

## A CASE STUDY ON PARAMETRIC VERIFICATION OF FAILURE DETECTORS

THANH-HAI TRAN <sup>a,b</sup>, IGOR KONNOV <sup>c</sup>, AND JOSEF WIDDER <sup>c</sup>

<sup>a</sup> TU Wien, Austria  
*e-mail address:* thanh.tran@tuwien.ac.at

<sup>b</sup> ConsenSys, Australia  
*e-mail address:* thanh-hai.tran@consensys.net

<sup>c</sup> Informal Systems, Austria  
*e-mail address:* igor@informal.systems, josef@informal.systems

**ABSTRACT.** Partial synchrony is a model of computation in many distributed algorithms and modern blockchains. These algorithms are typically parameterized in the number of participants, and their correctness requires the existence of bounds on message delays and on the relative speed of processes after reaching Global Stabilization Time (GST). These characteristics make partially synchronous algorithms both parameterized and parametric, which render automated verification of partially synchronous algorithms challenging. In this paper, we present a case study on formal verification of both safety and liveness of the Chandra and Toueg failure detector that is based on partial synchrony. To this end, we first introduce and formalize the class of symmetric point-to-point algorithms that contains the failure detector. Second, we show that these symmetric point-to-point algorithms have a cutoff, and the cutoff results hold in three models of computation: synchrony, asynchrony, and partial synchrony. As a result, one can verify them by model checking small instances, but the verification problem stays parametric in time. Next, we specify the failure detector and the partial synchrony assumptions in three frameworks:  $TLA^+$ , IVy, and counter automata. Importantly, we tune our modeling to use the strength of each method: (1) We are using counters to encode message buffers with counter automata, (2) we are using first-order relations to encode message buffers in IVy, and (3) we are using both approaches in  $TLA^+$ . By running the tools for  $TLA^+$  (TLC and APALACHE) and counter automata (FAST), we demonstrate safety for fixed time bounds. This helped us to find the inductive invariants for fixed parameters, which we used as a starting point for the proofs with IVy. By running IVy, we prove safety for arbitrary time bounds. Moreover, we show how to verify liveness of the failure detector by reducing the verification problem to safety verification. Thus, both properties are verified by developing inductive invariants with IVy. We conjecture that correctness of other partially synchronous algorithms may be proven by following the presented methodology.

*Key words and phrases:* Failure detectors,  $TLA^+$ , counter automata, FAST, and IVy.

This work was supported by Interchain Foundation (Switzerland) and the Austrian Science Fund (FWF) via the Doctoral College LogiCS W1255. This work was done when the first author was at TU Wien. This paper is an extended version of papers [TKW20] and [TKW21] that adds the formalization of the model of computation under partial synchrony and detailed proofs.

## 1. INTRODUCTION

Distributed algorithms play a crucial role in modern infrastructure, but they are notoriously difficult to understand and to get right. Network topologies, message delays, faulty processes, the relative speed of processes, and fairness conditions might lead to behaviors that were neither intended nor anticipated by algorithm designers. To be able to make meaningful statements about correctness, many specification and verification techniques for distributed algorithms [Lam02, LT88, MP20, DWZ20] have been developed.

Verification techniques for distributed algorithms usually focus on two models of computation: synchrony [SKWZ19] and asynchrony [KLVW17a, KLVW17b]. Synchrony is hard to implement in real systems, while many basic problems in fault-tolerant distributed computing are unsolvable in asynchrony.

Partial synchrony lies between synchrony and asynchrony, and escapes their shortcomings. To guarantee liveness properties, proof-of-stake blockchains [BKM18, YMR<sup>+</sup>19] and distributed algorithms [CT96, BCG20] assume time constraints under partial synchrony. That is the existence of bounds  $\Delta$  on message delay, and  $\Phi$  on the relative speed of processes after some time point. This combination makes partially synchronous algorithms parametric in time bounds. While partial synchrony is important for system designers, it is challenging for verification.

We thus investigate verification of distributed algorithms under partial synchrony, and start with the specific class of failure detectors: the Chandra and Toueg failure detector [CT96]. This is a well-known algorithm under partial synchrony that provides a service to solve many problems in fault-tolerant distributed computing.

**Contributions.** In this paper, we do formal verification of both safety and liveness of the Chandra and Toueg failure detector in case of unknown bounds  $\Delta$  and  $\Phi$ . In this case, both  $\Delta$  and  $\Phi$  are arbitrary, and the constraints on message delay and the relative speeds hold in every execution from the start.

- (1) We introduce and formalize the class of symmetric point-to-point algorithms that contains the failure detector.
- (2) We prove that the symmetric point-to-point algorithms have a cutoff, and the cutoff properties hold in three models of computation: synchrony, asynchrony, and partial synchrony. In a nutshell, a cutoff for a parameterized algorithm  $\mathcal{A}$  and a property  $\phi$  is a number  $k$  such that  $\phi$  holds for every instance of  $\mathcal{A}$  if and only if  $\phi$  holds for instances with  $k$  processes [EN95, BJK<sup>+</sup>15]. Our cutoff results with  $k = 2$  were presented in [TKW20, TKW21]. Hence, we verify the Chandra and Toueg failure detector under partial synchrony by checking instances with two processes.
- (3) We introduce encoding techniques to efficiently specify the failure detector based on our cutoff results. These techniques can tune our modeling to use the strength of the tools: FAST [BFLP08], Ivy [MP20], and model checkers for TLA<sup>+</sup> [YML99, KKT19].
- (4) We demonstrate how to reduce the liveness properties Eventually Strong Accuracy, and Strong Completeness to safety properties.
- (5) We check the safety property Strong Accuracy, and the mentioned liveness properties on instances with fixed parameters by using FAST, and model checkers for TLA<sup>+</sup>.
- (6) To verify cases of arbitrary bounds  $\Delta$  and  $\Phi$ , we find and prove inductive invariants of the failure detector with the interactive theorem prover Ivy. We reduce the liveness properties to safety properties by applying the mentioned techniques. While our specifications are

---

**Algorithm 1** The eventually perfect failure detector algorithm in [CT96]

---

```

1: Every process  $p \in 1..N$  executes the following:
2: for all  $q \in 1..N$  do ▷ Initialization step
3:    $timeout[p, q] := \text{default-value}$ 
4:    $suspected[p, q] := \perp$ 
5: Send “alive” to all  $q \in 1..N$  ▷ Task 1: repeat periodically
6: for all  $q \in 1..N$  do ▷ Task 2: repeat periodically
7:   if  $suspected[p, q] = \perp$  and not hear  $q$  during last  $timeout[p, q]$  ticks then
8:      $suspected[p, q] := \top$ 
9: if  $suspected[p, q]$  then ▷ Task 3: when receive “alive” from  $q$ 
10:   $timeout[p, q] := timeout[p, q] + 1$ 
11:   $suspected[p, q] := \perp$ 

```

---

not in the decidable theories that Ivy supports, Ivy requires no additional user assistance to prove most of our inductive invariants.

**Structure.** In Section 2, we discuss challenges in verification of the Chandra and Toueg failure detector. In Section 3, we introduce the class of symmetric point-to-point algorithms, and present how to formalize this class. Our cutoff results in the asynchronous model are presented in Section 4, and the detailed proofs are provided in Section 5. We extend the cutoff results for partial synchrony in Section 6. Our encoding technique to efficiently specify the failure detector is presented in Section 7. In Section 8, we present how to reduce the mentioned liveness properties to safety ones. Experiments for small  $\Delta$  and  $\Phi$  are described in Section 9. Ivy proofs for parametric  $\Delta$  and  $\Phi$  are discussed in Section 10. Finally, we discuss related work in Section 11.

## 2. CHALLENGES IN VERIFICATION OF FAILURE DETECTORS

The Chandra and Toueg failure detector [CT96] can be seen as an oracle to get information about crash failures in the distributed system. The failure detector usually guarantees some of the following properties [CT96] (numbers  $1..N$  denote the process identifiers):

- Strong Accuracy: No process is suspected before it crashes.  
 $\mathbf{G}(\forall p, q \in 1..N: (Correct(p) \wedge Correct(q)) \Rightarrow \neg Suspected(p, q))$
- Eventual Strong Accuracy: There is a time after which correct processes are not suspected by any correct process.  
 $\mathbf{F G}(\forall p, q \in 1..N: (Correct(p) \wedge Correct(q)) \Rightarrow \neg Suspected(p, q))$
- Strong Completeness: Eventually every crashed process is permanently suspected by every correct process.  
 $\mathbf{F G}(\forall p, q \in 1..N: (Correct(p) \wedge \neg Correct(q)) \Rightarrow Suspected(p, q))$

where  $\mathbf{F}$  and  $\mathbf{G}$  are temporal operators in linear temporal logic (LTL) [Pnu77]<sup>1</sup>, predicate  $Suspect(p, q)$  refers to whether process  $p$  suspects process  $q$  to have crashed, and predicate  $Correct(p)$  refers to whether process  $p$  is correct. Given an execution trace, process  $p$  is

---

<sup>1</sup>A brief introduction of LTL is provided in Appendix A.

correct if  $Correct(p)$  is true for every time point <sup>2</sup>. However, a process might crash later (and not recover). Given an execution trace, if process  $q$  crashes at time  $t$ , predicate  $Correct(q)$  is evaluated to false from time  $t$ . Predicate  $Suspected(p, q)$  corresponds to the variable *suspected* in Algorithm 1, and depends on the variable  $timeout[p, q]$  and the waiting time of process  $p$  for process  $q$ .

Algorithm 1 presents the pseudo code of the failure detector of [CT96]. A system instance has  $N$  processes that communicate with each other by sending-to-all and receiving messages through unbounded  $N^2$  point-to-point communication channels. A process performs local computation based on received messages (we assume that a process also receives the messages that it sends to itself). In one system step, all processes may take up to one step. Locally in each step, a process can only make a step in at most one of the locally concurrent tasks. Some processes may crash, i.e., stop operating. Correct processes follow Algorithm 1 to detect crashes in the system. Initially, every correct process sets a default value for a timeout of each other (Line 3), i.e., how long it should wait for others, and assumes that no processes have crashed (Line 4). Symbols  $\perp$  and  $\top$  refer to truth values false and true, respectively. Every correct process  $p$  has three tasks: (i) repeatedly sends an “alive” message to all processes (Line 5), and (ii) repeatedly produces predictions about crashes of other processes based on timeouts (Line 6), and (iii) increases a timeout for process  $q$  if  $p$  has learned that its suspicion on  $q$  is wrong (Line 9). Notice that process  $p$  raises suspicion on the operation of process  $q$  (Line 6) by considering only information related to  $q$ :  $timeout[p, q]$ ,  $suspected[p, q]$ , and messages that  $p$  has received from  $q$  recently.

Algorithm 1 does not satisfy Eventually Strong Accuracy under asynchrony since there exists no bound on message delay, and messages sent by correct processes might always arrive after the timeout expired. Liveness of the failure detector is based on the existence of bounds  $\Delta$  on the message delay, and  $\Phi$  on the relative speed of processes after reaching the Global Stabilization Time (GST) at some time point  $T_0$  [CT96].<sup>3</sup> There are many models of partial synchrony [DLS88, CT96]. In this paper, we focus only on the case of unknown bounds  $\Delta$  and  $\Phi$  because other models might call for abstractions which are out of scope of this paper. In our case,  $T_0 = 1$ , and both parameters  $\Delta$  and  $\Phi$  are arbitrary. Moreover, the following constraints hold in every execution:

- (TC1) If message  $m$  is placed in the message buffer from process  $q$  to process  $p$  by some operation  $Send(m, p)$  at a time  $s_1 \geq 1$ , and if process  $p$  executes an operation  $Receive(p)$  at a time  $s_2$  with  $s_2 \geq s_1 + \Delta$ , then message  $m$  must be delivered to  $p$  at time  $s_2$  or earlier.
- (TC2) In every contiguous time interval  $[t, t + \Phi]$  with  $t \geq 1$ , every correct process must take at least one step.

These constraints make the failure detector parametric in  $\Delta$  and  $\Phi$ .

Moreover, Algorithm 1 is parameterized by the number of processes and by the initial value of the timeout. If a default value of the timeout is too small, there exists a case in

---

<sup>2</sup>We deviate from the original definition in [CT96], as it allows us to describe global states at specific times, without reasoning about potential crashes that happen in the future. Actually, our modeling captures more closely the failure patterns from [CT96]. Regarding the failure detector properties, the strong accuracy property is equivalent to the one in [CT96]. The other two properties have the form  $\mathbf{F}\mathbf{G}(\dots)$ , where we may consider satisfaction only at times after the last process has crashed and thus our crashed predicates coincide with the ones in [CT96].

<sup>3</sup>A time  $T_0$  is called the Global Stabilization Time (GST) if  $\Delta$  or  $\Phi$  holds in  $[T_0, \infty]$ .

which sent messages are delivered after the timeout expired. This behavior violates Strong Accuracy.

As a result, verification of the failure detector faces the following challenges:

- (1) Its model of computation lies between synchrony and asynchrony since multiple processes can take a step in a global step.
- (2) The failure detector is parameterized by the number of processes. Hence, we need to verify infinitely many instances of algorithms.
- (3) The initial value of the timeout is an additional parameter in Algorithm 1.
- (4) The failure detector relies on a global clock and local clocks. A straightforward encoding of a clock with an integer would produce an infinite state space.
- (5) The algorithm is parametric by time bounds  $\Delta$  and  $\Phi$ .
- (6) Eventually Strong Accuracy and Strong Completeness are liveness properties.

### 3. MODEL OF COMPUTATION

In this section, we introduce the class of symmetric point-to-point algorithms, and present how to formalize such algorithms as transition systems. Since every process follows the same algorithm, we first define a process template that captures the process behavior in Section 3.1. Every process is an instance of the process template.

