)$
  then
    act1: $pc(proc) := wa$
  end
Event *receiveAnswer* $\widehat{=}$
  any *proc source message r*
  where
    grd1: $proc \in P$
    grd2: $source \in \mathsf{Nodes}$
    grd3: $message \in \mathsf{Messages}$
    grd4: $r \in \mathbb{Z}$
    grd5: $pc(proc) = wa$
    grd7: $message = answer \mapsto r$
  then
    act1: $result(proc) := result(proc) \lhd\!\!\!- \{source \mapsto r\}$
    act2: $channels := \mathsf{receive}(channels \mapsto (source \mapsto proc) \mapsto message)$
  end

Figure 6: Events for the Example 3.1

process p). The processes of Q feature similar events: we have a receive and a send event which model respectively the reception of requests from p and the dispatching of an answer with the stored value of the concerned process. We also have an internal event for terminating the local algorithm of a process of Q once it has sent the answer.

4 Translation in DistAlgo

A pair of a machine and a context compliant with the form described in the previous section is translated towards a DistAlgo program composed of a set of process classes and a main function which defines the processes and starts them. Some specific additional restrictions on the context and machines are necessary for the translation into DistAlgo; we mention them explicitly only if not implicit in the presentation. In particular, the types of variables and constants cannot involve sets of sets, sets of functions, functions on sets and functions on functions. Types cannot be relations in the current version. The main function and the process class definitions are generated from the (axioms in the) context while the process class methods are generated from the (invariants and events in the) machine. The generated

main function purpose is to simulate the EVENT-B model on a single machine; in order to instantiate the processes on different machines some external configuration might be needed.

4.1 Translation of Expressions

We first define a translation function, denoted $\mathscr{T}_{\overrightarrow{x}}()$, which transforms a well-formed EVENT-B expression (or predicate) e into the corresponding DISTALGO code $\mathscr{T}_{\overrightarrow{x}}(e)$ *w.r.t.* a set $\overrightarrow{x}$ of bound variables.

Arithmetic expressions are translated in an obvious way, the only worth mentioning case being that of intervals:

$$\mathscr{T}_{\overrightarrow{x}}(e_1 \mathinner{..} e_2) \triangleq \texttt{set(range(}\mathscr{T}_{\overrightarrow{x}}(e_1)\texttt{,}\ \mathscr{T}_{\overrightarrow{x}}(e_2)\texttt{+1))}$$

Set expressions are also translated in a straightforward way with the empty set encoded by the PYTHON expression `set()`, a set $\{e_1,\ldots,e_n\}$ encoded by $\{\mathscr{T}_{\overrightarrow{x}}(e_1)\texttt{, ..., }\mathscr{T}_{\overrightarrow{x}}(e_n)\}$ and the set operations encoded by corresponding PYTHON operations. In particular coercions are translated as follows:

$$\mathscr{T}_{\overrightarrow{y}}(\{x_1,\ldots,x_n \cdot x_1 \in s_1 \land \cdots \land\ x_n \in s_n \land\ pred | expr\}) \triangleq \texttt{setof(}\mathscr{T}_{\overrightarrow{y}\cup\overrightarrow{x}}(expr)\texttt{,}x_1\ \texttt{in}\ \mathscr{T}_{\overrightarrow{y}}(s_1)\texttt{,}\ldots\texttt{,}\ x_n\ \texttt{in}\ \mathscr{T}_{\overrightarrow{y}}(s_n)\texttt{,}\mathscr{T}_{\overrightarrow{y}\cup\overrightarrow{x}}(pred)\texttt{)}$$

with $\overrightarrow{x} = \{x_1,\ldots,x_n\}$ and $\mathscr{T}_{\overrightarrow{x}}(x_i) = x_i$.

Finite functions are translated using PYTHON dictionaries which map keys to values:

$$\mathscr{T}_{\overrightarrow{x}}(\{e_1 \mapsto v_1,\ldots,e_n \mapsto v_n\}) \triangleq \mathscr{T}_{\overrightarrow{x}}(e_1)\texttt{:}\mathscr{T}_{\overrightarrow{x}}(v_1)\texttt{,}\ldots\texttt{,}\mathscr{T}_{\overrightarrow{x}}(e_n)\texttt{:}\mathscr{T}_{\overrightarrow{x}}(v_n)$$

Besides the obvious translations for the classical operations on functions we have:

$$\begin{aligned}
\mathscr{T}_{\overrightarrow{y}}(\{x_1,\ldots,x_n \cdot x_1 \in s_1 \land\ \cdots \land\ x_n \in s_n \land\ pred | args \mapsto expr\}) &\triangleq \{\mathscr{T}_{\overrightarrow{y}}(args)\texttt{:}\mathscr{T}_{\overrightarrow{y}\cup\overrightarrow{x}}(expr)\ \texttt{for}\ x_1\ \texttt{in}\ \mathscr{T}_{\overrightarrow{y}}(s_1)\ \texttt{for}\ \ldots\ \texttt{for}\ x_n\ \texttt{in}\ \mathscr{T}_{\overrightarrow{y}}(s_n)\ \texttt{if}\ \mathscr{T}_{\overrightarrow{y}\cup\overrightarrow{x}}(pred)\}\\
\mathscr{T}_{\overrightarrow{y}}(\lambda x_1 \mapsto \cdots \mapsto x_n \cdot x_1 \in s_1 \land\ \cdots \land\ x_n \in s_n \land\ pred | expr) &\triangleq \{(x_1\texttt{,}\ldots\texttt{,}x_n)\texttt{:}\mathscr{T}_{\overrightarrow{y}\cup\overrightarrow{x}}(expr)\ \texttt{for}\ x_1\ \texttt{in}\ \mathscr{T}_{\overrightarrow{y}}(s_1)\ \texttt{for}\ \ldots\ \texttt{for}\ x_n\ \texttt{in}\ \mathscr{T}_{\overrightarrow{y}}(s_n)\ \texttt{if}\ \mathscr{T}_{\overrightarrow{y}\cup\overrightarrow{x}}(pred)\}\\
\mathscr{T}_{\overrightarrow{x}}(f_1 := f_2) &\triangleq \mathscr{T}_{\overrightarrow{x}}(f_1)\texttt{=deepcopy(}\mathscr{T}_{\overrightarrow{x}}(f_2)\texttt{)}\\
\mathscr{T}_{\overrightarrow{x}}(f_1 := f_1 \lhd f_2) &\triangleq \mathscr{T}_{\overrightarrow{x}}(f_1)\texttt{.update(deepcopy(}\mathscr{T}_{\overrightarrow{x}}(f_2)\texttt{))}\\
\mathscr{T}_{\overrightarrow{x}}(f(expr)) &\triangleq \mathscr{T}_{\overrightarrow{x}}(f)\texttt{[}\mathscr{T}_{\overrightarrow{x}}(expr)\texttt{]}
\end{aligned}$$

Predicates are translated into boolean expressions with a special care given to quantified variables:

$$\mathscr{T}_{\overrightarrow{y}}(\forall x_1,\ldots,x_n \cdot (x_1 \in s_1 \land\ \cdots \land\ x_n \in s_n \Rightarrow pred)) \triangleq \texttt{each(}x_1\ \texttt{in}\ \mathscr{T}_{\overrightarrow{y}}(s_1)\texttt{,}\ldots\texttt{,}x_n\ \texttt{in}\ \mathscr{T}_{\overrightarrow{y}}(s_n)\texttt{,}\ \texttt{has=}\mathscr{T}_{\overrightarrow{y}\cup\overrightarrow{x}}(pred)\texttt{)}$$

$$\mathscr{T}_{\overrightarrow{y}}(\exists x_1,\ldots,x_n \cdot (x_1 \in s_1 \land\ \cdots \land\ x_n \in s_n \land\ pred)) \triangleq \texttt{some(}x_1\ \texttt{in}\ \mathscr{T}_{\overrightarrow{y}}(s_1)\texttt{,}\ldots\texttt{,}x_n\ \texttt{in}\ \mathscr{T}_{\overrightarrow{y}}(s_n)\texttt{,}\ \texttt{has=}\mathscr{T}_{\overrightarrow{y}\cup\overrightarrow{x}}(pred)\texttt{)}$$

The action for the sending of a message is translated using the DISTALGO function **send**:

$$\mathscr{T}_{\overrightarrow{x}}(channels := \mathsf{send}(channels \mapsto (proc \mapsto dest) \mapsto msg)) \triangleq \texttt{send(}\mathscr{T}_{\overrightarrow{x}}(msg)\texttt{,}\ \texttt{to=}\mathscr{T}_{\overrightarrow{x}}(dest)\texttt{)}$$

Note that *channels* and p are not present in the resulting code since *channels* is implicit in DISTALGO and *proc* corresponds to the process executing the **send** statement.