In Section 3.2, we present the formalization of the global system. This formalization is adapted with the time constraints under partial synchrony in Section 3.3, and our analysis is for the model under partial synchrony.

Intuitively, a global system is a composition of  $N$  processes,  $N^2$  point-to-point outgoing message buffers, and  $N$  control components that capture what processes can take a step. Every process is identified with a unique index in  $1..N$ , and follows the same deterministic algorithm. Moreover, a global system allows: (i) multiple processes to take (at most) one step in one global step, and (ii) some processes to crash. Every process may execute three kinds of transitions: *internal*, *round*, and *stuttering*. Notice that in one global step, some processes may send a message to all, and some may receive messages and do computation. Hence, we need to decide which processes move, and what happens to the message buffers. We introduce four sub-rounds: *Schedule*, *Send*, *Receive*, and *Computation*. The transitions for these sub-rounds are called internal ones. A global round transition is a composition of four internal transitions. We formalize sub-rounds and global steps later. As a result of modeling, there exists an arbitrary sequence of global configurations which is not accepted in asynchrony. So, we define so-called *admissible* sequences of global configurations under asynchrony.

Recall that the network topology of algorithms in the symmetric point-to-point class contains  $N^2$  *point-to-point* message buffers. Every transposition on a set of process indexes preserves the network topology. Importantly, every transposition on process indexes also preserves the structures of both the process template and the global transition system. It implies that both the process template and the global transition system are *symmetric*.

**3.1. The Process Template.** We fix a set of process indexes as  $1..N$ . Moreover, we assume that the message content does not have indexes of its receiver and sender. We let  $\mathbf{Msg}$  denote a set of potential messages, and  $\mathbf{Set}(\mathbf{Msg})$  denote the set of sets of messages.

We model a process template as a transition system  $\mathcal{U}_N = (Q_N, Tr_N, Rel_N, q_N^0)$  where

$$Q_N = Loc \times \underbrace{\text{Set}(\text{Msg}) \times \dots \times \text{Set}(\text{Msg})}_{N \text{ times}} \times \underbrace{\mathcal{D} \times \dots \times \mathcal{D}}_{N \text{ times}}$$

is a set of template states <sup>4</sup>,  $Tr_N$  is a set of template transitions,  $Rel_N \subseteq Q_N \times Tr_N \times Q_N$  is a template transition relation, and  $q_N^0 \in Q_N$  is an initial state. These components of  $\mathcal{U}_N$  are defined as follows.

**States.** A *template state*  $\rho$  is a tuple  $(\ell, S_1, \dots, S_N, d_1, \dots, d_N)$  where:

- $\ell \in Loc$  refers to the value of a program counter that ranges over a set  $Loc$  of locations. We assume that  $Loc = Loc_{snd} \cup Loc_{rcv} \cup Loc_{comp} \cup \{\ell_{crash}\}$ , and three sets  $Loc_{snd}$ ,  $Loc_{rcv}$ ,  $Loc_{comp}$  are disjoint, and  $\ell_{crash}$  is a special location of crashes. To access the program counter, we use a function  $pc: Q_N \rightarrow Loc$  that takes a template state at its input, and produces its program counter as the output. Let  $\rho(k)$  denote the  $k^{th}$  component in a template state  $\rho$ . For every  $\rho \in Q_N$ , we have  $pc(\rho) = \rho(1)$ .
- $S_i \in \text{Set}(\text{Msg})$  refers to a set of messages. It is to store the messages received from a process  $p_i$  for every  $i \in 1..N$ . To access a set of received messages from a particular process whose index is in  $1..N$ , we use a function  $rcvd: Q_N \times 1..N \rightarrow \text{Set}(\text{Msg})$  that takes a template state  $\rho$  and a process index  $i$  at its input, and produces the  $(i+1)^{th}$  component of  $\rho$  at the output, i.e. for every  $\rho \in Q_N$ , we have  $rcvd(\rho, i) = \rho(1+i)$ .
- $d_i \in \mathcal{D}$  refers to a local variable related to a process  $p_i$  for every  $i \in 1..N$ . To access a local variable related to a particular process whose index in  $1..N$ , we use a function  $lvar: Q_N \times 1..N \rightarrow \mathcal{D}$  that takes a template state  $\rho$  and a process index  $i$  at its input, and produces the  $(1+N+i)^{th}$  component of  $\rho$  as the output, i.e.  $lvar(\rho, i) = \rho(1+N+i)$  for every  $\rho \in Q_N$ . For example, for every process  $p$  in Algorithm 1, variable  $d_i$  of process  $p$  refers to a tuple of the two variables  $timeout[p, i]$  and  $suspect[p, i]$ .

**Initial state.** The initial state  $q_N^0$  is a tuple  $q_N^0 = (\ell_0, \emptyset, \dots, \emptyset, d_0, \dots, d_0)$  where  $\ell_0$  is a location, every box for received messages is empty, and every local variable is assigned a constant  $d_0 \in \mathcal{D}$ .

**Transitions.** We define  $Tr_N = CSnd \cup CRcv \cup \{comp, crash, stutter\}$  where

- $CSnd$  is a set of transitions. Every transition in  $CSnd$  refers to a task that does some internal computation, and sends a message to all. For example, in task 1 in Algorithm 1, a process increases its local clock, and performs an instruction to send “alive” to all. We let  $csnd(m)$  denote a transition referring to a task with an action to send a message  $m \in \text{Msg}$  to all.
- $CRcv$  is a set of transitions. Every transition in  $CRcv$  refers to a task that receives  $N$  sets of messages, and does some internal computation. For example, in task 2 in Algorithm 1, a process increases its local clock, receives messages, and removes false-negative predictions. We let  $crcv(S_1, \dots, S_N)$  denote a transition referring to a task with an action to receive sets  $S_1, \dots, S_N$  of messages. These sets  $S_1, \dots, S_N$  are delivered by the global system.
- $comp$  is a transition which refers to a task with purely local computation. In other words, this task has neither send actions nor receive actions.
- $crash$  is a transition for crashes.

<sup>4</sup>We denote  $S_1 \times \dots \times S_m$  by a set  $\{(s_1, \dots, s_m) \mid \bigwedge_{1 \leq i \leq m} s_i \in S_i\}$  of tuples. The elements of the set  $Q_N$  are tuples with  $2N + 1$  elements.

- *stutter* is a transition for stuttering steps.

**Transition relation.** For two states  $\rho, \rho' \in Q_N$  and a transition  $tr \in Tr_N$ , instead of  $(\rho, tr, \rho')$ , we write  $\rho \xrightarrow{tr} \rho'$ . In the model of [DLS88, CT96], each process follows the same deterministic algorithm. Hence, we assume that for every  $\rho_0 \xrightarrow{tr_0} \rho'_0$  and  $\rho_1 \xrightarrow{tr_1} \rho'_1$ , if  $\rho_0 = \rho_1$  and  $tr_0 = tr_1$ , then it follows that  $\rho'_0 = \rho'_1$ . Moreover, we assume that there exist the following functions which are used to define constraints on the template transition relation:

- A function  $nextLoc: Loc \rightarrow Loc$  takes a location at its input and produces the next location as the output.
- A function  $genMsg: Loc \rightarrow \mathbf{Set}(\mathbf{Msg})$  takes a location at its input, and produces a singleton set that contains the message that is sent to all processes in the current task. The output can be an empty set. For example, if a process is performing a Receive task, the output of  $genMsg$  is an empty set.
- A function  $nextVal: Loc \times \mathbf{Set}(\mathbf{Msg}) \times \mathcal{D} \rightarrow \mathcal{D}$  takes a location, a set of messages, and a local variable's value, and produces a new value of a local variable as the output.

Let us fix functions  $nextLoc, genMsg$  and  $nextVal$ . We define the template transitions as follows.

- (1) For every message  $m \in \mathbf{Msg}$ , for every pair of states  $\rho, \rho' \in Q_N$ , we have  $\rho \xrightarrow{csnd(m)} \rho'$  if and only if
  - (a)  $pc(\rho) \in Loc_{snd} \wedge pc(\rho') = nextLoc(pc(\rho)) \wedge \{m\} = genMsg(pc(\rho))$
  - (b)  $\forall i \in 1..N: rcvd(\rho, i) = rcvd(\rho', i)$
  - (c)  $\forall i \in 1..N: lvar(\rho', i) = nextVal(pc(\rho), \emptyset, lvar(\rho, i))$

Constraint (a) implies that the update of a program counter and the construction of a sent message  $m$  depend on only the current value of a program counter, and a process sends only  $m$  to all in this step. For example, process  $p$  in Algorithm 1 sends only message “alive” in Task 1. Constraint (b) refers to that no message was delivered. Constraint (c) implies that the value of  $lvar(\rho', i)$  depends only on the current location and the value of  $lvar(\rho, i)$ . The empty set in Constraint (c) means that no messages have been delivered.

- (2) For arbitrary sets of messages  $S_1, \dots, S_N \subseteq \mathbf{Msg}$ , for every pair of states  $\rho, \rho' \in Q_N$ , we have  $\rho \xrightarrow{crcv(S_1, \dots, S_N)} \rho'$  if and only if the following constraints hold:
  - (a)  $pc(\rho) \in Loc_{rcv} \wedge pc(\rho') = nextLoc(pc(\rho)) \wedge \emptyset = genMsg(pc(\rho))$
  - (b)  $\forall i \in 1..N: rcvd(\rho', i) = rcvd(\rho, i) \cup S_i$
  - (c)  $\forall i \in 1..N: lvar(\rho', i) = nextVal(pc(\rho), S_i, lvar(\rho, i))$

Constraint (a) in  $crcv$  is similar to constraint (a) in  $csnd$ , except that no message is sent in this sub-round. Constraint (b) refers that messages in a set  $S_i$  are from a process indexed  $i$ , and have been delivered in this step. For example, in Algorithm 1 Constraint (b) implies that  $rcvd(\rho, i) \subseteq \{\text{“alive”}\}$  for every template state  $\rho$  and every index  $1 \leq i \leq N$ . After the first “alive” message was received, the value of  $rcvd(\rho, i)$  is unchanged. This does not raise any issues in our analysis as Line 7 in Algorithm 1 considers only how long process  $p$  has waited for a new message from process  $q$ . Constraint (c) in  $crcv$  implies that the value of  $lvar(\rho', i)$  depends on only the current location, the set  $S_i$  of messages that have been delivered, and the value of  $lvar(\rho, i)$ .

- (3) For every pair of states  $\rho, \rho' \in Q_N$ , we have  $\rho \xrightarrow{comp} \rho'$  if and only if the following constraints hold:

- (a)  $pc(\rho) \in Loc_{comp} \wedge pc(\rho') = nextLoc(pc(\rho)) \wedge \emptyset = genMsg(pc(\rho))$
- (b)  $\forall i \in 1..N: rcvd(\rho', i) = rcvd(\rho, i)$
- (c)  $\forall i \in 1..N: lvar(\rho', i) = nextVal(pc(\rho), \emptyset, lvar(\rho, i))$

Hence, this step has only local computation. No message is sent or delivered.

- (4) For every pair of states  $\rho, \rho' \in Q_N$ , we have  $\rho \xrightarrow{crash} \rho'$  if and only if the following constraints hold:
- (a)  $pc(\rho) \neq \ell_{crash} \wedge pc(\rho') = \ell_{crash}$
  - (b)  $\forall i \in 1..N: rcvd(\rho, i) = rcvd(\rho', i) \wedge lvar(\rho, i) = lvar(\rho', i)$
- Only the program counter is updated by switching to  $\ell_{crash}$ .
- (5) For every pair of states  $\rho, \rho' \in Q_N$ , we have  $\rho \xrightarrow{stutter} \rho'$  if and only if  $\rho = \rho'$ .

**3.2. Modeling the Global Distributed Systems.** We now present the formalization of the global system. In this model, multiple processes might take a step in a global step. This characteristic allows us to extend this model with partial synchrony constraints that are formalized in Section 3.3. To capture the semantics of asynchrony, we simply need a constraint that only one process can take a step in a global step [AW04]. This constraint is formalized in the end of this subsection.

Given  $N$  processes which are instantiated from the same process template  $\mathcal{U}_N = (Q_N, Tr_N, Rel_N, q_N^0)$ , the global system is a composition of (i) these processes, and (ii)  $N^2$  point-to-point buffers for in-transit messages, and (iii)  $N$  control components that capture what processes can take a step. We formalize the global system as a transition system  $\mathcal{G}_N = (\mathcal{C}_N, Tr_N, R_N, g_N^0)$  where

- $\mathcal{C}_N = (Q_N)^N \times \mathbf{Set}(\mathbf{Msg})^{N \cdot N} \times \mathbf{Bool}^N$  is a set of global configurations,
- $Tr_N$  is a set of global *internal*, *round*, and *stuttering* transitions,
- $R_N \subseteq \mathcal{C}_N \times Tr_N \times \mathcal{C}_N$  is a global transition relation, and
- $g_N^0$  is an initial configuration.

These components are defined as follows.

**Configurations.** A *global configuration*  $\kappa$  is defined as a following tuple

$$\kappa = (q_1, \dots, q_N, S_1^1, S_1^2, \dots, S_s^r, \dots, S_N^N, act_1, \dots, act_N)$$

where:

- $q_i \in Q_N$ : This component is a state of a process  $p_i$  for every  $i \in 1..N$ . To access a local state of a particular process, we use a function  $lstate: \mathcal{C}_N \times 1..N \rightarrow Q_N$  that takes input as a global configuration  $\kappa$  and a process index  $i$ , and produces output as the  $i^{th}$  component of  $\kappa$  which is a state of a process  $p_i$ . Let  $\kappa(i)$  denote the  $i^{th}$  component of a global configuration  $\kappa$ . For every  $i \in 1..N$ , we have  $lstate(\kappa, i) = \kappa(i) = q_i$ .
- $S_s^r \in \mathbf{Set}(\mathbf{Msg})$ : This component is a set of in-transit messages from a process  $p_s$  to a process  $p_r$  for every  $s, r \in 1..N$ . To access a set of in-transit messages between two processes, we use a function  $buf: \mathcal{C}_N \times 1..N \times 1..N \rightarrow \mathbf{Set}(\mathbf{Msg})$  that takes input as a global configuration  $\kappa$ , and two process indexes  $s, r$ , and produces output as the  $(s \cdot N + r)^{th}$  component of  $\kappa$  which is a message buffer from a process  $p_s$  (sender) to a process  $p_r$  (receiver). Formally, we have  $buf(\kappa, s, r) = \kappa(s \cdot N + r) = S_s^r$  for every  $s, r \in 1..N$ .
- $act_i \in \mathbf{Bool}$ : This component says whether a process  $p_i$  can take one step in a global step for every  $i \in 1..N$ . To access a control component, we use a function  $active: \mathcal{C}_N \times 1..N \rightarrow \mathbf{Bool}$  that takes input as a configuration  $\kappa$  and a process index  $i$ , and produces output as the



$((N + 1) \cdot N + i)^{th}$  component of  $\kappa$  which refers to whether a process  $p_i$  can take a step. Formally, we have  $active(\kappa, i) = \kappa((N + 1) \cdot N + i)$  for every  $i \in 1..N$ . The environment sets the values of  $act_1, \dots, act_N$  in the sub-round *Schedule* defined later.

We will write  $\kappa \in (Q_N)^N \times \mathbf{Set}(\mathbf{Msg})^{N \cdot N} \times \mathbf{Bool}^N$  or  $\kappa \in \mathcal{C}_N$ .

**Initial configuration.** The global system  $\mathcal{G}_N$  has one initial configuration  $g_N^0$ , and it must satisfy the following constraints:

- (1)  $\forall i \in 1..N: \neg active(g_N^0, i) \wedge lstate(g_N^0, i) = q_N^0$
- (2)  $\forall s, r \in 1..N: buf(g_N^0, s, r) = \emptyset$

**Global stuttering transition.** We extend the relation  $\rightsquigarrow$  with stuttering: for every configuration  $\kappa$ , we allow  $\kappa \rightsquigarrow \kappa$ . The stuttering transition is necessary in the proof of Lemma 4.13 presented in Section 4.

**Global internal transitions.** In the model of [DLS88, CT96], many processes can take a step in a global step. We assume that a computation of the distributed system is organized in rounds, i.e. global ticks, and every round is organized as four sub-rounds called *Schedule*, *Send*, *Receive*, and *Computation*. To model that as a transition system, for every sub-round we define a corresponding transition:  $\xrightarrow{\text{Sched}}$  for the sub-round *Schedule*,  $\xrightarrow{\text{Snd}}$  for the sub-round *Send*,  $\xrightarrow{\text{Rcv}}$  for the sub-round *Receive*,  $\xrightarrow{\text{Comp}}$  for the sub-round *Comp*. These transitions are called global *internal* transitions. We define the semantics of these sub-rounds as follows.

- (1) Sub-round *Schedule*. The environment starts with a global configuration where every process is inactive, and move to another by non-deterministically deciding what processes become crashed, and what processes take a step in the current global step. Every correct process takes a stuttering step, and every faulty process is inactive. If a process  $p$  is crashed in this sub-round, every incoming message buffer to  $p$  is set to the empty set.

Formally, for  $\kappa, \kappa' \in \mathcal{C}_N$ , we have  $\kappa \xrightarrow{\text{Sched}} \kappa'$  if the following constraints hold:

- (a)  $\forall i \in 1..N: \neg active(\kappa, i)$
- (b)  $\forall i \in 1..N: lstate(\kappa, i) \xrightarrow{\text{stutter}} lstate(\kappa', i) \vee lstate(\kappa, i) \xrightarrow{\text{crash}} lstate(\kappa', i)$
- (c)  $\forall i \in 1..N: pc(lstate(\kappa', i)) = \ell_{\text{crash}} \Rightarrow \neg active(\kappa', i)$
- (d)  $\forall s, r \in 1..N: pc(lstate(\kappa', r)) \neq \ell_{\text{crash}} \Rightarrow buf(\kappa, s, r) = buf(\kappa', s, r)$
- (e)  $\forall r \in 1..N: pc(lstate(\kappa', r)) = \ell_{\text{crash}} \Rightarrow (\forall s \in 1..N: buf(\kappa', s, r) = \emptyset)$

We let predicate  $Enabled(\kappa, i, L)$  denote whether process  $i$  whose location at the configuration  $\kappa$  is in  $L$  takes a step from  $\kappa$ . Formally, we have

$$Enabled(\kappa, i, L) \triangleq active(\kappa, i) \wedge pc(lstate(\kappa, i)) \in L$$

Predicate  $Enabled$  is used in the definitions of other sub-rounds.

- (2) Sub-round *Send*. Only processes that perform send actions can take a step in this sub-round. Such processes become inactive at the end of this sub-round. Fresh sent messages are added to corresponding message buffers. To define the semantics of the sub-round *Send*, we use the following predicates:

$$\begin{aligned} Frozen_S(\kappa, \kappa', i) &\triangleq lstate(\kappa, i) \xrightarrow{\text{stutter}} lstate(\kappa', i) \\ &\wedge active(\kappa, i) = active(\kappa', i) \\ &\wedge \forall r \in 1..N: buf(\kappa, i, r) = buf(\kappa', i, r) \end{aligned}$$

$$\begin{aligned}
\text{Sending}(\kappa, \kappa', i, m) &\triangleq \forall r \in 1..N: m \notin \text{buf}(\kappa, i, r) \\
&\wedge \forall r \in 1..N: \text{buf}(\kappa', i, r) = \{m\} \cup \text{buf}(\kappa, i, r) \\
&\wedge \text{lstate}(\kappa, i) \xrightarrow{\text{csnd}(m)} \text{lstate}(\kappa', i)
\end{aligned}$$

Formally, for  $\kappa, \kappa' \in \mathcal{C}_N$ , we have  $\kappa \xrightarrow{\text{Snd}} \kappa'$  if the following constraints hold:

- (a)  $\forall i \in 1..N: \neg \text{Enabled}(\kappa, i, \text{Loc}_{\text{snd}}) \Leftrightarrow \text{Frozen}_S(\kappa, \kappa', i)$
- (b)  $\forall i \in 1..N: \text{Enabled}(\kappa, i, \text{Loc}_{\text{snd}}) \Leftrightarrow \exists m \in \text{Msg}: \text{Sending}(\kappa, \kappa', i, m)$
- (c)  $\forall i \in 1..N: \text{Enabled}(\kappa, i, \text{Loc}_{\text{snd}}) \Rightarrow \neg \text{active}(\kappa', i)$

The semantics of the Send sub-round forces that the Send primitive is atomic.

- (3) Sub-round *Receive*. Only processes that perform receive actions can take a step in this sub-round. Such processes become inactive at the end of this sub-round. Sets of delivered messages that may be empty are removed from corresponding message buffers. To define the semantics of this sub-round, we use the following predicates:

$$\begin{aligned}
\text{Frozen}_R(\kappa, \kappa', i) &\triangleq \text{lstate}(\kappa, i) \xrightarrow{\text{stutter}} \text{lstate}(\kappa', i) \\
&\wedge \text{active}(\kappa, i) = \text{active}(\kappa', i) \\
&\wedge \forall s \in 1..N: \text{buf}(\kappa, s, i) = \text{buf}(\kappa', s, i) \\
\text{Receiving}(\kappa, \kappa', i, S_1, \dots, S_N) &\triangleq \forall s \in 1..N: S_s \cap \text{buf}(\kappa', s, i) = \emptyset \\
&\wedge \forall s \in 1..N: \text{buf}(\kappa', s, i) \cup S_s = \text{buf}(\kappa, s, i) \\
&\wedge \text{lstate}(\kappa, i) \xrightarrow{\text{rcrv}(S_1, \dots, S_N)} \text{lstate}(\kappa', i)
\end{aligned}$$

Formally, for  $\kappa, \kappa' \in \mathcal{C}_N$ , we have  $\kappa \xrightarrow{\text{Rcv}} \kappa'$  if the following constraints hold:

- (a)  $\forall i \in 1..N: \neg \text{Enabled}(\kappa, i, \text{Loc}_{\text{rcv}}) \Leftrightarrow \text{Frozen}_R(\kappa, \kappa', i)$
- (b)  $\forall i \in 1..N: \text{Enabled}(\kappa, i, \text{Loc}_{\text{rcv}}) \Leftrightarrow \exists S_1, \dots, S_N \subseteq \text{Msg}: \text{Receiving}(\kappa, \kappa', i, S_1, \dots, S_N)$
- (c)  $\forall i \in 1..N: \text{Enabled}(\kappa, i, \text{Loc}_{\text{rcv}}) \Rightarrow \neg \text{active}(\kappa', i)$

- (4) Sub-round *Computation*. Only processes that perform internal computation actions can take a step in this sub-round. Such processes become inactive at the end of this sub-round. Every message buffer is unchanged. Formally, for  $\kappa, \kappa' \in \mathcal{C}_N$ , we have  $\kappa \xrightarrow{\text{Comp}} \kappa'$  if the following constraints hold:

- (a)  $\forall i \in 1..N: \text{Enabled}(\kappa, i, \text{Loc}_{\text{comp}}) \Leftrightarrow \text{lstate}(\kappa, i) \xrightarrow{\text{comp}} \text{lstate}(\kappa', i)$
- (b)  $\forall i \in 1..N: \neg \text{Enabled}(\kappa, i, \text{Loc}_{\text{comp}}) \Leftrightarrow \text{lstate}(\kappa, i) \xrightarrow{\text{stutter}} \text{lstate}(\kappa', i)$
- (c)  $\forall s, r \in 1..N: \text{buf}(\kappa, s, r) = \text{buf}(\kappa', s, r)$
- (d)  $\forall i \in 1..N: \text{Enabled}(\kappa, i, \text{Loc}_{\text{comp}}) \Rightarrow \neg \text{active}(\kappa', i)$

**Remark 3.1.** Predicate *Sending* refers that at most one “alive” message in Algorithm 1 is in every message buffer. In Section 3.3, we extend our formalization by introducing the notion of time and by modeling time constraints under partial synchrony. In that formalization, every “alive” message is tagged with its age, and therefore, the message buffers can have multiple messages.

**Remark 3.2.** Observe that the definitions of  $\kappa \xrightarrow{\text{Sched}} \kappa'$ , and  $\kappa \xrightarrow{\text{Snd}} \kappa'$ , and  $\kappa \xrightarrow{\text{Rcv}} \kappa'$ , and  $\kappa \xrightarrow{\text{Comp}} \kappa'$  allow  $\kappa = \kappa'$ , that is stuttering. This captures, e.g., global steps in [DLS88, CT96] where no process sends a message.

**Global round transitions.** Intuitively, every global *round* transition is induced by a sequence of four transitions: a  $\xrightarrow{\text{Sched}}$  transition, a  $\xrightarrow{\text{Snd}}$  transition, a  $\xrightarrow{\text{Rcv}}$  transition, and a  $\xrightarrow{\text{Comp}}$  transition. We let  $\rightsquigarrow$  denote global round transitions. For every pair of global configurations  $\kappa_0, \kappa_4 \in \mathcal{C}_N$ , we say  $\kappa_0 \rightsquigarrow \kappa_4$  if there exist three global configurations  $\kappa_1, \kappa_2, \kappa_3 \in \mathcal{C}_N$  such that  $\kappa_0 \xrightarrow{\text{Sched}} \kappa_1 \xrightarrow{\text{Snd}} \kappa_2 \xrightarrow{\text{Rcv}} \kappa_3 \xrightarrow{\text{Comp}} \kappa_4$ . Moreover, global round transitions allow some processes to crash only in the sub-round Schedule. We call these faults *clean crashes*. Notice that correct process  $i$  can make at most one global internal transition in every global round transition since the component  $act_i$  is false after process  $i$  makes a transition.

**Admissible sequences.** An infinite sequence  $\pi = \kappa_0 \kappa_1 \dots$  of global configurations in  $\mathcal{G}_N$  is *admissible* if the following constraints hold:

- (1)  $\kappa_0$  is the initial state, i.e.  $\kappa_0 = g_N^0$ , and
- (2)  $\pi$  is stuttering equivalent with an infinite sequence  $\pi' = \kappa'_0 \kappa'_1 \dots$  such that  $\kappa'_{4k} \xrightarrow{\text{Sched}} \kappa'_{4k+1} \xrightarrow{\text{Snd}} \kappa'_{4k+2} \xrightarrow{\text{Rcv}} \kappa'_{4k+3} \xrightarrow{\text{Comp}} \kappa'_{4k+4}$  for every  $k \geq 0$ .

Notice that it immediately follows by this definition that if  $\pi = \kappa_0 \kappa_1 \dots$  is an admissible sequence of configurations in  $\mathcal{G}_N$ , then  $\kappa'_{4k} \rightsquigarrow \kappa'_{4k+4}$  for every  $k \geq 0$ . From now on, we only consider admissible sequences of global configurations.