The sent and received events defined in EVENT-B are translated as DISTALGO queries on message history. DISTALGO allows patterns inside queries on messages and any plain variable `x` in such a query is considered free and is potentially instantiated by a value following a successful matching. To indicate that a variable is bound in a query it should be of the form `_x`. We consider thus the translation function $\mathscr{T}^b_{\overrightarrow{x}}()$ which is defined exactly as the function $\mathscr{T}_{\overrightarrow{x}}()$ except for variables for which we have

$$\begin{aligned}
\mathscr{T}^b_{\overrightarrow{x}}(x) &\triangleq \texttt{_x} && \text{when } x \in \overrightarrow{x}\\
\mathscr{T}^b_{\overrightarrow{x}}(x) &\triangleq \mathscr{T}_{\overrightarrow{x}}(x) && \text{when } x \notin \overrightarrow{x}
\end{aligned}$$

The two expressions involving *sent* or *received* events supported by our approach are translated using the **sent** and **received** DISTALGO primitives:

$$\mathscr{T}_{\vec{x}}(sent(channels \mapsto (proc \mapsto dest) \mapsto msg) > 0) \triangleq \texttt{some(sent(}\mathscr{T}^b_{\vec{x}}(msg)\texttt{,to=}\mathscr{T}^b_{\vec{x}}(dest)\texttt{))}$$
$$\mathscr{T}_{\vec{x}}(received(channels \mapsto (source \mapsto proc) \mapsto msg) > 0) \triangleq \texttt{some(received(}\mathscr{T}^b_{\vec{x}}(msg)\texttt{, from\_=}\mathscr{T}^b_{\vec{x}}(source)\texttt{))}$$

An equality test ($= 0$) is translated by a negation of the form **not**(**some**(...)).

For example, the expression $\forall q \cdot (q \in \mathsf{network}(proc) \Rightarrow sent(channels \mapsto (proc \mapsto q) \mapsto request) > 0)$ from event *stopSending* defined in the previous section is translated into

```
each(q in 𝒯∅(network(proc)),
     has=some(sent(msg=(𝒯∅(request)),to=_q)))
```

with $\mathscr{T}_\varnothing(\mathsf{network}(proc))$ =`self`network and $\mathscr{T}_\varnothing(request)$ =`MessagePrefixes.request` as explained in the next sections.

4.2 Generation of the Main Function

The main function of the generated DISTALGO program defines different local constants as well as the different processes to execute, and starts the local algorithms of all the processes. This function is generated using exclusively the context CONTEXT-CM and more precisely, only the axioms of the context. The (identifiers of these) axioms should thus respect the rules given in Section 3.1 and the names of the variables and constants are inferred correspondingly.

The code of the main function contains a fixed part independent of the algorithm and specifying, for example, the behaviour of the communication channels. We omit here the fixed part and the various imports that might be needed and focus on the part generated from the EVENT-B model.

The axiom `Nodes` allows us to infer the set $\{PCl_1, \ldots, PCl_n\}$ of process classes and to generate, for each process class, a fresh variable $\texttt{PClSet}_i$ corresponding to the set of processes in PCl_i. We can thus initialize each variable $\texttt{PClSet}_i$ as a set of $\texttt{NPCl}_i$ processes of class $\texttt{PCl}_i$ (generated later on) and then, the variable `Nodes` corresponding to the set of all processes:

```
PClSet1 = new(PCl1, num=NPCl1)
...
PClSetn = new(PCln, num=NPCln)
Nodes = set.union(PClSet1,...,PClSetn)
```

We use the axioms $\texttt{PCl}_i$ to initialize the variables for each set and $\texttt{NPCl}_i$ to the cardinal of the corresponding set ($\texttt{NPCl}_i$ should be configured manually if the axiom is not present):

```
(proc1,...,procm) = list(PClSeti)
NPCli = |{proc1,...,procm}|
```

Starting from the axiom `network_value` we generate the map network for the topology

```
network = {proc:𝒯∅(expr1) for proc in PClSet1}
network.update({proc:𝒯∅(expr2) for proc in PClSet2})
...
network.update({proc:𝒯∅(exprn) for proc in PClSetn})
```

If this axiom is not present in the EVENT-B context, then it should be filled by hand in DISTALGO.

In fact, for each (local) constant *cst* in the context which is a function ($cst \in PCl \to cstType$) and features an axiom `cst_value`: $cst = \{proc \cdot proc \in PCl | proc \mapsto expr\}$ for some *PCl* we generate an initialization:

```
cst = {proc:T_∅(expr) for proc in PClSet}
```

For each process class PCl_i the following code is generated for the initialisation:

```
for proc in PClSet_i:
    setup({proc}, (cst_1[proc],...,cst_n[proc])
```

with $\{cst_1,\ldots,cst_n\} = \mathsf{LC}(PCl_i)$.

Finally, the processes are executed with the DISTALGO command `start(Nodes)`.

Example 4.1. *Given the context in Section 3.1 the following main function is generated.*

```
def main():
    NP = 1
    NQ = #NQ - to be configured

    PSet = new(P, num=NP)
    (p,) = list(PSet)
    QSet = new(Q, num=NQ)

    NODES = set.union(PSet, QSet)
    network = {proc:QSet for proc in PSet}
    network.update({q:{p} for q in QSet})
    availableResources = #availableResources - to be configured

    for proc in PSet:
        setup({proc}, (network[proc],))
    for proc in QSet:
        setup({proc}, (network[proc], availableResources[proc]))
    start(NODES)
```

In the same time with the main class we generate the code corresponding to the enumerated sets defined in the context using an axiom $\mathtt{S} : partition(S,\{el_1\},\{el_2\},\ldots)$ like, *e.g.*, $MessagePrefixes$. For all these sets we generate a separate file (imported when needed) containing the corresponding code:

```
class S(Enum):
    el_1 = "el_1"
    el_2 = "el_2"
    ...
```

The access to the elements of the respective set is done as expected: $\mathscr{T}_{\vec{x}}(el_i) \triangleq \mathtt{S.}el_i$, for any member el_i of the enumerated set.

4.3 Generation of the Process Classes

For each process class *PCl* we generate (in an individual file) a DISTALGO process class `PCl` featuring the necessary methods. More precisely, we generate the **setup** method, the **run** method, **receive** methods, and additional methods for the events concerned by the process class.

For the purpose of the translations in this section we consider the function $\mathscr{T}^l_{\vec{x}}()$ which behaves exactly like $\mathscr{T}_{\vec{x}}()$ except for one case: $\mathscr{T}^l_{\vec{x}}(f(proc)) \triangleq \mathtt{self.f}$ when $f \in \mathsf{LV}(PCl) \cup \mathsf{LC}(PCl), p \in PCl$.

The **setup** method gets the values of the local constants as parameters and initializes the local variables. We have thus for each process class *PCl* in the context a DISTALGO class:

```
class PCl( process ) :
    def setup(cst_1,...,cst_n) :
        self.var_1 = T^l_∅(expr_1)
        ⋮
        self.var_m = T^l_∅(expr_m)
```

with $\{cst_1,\ldots,cst_n\} = \mathsf{LC}(PCl)$, $\{var_1,\ldots,var_m\} = \mathsf{LV}(PCl)$, and $\{expr_1,\ldots,expr_m\}$ the corresponding expressions $var_i := \{proc \cdot proc \in PCl | proc \mapsto expr_i\}$ in the **Initialisation** section of the machine. For a variable *var* (resp. constant *cst*), the translation of $var(proc)$ (resp. $cst(proc)$) is then `self.var` (resp. `self.cst`).

For each state $st \in \mathsf{StatesSet}(PCl)$ a method `st` describing the behavior on reception of an event observable in state *st* is generated as explained below. The **run** method defining the control flow of the program for the respective process consists of a loop which calls at each iteration the method `st` corresponding to the current value of `self.pc` and terminates when `self.pc` reaches the termination state done. When $\mathsf{StatesSet}(PCl) = \{st_1,\ldots,st_n\}$ the following code is generated:

```
def run():
    stateFunctions = {"st1":st1,...,"stn":stn}
    while(self.pc!=done):
        stateFunctions[self.pc]()
```

Given an event $evt \in \mathsf{Events}(PCl)$ we denote by $\mathsf{Guards}(evt)$ the set of its guards, by $\mathsf{Actions}(evt)$ the set of its actions and by $\mathsf{Params}(evt)$ the set of its parameters. The translation $\mathscr{G}^i()$ of a set of guards of an *internal* or a *send* event is as follows:

$$\mathscr{G}^i(\{proc \in PCl, t_1 \in S_1,\ldots,t_l \in S_l,\ pc(proc) = st, g_1,\ldots,g_n\}) \triangleq \texttt{self.pc=="st" and some}(t_1 \texttt{in} \mathscr{T}^l_\emptyset(S_1),\ldots,t_l \texttt{in} \mathscr{T}^l_\emptyset(S_l),\ \texttt{has}=\mathscr{T}^l_{\mathsf{Params}(evt)}(g_1) \texttt{and} \ldots \texttt{and} \mathscr{T}^l_{\mathsf{Params}(evt)}(g_n))$$

where $\mathsf{Params}(evt) = \{t_1,\ldots,t_l\}$ and $S_1,\ldots,S_l$ are finite sets. The translation $\mathscr{A}_{\overrightarrow{x}}(\mathsf{Actions}(evt))$ of a set of actions of an *internal* or *send* event *evt* is defined as the juxtaposition of the translations $\mathscr{T}^l_{\overrightarrow{x}}(a_j)$ of each action in the set $\mathsf{Actions}(evt)$. Since the actions of $\mathsf{Actions}(evt)$ are observed concurrently but translated as a sequence of assignments, fresh temporary variables are defined as copies of the local variables prior to the event and are used to access the old values of the local variables. However, for simplicity, we omit these temporary fresh variables in this section and explicit them only in the appendix.