**Admissible sequences under synchrony.** Let  $\pi = \kappa_0 \kappa_1 \dots$  be an admissible sequence of global configurations in  $\mathcal{G}_N$ . As every correct process makes a transition in every global step under synchrony[AW04], we say that  $\pi$  is under synchrony if every correct process is active after a sub-round Schedule. Formally, for every transition  $\kappa \xrightarrow{\text{Sched}} \kappa'$  in  $\pi$ , the following constraint holds:  $\forall i \in 1..N: pc(\text{lstate}(\kappa', i)) \neq \ell_{\text{crash}} \Rightarrow \text{active}(\kappa', i)$ .

**Admissible sequences under asynchrony.** Let  $\pi = \kappa_0 \kappa_1 \dots$  be an admissible sequence of global configurations in  $\mathcal{G}_N$ . As at most one process can make a transition in every global step under asynchrony[AW04], we say that  $\pi$  is under asynchrony if at most one process is active after a sub-round Schedule. Formally, for every transition  $\kappa \xrightarrow{\text{Sched}} \kappa'$  in  $\pi$ , the following constraint holds:  $\forall i, j \in 1..N: \text{active}(\kappa', i) \wedge \text{active}(\kappa', j) \Rightarrow i = j$ .

**3.3. Modeling Time Constraints under Partial Synchrony.** Time parameters in partial synchrony only reduce the execution space compared to asynchrony. Hence, we can formalize the system behaviors under partial synchrony by extending the above formalization of the system behaviors with the notion of time, message ages, time constraints, and admissible sequences of configurations under partial synchrony. They are defined as follows.

**Time.** Time is progressing with global round transitions. Formally, let  $\pi = \kappa_0 \kappa_1 \dots$  be an admissible sequence of global configurations in  $\mathcal{G}_N$ . We say that the configuration  $\kappa_0$  is at time 0, and that four configurations  $\kappa_{4k-3}, \dots, \kappa_{4k}$  are at time  $k$  for every  $k > 0$ .

Recall that in Section 3.2, a global round transition is induced of a sequence of four sub-rounds: Schedule, Send, Receive, and Computation. In an admissible sequence  $\pi = \kappa_0 \kappa_1 \dots$  of global configurations in  $\mathcal{G}_N$ , for every  $k > 0$ , every sub-sequence of four configurations  $\kappa_{4k-3}, \dots, \kappa_{4k}$  presents one global round transition. Configuration  $\kappa_{4k-3}$  is in sub-round Schedule, and configuration  $\kappa_{4k}$  is in sub-round Computation for every  $k > 0$ . So, the notion of time says that the global round transition  $\kappa_{4k-3} \rightsquigarrow \kappa_{4k}$  happens at time  $k$ .

**Message ages.** Now we discuss the formalization of message ages. For every sent message  $m$ , the global system tags it with its current age, i.e.,  $(m, age_m)$ . Message ages require that the type of message buffers needs to be changed to  $buf: \mathcal{C}_N \times 1..N \times 1..N \rightarrow \mathbf{Set}(\mathbf{Msg} \times \mathbb{N})$ .

In our formalization, when message  $m$  was added to the message buffer in sub-round Send, its age is 0. Instead of predicate *Sending*, our formalization now uses the following predicate *Sending'*.

$$\begin{aligned} Sending'(\kappa, \kappa', i, m) \triangleq & \quad \forall r \in 1..N: (m, 0) \notin buf(\kappa, i, r) \\ & \wedge \forall r \in 1..N: buf(\kappa', i, r) = \{(m, 0)\} \cup buf(\kappa, i, r) \\ & \wedge lstate(\kappa, i) \xrightarrow{csnd(m)} lstate(\kappa', i) \end{aligned}$$

Message ages are increased by 1 when the global system takes a  $\xrightarrow{\text{Sched}}$  transition. Formally, for every time  $k \geq 0$ , for every process  $s, r \in 1..N$ , the following constraints hold:

- (i) For every message  $(m, age_m)$  in  $buf(\kappa_{4k}, s, r)$ , there exists a message  $(m', age_{m'})$  in  $buf(\kappa_{4k+1}, s, r)$  such that  $m = m'$  and  $age_{m'} = age_m + 1$ .
- (ii) For every message  $(m', age_{m'})$  in  $buf(\kappa_{4k+1}, s, r)$ , there exists a message  $(m, age_m)$  in  $buf(\kappa_{4k}, s, r)$  such that  $m = m'$  and  $age_m = age_{m'} + 1$ .

Constraint (i) ensures that every in-transit message age will be added by one time-unit in the sub-round Schedule. Constraint (ii) ensures that no new messages will be added in  $buf(\kappa_{4k+1}, s, r)$ . These two constraints are used to replace Constraint (1d) about unchanged message buffers in the definition of sub-round Schedule in Section 3.2.

Moreover, the age of an in-transit message is unchanged in other sub-rounds. Formally, for every time  $k > 0$ , for every  $0 \leq \ell \leq 3$ , for every pair of processes  $s, r \in 1..N$ , for every message  $(m, age_m)$  in  $buf(\kappa_{4k-\ell}, s, r)$ , there exists  $(m', age_{m'})$  in  $buf(\kappa_{4k-3}, s, r)$  such that  $m = m'$  and  $age_m = age_{m'}$ .

Finally, message ages are not delivered to processes in sub-round Receive. Instead of predicate *Receiving*, our formalization now uses the following predicate *Receiving'*.

$$\begin{aligned} Receiving'(\kappa, \kappa', i, S_1, \dots, S_N) \triangleq & \quad \forall s \in 1..N: S_s \cap buf(\kappa', s, i) = \emptyset \\ & \wedge \forall s \in 1..N: buf(\kappa', s, i) \cup S_s = buf(\kappa, s, i) \\ & \wedge lstate(\kappa, i) \xrightarrow{crvc(g(S_1), \dots, g(S_N))} lstate(\kappa', i) \end{aligned}$$

where function  $g: \mathbf{Set}(\mathbf{Msg} \times \mathbb{N}) \rightarrow \mathbf{Set}(\mathbf{Msg})$  is to detag message ages in a set  $S$ . Formally, we have two following constraints:

- (1) For every  $(m, age_m) \in S$ , it holds  $m \in g(S)$ .
- (2) For every  $m \in g(S)$ , there exists  $age_m \in \mathbb{N}$  such that  $(m, age_m) \in S$ .

**Partial synchrony constraints.** We here focus on the case of unknown bounds. Recall that Constraints (TC1) and (TC2) hold in this case. Given an admissible sequence  $\pi = \kappa_0 \kappa_1 \dots$  of global configurations in  $\mathcal{G}_N$ , Constraints (TC1) and (TC2) on  $\pi$  can be formalized as follows, respectively:

- (PS1) For every process  $r \in 1..N$ , for every time  $k > 0$ , if  $Enabled(\kappa_{4k-2}, r, Loc_{rcv})$ , then for every process  $s \in 1..N$ , there exists no message  $(m, age_m)$  in  $buf(\kappa_{4k-1}, s, r)$  such that  $age_m \geq \Delta$ .
- (PS2) For every process  $i \in 1..N$ , for every time interval  $[k, k + \Phi]$ , if we have that  $pc(lstate(\kappa_\ell, i)) \neq \ell_{crash}$  for every configuration index in the interval  $[4k - 3, 4(k + \Phi)]$ ,

then there exist a configuration index  $t$  in  $[4k - 3, 4(k + \Phi)]$  and a set  $L$  of locations such that  $Enabled(\kappa_t, i, L)$  where  $L$  is one of  $Loc_{snd}$ ,  $Loc_{rcv}$ , and  $Loc_{comp}$ .

Constraint (PS1) requires that if process  $r$  takes a step from  $\kappa_{4k-2}$  in the sub-round Receive, then there exists no in-transit messages (sent to process  $r$ ) whose ages are at least  $\Delta$  time-units in  $\kappa_{4k-1}$ , that is, older messages must have been received before that. In principle, partial synchrony allows messages to be older than  $\Delta$  time-units as long as the receiver does not take a step after the message reaches age Delta. Consistent to (TC1), whenever a receiver takes a step after a message is older than  $\Delta$  time-units, the reception step removes it from the buffer. This limitation is to enabled processes. Constraint (PS2) ensures that for every time interval  $[k, k + \Phi]$  with configurations  $\kappa_{4k-3}, \dots, \kappa_{4(k+\Phi)}$ , for every process  $i \in 1..N$ , if process  $i$  is correct in this time interval, there exist a configuration  $\kappa_{\ell_0} \in \{\kappa_{4k-3}, \dots, \kappa_{4(k+\Phi)}\}$  and a set  $L$  of locations such that the location of process  $i$  at  $\kappa_{\ell_0}$  is in  $L$  and process  $i$  takes a step from  $\kappa_{\ell_0}$ .

**Admissible sequences under partial synchrony.** Let  $\pi = \kappa_0 \kappa_1 \dots$  be an admissible sequence of global configurations in  $\mathcal{G}_N$ . We say that  $\pi$  is under partial synchrony if Constraints (PS1) and (PS2) hold in  $\pi$ . Notice that admissible sequences under partial synchrony allow multiple processes to make a transition in a time unit.

#### 4. CUTOFF RESULTS IN THE MODEL OF THE GLOBAL DISTRIBUTED SYSTEMS

Let  $\mathcal{A}$  be a symmetric point-to-point algorithm. In this section, we show cutoff results for the number of processes in the algorithm  $\mathcal{A}$  in the unrestricted model. These results are Theorems 4.1 and 4.2, and the detailed proofs are provided in Section 5. With these cutoff results, one can verify two properties Strong Completeness and Eventually Strong Accuracy of the failure detector of [CT96] by model checking two instances of sizes 1 and 2 in case of synchrony.

**Theorem 4.1.** *Let  $\mathcal{A}$  be a symmetric point-to-point algorithm under the unrestricted model. Let  $\mathcal{G}_1$  and  $\mathcal{G}_N$  be instances of 1 and  $N$  processes respectively for some  $N \geq 1$ . Let  $Path_1$  and  $Path_N$  be sets of all admissible sequences of configurations in  $\mathcal{G}_1$  and in  $\mathcal{G}_N$ , respectively. Let  $\omega_{\{i\}}$  be a LTL\X formula in which every predicate takes one of the forms:  $P_1(i)$  or  $P_2(i, i)$  where  $i$  is an index in  $1..N$ . Then, it follows that:*

$$\left( \forall \pi_N \in Path_N : \mathcal{G}_N, \pi_N \models \bigwedge_{i \in 1..N} \omega_{\{i\}} \right) \Leftrightarrow \left( \forall \pi_1 \in Path_1 : \mathcal{G}_1, \pi_1 \models \omega_{\{1\}} \right)$$

**Theorem 4.2.** *Let  $\mathcal{A}$  be a symmetric point-to-point algorithm under the unrestricted model. Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be instances of 2 and  $N$  processes respectively for some  $N \geq 2$ . Let  $Path_2$  and  $Path_N$  be sets of all admissible sequences of configurations in  $\mathcal{G}_2$  and in  $\mathcal{G}_N$ , respectively. Let  $\psi_{\{i,j\}}$  be an LTL\X formula in which every predicate takes one of the forms:  $P_1(i)$ , or  $P_2(j)$ , or  $P_3(i, j)$ , or  $P_4(j, i)$  where  $i$  and  $j$  are different indexes in  $1..N$ . It follows that:*

$$\left( \forall \pi_N \in Path_N : \mathcal{G}_N, \pi_N \models \bigwedge_{\substack{i \neq j \\ i, j \in 1..N}} \psi_{\{i,j\}} \right) \Leftrightarrow \left( \forall \pi_2 \in Path_2 : \mathcal{G}_2, \pi_2 \models \psi_{\{1,2\}} \right)$$

Since the proof of Theorem 4.1 is similar to the one of Theorem 4.2, we focus on Theorem 4.2 here. Its proof is based on the symmetric characteristics in the system

model (the network topology and the three functions  $nextLoc$ ,  $genMsg$ , and  $nextVal$ ) and correctness properties, and on the following lemmas.

- Lemma 4.6 says that every transposition on a set of process indexes  $1..N$  preserves the structure of the process template  $\mathcal{U}_N$ .
- Lemma 4.7 says that every transposition on a set of process indexes  $1..N$  preserves the structure of the global transition system  $\mathcal{G}_N$  for every  $N \geq 1$ .
- Lemma 4.13 says that  $\mathcal{G}_2$  and  $\mathcal{G}_N$  are trace equivalent under a set  $AP_{\{1,2\}}$  of predicates that take one of the forms:  $P_1(i)$ , or  $P_2(j)$ , or  $P_3(i, j)$ , or  $P_4(j, i)$ .

In the following, we present definitions and constructions to prove these lemmas.

**4.1. Index Transpositions and Symmetric Point-to-point Systems.** We first recall the definition of transposition. Given a set  $1..N$  of indexes, we call a bijection  $\alpha: 1..N \rightarrow 1..N$  a transposition between two indexes  $i, j \in 1..N$  if the following properties hold:  $\alpha(i) = j$ , and  $\alpha(j) = i$ , and  $\forall k \in 1..N: (k \neq i \wedge k \neq j) \Rightarrow \alpha(k) = k$ . We let  $(i \leftrightarrow j)$  denote a transposition between two indexes  $i$  and  $j$ .

The application of a transposition to a template state is given in Definition 4.3. Informally, applying a transposition  $\alpha = (i \leftrightarrow j)$  to a template state  $\rho$  generates a new template state by switching only the evaluation of  $rcvd$  and  $lvar$  at indexes  $i$  and  $j$ . The application of a transposition to a global configuration is provided in Definition 4.4. In addition to process configurations, we need to change message buffers and control components. We override notation by writing  $\alpha_Q(\rho)$  and  $\alpha_C(\kappa)$  to refer the application of a transposition  $\alpha$  to a state  $\rho$  and to a configuration  $\kappa$ , respectively. These functions  $\alpha_Q$  and  $\alpha_C$  are named a local transposition and a global transposition, respectively.

**Definition 4.3** (Local Transposition). Let  $\mathcal{U}_N$  be a process template with process indexes  $1..N$ , and  $\rho = (\ell, S_1, \dots, S_N, d_1, \dots, d_N)$  be a state in  $\mathcal{U}_N$ . Let  $\alpha = (i \leftrightarrow j)$  be a transposition on  $1..N$ . The application of  $\alpha$  to  $\rho$ , denoted as  $\alpha_Q(\rho)$ , generates a tuple  $(\ell', S'_1, \dots, S'_N, d'_1, \dots, d'_N)$  such that

- (1)  $\ell = \ell'$ , and  $S_i = S'_j$ , and  $S_j = S'_i$ , and  $d_i = d'_j$  and  $d_j = d'_i$ , and
- (2)  $\forall k \in 1..N: (k \neq i \wedge k \neq j) \Rightarrow (S_k = S'_k \wedge d_k = d'_k)$

**Definition 4.4** (Global Transposition). Let  $\mathcal{G}_N$  be a global system with process indexes  $1..N$ , and  $\kappa$  be a configuration in  $\mathcal{G}_N$ . Let  $\alpha = (i \leftrightarrow j)$  be a transposition on  $1..N$ . The application of  $\alpha$  to  $\kappa$ , denoted as  $\alpha_C(\kappa)$ , generates a configuration in  $\mathcal{G}_N$  which satisfies following properties:

- (1)  $\forall i \in 1..N: lstate(\alpha_C(\kappa), \alpha(i)) = \alpha_Q(lstate(\kappa, i))$ .
- (2)  $\forall s, r \in 1..N: buf(\alpha_C(\kappa), \alpha(s), \alpha(r)) = buf(\kappa, s, r)$
- (3)  $\forall i \in 1..N: active(\alpha_C(\kappa), \alpha(i)) = active(\kappa, i)$

Since the content of every message in  $Msg$  does not have indexes of the receiver and sender, no transposition affects the messages. We define the application of a transposition to one of send, compute, crash, and stutter template transitions return the same transition. We extend the application of a transposition to a receive template transition as in Definition 4.5.

**Definition 4.5** (Receive-transition Transposition). Let  $\mathcal{U}_N$  be a process template with indexes  $1..N$ , and  $\alpha = (i \leftrightarrow j)$  be a transposition on  $1..N$ . Let  $crcv(S_1, \dots, S_N)$  be a transition in  $\mathcal{U}_N$  which refers to a task with a receive action. We let  $\alpha_R(crcv(S_1, \dots, S_N))$

denote the application of  $\alpha$  to  $crcv(S_1, \dots, S_N)$ , and this application returns a new transition  $crcv(S'_1, \dots, S'_N)$  in  $\mathcal{U}_N$  such that:

- (1)  $S_i = S'_j$ , and  $S_j = S'_i$ , and
- (2)  $\forall k \in 1..N: (k \neq i \wedge k \neq j) \Rightarrow (S_k = S'_k \wedge d_k = d'_k)$

We let  $\alpha_U(\mathcal{U}_N)$  and  $\alpha_G(\mathcal{G}_N)$  denote the application of a transposition  $\alpha$  to a process template  $\mathcal{U}_N$  and a global transition system  $\mathcal{G}_N$ , respectively. Since these definitions are straightforward, we skip them in this chapter. We prove later that  $\alpha_Q(\mathcal{U}_N) = \mathcal{U}_N$  and  $\alpha_C(\mathcal{G}_N) = \mathcal{G}_N$  (see Lemmas 4.6 and 4.7).

**Lemma 4.6** (Symmetric Process Template). *Let  $\mathcal{U}_N = (Q_N, Tr_N, Rel_N, q_N^0)$  be a process template with indexes  $1..N$ . Let  $\alpha = (i \leftrightarrow j)$  be a transposition on  $1..N$ , and  $\alpha_Q$  be a local transposition based on  $\alpha$  (from Definition 4.3). The following properties hold:*

- (1)  $\alpha_Q$  is a bijection from  $Q_N$  to itself.
- (2) The initial state is preserved under  $\alpha_Q$ , i.e.  $\alpha_Q(q_N^0) = q_N^0$ .
- (3) Let  $\rho, \rho' \in \mathcal{U}_N$  be states such that  $\rho \xrightarrow{crcv(S_1, \dots, S_N)} \rho'$  for some sets of messages  $S_1, \dots, S_N$  in  $\mathbf{Set}(\mathbf{Msg})$ . It follows  $\alpha_Q(\rho) \xrightarrow{\alpha_R(crcv(S_1, \dots, S_N))} \alpha_Q(\rho')$ .
- (4) Let  $\rho, \rho'$  be states in  $\mathcal{U}_N$ , and  $tr \in Tr_N$  be one of send, local computation, crash and stutter transitions such that  $\rho \xrightarrow{tr} \rho'$ . Then,  $\alpha_Q(\rho) \xrightarrow{tr} \alpha_Q(\rho')$ .

**Lemma 4.7** (Symmetric Global System). *Let  $\mathcal{G}_N = (\mathcal{C}_N, Tr_N, R_N, g_N^0)$  be a global transition system. Let  $\alpha$  be a transposition on  $1..N$ , and  $\alpha_C$  be a global transposition based on  $\alpha$  (from Definition 4.4). The following properties hold:*

- (1)  $\alpha_C$  is a bijection from  $\mathcal{C}_N$  to itself.
- (2) The initial configuration is preserved under  $\alpha_C$ , i.e.  $\alpha_C(g_N^0) = g_N^0$ .
- (3) Let  $\kappa$  and  $\kappa'$  be configurations in  $\mathcal{G}_N$ , and  $tr \in Tr_N$  be either a internal transition such that  $\kappa \xrightarrow{tr} \kappa'$ . It follows  $\alpha_C(\kappa) \xrightarrow{tr} \alpha_C(\kappa')$ .
- (4) Let  $\kappa$  and  $\kappa'$  be configurations in  $\mathcal{G}_N$ . If  $\kappa \rightsquigarrow \kappa'$ , then  $\alpha_C(\kappa) \rightsquigarrow \alpha_C(\kappa')$ .

**4.2. Trace Equivalence of  $\mathcal{G}_2$  and  $\mathcal{G}_N$  under  $AP_{\{1,2\}}$ .** Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be two global transition systems whose processes follow the same symmetric point-to-point algorithm. In the following, our goal is to prove Lemma 4.13 that says  $\mathcal{G}_2$  and  $\mathcal{G}_N$  are trace equivalent under a set  $AP_{\{1,2\}}$  of predicates which take one of the forms:  $Q_1(1)$ ,  $Q_2(2)$ ,  $Q_3(1, 2)$ , or  $Q_4(2, 1)$ . To do that, we first present two construction techniques: Construction 4.8 to construct a state in  $\mathcal{U}_2$  from a state in  $\mathcal{U}_N$ , and Construction 4.9 to construct a global configuration in  $\mathcal{G}_2$  from a given global configuration in  $\mathcal{G}_N$ . Second, we define trace equivalence under a set  $AP_{\{1,2\}}$  of predicates in which every predicate takes one of the forms:  $P_1(i)$ , or  $P_2(j)$ , or  $P_3(i, j)$ , or  $P_4(j, i)$ . Our definition of trace equivalence under  $AP_{\{1,2\}}$  is extended from the definition of trace equivalence in [Hoa80]. Next, we present two Lemmas 4.10 and 4.12. These lemmas are required in the proof of Lemma 4.13.

To keep the presentation simple, when the context is clear, we simply write  $\mathcal{U}_N$ , instead of fully  $\mathcal{U}_N = (Q_N, Tr_N, Rel_N, q_N^0)$ . We also write  $\mathcal{G}_N$ , instead of fully  $\mathcal{G}_N = (\mathcal{C}_N, Tr_N, R_N, g_N^0)$ .

**Construction 4.8** (State Projection). *Let  $\mathcal{A}$  be an arbitrary symmetric point-to-point algorithm. Let  $\mathcal{U}_N$  be a process template of  $\mathcal{A}$  for some  $N \geq 2$ , and  $\rho^N$  be a process*

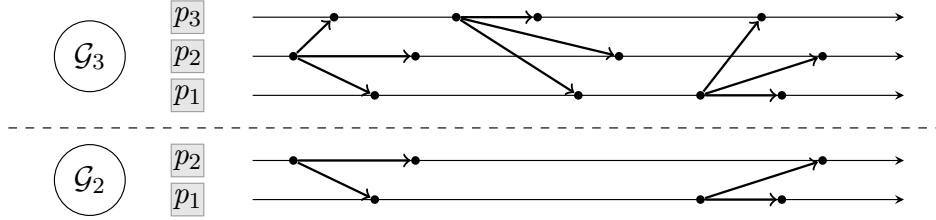


FIGURE 1. Given execution in  $\mathcal{G}_3$ , construct an execution in  $\mathcal{G}_2$  by index projection.

configuration of  $\mathcal{U}_N$ . We construct a tuple  $\rho^2 = (pc_1, rcvd_1, rcvd_2, v_1, v_2)$  based on  $\rho^N$  and a set  $\{1, 2\}$  of process indexes in the following way:

- (1)  $pc_1 = pc(\rho^N)$ .
- (2) For every  $i \in \{1, 2\}$ , it follows  $rcvd_i = rcvd(\rho^N, i)$ .
- (3) For every  $i \in \{1, 2\}$ , it follows  $v_i = lvar(\rho^N, i)$ .

**Construction 4.9** (Configuration Projection). Let  $\mathcal{A}$  be a symmetric point-to-point algorithm. Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be two global transition systems of two instances of  $\mathcal{A}$  for some  $N \geq 2$ , and  $\kappa^N \in \mathcal{C}_N$  be a global configuration in  $\mathcal{G}_N$ . A tuple

$$\kappa^2 = (s_1, s_2, buf_1^1, buf_1^2, buf_2^1, buf_2^2, act_1, act_2)$$

is constructed based on the configuration  $\kappa^N$  and a set  $\{1, 2\}$  of indexes in the following way:

- (1) For every  $i \in \{1, 2\}$ , a component  $s_i$  is constructed from  $lstate(\kappa^N, i)$  with Construction 4.8 and indexes  $\{1, 2\}$ .
- (2) For every  $s, r \in \{1, 2\}$ , it follows  $buf_s^r = buf(\kappa^N, s, r)$ .
- (3) For every process  $i \in \{1, 2\}$ , it follows  $act_i = active(\kappa^N, i)$ .

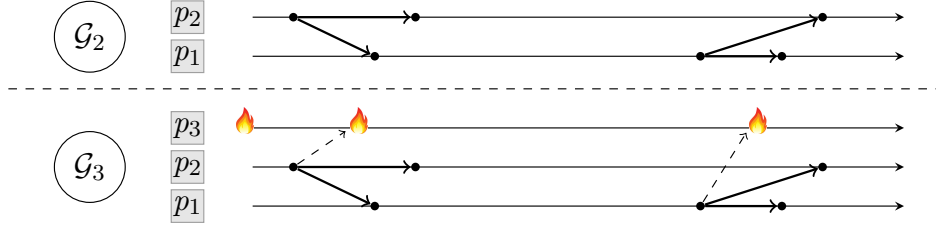
Note that a tuple  $\rho^2$  constructed with Construction 4.8 is a state in  $\mathcal{U}_2$ , and a tuple  $\kappa^2$  constructed with Construction 4.9 is a configuration in  $\mathcal{G}_2$ . We call  $\rho^2$  (and  $\kappa^2$ ) the *index projection* of  $\rho^N$  (and  $\kappa^N$ ) on indexes  $\{1, 2\}$ . The following Lemma 4.10 says that Construction 4.9 allows us to construct an admissible sequence of global configurations in  $\mathcal{G}_2$  based on a given admissible sequence in  $\mathcal{G}_N$ . Intuitively, the index projection throws away processes  $3..N$  as well as their corresponding messages and buffers. Moreover, for every  $i, j \in \{1, 2\}$ , the index projection preserves (i) when process  $i$  takes a step, and (ii) what action process  $i$  takes at time  $t \geq 0$ , and (iii) messages between process  $i$  and process  $j$ . For example, Figure 1 demonstrates an execution in  $\mathcal{G}_2$  that is constructed based on a given execution in  $\mathcal{G}_3$  with the index projection.

**Lemma 4.10.** Let  $\mathcal{A}$  be a symmetric point-to-point algorithm. Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be two transition systems such that all processes in  $\mathcal{G}_2$  and  $\mathcal{G}_N$  follow  $\mathcal{A}$ , and  $N \geq 2$ . Let  $\pi^N = \kappa_0^N \kappa_1^N \dots$  be an admissible sequence of configurations in  $\mathcal{G}_N$ . Let  $\pi^2 = \kappa_0^2 \kappa_1^2 \dots$  be a sequence of configurations in  $\mathcal{G}_2$  such that  $\kappa_k^2$  is the index projection of  $\kappa_k^N$  on indexes  $\{1, 2\}$  for every  $k \geq 0$ . Then,  $\pi^2$  is admissible in  $\mathcal{G}_2$ .

*Sketch of proof.* The proof of Lemma 4.10 is based on the following observations:

- (1) The application of Construction 4.8 to an initial template state of  $\mathcal{U}_N$  constructs an initial template state of  $\mathcal{U}_2$ .
- (2) Construction 4.8 preserves the template transition relation.



FIGURE 2. Construct an execution in  $\mathcal{G}_3$  based on a given execution in  $\mathcal{G}_2$ .