For each state $st \in \mathsf{StatesSet}(PCl)$ we use the set $\{evt_1,\ldots,evt_m\} \subseteq \mathsf{Events}(PCl, st)$ of all *internal* and *send* events observable in state *st* to generate the method `st`:

```
def st():
    --st
    if await (G^i(Guards(evt_1))):
        A_{Params(evt_1)}(Actions(evt_1))
    ⋮
    elif(G^i(Guards(evt_m))):
        A_{Params(evt_m)}(Actions(evt_m))
    elif(self.pc != "st"):
        pass
```

with the label `--st` and the keyword **await** added only if there is a *receive* event in $\mathsf{Events}(PCl, st)$; this statement is used to enable the reception of messages. When an **await** statement is reached every message that has arrived to destination but has not been processed yet, *i.e.* messages in the message

queue of this process, is handled (using the **receive** methods) before the **if** conditions are evaluated. Messages are received until the message queue is empty and one of the guard conditions is satisfied.

Example 4.2. *In our example, we have* $\mathsf{Events}(P, sr) = \{sendRequest, stopSending\}$ *and thus the following code is generated for the method* `sr`.

```
def sr():
    # event sendRequest
    if(self.pc == "sr" and
       some(q in self.network,
            has=not(some(sent((MessagePrefixes.request,), to=_q)))
              ):
       send((MessagePrefixes.request,), to=q)
    # event stopSending
    elif(self.pc == "sr" and
         each(q in self.network,
              has=some(sent((MessagePrefixes.request,), to=_q)))):
       self.pc = "wa"
    elif(self.pc != "sr"):
       pass
```

For each *receive* event *evt* in $\mathsf{Events}(PCl, st)$ we generate a **receive** method in the class `PCl`:

def receive$(\mathscr{G}^r(\mathsf{Guards}(evt)))$**:**
$\mathscr{A}_{\mathsf{Params}(evt)}(\mathsf{Actions}(evt))$

where the translation $\mathscr{G}^r(\mathsf{Guards}(evt))$ of a set of guards of a *receive* event *evt* is as follows:

$$\mathscr{G}^r(\{proc \in PCl, msg \in \mathsf{Messages}, source \in \mathsf{Nodes}, t_1 \in S_1, \ldots, t_l \in S_l, \\ pc(proc) = st, msg = msgExpr, source = procExpr\}) \triangleq$$

msg$= (\mathscr{T}_{\varnothing}(msgExpr))$**,**
from_$=\mathscr{T}_{\varnothing}(procExpr)$**,**
at$=$`(st,)`

If *procExpr* is empty, *i.e.* not specified in the model then a free variable it is used in the translation (to indicate the source of the message is not specified). We proceed similarly when *msgExpr* is empty. The parameters $\mathsf{Params}(evt)$ are used in the expressions *msgExpr* and *procExpr* to specify the expected message *msg* that is received from the emitter *source*. Note that the reception of the message is performed automatically by DISTALGO before the **receive** method is executed and therefore the reception action in LB does not need to be translated; only the message handler should be translated. The actions of a *receive* event are translated in the same way as the actions of an *internal* or *send* event.

The **receive** methods of DISTALGO (*i.e.* the message handlers) also have the particularity that if multiple **receive** methods can be executed for the reception of a message, they will all be executed. Therefore, the *receive* events of the model must have exclusive guards in order to have only one **receive** method executed at a time.

Example 4.3. *The following code corresponds to the* receive *event receiveAnswer.*

```
def receive(msg=(MessagePrefixes.answer, r), from_=source,
            at=(wa,)):
    self.result[source] = r
```

The translation has been implemented in Java as a RODIN plugin and the source code together with the installation instructions are available at `https://gitlab.inria.fr/agrall/eb2da`.

5 Concluding Remarks and Future Work

The localization of EVENT-B has been used when a distributed algorithm [3, 1] has been developed using the correct-by-construction paradigm and especially the refinement relationship among levels of abstractions. The translation of local EVENT-B models was a manual process and the current work provides a systematic way to produce a DISTALGO program from a local EVENT-B model.

We claim the LB modelling language is sufficiently powerful to model a large variety of distributed algorithms and abstract enough to be considered as the basis for the translation towards different target distributed programming. A couple of algorithms have been modelled and the programs obtained by translation allowed the simulation of the algorithms for different numbers of nodes. We continue to develop more and more elaborated case studies.

In the short term we plan of course to produce the proof of soundness of the translation. The communication model used for the algorithms implemented so far although reliable does not guarantee the order of messages; we intend to provide the model for other communications models together with the corresponding translation. At the implementation level, we should first provide an automatic packaging and facilitate the installation as a RODIN plugin. The definition of transformations for other target distributed programming languages is a more long term objective.

References

[1] J.-R. Abrial (2010): *Modeling in Event-B: System and Software Engineering*. Cambridge University Press.

[2] Jean-Raymond Abrial, Michael Butler, Stefan Hallerstede, Thai Son Hoang, Farhad Mehta & Laurent Voisin (2010): *Rodin: an open toolset for modelling and reasoning in Event-B*. *International Journal on Software Tools for Technology Transfer* 12(6), pp. 447–466, doi:10.1007/s10009-010-0145-y.

[3] Jean-Raymond Abrial, D. Cansell & D. Méry (2003): *A Mechanically Proved and Incremental Development of IEEE 1394 Tree Identify Protocol*. *Formal Aspects of Computing* 14(3), pp. 215–227, doi:10.1007/s001650300002.

[4] Néstor Cataño & Víctor Rivera (2016): *EventB2Java: A Code Generator for Event-B*. In Sanjai Rayadurgam & Oksana Tkachuk, editors: *NASA Formal Methods*, Springer International Publishing, Cham, pp. 166–171, doi:10.1007/978-3-319-40648-0_13.

[5] Zheng Cheng, Dominique Méry & Rosemary Monahan (2016): *On Two Friends for Getting Correct Programs - Automatically Translating Event B Specifications to Recursive Algorithms in Rodin*. In: *Leveraging Applications of Formal Methods, Verification and Validation: Foundational Techniques - 7th International Symposium, ISoLA 2016, Imperial, Corfu, Greece, October 10-14, 2016, Proceedings, Part I*, pp. 821–838, doi:10.1007/978-3-319-47166-2_57.

[6] Andrew Edmunds & Michael Butler (2011): *Tasking Event-B: An extension to Event-B for generating concurrent code*. In: *PLACES 2011*. Available at `http://eprints.soton.ac.uk/id/eprint/272006`.

[7] Yanhong A Liu, Scott D Stoller, Bo Lin & Michael Gorbovitski (2012): *From clarity to efficiency for distributed algorithms*. In: *ACM SIGPLAN Notices*, 47, ACM, pp. 395–410, doi:10.1145/2384616.2384645.

[8] Dominique Méry (2009): *Refinement-based guidelines for algorithmic systems*. *International Journal of Software and Informatics* 3(2-3), pp. 197–239.

[9] Dominique Méry (2018): *Modelling by Patterns for Correct-by-Construction Process*. In: *Leveraging Applications of Formal Methods, Verification and Validation. Modeling - 8th International Symposium, ISoLA 2018, Limassol, Cyprus, November 5-9, 2018, Proceedings, Part I*, pp. 399–423, doi:10.1007/978-3-030-03418-4_24.

[10] Dominique Méry (2019): *Verification by Construction of Distributed Algorithms*. In: *Theoretical Aspects of Computing - ICTAC 2019 - 16th International Colloquium, Hammamet, Tunisia, October 31 - November 4, 2019, Proceedings*, pp. 22–38, doi:10.1007/978-3-030-32505-3_2.

[11] Dominique Méry & Rosemary Monahan (2013): *Transforming Event B Models into Verified C# Implementations*. In Alexei Lisitsa & Andrei P. Nemytykh, editors: *First International Workshop on Verification and Program Transformation, VPT 2013, Saint Petersburg, Russia, July 12-13, 2013*, *EPiC Series in Computing* 16, EasyChair, pp. 57–73.

[12] Gerard Tel (2000): *Introduction to distributed algorithms*. Cambridge University Press.

[13] Mohamed Tounsi, Mohamed Mosbah & Dominique Méry (2016): *From Event-B specifications to programs for distributed algorithms*. *IJAACS* 9(3/4), pp. 223–242, doi:10.1504/IJAACS.2016.079623.

A Translation of expressions

The tables 1, 3, 2, 4, 5, 6 give the translation rules for the expressions that are supported by the tool.