- (3) The application of Construction 4.9 to an initial global configuration of  $\mathcal{G}_N$  constructs an initial global configuration of  $\mathcal{G}_2$ .
- (4) Construction 4.9 preserves the global transition relation.  $\square$

Moreover, Lemma 4.12 says that given an admissible sequence  $\pi^2 = \kappa_0^2 \kappa_1^2 \dots$  in  $\mathcal{G}_2$ , there exists an admissible sequence  $\pi^N = \kappa_0^N \kappa_1^N \dots$  in  $\mathcal{G}_N$  such that  $\kappa_i^2$  is the index projection of  $\kappa_i^N$  on indexes  $\{1, 2\}$  for every  $0 \leq i$ .

**Definition 4.11** (Trace Equivalence under  $AP_{\{1,2\}}$ ). Let  $\mathcal{A}$  be an arbitrary symmetric point-to-point algorithm. Let  $\mathcal{G}_2 = (Q_2, Tr_2, Rel_2, q_2^0)$  and  $\mathcal{G}_N = (Q_N, Tr_N, Rel_N, q_N^0)$  be global transition systems of  $\mathcal{A}$  for some  $N \geq 2$ . Let  $AP_{\{1,2\}}$  be a set of predicates that take one of the forms:  $P_1(i)$ , or  $P_2(j)$ , or  $P_3(i, j)$ , or  $P_4(j, i)$ . Let  $L: Q_2 \cup Q_N \rightarrow 2^{AP}$  be an evaluation function. We say that  $\mathcal{G}_2$  and  $\mathcal{G}_N$  are trace equivalent under  $AP_{\{1,2\}}$  if the following constraints hold:

- (1) For every admissible sequence  $\pi^2 = \kappa_0^2 \kappa_1^2 \dots$  of configurations in  $\mathcal{G}_2$ , there exists an admissible sequence of configurations  $\pi^N = \kappa_0^N \kappa_1^N \dots$  in  $\mathcal{G}_N$  such that  $L(\kappa_i^2) = L(\kappa_i^N)$  for every  $i \geq 0$ .
- (2) For every admissible sequence  $\pi^N = \kappa_0^N \kappa_1^N \dots$  in  $\mathcal{G}_N$ , there exists an admissible sequence  $\pi^2 = \kappa_0^2 \kappa_1^2 \dots$  of configurations in  $\mathcal{G}_2$  such that  $L(\kappa_i^2) = L(\kappa_i^N)$  for every  $i \geq 0$ .

**Lemma 4.12.** *Let  $\mathcal{A}$  be an arbitrary symmetric point-to-point algorithm. Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be global transition systems of  $\mathcal{A}$  for some  $N \geq 2$ . Let  $\pi^2 = \kappa_0^2 \kappa_1^2 \dots$  be an admissible sequence of configurations in  $\mathcal{G}_2$ . There exists an admissible sequence  $\pi^N = \kappa_0^N \kappa_1^N \dots$  of configurations in  $\mathcal{G}_N$  such that  $\kappa_i^2$  is the index projection of  $\kappa_i^N$  on indexes  $\{1, 2\}$  for every  $i \geq 0$ .*

*Sketch of proof.* We construct an execution  $\pi_N$  in  $\mathcal{G}_N$  based on  $\pi_2$  such that all processes  $3..N$  crash from the beginning, and  $\pi_2$  is an index projection of  $\pi_N$ . For instance, Figure 2 demonstrates an execution in  $\mathcal{G}_3$  that is constructed based on one in  $\mathcal{G}_2$ . We have that  $\pi_2$  is admissible in  $\mathcal{G}_2$ .  $\square$

**Lemma 4.13.** *Let  $\mathcal{A}$  be a symmetric point-to-point algorithm. Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be its instances for some  $N \geq 2$ . Let  $AP_{\{1,2\}}$  be a set of predicates that take one of the forms:  $P_1(1)$ ,  $P_2(2)$ ,  $P_3(1, 2)$  or  $P_4(2, 1)$ . It follows that  $\mathcal{G}_2$  and  $\mathcal{G}_N$  are trace equivalent under  $AP_{\{1,2\}}$ .*

*Sketch of proof.* The proof of Lemma 4.13 is based on Definition 4.11, Lemma 4.10, and Lemma 4.12.  $\square$

## 5. DETAILED PROOFS FOR CUTOFF RESULTS IN THE MODEL OF THE GLOBAL DISTRIBUTED SYSTEMS

In this section, we present the detailed proofs for Theorems 4.1 and 4.2. In Sections 5.1 and 5.2 we prove that every transposition on a set of process indexes  $1..N$  preserves the structure of the process template  $\mathcal{U}_N$  and the structure of the global transition system  $\mathcal{G}_N$  for every  $N \geq 1$ , respectively. In Section 5.3 we show that  $\mathcal{G}_2$  and  $\mathcal{G}_N$  are trace equivalent under  $AP_{\{1,2\}}$ . Next, we prove that  $\mathcal{G}_1$  and  $\mathcal{G}_N$  are trace equivalent under  $AP_{\{1\}}$  in Section 5.4. Then, the detailed proofs for Theorems 4.1 and 4.2 is presented in Section 5.5. Finally, we discuss why we can verify the strong completeness property of the failure detector of [CT96] under synchrony by model checking instances of size 2 by applying our cutoff results.

**5.1. Transpositions and Process Templates.** The proof of Lemma 4.6 requires the following propositions:

- Given a transposition  $\alpha$ , Proposition 5.1 says that a function  $\alpha_Q$ , which refers to the application of  $\alpha$  to a state in  $Q_N$ , is a bijection from  $Q_N$  to itself.
- Proposition 5.2 says that  $\alpha_Q$  has no effect on the initial template state  $q_N^0$ .
- Propositions 5.3 and 5.4 describe the relationship between transpositions and template transitions.

**Lemma 4.6.** *Let  $\mathcal{U}_N = (Q_N, Tr_N, Rel_N, q_N^0)$  be a process template with indexes  $1..N$ . Let  $\alpha = (i \leftrightarrow j)$  be a transposition on  $1..N$ , and  $\alpha_Q$  be a local transposition based on  $\alpha$  (from Definition 4.3). The following properties hold:*

- (1)  $\alpha_Q$  is a bijection from  $Q_N$  to itself.
- (2) The initial state is preserved under  $\alpha_Q$ , i.e.  $\alpha_Q(q_N^0) = q_N^0$ .
- (3) Let  $\rho, \rho' \in \mathcal{U}_N$  be states such that  $\rho \xrightarrow{crcv(S_1, \dots, S_N)} \rho'$  for some sets of messages  $S_1, \dots, S_N$  in  $\mathbf{Set}(\mathbf{Msg})$ . It follows  $\alpha_Q(\rho) \xrightarrow{\alpha_R(crcv(S_1, \dots, S_N))} \alpha_Q(\rho')$ .
- (4) Let  $\rho, \rho'$  be states in  $\mathcal{U}_N$ , and  $tr \in Tr_N$  be one of send, local computation, crash and stutter transitions such that  $\rho \xrightarrow{tr} \rho'$ . Then,  $\alpha_Q(\rho) \xrightarrow{tr} \alpha_Q(\rho')$ .

*Proof.* We have: point 1 holds by Proposition 5.1, and point 2 holds by Proposition 5.2, and point 3 holds by Proposition 5.3, and point 4 holds by Proposition 5.4.  $\square$

**Proposition 5.1.** *Let  $\mathcal{U}_N = (Q_N, Tr_N, Rel_N, q_N^0)$  be a process template with indexes  $1..N$ . Let  $\alpha = (i \leftrightarrow j)$  be a transposition on  $1..N$ , and  $\alpha_Q$  be a local transposition based on  $\alpha$  (from Definition 4.3). Then,  $\alpha_Q$  is a bijection from  $Q_N$  to itself.*

*Proof.* Since two transpositions  $(i \leftrightarrow j)$  and  $(j \leftrightarrow i)$  are equivalent, we assume  $i < j$ . To show that  $\alpha_Q$  is a bijection from  $Q_N$  to itself, we prove that the following properties hold:

- (1) For every template state  $\rho' \in Q_N$ , there exists a template configuration  $\rho \in Q_N$  such that  $\alpha_Q(\rho) = \rho'$ .
- (2) For every pair of states  $\rho_1, \rho_2 \in Q_N$ , if  $\alpha_Q(\rho_1) = \alpha_Q(\rho_2)$ , then  $\rho_1 = \rho_2$ .

We first show that Point 1 holds. Assume that  $\rho'$  is a following tuple

$$\rho' = (\ell, S_1, \dots, S_i, \dots, S_j, \dots, S_N, d_1, \dots, d_i, \dots, d_j, \dots, d_N)$$

where  $\ell \in Loc$ ,  $S_i \in \mathbf{Set}(\mathbf{Msg})$ ,  $d_i \in \mathcal{D}$  for every  $i \in 1..N$ . Let  $\rho$  be the following tuple

$$\rho = (\ell, S_1, \dots, S_j, \dots, S_i, \dots, S_N, d_1, \dots, d_j, \dots, d_i, \dots, d_N)$$

where  $S_k = S'_k \wedge d_k = d'_k$  for every  $k \in 1..N \setminus \{i, j\}$ . By Definition 4.3, we have  $\alpha_Q(\rho) = \rho'$ . Moreover, by the definition of a process template in Section 3.1, it follows  $\rho \in Q_N$ .

We now focus on Point 2. By definition of the application of a process-index transposition to a template state, it is easy to check that  $\alpha_Q((\alpha_Q(\rho))) = \rho$  for every  $\rho \in Q_N$ . It follows that  $\rho_1 = \alpha_Q((\alpha_Q(\rho_1))) = \alpha_Q((\alpha_Q(\rho_2))) = \rho_2$  since  $\alpha_Q(\rho_1) = \alpha_Q(\rho_2)$ .

Therefore, Proposition 5.1 holds.  $\square$

**Proposition 5.2.** *Let  $\mathcal{U}_N = (Q_N, Tr_N, Rel_N, q_N^0)$  be a process template. Let  $\alpha = (i \leftrightarrow j)$  be a transposition on  $1..N$ , and  $\alpha_Q$  be a local transposition based on  $\alpha$  (from Definition 4.3). It follows that  $\alpha_Q(q_N^0) = q_N^0$ .*

*Proof.* By definition of  $q_N^0$  in Section 3.1, we have  $rcvd(q_N^0, i) = rcvd(q_N^0, j)$  and  $lvar(q_N^0, i) = lvar(q_N^0, j)$ . It immediately follows  $\alpha_Q(q_N^0) = q_N^0$ .  $\square$

**Proposition 5.3.** *Let  $\mathcal{U}_N = (Q_N, Tr_N, Rel_N, q_N^0)$  be a process template with indexes  $1..N$ . Let  $\rho_0$  and  $\rho_1$  be states in  $\mathcal{U}_N$  such that  $\rho_0 \xrightarrow{crcv(S_1, \dots, S_N)} \rho_1$  for some sets of messages:  $S_1, \dots, S_N \subseteq \text{Set}(\text{Msg})$ . Let  $\alpha = (i \leftrightarrow j)$  be a transposition on  $1..N$ , and  $\alpha_R$  be a receive-transition transposition based on  $\alpha$  (from Definition 4.5). It follows  $\alpha_Q(\rho_0) \xrightarrow{\alpha_R(crcv(S_1, \dots, S_N))} \alpha_Q(\rho_1)$ .*

*Proof.* We prove that all Constraints (a)–(c) between two states  $\alpha_Q(\rho_0)$  and  $\alpha_Q(\rho_1)$  in the transition  $csnd$  defined in Section 3.1 hold. First, we focus on Constraint (a). We have  $pc(\alpha_Q(\rho_1)) = pc(\rho_1)$  by Definition 4.3. We have  $pc(\rho_1) = nextLoc(pc(\rho_0))$  by the semantics of  $crcv(S_1, \dots, S_N)$  in Section 3.1. We have  $nextLoc(pc(\rho_0)) = nextLoc(pc(\alpha_Q(\rho_0)))$  by Definition 4.3. It follows  $pc(\alpha_Q(\rho_1)) = nextLoc(pc(\alpha_Q(\rho_0)))$ . Moreover, we have

$$\begin{aligned} \{m\} &= genMsg(pc(\rho_0)) && \text{(by the semantics of } crcv \text{ in Section 3.1)} \\ &= genMsg(pc(\alpha_Q(\rho_0))) && \text{(by Definition 4.3)} \end{aligned}$$

Hence, Constraint (a) holds.

Now we focus on Constraint (b). By Definition 4.3, we have  $rcvd(\alpha_Q(\rho_0), k) = rcvd(\rho_0, k)$  and  $rcvd(\alpha_Q(\rho_1), k) = rcvd(\rho_1, k)$  for every  $k \in 1..N \setminus \{i, j\}$ . We have  $rcvd(\rho_1, k) = S_k \cup rcvd(\rho_0, k)$  by the semantics of  $crcv(S_1, \dots, S_N)$  in Section 3.1. It follows  $rcvd(\alpha_Q(\rho_1), k) = S_k \cup rcvd(\alpha_Q(\rho_0), k)$  for every  $k \in 1..N \setminus \{i, j\}$ . Now we focus on  $rcvd(\alpha_Q(\rho_1), i)$ . We have  $rcvd(\alpha_Q(\rho_1), i) = rcvd(\rho_1, j)$  and  $rcvd(\alpha_Q(\rho_0), i) = rcvd(\rho_0, j)$  by Definition 4.3. Since  $rcvd(\rho_1, j) = rcvd(\rho_0, j) \cup S_j$ , it follows  $rcvd(\alpha_Q(\rho_1), i) = rcvd(\alpha_Q(\rho_0), i) \cup S_j$ . By similar arguments, we have  $rcvd(\alpha_Q(\rho_1), j) = rcvd(\alpha_Q(\rho_0), j) \cup S_i$ . Hence, Constraint (b) holds.