EVENT-B	DISTALGO
$\mathcal{T}_{\vec{x}}(var := e)$	$\mathcal{T}_{\vec{x}}(var)$ = $\mathcal{T}_{\vec{x}}(e)$
$\mathcal{T}_{\vec{x}}(e_1 \mathinner{..} e_2)$	**set**(**range**($\mathcal{T}_{\vec{x}}(e_1)$,$\mathcal{T}_{\vec{x}}(e_2)$+1))
$\mathcal{T}_{\vec{x}}(e_1 + e_2)$	$\mathcal{T}_{\vec{x}}(e_1)$+$\mathcal{T}_{\vec{x}}(e_2)$
$\mathcal{T}_{\vec{x}}(e_1 - e_2)$	$\mathcal{T}_{\vec{x}}(e_1)$-$\mathcal{T}_{\vec{x}}(e_2)$
$\mathcal{T}_{\vec{x}}(e_1 * e_2)$	$\mathcal{T}_{\vec{x}}(e_1)$*$\mathcal{T}_{\vec{x}}(e_2)$
$\mathcal{T}_{\vec{x}}(e_1 \div e_2)$	**int**($\mathcal{T}_{\vec{x}}(e_1)$/$\mathcal{T}_{\vec{x}}(e_2)$)
$\mathcal{T}_{\vec{x}}(e_1 \; mod \; e_2)$	$\mathcal{T}_{\vec{x}}(e_1)$%$\mathcal{T}_{\vec{x}}(e_2)$
$\mathcal{T}_{\vec{x}}(e_1 \mathbin{\hat{}} e_2)$	$\mathcal{T}_{\vec{x}}(e_1)$**$\mathcal{T}_{\vec{x}}(e_2)$
$\mathcal{T}_{\vec{x}}(min(s))$	**min**($\mathcal{T}_{\vec{x}}(s)$)
$\mathcal{T}_{\vec{x}}(max(s))$	**max**($\mathcal{T}_{\vec{x}}(s)$)
$\mathcal{T}_{\vec{x}}(e_1 = e_2)$	$\mathcal{T}_{\vec{x}}(e_1)$ == $\mathcal{T}_{\vec{x}}(e_2)$
$\mathcal{T}_{\vec{x}}(e_1 < e_2)$	$\mathcal{T}_{\vec{x}}(e_1)$ < $\mathcal{T}_{\vec{x}}(e_2)$
$\mathcal{T}_{\vec{x}}(e_1 \leq e_2)$	$\mathcal{T}_{\vec{x}}(e_1)$ <= $\mathcal{T}_{\vec{x}}(e_2)$
$\mathcal{T}_{\vec{x}}(e_1 > e_2)$	$\mathcal{T}_{\vec{x}}(e_1)$ > $\mathcal{T}_{\vec{x}}(e_2)$
$\mathcal{T}_{\vec{x}}(e_1 \geq e_2)$	$\mathcal{T}_{\vec{x}}(e_1)$ >= $\mathcal{T}_{\vec{x}}(e_2)$
$\mathcal{T}_{\vec{x}}(e_1 \neq e_2)$	$\mathcal{T}_{\vec{x}}(e_1)$!= $\mathcal{T}_{\vec{x}}(e_2)$

Table 1: Arithmetic expressions

EVENT-B	DISTALGO
$\mathcal{T}_{\vec{x}}(\{e_1 \mapsto v_1, \ldots, e_n \mapsto v_n\})$	{$\mathcal{T}_{\vec{x}}(e_1)$:$\mathcal{T}_{\vec{x}}(v_1)$, ...,$\mathcal{T}_{\vec{x}}(e_n)$:$\mathcal{T}_{\vec{x}}(v_n)$})
$\mathcal{T}_{\vec{y}}(\{x_1, \ldots, x_n \cdot x_1 \in s_1 \wedge \cdots \wedge x_n \in s_n \wedge pred \mid args \mapsto expr\})$	{$\mathcal{T}_{\vec{x}\cup\vec{y}}(args)$:$\mathcal{T}_{\vec{x}\cup\vec{y}}(expr)$ **for** $\mathcal{T}_{\vec{x}}(x_1)$ **in** $\mathcal{T}_{\vec{x}\cup\vec{y}}(s_1)$ **for** ... **for** $\mathcal{T}_{\vec{x}}(x_n)$ **in** $\mathcal{T}_{\vec{x}\cup\vec{y}}(s_n)$ **if** $\mathcal{T}_{\vec{x}\cup\vec{y}}(pred)$}
$\mathcal{T}_{\vec{y}}(\lambda args \cdot x_1 \in s_1 \wedge \ldots x_n \in s_n \wedge pred \mid expr)$	{$\mathcal{T}_{\vec{x}\cup\vec{y}}(args)$:$\mathcal{T}_{\vec{x}\cup\vec{y}}(expr)$ **for** $\mathcal{T}_{\vec{x}}(x_1)$ **in** $\mathcal{T}_{\vec{x}\cup\vec{y}}(s_1)$ **for** ... **for** $\mathcal{T}_{\vec{x}}(x_n)$ **in** $\mathcal{T}_{\vec{x}\cup\vec{y}}(s_n)$ **if** $\mathcal{T}_{\vec{x}\cup\vec{y}}(pred)$}
$\mathcal{T}_{\vec{x}}(dom(f))$	**set**($\mathcal{T}_{\vec{x}}(f)$.keys())
$\mathcal{T}_{\vec{x}}(ran(f))$	**set**($\mathcal{T}_{\vec{x}}(f)$.values())
$\mathcal{T}_{\vec{x}}(f_1 = f_2)$	$\mathcal{T}_{\vec{x}}(f_1)$ == $\mathcal{T}_{\vec{x}}(f_2)$
$\mathcal{T}_{\vec{x}}(\varnothing)$	{}
$\mathcal{T}_{\vec{x}}(f(x))$	$\mathcal{T}_{\vec{x}}(f)$[$\mathcal{T}_{\vec{x}}(x)$]
$\mathcal{T}_{\vec{x}}(f_1 := f_2)$	$\mathcal{T}_{\vec{x}}(f_1)$ = deepcopy($\mathcal{T}_{\vec{x}}(f_2)$)
$\mathcal{T}_{\vec{x}}(f_1 := f_1 \lhd f_2)$	$\mathcal{T}_{\vec{x}}(f_1)$.update(deepcopy($\mathcal{T}_{\vec{x}}(f_2)$))

Table 2: Translations of expression with functions

EVENT-B	DISTALGO
$\mathcal{T}_{\vec{x}}(var := s)$	$\mathcal{T}_{\vec{x}}(var)$ = **set**($\mathcal{T}_{\vec{x}}(s)$)
$\mathcal{T}_{\vec{y}}(\{x_1,\ldots,x_n \cdot x_1 \in s_1 \wedge \cdots \wedge x_n \in s_n \wedge pred \mid expr\})$	setof($\mathcal{T}_{\vec{x}\cup\vec{y}}(expr)$, $\mathcal{T}_{\vec{x}}(x_1)$ **in** $\mathcal{T}_{\vec{x}\cup\vec{y}}(s_1)$, ..., $\mathcal{T}_{\vec{x}}(x_n)$ **in** $\mathcal{T}_{\vec{x}\cup\vec{y}}(s_n)$, $\mathcal{T}_{\vec{x}\cup\vec{y}}(pred)$)
$\mathcal{T}_{\vec{x}}(\{e_1,\ldots,e_n\})$	{$\mathcal{T}_{\vec{x}}(e_1)$, ..., $\mathcal{T}_{\vec{x}}(e_n)$}
$\mathcal{T}_{\vec{x}}(\varnothing)$	**set**()
$\mathcal{T}_{\vec{x}}(s_1 \cup s_2)$	$\mathcal{T}_{\vec{x}}(s_1)$ | $\mathcal{T}_{\vec{x}}(s_2)$
$\mathcal{T}_{\vec{x}}(s_1 \cap s_2)$	$\mathcal{T}_{\vec{x}}(s_1)$ & $\mathcal{T}_{\vec{x}}(s_2)$
$\mathcal{T}_{\vec{x}}(s_1 \setminus s_2)$	$\mathcal{T}_{\vec{x}}(s_1)$ - $\mathcal{T}_{\vec{x}}(s_2)$
$\mathcal{T}_{\vec{x}}(s_1 \subseteq s_2)$	$\mathcal{T}_{\vec{x}}(s_1)$ <= $\mathcal{T}_{\vec{x}}(s_2)$
$\mathcal{T}_{\vec{x}}(s_1 \not\subseteq s_2)$	**not** ($\mathcal{T}_{\vec{x}}(s_1)$ <= $\mathcal{T}_{\vec{x}}(s_2)$)
$\mathcal{T}_{\vec{x}}(s_1 \subset s_2)$	$\mathcal{T}_{\vec{x}}(s_1)$ < $\mathcal{T}_{\vec{x}}(s_2)$
$\mathcal{T}_{\vec{x}}(s_1 \not\subset s_2)$	**not** ($\mathcal{T}_{\vec{x}}(s_1)$ < $\mathcal{T}_{\vec{x}}(s_2)$)
$\mathcal{T}_{\vec{x}}(card(s))$	**len**($\mathcal{T}_{\vec{x}}(s)$)
$\mathcal{T}_{\vec{x}}(expr \in s)$	$\mathcal{T}_{\vec{x}}(expr)$ **in** $\mathcal{T}_{\vec{x}}(s)$
$\mathcal{T}_{\vec{x}}(expr \notin s)$	$\mathcal{T}_{\vec{x}}(expr)$ **not in** $\mathcal{T}_{\vec{x}}(s)$
$\mathcal{T}_{\vec{x}}(s_1 = s_2)$	$\mathcal{T}_{\vec{x}}(s_1)$ == $\mathcal{T}_{\vec{x}}(s_2)$
$\mathcal{T}_{\vec{x}}(s_1 \neq s_2)$	$\mathcal{T}_{\vec{x}}(s_1)$!= $\mathcal{T}_{\vec{x}}(s_2)$
$\mathcal{T}_{\vec{x}}(s_1 \times \cdots \times s_n)$	product($\mathcal{T}_{\vec{x}}(s_1),\ldots,\mathcal{T}_{\vec{x}}(s_n)$)

Table 3: Translation of expressions with sets

EVENT-B	DISTALGO
$\mathcal{T}_{\vec{y}}(\forall x_1,\ldots,x_n \cdot (x_1 \in s_1 \wedge \cdots \wedge x_n \in s_n \Rightarrow pred))$	each($\mathcal{T}_{\vec{x}}(x_1)$ **in** $\mathcal{T}_{\vec{x}\cup\vec{y}}(s_1)$, ..., $\mathcal{T}_{\vec{x}}(x_n)$ **in** $\mathcal{T}_{\vec{x}\cup\vec{y}}(s_n)$, has=$\mathcal{T}_{\vec{x}\cup\vec{y}}(pred)$)
$\mathcal{T}_{\vec{y}}(\exists x_1,\ldots,x_n \cdot (x_1 \in s_1 \wedge \cdots \wedge x_n \in s_n \wedge pred))$	some($\mathcal{T}_{\vec{x}}(x_1)$ **in** $\mathcal{T}_{\vec{x}\cup\vec{y}}(s_1)$, ..., $\mathcal{T}_{\vec{x}}(x_n)$ **in** $\mathcal{T}_{\vec{x}\cup\vec{y}}(s_n)$, has=$\mathcal{T}_{\vec{x}\cup\vec{y}}(pred)$)
$\mathcal{T}_{\vec{x}}(pred_1 \wedge pred_2)$	$\mathcal{T}_{\vec{x}}(pred_1)$ **and** $\mathcal{T}_{\vec{x}}(pred_2)$
$\mathcal{T}_{\vec{x}}(pred_1 \vee pred_2)$	$\mathcal{T}_{\vec{x}}(pred_1)$ **or** $\mathcal{T}_{\vec{x}}(pred_2)$
$\mathcal{T}_{\vec{x}}(\neg pred)$	**not**($\mathcal{T}_{\vec{x}}(pred)$)
$\mathcal{T}_{\vec{x}}(pred_1 \Rightarrow pred_2)$	**not**($\mathcal{T}_{\vec{x}}(pred_1)$) **or** $\mathcal{T}_{\vec{x}}(pred_2)$

Table 4: Translations of predicates

EVENT-B	DISTALGO
$partition(EnumSet, \{el_1\}, \{el_2\}, \ldots)$	**class** EnumSet(Enum): el_1 = "el_1" el_2 = "el_2" ...
$\mathcal{T}_{\vec{x}}(el_i)$	EnumSet.el_i

Table 5: Translation of enumerated sets and of an element of an enumerated set.

EVENT-B	DISTALGO
$\mathcal{T}_{\overrightarrow{x}}(sent(channels \mapsto (proc \mapsto dest) \mapsto msg) > 0)$	`some(sent(`$\mathcal{T}^b_{\overrightarrow{x}}(msg)$`, to=`$\mathcal{T}^b_{\overrightarrow{x}}(dest)$`))`
$\mathcal{T}_{\overrightarrow{x}}(sent(channels \mapsto (proc \mapsto dest) \mapsto msg) = 0)$	**not** `(some(sent(`$\mathcal{T}^b_{\overrightarrow{x}}(msg)$ `, to=`$\mathcal{T}^b_{\overrightarrow{x}}(dest)$`)))`
$\mathcal{T}_{\overrightarrow{x}}(received(channels \mapsto (source \mapsto proc) \mapsto msg) > 0)$	`some(received(`$\mathcal{T}^b_{\overrightarrow{x}}(msg)$ `, _from=`$\mathcal{T}^b_{\overrightarrow{x}}(source)$`))`
$\mathcal{T}_{\overrightarrow{x}}(received(channels \mapsto (source \mapsto proc) \mapsto msg) = 0)$	**not** `(some(received(`$\mathcal{T}^b_{\overrightarrow{x}}(msg)$`, _from=`$\mathcal{T}^b_{\overrightarrow{x}}(source)$`)))`
$\mathcal{T}_{\overrightarrow{x}}(msgT(m_1 \mapsto m_2 \mapsto \cdots \mapsto m_n))$	`("msgT",` $\mathcal{T}_{\overrightarrow{x}}(m_1)$`,` $\mathcal{T}_{\overrightarrow{x}}(m_2)$`, . . . ,` $\mathcal{T}_{\overrightarrow{x}}(m_n)$`)`

Table 6: Queries of message history

B CM and CONTEXT-CM for the example

We have used the example of a process p sending a request to a set Q of processes and we give the full text of the machine CM and the context CONTEXT-CM used for the translation. The complete development of the model is in section D. Some elements were not described in section 3.1 for simplification reasons.

The predicate readyForReception states if some message is ready to be received by a process on a channel between two processes. For a *non fifo* channel, *i.e.* a channel which does not preserve the order of sent messages, readyForReception is true if and only if the message is present in the inChannel part of the channel. This predicate is used as a guard of *receive* events to make sure receiving is possible.

Message bodies can have different types and for each type T an injective function $msgT \in T \rightarrowtail$ Messages is used as a wrapper to generate messages in Messages. For the purpose of our example we define the wrapper functions $req2msg \in MessagePrefixes \rightarrowtail$ Messages and $ans2msg \in MessagePrefixes \times \mathbb{Z} \rightarrowtail$ Messages corresponding to request messages and answer messages. Then, when p makes a request to a process $q \in Q$ the message $req2msg(request)$ is sent and the process q answers with a message $ans2msg(answer \mapsto availableResources(q))$.

Assertions called axioms may be labelled as theorems: these assertions have been proved using previous axioms and derived theorems from the context and the seen contexts. These theorems are used as intermediate results while discharging proof obligations of the machines which see the context.

CONTEXT CONTEXT-CM
EXTENDS C00
SETS
Nodes States Messages // Mandatory general sets
MessagePrefixes // Algorithm specific sets
CONSTANTS
network // The topology (general)
Channels emptyChannel sent received inChannel readyForReception reliable // Communication channels
send receive lose // Communication primitives (general)
P p Q // Process classes and processes (specific to the algorithm)
request answers // Algorithm specific constants
availableResources // Algorithm specific constants
sr wa wr done // Process states (specific to the algorithm except for done, general)
req2msg ans2msg // Message constructors (specific to the algorithm)
AXIOMS

Nodes: $partition(\text{Nodes}, P, Q)$ // Partition of the set of processes
P: $partition(P, \{p\})$ // Partition of the classes of processes
network_typing: $\text{network} \in \text{Nodes} \rightarrow \mathbb{P}(\text{Nodes})$ // Network specification
network_value: $\text{network} = \{proc \cdot proc \in P | proc \mapsto Q\} \cup \{proc \cdot proc \in Q | proc \mapsto \{p\}\}$
// States of the processes
States: $partition(\text{States}, \{sr\}, \{wa\}, \{wr\}, \{done\})$ // Process states
req2msg_typing: $req2msg \in MessagePrefixes \rightarrowtail \text{Messages}$ // Message types
ans2msg_typing: $ans2msg \in MessagePrefixes \times \mathbb{Z} \rightarrowtail \text{Messages}$ // Message types
Messages: $partition(\text{Messages}, ran(req2msg), ran(ans2msg))$ // Messages
// Communication channels
Channels: $\text{Channels} = \text{Nodes} \times \text{Nodes} \rightarrow (\text{Messages} \rightarrow \mathbb{N} \times \mathbb{N} \times \mathbb{N})$
// Algorithm specific constants (types of exchanged messages, process ressources)
MessagePrefixes: $partition(MessagePrefixes, \{request\}, \{answer\})$ //@P@Q
availableResources_typing: $availableResources \in Q \rightarrow \mathbb{N}$
// Communication axioms (general to all algorithms)
send: $\text{send} \in \text{Channels} \times (\text{Nodes} \times \text{Nodes}) \times \text{Messages} \rightarrow \text{Channels}$
receive: $\text{receive} \in \text{Channels} \times (\text{Nodes} \times \text{Nodes}) \times \text{Messages} \nrightarrow \text{Channels}$
received: $\text{received} \in \text{Channels} \times (\text{Nodes} \times \text{Nodes}) \times \text{Messages} \rightarrow \mathbb{N}$
inChannel: $\text{inChannel} \in \text{Channels} \times (\text{Nodes} \times \text{Nodes}) \times \text{Messages} \rightarrow \mathbb{N}$
sent: $\text{sent} \in \text{Channels} \times (\text{Nodes} \times \text{Nodes}) \times (\text{Messages}) \rightarrow \mathbb{N}$
reliable: $\text{reliable} \in \text{Channels} \rightarrow BOOL$
emptyChannel: $\text{emptyChannel} \in \text{Channels}$
axm9: $\text{emptyChannel} = \{x \cdot x \in \text{Nodes} \times \text{Nodes} | x \mapsto \{y \cdot y \in \text{Messages} | y \mapsto (0 \mapsto 0 \mapsto 0)\}\}$
axm10: $\text{inChannel} = (\lambda c \mapsto x \mapsto y \cdot c \in \text{Channels} \land x \in \text{Nodes} \times \text{Nodes} \land y \in \text{Messages} | prj2(prj1(c(x)(y))))$