Now we focus on Constraint (c). By similar arguments in the proof of Constraint (b), for every  $k \in 1..N \setminus \{i, j\}$ , we have

$$lvar(\alpha_Q(\rho_1), k) = nextVal(pc(\alpha_Q(\rho_0)), S_k, lvar(\alpha_Q(\rho_0), k))$$

Now we focus on  $lvar(\alpha_Q(\rho_1), i)$ . We have  $lvar(\alpha_Q(\rho_1), i) = lvar(\rho_1, j)$  by Definition 4.3. By the semantics of  $crcv(S_1, \dots, S_N)$  in Section 3.1, it follows that  $lvar(\rho_1, j) = nextVal(pc(\rho_0), S_j, lvar(\rho_0, j))$ . By Definition 4.3, we have

$$\begin{aligned} &lvar(\alpha_Q(\rho_1), i) \\ &= lvar(\rho_1, j) \\ &= nextVal(pc(\rho_0), S_j, lvar(\rho_0, j)) \\ &= nextVal(pc(\alpha_Q(\rho_0)), S_j, lvar(\alpha_Q(\rho_0), i)) \end{aligned}$$

Moreover, by similar arguments, we have

$$lvar(\alpha_Q(\rho_1), j) = nextVal(pc(\alpha_Q(\rho_0)), S_i, lvar(\alpha_Q(\rho_0), i))$$

Constraint (c) holds. Hence, we have  $\alpha_Q(\rho_0) \xrightarrow{\alpha_R(crcv(S_1, \dots, S_N))} \alpha_Q(\rho_1)$ .  $\square$

**Proposition 5.4.** *Let  $\mathcal{U}_N = (Q_N, Tr_N, Rel_N, q_N^0)$  be a process template with indexes  $1..N$ . Let  $\rho$  and  $\rho'$  be states in  $\mathcal{U}_N$ , and  $tr \in Tr_N$  be a transition such that  $\rho \xrightarrow{tr} \rho'$  and  $tr$  refers to a task without a receive action. Let  $\alpha = (i \leftrightarrow j)$  be a transposition on  $1..N$ , and  $\alpha_Q$  be a local transposition based on  $\alpha$  (from Definition 4.3). It follows  $\alpha_Q(\rho) \xrightarrow{tr} \alpha_Q(\rho')$ .*

*Proof.* We prove Proposition 5.4 by case distinction.

- *Case  $\rho_0 \xrightarrow{csnd(m)} \rho_1$ .* By similar arguments in the proof of Proposition 5.3, it follows  $pc(\alpha_Q(\rho_1)) = nextLoc(pc(\alpha_Q(\rho_0)))$  and  $\{m\} = genMsg(pc(\alpha_Q(\rho_0)))$ . Constraint (a) holds. By Definition 4.3, for every  $k \in 1..N \setminus \{i, j\}$ , we have  $rcvd(\alpha_Q(\rho_0), k) = rcd(\rho_0, k)$  and  $rcvd(\alpha_Q(\rho_1), k) = rcd(\rho_1, k)$ . Hence, it follows  $rcvd(\alpha_Q(\rho_1), k) = rcd(\alpha_Q(\rho_0), k)$  for every  $k \in 1..N \setminus \{i, j\}$ . Now we focus on  $rcvd(\alpha_Q(\rho_1), i)$ . We have  $rcvd(\alpha_Q(\rho_1), i) = rcd(\rho_1, j)$  and  $rcvd(\alpha_Q(\rho_0), i) = rcd(\rho_0, j)$  by Definition 4.3. Since  $rcvd(\rho_1, j) = rcd(\rho_0, j)$ , it follows that  $rcvd(\alpha_Q(\rho_1), i) = rcd(\alpha_Q(\rho_0), i)$ . By similar arguments, we have  $rcvd(\alpha_Q(\rho_1), j) = rcd(\alpha_Q(\rho_0), j)$ . Constraint (b) holds. By similar arguments in the proof of Proposition 5.3, for every  $k \in 1..N$ , we have

$$lvar(\alpha_Q(\rho_1), k) = nextVal(pc(\alpha_Q(\rho_0)), \emptyset, lvar(\alpha_Q(\rho_0), k))$$

Constraint (c) holds. It follows  $\alpha_Q(\rho_1) \xrightarrow{csnd(m)} \alpha_Q(\rho'_1)$ .

- *Case  $\rho_0 \xrightarrow{comp} \rho_1$ .* Similar to the case of *csnd*.
- *Case  $\rho_0 \xrightarrow{crash} \rho_1$ .* We have  $pc(\alpha_Q(\rho_1)) = pc(\rho_1)$  and  $pc(\alpha_Q(\rho_0)) = pc(\rho_0)$  by Definition 4.3. By the transitions' assumptions, we have  $pc(\alpha_Q(\rho_1)) = \ell_{crash}$  and  $pc(\alpha_Q(\rho_0)) \neq \ell_{crash}$ . By similar arguments in the case of *csnd*, it follows  $\forall k \in 1..N: rcd(\alpha_Q(\rho_1), k) = rcd(\alpha_Q(\rho_0), k) \wedge lvar(\alpha_Q(\rho_1), k) = lvar(\alpha_Q(\rho_0), k)$ . Hence, it holds  $\alpha_Q(\rho_0) \xrightarrow{crash} \alpha_Q(\rho_1)$ .
- *Case  $\rho \xrightarrow{stutter} \rho'$ .* Similar to the case of *csnd*.

Hence, Proposition 5.4 holds.  $\square$

**5.2. Transpositions and Global Systems.** The proof strategy of Lemma 4.7 is similar to the one of Lemma 4.6, and the proof of Lemma 4.7 requires the following Propositions 5.5, 5.6, 5.7 and 5.8.

**Lemma 4.7.** *Let  $\mathcal{G}_N = (\mathcal{C}_N, Tr_N, R_N, g_N^0)$  be a global transition system. Let  $\alpha$  be a transposition on  $1..N$ , and  $\alpha_C$  be a global transposition based on  $\alpha$  (from Definition 4.4). The following properties hold:*

- (1)  $\alpha_C$  is a bijection from  $\mathcal{C}_N$  to itself.
- (2) The initial configuration is preserved under  $\alpha_C$ , i.e.  $\alpha_C(g_N^0) = g_N^0$ .
- (3) Let  $\kappa$  and  $\kappa'$  be configurations in  $\mathcal{G}_N$ , and  $tr \in Tr_N$  be either a internal transition such that  $\kappa \xrightarrow{tr} \kappa'$ . It follows  $\alpha_C(\kappa) \xrightarrow{tr} \alpha_C(\kappa')$ .
- (4) Let  $\kappa$  and  $\kappa'$  be configurations in  $\mathcal{G}_N$ . If  $\kappa \rightsquigarrow \kappa'$ , then  $\alpha_C(\kappa) \rightsquigarrow \alpha_C(\kappa')$ .

*Proof.* We have: point 1 holds by Proposition 5.5, and point 2 holds by Proposition 5.6, and point 3 holds by Proposition 5.7, and point 4 holds by Proposition 5.8.  $\square$

**Proposition 5.5.** *Let  $\mathcal{G}_N = (\mathcal{C}_N, Tr_N, R_N, g_N^0)$  be a global transition system with indexes  $1..N$ . Let  $\alpha$  be a process-index transposition on  $1..N$ , and  $\alpha_C$  be a global transposition based on  $\alpha$  (from Definition 4.4). Then,  $\alpha_C$  is a bijection from  $\mathcal{C}_N$  to itself.*

*Proof.* By applying similar arguments in the proof of Proposition 5.1.  $\square$

**Proposition 5.6.** *Let  $\mathcal{G}_N = (\mathcal{C}_N, Tr_N, R_N, g_N^0)$  be a global transition system with indexes  $1..N$ . Let  $\alpha$  be a process-index transposition on  $1..N$ , and  $\alpha_C$  be a global transposition based on  $\alpha$  (from Definition 4.4). It follows that  $\alpha_C(g_N^0) = g_N^0$ .*

*Proof.* By applying similar arguments in the proof of Proposition 5.2.  $\square$

**Proposition 5.7.** *Let  $\mathcal{G}_N = (\mathcal{C}_N, Tr_N, R_N, g_N^0)$  be a global transition system with indexes  $1..N$  and a process template  $\mathcal{U}_N = (Q_N, Tr_N, Rel_N, q_N^0)$ . Let  $\alpha$  be a process-index transposition on  $1..N$ , and  $\alpha_C$  be a global transposition based on  $\alpha$  (from Definition 4.4). Let  $\kappa$  and  $\kappa'$  be configurations in  $\mathcal{G}_N$ , and  $tr \in Tr_N$  be an internal transition such that  $\kappa \xrightarrow{tr} \kappa'$ . Then,  $\alpha_C(\kappa) \xrightarrow{tr} \alpha_C(\kappa')$ .*

*Proof.* We prove Proposition 5.7 by case distinction.

(1) *Sub-round Schedule.* We prove that all Constraints (a)–(e) for the sub-round Schedule hold as follows.

First, we focus on Constraint (a). By Proposition 5.5, both  $\alpha_C(\kappa)$  and  $\alpha_C(\kappa')$  are configurations in  $\mathcal{G}_N$ . By Definition 4.4, for every  $i \in 1..N$ , we have  $active(\alpha_C(\kappa), \alpha(i)) = active(\kappa, i)$ . We have  $\neg active(\kappa, i)$  by the semantics of the sub-round Schedule in Section 3.2. It follows  $\neg active(\alpha_C(\kappa), \alpha(i))$ . Hence, the sub-round Schedule can start with a configuration  $\alpha_C(\kappa_0)$ . Constraint (a) holds.

Now we focus on Constraint (b) by examining process transitions. For every  $i \in 1..N$ , by Lemma 4.6, we have

$$lstate(\kappa, i) \xrightarrow{stutter} lstate(\kappa', i) \Rightarrow \alpha_Q(lstate(\kappa, i)) \xrightarrow{stutter} \alpha_Q(lstate(\kappa', i))$$

By Definition 4.4, it follows  $\alpha_Q(lstate(\kappa, i)) = lstate(\alpha_C(\kappa), \alpha(i))$  and  $\alpha_Q(lstate(\kappa', i)) = lstate(\alpha_C(\kappa'), \alpha(i))$ . Hence, it follows

$$\begin{aligned} lstate(\kappa, i) &\xrightarrow{stutter} lstate(\kappa', i) \\ &\Rightarrow lstate(\alpha_C(\kappa), \alpha(i)) \xrightarrow{stutter} lstate(\alpha_C(\kappa'), \alpha(i)) \end{aligned}$$

By similar arguments, we have

$$\begin{aligned} lstate(\kappa, i) &\xrightarrow{crash} lstate(\kappa', k) \\ &\Rightarrow lstate(\alpha_C(\kappa), \alpha(i)) \xrightarrow{crash} lstate(\alpha_C(\kappa'), \alpha(k)) \end{aligned}$$

Hence, every process makes either a crash transition or a stuttering step from a configuration  $\alpha_C(\kappa)$  to a configuration  $\alpha_C(\kappa')$ . Constraint (b) holds.

We now focus on Constraint (c) by examining control components of crashed processes. Assume that  $pc(lstate(\kappa', r)) = \ell_{crash}$  for some  $i \in 1..N$ . By the semantics of the sub-round Schedule in Section 3.2, we have  $\neg active(\kappa', i)$ . By Definition 4.4, it follows  $\neg active(\alpha_C(\kappa), \alpha(i)) \wedge \neg active(\kappa', i)$ . Constraint (c) holds.

Now we focus on Constraint (d) by examining incoming message buffers to correct processes. By Definition 4.4, we have  $buf(\alpha_C(\kappa'), \alpha(s), \alpha(r)) = buf(\kappa', s, r)$  for every  $s, r \in 1..N$ . By the semantic of the sub-round Schedule in Section 3.2, if  $pc(lstate(\kappa', r)) \neq \ell_{crash}$ , then  $buf(\kappa', s, r) = buf(\kappa, s, r)$ . By Definition 4.4, we have  $buf(\kappa, s, r) = buf(\alpha_C(\kappa), \alpha(s), \alpha(r))$ . Hence, Constraint (d) holds since  $buf(\alpha_C(\kappa'), \alpha(s), \alpha(r)) = buf(\alpha_C(\kappa), \alpha(s), \alpha(r))$

Now we focus on Constraint (e) by examining incoming message buffers to a crashed process. Let  $r$  be an index in  $1..N$  such that  $pc(lstate(\kappa', r)) = \ell_{crash}$ . By similar arguments in the above case of  $pc(lstate(\kappa', r)) \neq \ell_{crash}$ , if  $pc(lstate(\kappa', r)) = \ell_{crash}$ , then  $buf(\alpha_C(\kappa'), \alpha(s), \alpha(r)) = buf(\kappa', s, r)$ . By the semantics of the sub-round Schedule in Section 3.2, we have  $buf(\kappa', s, r) = \emptyset$ . It follows  $buf(\alpha_C(\kappa'), \alpha(s), \alpha(r)) = \emptyset$ . Therefore, Constraint (e) holds.

It implies  $\alpha_C(\kappa) \xrightarrow{\text{Sched}} \alpha_C(\kappa')$ .