axm11: $\text{sent} = (\lambda c \mapsto x \mapsto y \cdot c \in \text{Channels} \land x \in \text{Nodes} \times \text{Nodes} \land y \in \text{Messages} | prj1(prj1(c(x)(y))))$
axm12: $\text{received} = (\lambda c \mapsto x \mapsto y \cdot c \in \text{Channels} \land x \in \text{Nodes} \times \text{Nodes} \land y \in \text{Messages} | prj2(c(x)(y)))$
axm13: $\text{send} = (\lambda c \mapsto x \mapsto y \cdot c \in \text{Channels} \land x \in \text{Nodes} \times \text{Nodes} \land y \in \text{Messages} | c \lhd \{x \mapsto (c(x) \lhd \{y \mapsto (\text{sent}(c \mapsto x \mapsto y) + 1 \mapsto \text{inChannel}(c \mapsto x \mapsto y) + 1 \mapsto \text{received}(c \mapsto x \mapsto y))\})\})$
axm14: $dom(\text{receive}) = \{c, x, y \cdot c \in \text{Channels} \land x \in \text{Nodes} \times \text{Nodes} \land y \in \text{Messages} \land \text{inChannel}(c \mapsto x \mapsto y) > 0 | c \mapsto x \mapsto y\}$
axm15: $\text{receive} = (\lambda c \mapsto x \mapsto y \cdot c \in \text{Channels} \land x \in \text{Nodes} \times \text{Nodes} \land y \in \text{Messages} \land \text{inChannel}(c \mapsto x \mapsto y) > 0 | c \lhd \{x \mapsto (c(x) \lhd \{y \mapsto (\text{sent}(c \mapsto x \mapsto y) \mapsto \text{inChannel}(c \mapsto x \mapsto y) - 1 \mapsto \text{received}(c \mapsto x \mapsto y) + 1)\})\})$
axm16: $\text{reliable} = (\lambda c \cdot c \in \text{Channels} | bool(\forall x, y \cdot (x \in \text{Nodes} \times \text{Nodes} \land y \in \text{Messages} \Rightarrow \text{sent}(c \mapsto x \mapsto y) = \text{inChannel}(c \mapsto x \mapsto y) + \text{received}(c \mapsto x \mapsto y))))$
axm17: ⟨theorem⟩ $\forall c, x, y \cdot (c \in \text{Channels} \land x \in \text{Nodes} \times \text{Nodes} \land y \in \text{Messages} \Rightarrow (\text{reliable}(c) = TRUE \Rightarrow \text{reliable}(\text{send}(c \mapsto x \mapsto y)) = TRUE))$
axm18: ⟨theorem⟩ $\forall c, x, y \cdot (c \in \text{Channels} \land x \in \text{Nodes} \times \text{Nodes} \land y \in \text{Messages} \Rightarrow (\text{reliable}(c) = TRUE \land \text{inChannel}(c \mapsto x \mapsto y) > 0 \Rightarrow \text{reliable}(\text{receive}(c \mapsto x \mapsto y)) = TRUE))$
axm19: ⟨theorem⟩ $\text{reliable}(\text{emptyChannel}) = TRUE$
axm20: ⟨theorem⟩ $\forall c, x1, x2, y1, y2 \cdot (c \in \text{Channels} \land x1 \in \text{Nodes} \times \text{Nodes} \land y1 \in \text{Messages} \land x2 \in \text{Nodes} \times \text{Nodes} \land y2 \in \text{Messages} \Rightarrow \text{received}(\text{send}(c \mapsto x1 \mapsto y1) \mapsto x2 \mapsto y2) = \text{received}(c \mapsto x2 \mapsto y2))$
axm21: ⟨theorem⟩ $\forall c, x1, x2, y1, y2 \cdot (c \in \text{Channels} \land x1 \in \text{Nodes} \times \text{Nodes} \land y1 \in \text{Messages} \land x2 \in \text{Nodes} \times \text{Nodes} \land y2 \in \text{Messages} \land x1 \mapsto y1 \neq x2 \mapsto y2 \Rightarrow \text{sent}(\text{send}(c \mapsto x1 \mapsto y1) \mapsto x2 \mapsto y2) = \text{sent}(c \mapsto x2 \mapsto y2) \land \text{inChannel}(\text{send}(c \mapsto x1 \mapsto y1) \mapsto x2 \mapsto y2) = \text{inChannel}(c \mapsto x2 \mapsto y2))$
axm22: ⟨theorem⟩ $\forall c, x1, x2, y1, y2 \cdot (c \in \text{Channels} \land x1 \in \text{Nodes} \times \text{Nodes} \land y1 \in \text{Messages} \land x2 \in \text{Nodes} \times \text{Nodes} \land y2 \in \text{Messages} \land x1 \mapsto y1 \neq x2 \mapsto y2 \land \text{inChannel}(c \mapsto x1 \mapsto y1) > 0 \Rightarrow \text{inChannel}(\text{receive}(c \mapsto x1 \mapsto y1) \mapsto x2 \mapsto y2) = \text{inChannel}(c \mapsto x2 \mapsto y2) \land \text{received}(\text{receive}(c \mapsto x1 \mapsto y1) \mapsto x2 \mapsto y2) = \text{received}(c \mapsto x2 \mapsto y2))$

axm23: $\langle$theorem$\rangle$ $\forall c,x1,x2,y1,y2\cdot(c\in \text{Channels}\wedge x1\in \text{Nodes}\times\text{Nodes}\wedge y1\in \text{Messages}\wedge x2\in \text{Nodes}\times \text{Nodes}\wedge y2\in \text{Messages}\wedge \text{inChannel}(c\mapsto x1\mapsto y1)>0\Rightarrow \text{sent}(\text{receive}(c\mapsto x1\mapsto y1)\mapsto x2\mapsto y2)=\text{sent}(c\mapsto x2\mapsto y2))$

readyForReception: readyForReception $\in \text{Channels}\times(\text{Nodes}\times\text{Nodes})\times\text{Messages}\rightarrow BOOL$

axm25: readyForReception $=(\lambda c\mapsto x\mapsto y\cdot c\in \text{Channels}\wedge x\in \text{Nodes}\times\text{Nodes}\wedge y\in \text{Messages}|bool(\text{inChannel}(c\mapsto x\mapsto y)>0))$

END

MACHINE CM
REFINES M00000
SEES CONTEXT-CM
VARIABLES

channels pc result requestFrom

INVARIANTS

channels_typing: $channels\in \text{Channels}$

pc_typing: $pc\in \text{Nodes}\rightarrow STATES$

result_typing: $result\in P\rightarrow(\text{Nodes}\nrightarrow\mathbb{N})$

requestFrom_typing: $requestFrom\in Q\rightarrow\text{Nodes}$

channels_respect_network: $\forall x,y,m\cdot(x\in \text{Nodes}\wedge y\in \text{Nodes}\wedge m\in \text{Messages}\wedge \text{sent}(channels\mapsto(x\mapsto y)\mapsto m)>0\Rightarrow y\in \text{network}(x))$

requestFrom_correctness: $\forall q\cdot(q\in Q\wedge pc(q)=done\Rightarrow requestFrom(q)=\{p\})$

partial_correctness: $pc(p)=done\Rightarrow result(p)=availableResources$

EVENTS

Initialisation $\widehat{=}$

begin

act1: $channels:=\text{emptyChannel}$

act2: $pc:=\{proc\cdot proc\in P|proc\mapsto sr\}\cup\{q\cdot q\in Q|q\mapsto wr\}$

act3: $result:=\{proc\cdot proc\in P|proc\mapsto\varnothing\}$

act4: $requestFrom:=\{q\cdot q\in Q|q\mapsto\varnothing\}$

end

Event *sendRequest* $\widehat{=}$

refines *p_send*

any *proc q*

where

grd1: $proc\in P$

grd3: $q\in\text{network}(proc)$

grd2: $pc(proc)=sr$

grd4: $\text{sent}(channels\mapsto(proc\mapsto q)\mapsto(req2msg(request)))=0$

then

act1: $channels:=\text{send}(channels\mapsto(proc\mapsto q)\mapsto req2msg(request))$

end

Event *stopSending* $\widehat{=}$

refines *p_stop_sending*

any *proc*

where

grd1: $proc\in P$

grd2: $pc(proc)=sr$

grd3: $\forall q\cdot(q\in\text{network}(proc)\Rightarrow\text{sent}(channels\mapsto(proc\mapsto q)\mapsto req2msg(request))>0)$

then

act1: $pc(proc):=wa$

end

Event *receiveAnswer* $\widehat{=}$
refines *p_receive*
any *proc source message r*
where
grd1: $proc \in P$
grd3: $source \in \mathsf{Nodes}$
grd4: $message \in \mathsf{Messages}$
grd6: $r \in \mathbb{Z}$
grd2: $pc(proc) = wa$
grd5: $\mathsf{readyForReception}(channels \mapsto (source \mapsto proc) \mapsto message) = TRUE$
grd7: $message = ans2msg(answer \mapsto r)$
then
act1: $result(proc) := result(proc) \lhd\!\!+ \{source \mapsto r\}$
act2: $channels := \mathsf{receive}(channels \mapsto (source \mapsto proc) \mapsto message)$
end

Event *receiveRequestAndSendAnswer* $\widehat{=}$
refines *q_send_and_receive*
any *q source message*
where
grd1: $q \in Q$
grd3: $source \in \mathsf{Nodes}$
grd4: $message \in \mathsf{Messages}$
grd2: $pc(q) = wr$
grd5: $\mathsf{readyForReception}(channels \mapsto (source \mapsto q) \mapsto message) = TRUE$
grd6: $message = req2msg(request)$
then
act1: $channels := \mathsf{send}(\mathsf{receive}(channels \mapsto (source \mapsto q) \mapsto message) \mapsto (q \mapsto source) \mapsto ans2msg(answer \mapsto availableResources(q)))$
act2: $requestFrom(q) := requestFrom(q) \cup \{source\}$
end

Event *q_terminate* $\widehat{=}$
refines *q_terminate*
any *q proc*
where
grd1: $q \in Q$
grd3: $proc \in \mathsf{network}(q)$
grd2: $pc(q) = wr$
grd4: $\mathsf{sent}(channels \mapsto (q \mapsto proc) \mapsto ans2msg(answer \mapsto availableResources(q))) > 0$
then
act1: $pc(q) := done$
end

Event *p_terminate* $\widehat{=}$
refines *p_terminate*
any *proc*
where
grd1: $proc \in P$
grd2: $pc(proc) = wa$
grd3: $dom(result(proc)) = \mathsf{network}(proc)$
then
act1: $pc(proc) := done$
end

END

C DistAlgo program generated from LB models

C.1 Main file

```
from MessagePrefixes import MessagePrefixes
from itertools import product
from copy import deepcopy
from PClass import P
from QClass import Q

def main():
   config(handling=all)
   config(channel=reliable)

   NP = 1
   NQ = #NQ - to be configured

   PSet = new(P, num=NP)
   (p,) = list(PSet)
   QSet = new(Q, num=NQ)

   NODES = set.union(PSet, QSet)
   network = {proc:QSet for proc in PSet}
   network.update({q:{p} for q in QSet})
   availableResources = #availableResources - to be configured

   for proc in PSet:
      setup({proc}, (network[proc],))
   for proc in QSet:
      setup({proc}, (network[proc], availableResources[proc]))
   start(NODES)
```

C.2 MessagePrefixes

```
from enum import Enum

class MessagePrefixes(Enum):
   request = 'request'
   answer = 'answer'
```

C.3 Class P

```
from MessagePrefixes import MessagePrefixes
from itertools import product
from copy import deepcopy
```

```
class P(process):
   def setup(network):
      self.pc = "sr"
      self.result = {}
   # pc = sr
   def sr():
      # event sendRequest
      if(self.pc == "sr" and
        some(q in self.network,
            has= not(some(sent(("req2msg", MessagePrefixes.request),
                          to=_q))))):
         send(("req2msg", MessagePrefixes.request), to=q)
      # event stopSending
      elif(self.pc == "sr" and
          each(q in self.network,
              has=some(sent(("req2msg", MessagePrefixes.request),
                        to=_q)))):
         pctmp = self.pc
         self.pc = "wa"
      elif(self.pc != "sr"):
         pass
   # pc = wa
   def wa():
      --wa
      # event p_terminate
      if await (self.pc == "wa" and
              set(self.result.keys()) == self.network):
         pctmp = self.pc
         self.pc = "done"
      elif(self.pc != "wa"):
         pass
   # run
   def run():
     state_functions = {"sr":sr,
           "wa":wa}
      while(self.pc != "done"):
         state_functions[self.pc]()
      # Visualisation of the result.
      output(self.result)
   # event receiveAnswer
   def receive(msg=("ans2msg", MessagePrefixes.answer, r),
           from_=source,
           at=(wa,)):
      resulttmp = deepcopy(self.result)
      self.result.update(deepcopy({source:r}))
```

C.4 Class Q

```
from MessagePrefixes import MessagePrefixes
from itertools import product
from copy import deepcopy

class Q(process):
   def setup(network, availableResources):
      self.pc = "wr"
      self.requestFrom = set()
   # pc = wr
   def wr():
      --wr
      # event q_terminate
      if await(self.pc == "wr" and
              some(proc in self.network,
                  has=some(sent(("ans2msg", MessagePrefixes.answer,
                                 self.availableResources),
                                to=_proc)))):
         pctmp = self.pc
         self.pc = "done"
      elif(self.pc != "wr"):
         pass
   # run
   def run():
      state_functions = {"wr":wr}
      while(self.pc != "done"):
         stateFunctions[self.pc]()
   # event receiveRequestAndSendAnswer
   def receive(msg=("req2msg", MessagePrefixes.request),
            from_=source,
            at=(wr,)):
      requestFromtmp = set(self.requestFrom)
      self.requestFrom = requestFromtmp | {source}
      send(("ans2msg", MessagePrefixes.answer, self.
         availableResources),
          to=source)
```

D Complete Development of the Model

Due to the simplicity of the algorithm, the first machine M0 corresponds to the induction machine of figure 1 and directly introduces the description of the computing process. This machine sees context C0 which specifies the different processes. Machines M00 and M000 introduce the communications between process p and the processes of Q. Context C00 and machine M0000 specify the state machines of the processes and introduce the variable pc. Finally machine M00000 refines the communications to use the functions defined in CONTEXT-CM. This machine also refines the algorithm specific variables in order to have localized variables.

When invariant assertions are labelled as theorems, they have been preserved from the refined machines and proved using previous invariants in the refined machine and axioms in the seen context. These theorems are either interesting so called safety properties of the under construction algorithm we want to generate (such as `inv3` of M0 which states the partial correctness of the algorithm), invariants from abstract machines that are inherited and preserved by refinement (such as invariants `inv4` and `inv6` of machine M00) or properties that are technically useful for discharging proof obligations of given invariants (such as `inv3` of machine M00000).

When guards are labelled as theorems, they are proved using axioms of the context, invariants of the machine and previous guards of the given event.

CONTEXT C0
SETS
Nodes
CONSTANTS
P p Q $availableResources$
AXIOMS
`axm1`: $partition(\mathsf{Nodes}, P, Q)$
`axm2`: $partition(P, \{p\})$
`axm3`: $finite(Q)$
`axm4`: $Q \neq \varnothing$
`axm5`: $availableResources \in Q \rightarrow \mathbb{N}$
END

MACHINE M0
SEES C0
VARIABLES
res
INVARIANTS
`inv1`: $res \in Q \nrightarrow \mathbb{N}$
`inv2`: $res \subseteq availableResources$
`inv3`: $\langle$theorem$\rangle$ $dom(res) = Q \Rightarrow res = availableResources$
EVENTS
Initialisation $\langle$extended$\rangle$ $\widehat{=}$
begin
`act1`: $res := \varnothing$
end
Event $communications$ $\widehat{=}$
any q
where
`grd1`: $q \in Q \setminus dom(res)$
then
`act1`: $res(q) := availableResources(q)$
end
Event $termination$ $\widehat{=}$
when
`grd1`: $res = availableResources$
then
$skip$
end
END

MACHINE M00
REFINES M0
SEES C0
VARIABLES
res chan
INVARIANTS
inv1: $chan \subseteq Q \times \mathbb{N}$
inv2: $chan \subseteq availableResources$
inv3: $chan \cap res = \varnothing$
inv4: $\langle$theorem$\rangle$ $res \subseteq availableResources$
inv5: $\langle$theorem$\rangle$ $chan \cup res \subseteq availableResources$
inv6: $\langle$theorem$\rangle$ $dom(res) = Q \Rightarrow res = availableResources$
EVENTS
Initialisation $\widehat{=}$
begin
act1: $res := \varnothing$
act2: $chan := \varnothing$
end
Event *q_send* $\widehat{=}$
any q
where
grd1: $q \in Q$
grd2: $q \notin dom(chan \cup res)$
then
act1: $chan := chan \cup \{q \mapsto availableResources(q)\}$
end
Event *p_receive* $\widehat{=}$
refines *communications*
any $q\ r$
where
grd1: $q \mapsto r \in chan$
grd2: $\langle$theorem$\rangle$ $q \notin dom(res)$
then
act1: $res(q) := r$
act2: $chan := chan \setminus \{q \mapsto r\}$
end
Event *termination* $\widehat{=}$
refines *termination*
when
grd1: $dom(res) = Q$
then
skip
end
END

MACHINE M000
REFINES M00
SEES C0
VARIABLES
res chan request_channel sent_requests
INVARIANTS

inv1: $request\_channel \subseteq Q$
inv2: $sent\_requests \subseteq Q$
inv3: $partition(sent\_requests, request\_channel, dom(chan), dom(res))$
inv4: ⟨theorem⟩ $chan \subseteq availableResources$

EVENTS
Initialisation $\widehat{=}$
begin
act1: $res := \varnothing$
act2: $chan := \varnothing$
act3: $request\_channel := \varnothing$
act4: $sent\_requests := \varnothing$
end
Event $p\_send \widehat{=}$
any q
where
grd1: $q \in Q \setminus sent\_requests$
then
act1: $request\_channel := request\_channel \cup \{q\}$
act2: $sent\_requests := sent\_requests \cup \{q\}$
end
Event $q\_receive\_and\_send \widehat{=}$
refines q_send
any q
where
grd1: $q \in Q$
grd2: $q \in request\_channel$
then
act1: $chan := chan \cup \{q \mapsto availableResources(q)\}$
act2: $request\_channel := request\_channel \setminus \{q\}$
end
Event $p\_receive \widehat{=}$
refines $p\_receive$
any $q\ r$
where
grd1: $q \mapsto r \in chan$
grd2: ⟨theorem⟩ $q \notin dom(res)$
then
act1: $res(q) := r$
act2: $chan := chan \setminus \{q \mapsto r\}$
end
Event $termination \widehat{=}$
refines $termination$
when
grd1: $dom(res) = Q$
then
skip
end
END

CONTEXT C00
EXTENDS C0
SETS
States

CONSTANTS
sr wa wr done
AXIOMS
axm1: $partition(\mathsf{States}, \{sr\}, \{wa\}, \{wr\}, \{\mathsf{done}\})$
END

MACHINE M0000
REFINES M000
SEES C00
VARIABLES
res chan request_channel sent_requests pc has_answered
INVARIANTS
inv1: $pc \in \mathsf{Nodes} \to \mathsf{States}$
inv2: $pc(p) = done \Rightarrow res = availableResources$
inv3: $has\_answered \subseteq Q$
inv4: $\forall q \cdot (q \in Q \land q \mapsto availableResources(q) \in chan \Rightarrow q \in has\_answered)$
inv5: $dom(res) \subseteq has\_answered$
inv6: $pc(p) = \mathsf{done} \Rightarrow (Q \subseteq has\_answered)$
EVENTS
Initialisation $\widehat{=}$
begin
act1: $res := \varnothing$
act2: $chan := \varnothing$
act3: $request\_channel := \varnothing$
act4: $sent\_requests := \varnothing$
act5: $pc := \{p \mapsto sr\} \cup \{q \cdot q \in Q | q \mapsto wr\}$
act6: $has\_answered := \varnothing$
end
Event *p_send* $\widehat{=}$
refines *p_send*
any *q*
where
grd1: $q \in Q \setminus sent\_requests$
grd2: $pc(p) = sr$
then
act1: $request\_channel := request\_channel \cup \{q\}$
act2: $sent\_requests := sent\_requests \cup \{q\}$
end
Event *p_stop_sending* $\widehat{=}$
when
grd1: $pc(p) = sr$
grd2: $sent\_requests = Q$
then
act1: $pc(p) := wa$
end
Event *p_receive* $\widehat{=}$
extends *p_receive*
any *q r*
where
grd1: $q \mapsto r \in chan$
grd2: $\langle \text{theorem} \rangle\ q \notin dom(res)$
grd3: $pc(p) = wa$

then

act1: $res(q) := r$
act2: $chan := chan \setminus \{q \mapsto r\}$

end

Event $q\_receive\_and\_send \widehat{=}$
extends $q\_receive\_and\_send$

any q
where

grd1: $q \in Q$
grd2: $q \in request\_channel$
grd3: $pc(q) = wr$

then

act1: $chan := chan \cup \{q \mapsto availableResources(q)\}$
act2: $request\_channel := request\_channel \setminus \{q\}$
act3: $has\_answered := has\_answered \cup \{q\}$

end

Event $q\_terminate \widehat{=}$

any q
where

grd1: $q \in has\_answered$
grd2: $pc(q) = wr$

then

act1: $pc(q) := done$

end

Event $p\_terminate \widehat{=}$
extends $termination$

when

grd1: $dom(res) = Q$
grd2: $pc(p) = wa$

then

act1: $pc(p) := done$

end

END

MACHINE M00000
REFINES M0000
SEES CONTEXT-CM
VARIABLES

$result\ pc\ channels\ requestsFrom$

INVARIANTS

typing_channels: $channels \in \mathsf{Channels}$
channels_reliability: $reliable(channels) = TRUE$
typing_pc: ⟨theorem⟩ $pc \in \mathsf{Nodes} \rightarrow \mathsf{States}$
typing_result: $result \in P \rightarrow (\mathsf{Nodes} \nrightarrow \mathbb{N})$
GI_res: $res = result(p)$
GI_request_channels: $request\_channels = \{q \cdot q \in Q \wedge \mathsf{inChannel}(channels \mapsto (p \mapsto q) \mapsto (req2msg(request))) > 0 | q\}$
GI_sent_requests: $sent\_requests = \{q \cdot q \in Q \wedge \mathsf{sent}(channels \mapsto (p \mapsto q) \mapsto (req2msg(request))) > 0 | q\}$
GI_chan: $chan = \{q, r \cdot q \in Q \wedge r \in \mathbb{Z} \wedge \mathsf{inChannel}(channels \mapsto (q \mapsto p) \mapsto (ans2msg(answer \mapsto r))) > 0 | q \mapsto r\}$
GI_has_answered: $has\_answered = \{q, r \cdot q \in Q \wedge r \in \mathbb{Z} \wedge \mathsf{sent}(channels \mapsto (q \mapsto p) \mapsto (ans2msg(answer \mapsto r))) > 0 | q\}$

inv2: $\forall nodes, m \cdot (nodes \in \text{Nodes} \times \text{Nodes} \land m \in \text{Messages} \Rightarrow \text{sent}(channels \mapsto nodes \mapsto m) \leq 1)$
inv3: ⟨theorem⟩ $\forall nodes, m \cdot (nodes \in \text{Nodes} \times \text{Nodes} \land m \in \text{Messages} \Rightarrow \text{inChannel}(channels \mapsto nodes \mapsto m) \leq 1)$
inv4: $\forall q, r \cdot (q \in Q \land r \in \mathbb{Z} \land \text{sent}(channels \mapsto (q \mapsto p) \mapsto ans2msg(answer \mapsto r)) > 0 \Rightarrow r = availableResources(q))$

inv5: $\forall source, q, m \cdot (source \in \text{Nodes} \land q \in Q \land m \in \text{Messages} \land \text{inChannel}(channels \mapsto (source \mapsto q) \mapsto m) > 0 \Rightarrow source = p \land m = req2msg(request))$
inv6: $\forall source, m \cdot (source \in \text{Nodes} \land m \in \text{Messages} \land \text{inChannel}(channels \mapsto (source \mapsto p) \mapsto m) > 0 \Rightarrow source \in Q \land m = ans2msg(answer \mapsto availableResources(source)))$
inv7: $\forall q \cdot (q \in Q \Rightarrow \text{sent}(channels \mapsto (q \mapsto p) \mapsto (ans2msg(answer \mapsto availableResources(q)))) = \text{received}(channels \mapsto (p \mapsto q) \mapsto (req2msg(request))))$
inv8: $requestsFrom \in Q \to \mathbb{P}(\text{Nodes})$
inv9: $\forall q, proc \cdot (q \in Q \land proc \in \text{network}(q) \land pc(q) = wr \land \text{sent}(channels \mapsto (q \mapsto proc) \mapsto (ans2msg(answer \mapsto availableResources(q)))) > 0 \Rightarrow proc \in requestsFrom(q))$
inv10: $\forall q \cdot (q \in Q \Rightarrow requestsFrom(q) \subseteq \{p\})$
inv11: $\forall q \cdot (q \in Q \land pc(q) = done \Rightarrow requestsFrom(q) = \{p\})$

EVENTS
Initialisation $\widehat{=}$
begin
act1: $result := \{proc \cdot proc \in P | proc \mapsto \varnothing\}$
act2: $pc := \{p \mapsto sr\} \cup \{q \cdot q \in Q | q \mapsto wr\}$
act3: $channels := emptyChannel$
act4: $requestsFrom := \{q \cdot q \in Q | q \mapsto \varnothing\}$
end
Event $p\_send \widehat{=}$
refines p_send
any q
where
grd1: $pc(p) = sr$
grd2: $q \in \text{network}(p)$
grd3: $\text{sent}(channels \mapsto (p \mapsto q) \mapsto (req2msg(request))) = 0$
then
act3: $channels := \text{send}(channels \mapsto (p \mapsto q) \mapsto req2msg(request))$
end
Event $p\_stop\_sending \widehat{=}$
refines $p\_stop\_sending$
when
grd2: $pc(p) = sr$
grd3: $\forall q \cdot (q \in \text{network}(p) \Rightarrow \text{sent}(channels \mapsto (p \mapsto q) \mapsto req2msg(request)) > 0)$
then
act1: $pc(p) := wa$
end
Event $p\_receive \widehat{=}$
refines $p\_receive$
any $source\ message\ r$
where
grd2: $pc(p) = wa$
grd3: $source \in \text{Nodes}$
grd4: $message \in \text{Messages}$
grd5: $\text{readyForReception}(channels \mapsto (source \mapsto p) \mapsto message) = TRUE$
grd6: $r \in \mathbb{Z}$
grd7: $message = ans2msg(answer \mapsto r)$

grd8: ⟨theorem⟩ $\mathsf{inChannel}(channels \mapsto (source \mapsto p) \mapsto message) = 1$

with

q: $q = source$

then

act1: $result(p) := result(p) \lhd\!\!+ \{source \mapsto r\}$
act2: $channels := \mathsf{receive}(channels \mapsto (source \mapsto p) \mapsto message)$

end

Event *q_receive_and_send* $\widehat{=}$
refines *q_receive_and_send*

any *q source message*
where

grd1: $q \in Q$
grd2: $pc(q) = wr$
grd3: $source \in \mathsf{Nodes}$
grd4: $message \in \mathsf{Messages}$
grd5: $\mathsf{readyForReception}(channels \mapsto (source \mapsto q) \mapsto message) = TRUE$
grd6: $source \in \mathsf{network}(q)$
grd10: ⟨theorem⟩ $source = p$
grd7: $message = req2msg(request)$
grd8: ⟨theorem⟩ $\mathsf{inChannel}(channels \mapsto (source \mapsto q) \mapsto message) = 1$
grd9: ⟨theorem⟩ $\mathsf{sent}(channels \mapsto (q \mapsto p) \mapsto ans2msg(answer \mapsto availableResources(q))) = 0$

then

act1: $channels := \mathsf{send}(\mathsf{receive}(channels \mapsto (source \mapsto q) \mapsto message) \mapsto (q \mapsto source) \mapsto ans2msg(answer \mapsto availableResources(q)))$
act2: $requestsFrom(q) := requestsFrom(q) \cup \{source\}$

end

Event *q_terminate* $\widehat{=}$
refines *q_terminate*

any *q proc*
where

grd1: $q \in Q$
grd2: $pc(q) = wr$
grd3: $proc \in \mathsf{network}(q)$
grd4: ⟨theorem⟩ $proc = p$
grd5: $\mathsf{sent}(channels \mapsto (q \mapsto proc) \mapsto ans2msg(answer \mapsto availableResources(q))) > 0$

then

act1: $pc(q) := done$

end

Event *p_terminate* $\widehat{=}$
refines *p_terminate*

when

grd2: $pc(p) = wa$
grd3: $dom(result(p)) = \mathsf{network}(p)$

then

act1: $pc(p) := done$

end

END