- (2) *Sub-round Send*. We prove that all Constraints (a)–(c) for the sub-round Send hold as follows. By Definition 4.4, we have

$$\begin{aligned} active(\alpha_C(\kappa), \alpha(i)) &= active(\kappa, i) \\ pc(lstate(\alpha_C(\kappa), \alpha(i))) &= pc(\alpha_Q(lstate(\kappa, i))) \end{aligned}$$

By Definition 4.3, we have  $pc(\alpha_Q(lstate(\kappa, i))) = pc(lstate(\kappa, i))$  for every  $i \in 1..N$ . Hence, we have  $pc(lstate(\alpha_C(\kappa), \alpha(i))) = pc(lstate(\kappa, i))$ . For every  $i \in 1..N$ , we have  $Enabled(\kappa, i, Loc_{snd}) \Leftrightarrow Enabled(\alpha_C(\kappa), \alpha(i), Loc_{snd})$  by the definition of *Enabled* in Section 3.2. It implies that a process  $lstate(\kappa, s)$  is enabled in this sub-round if and only if a process  $lstate(\alpha_C(\kappa), \alpha(s))$  is enabled in this sub-round for every  $s \in 1..N$ .

Now we focus on Constraint (a) by examining processes which are not enabled in this sub-round Send. Let  $i$  be an arbitrary index in  $1..N$  such that  $\neg Enabled(\kappa, i, Loc_{snd})$ . By the semantics of the sub-round Send in Section 3.2, it follows that  $lstate(\kappa, i) \xrightarrow{\text{stutter}} lstate(\kappa', i)$ . By Definition 4.4, we have

$$Enabled(\alpha_C(\kappa), \alpha(i), Loc_{snd}) = Enabled(\kappa, i, Loc_{snd})$$

Since  $\neg Enabled(\kappa, i, Loc_{snd})$  (we are examining inactive processes in this sub-round Send), we have  $\neg Enabled(\alpha_C(\kappa), \alpha(i), Loc_{snd})$ . We prove that

$$Frozen_S(\alpha_C(\kappa), \alpha_C(\kappa'), \alpha(i))$$

as follows. By Definition 4.4, we have

$$\begin{aligned} \alpha_Q(lstate(\kappa, i)) &= lstate(\alpha_C(\kappa), \alpha(i)) \\ \alpha_Q(lstate(\kappa', i)) &= lstate(\alpha_C(\kappa'), \alpha(i)) \end{aligned}$$

By Proposition 5.4, it follows that  $\alpha_Q(lstate(\kappa, i)) \xrightarrow{\text{stutter}} \alpha_Q(lstate(\kappa', i))$ . It follows  $lstate(\alpha_C(\kappa), \alpha(i)) \xrightarrow{\text{stutter}} lstate(\alpha_C(\kappa'), \alpha(i))$ . We now examine the control component for a process  $p_i$ . By Definition 4.4, we have

$$\begin{aligned} active(\kappa, i) &= active(\alpha_C(\kappa), \alpha(i)) \\ active(\kappa', i) &= active(\alpha_C(\kappa'), \alpha(i)) \end{aligned}$$

By definition of  $Frozen_S$  in Section 3.2, we have  $active(\kappa, i) = active(\kappa', i)$ . It follows  $active(\alpha_C(\kappa), \alpha(i)) = active(\alpha_C(\kappa'), \alpha(i))$ . We now show that each outgoing message buffer from a process  $p_i$  is unchanged from  $\alpha_C(\kappa)$  to  $\alpha_C(\kappa')$ . By Definition 4.4, we have

$buf(\alpha_C(\kappa'), \alpha(i), \alpha(\ell)) = buf(\kappa', i, \ell)$ . Since  $buf(\kappa', i, \ell) = buf(\kappa, i, \ell)$ , (we are examining inactive processes in this sub-round Send), it follows  $buf(\alpha_C(\kappa'), \alpha(i), \alpha(\ell)) = buf(\kappa, i, \ell)$ . By Definition 4.4, we have  $buf(\kappa, i, \ell) = buf(\alpha_C(\kappa), \alpha(i), \alpha(\ell))$ . It follows that

$$buf(\alpha_C(\kappa'), \alpha(i), \alpha(\ell)) = buf(\alpha_C(\kappa), \alpha(i), \alpha(\ell))$$

Therefore, it follows  $Frozen_S(\alpha_C(\kappa), \alpha_C(\kappa'), \alpha(i))$ . Constraint (a) holds.

Now we focus on Constraint (b) by examining processes which are enabled in this sub-round Send. Let  $s \in 1..N$  be an arbitrary index such that  $active(\kappa, i)$ . By the semantics of the sub-round Send in Section 3.2, it follows  $lstate(\kappa, s) \xrightarrow{csnd(m)} lstate(\kappa', s)$ . We have  $lstate(\kappa, s) = lstate(\alpha_C(\kappa), \alpha(s))$  and  $lstate(\kappa', s) = lstate(\alpha_C(\kappa'), \alpha(s))$  by Definition 4.4. By Proposition 5.4, it follows

$$lstate(\alpha_C(\kappa), \alpha(s)) \xrightarrow{csnd(m)} lstate(\alpha_C(\kappa'), \alpha(s))$$

We show that  $m$  is new in buffers  $buf(\alpha_C(\kappa), \alpha(s), 1), \dots, buf(\alpha_C(\kappa), \alpha(s), 1)$ . By Definition 4.4, for every  $s, r \in 1..N$ , we have

$$\begin{aligned} buf(\alpha_C(\kappa), \alpha(s), \alpha(r)) &= buf(\kappa, s, r) \\ buf(\alpha_C(\kappa'), \alpha(s), \alpha(r)) &= buf(\kappa', s, r) \end{aligned}$$

We have  $m \notin buf(\kappa, s, r)$  and  $m \in buf(\kappa', s, r)$  by the semantics of the sub-round Send in Section 3.2. It follows

$$m \notin buf(\alpha_C(\kappa), \alpha(s), \alpha(r)) \quad \text{and} \quad m \in buf(\alpha_C(\kappa'), \alpha(s), \alpha(r))$$

In other words, the message  $m$  is new in the buffer  $buf(\alpha_C(\kappa), \alpha(s), \alpha(r))$ . As a result, Constraint (b) holds.

Now we focus on Constraint (c). Let  $s \in 1..N$  be an arbitrary index such that  $Enabled(\kappa, i, Loc_{snd}) = \top$ . By arguments at the beginning of the proof of Proposition 5.15, we have  $Enabled(\alpha_C(\kappa), \alpha(i), Loc_{snd})$ . By the semantics of the sub-round Send in Section 3.2, we have  $\neg active(\kappa', i)$ . By Definition 4.4, we have  $active(\kappa', i) = active(\alpha_C(\kappa'), \alpha(i))$ . It follows  $\neg active(\alpha_C(\kappa'), \alpha(i))$ . Constraint (c) holds.

It implies that  $\alpha_C(\kappa) \xrightarrow{Snd} \alpha_C(\kappa')$ .

- (3) *Sub-round Receive*. By similar arguments in the case of the sub-round Send, we have that Constraints (a) and (c) in the sub-round Receive holds. In the following, we focus on Constraint (b). By similar arguments in the case of the sub-round Send, we have that a process  $lstate(\kappa, s)$  is enabled in this sub-round Receive if and only if a process  $lstate(\alpha_C(\kappa), \alpha(s))$  is enabled in this sub-round Receive for every  $s \in 1..N$ . Hence, we focus on processes which are enabled in this sub-round Receive. Let  $r \in 1..N$  be an index such that  $Enabled(\kappa, i, Loc_{rcv})$ . By the semantics of the sub-round Receive in Section 3.2, we have  $lstate(\kappa, r) \xrightarrow{crcv(S_1, \dots, S_N)} lstate(\kappa', r)$  for some sets  $S_1, \dots, S_N \subseteq \text{Set}(\text{Msg})$  of messages. By Definition 4.3, we have

$$\begin{aligned} \alpha_Q(lstate(\kappa, r)) &= lstate(\alpha_C(\kappa), \alpha(r)) \\ \alpha_Q(lstate(\kappa', r)) &= lstate(\alpha_C(\kappa'), \alpha(r)) \end{aligned}$$

By Proposition 5.3, it follows

$$lstate(\alpha_C(\kappa), \alpha(r)) \xrightarrow{\alpha_R(crcv(S_1, \dots, S_N))} lstate(\alpha_C(\kappa'), \alpha(r))$$

Now we focus on the update of message buffers. By the semantics of the sub-round Receive in Section 3.2, we have  $S_s \subseteq \text{buf}(\kappa, s, r)$  for every  $s \in 1..N$ . By Definition 4.4, we have  $\text{buf}(\kappa, s, r) = \text{buf}(\alpha_C(\kappa), \alpha(s), \alpha(r))$ . It follows that  $S_s \subseteq \text{buf}(\alpha_C(\kappa), \alpha(s), \alpha(r))$  for every  $s \in 1..N$ . We now prove that for every  $s \in 1..N$ ,  $S_s$  is removed from the message buffer  $\text{buf}(\alpha_C(\kappa'), \alpha(s), \alpha(r))$ . By Definition 4.4, we have

$$\begin{aligned} \text{buf}(\alpha_C(\kappa'), \alpha(s), \alpha(r)) &= \text{buf}(\kappa', s, r) \\ \text{buf}(\alpha_C(\kappa), \alpha(s), \alpha(r)) &= \text{buf}(\kappa, s, r) \end{aligned}$$

By the semantics of the sub-round Receive in Section 3.2, we have

$$\begin{aligned} S_s \cap \text{buf}(\kappa', s, r) &= \emptyset \\ \text{buf}(\kappa, s, r) &= \text{buf}(\kappa', s, r) \cup S_s \end{aligned}$$

It follows that

$$\begin{aligned} S_s \cap \text{buf}(\alpha_C(\kappa'), \alpha(s), \alpha(r)) &= \emptyset \\ \text{buf}(\alpha_C(\kappa), \alpha(s), \alpha(r)) &= \text{buf}(\alpha_C(\kappa'), \alpha(s), \alpha(r)) \cup S_s \end{aligned}$$

Constraint (b) holds. It implies that  $\alpha_C(\kappa') \xrightarrow{\text{Rcv}} \alpha_C(\kappa)$ .

(4) *Sub-round Computation.* By applying similar arguments in above sub-rounds.

Therefore, Proposition 5.7 holds.  $\square$

**Proposition 5.8.** *Let  $\mathcal{G}_N = (\mathcal{C}_N, \text{Tr}_N, R_N, g_N^0)$  be a global transition system with indexes  $1..N$  and a process template  $\mathcal{U}_N = (Q_N, \text{Tr}_N, \text{Rel}_N, q_N^0)$ . Let  $\kappa$  and  $\kappa'$  be configurations in  $\mathcal{G}_N$  such that  $\kappa \rightsquigarrow \kappa'$ . Let  $\alpha$  be a transposition on  $1..N$ , and  $\alpha_C$  be a global transposition based on  $\alpha$  (from Definition 4.4). It follows  $\alpha_C(\kappa) \rightsquigarrow \alpha_C(\kappa')$ .*

*Proof.* It immediately follows by Proposition 5.7 and the fact that for all  $i \in 1..N$ , we have  $\text{active}(\alpha_C(\kappa), \alpha(i)) = \text{active}(\kappa, i)$ .  $\square$

**5.3. Trace Equivalence of  $\mathcal{G}_2$  and  $\mathcal{G}_N$  under  $AP_{\{1,2\}}$ .** Recall that  $\mathcal{G}_2$  and  $\mathcal{G}_N$  are two global transition systems of 2 and  $N$  processes, respectively, such that every correct process runs the same arbitrary symmetric point-to-point algorithm, and a set  $AP_{\{1,2\}}$  contains predicates that takes one of the forms:  $P_1(1)$ ,  $P_2(2)$ ,  $P_3(1,2)$ , or  $P_4(2,1)$  where 1 and 2 are process indexes.

**Proposition 5.9.** *Let  $\mathcal{A}$  be an arbitrary symmetric point-to-point algorithm. Let  $\mathcal{U}_2$  and  $\mathcal{U}_N$  be two process templates of  $\mathcal{A}$  for some  $N \geq 2$ , and  $\rho^N \in Q_N$  be a state of  $\mathcal{U}_N$ . Let  $\rho^2$  be a tuple that is the application of Construction 4.8 to  $\rho^N$  and indexes  $\{1,2\}$ . Then,  $\rho^2$  is a template state of  $\mathcal{U}_2$ .*

*Proof.* It immediately follows by Construction 4.8.  $\square$

**Proposition 5.10.** *Let  $\mathcal{A}$  be an arbitrary symmetric point-to-point algorithm. Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be two global transition systems of two instances of  $\mathcal{A}$  for some  $N \geq 2$ , and  $\kappa^N \in \mathcal{C}_N$  be a global configuration in  $\mathcal{G}_N$ . Let  $\kappa^2$  be a tuple that is the application of Construction 4.9 to  $\kappa^N$  and indexes  $\{1,2\}$ . Then,  $\kappa^2$  is a global configuration of  $\mathcal{G}_2$ .*

*Proof.* It immediately follows by Construction 4.9.  $\square$



**Lemma 4.10.** *Let  $\mathcal{A}$  be a symmetric point-to-point algorithm. Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be two transition systems such that all processes in  $\mathcal{G}_2$  and  $\mathcal{G}_N$  follow  $\mathcal{A}$ , and  $N \geq 2$ . Let  $\pi^N = \kappa_0^N \kappa_1^N \dots$  be an admissible sequence of configurations in  $\mathcal{G}_N$ . Let  $\pi^2 = \kappa_0^2 \kappa_1^2 \dots$  be a sequence of configurations in  $\mathcal{G}_2$  such that  $\kappa_k^2$  is the index projection of  $\kappa_k^N$  on indexes  $\{1, 2\}$  for every  $k \geq 0$ . Then,  $\pi^2$  is admissible in  $\mathcal{G}_2$ .*

The proof of Lemma 4.10 requires the following propositions:

- (1) Proposition 5.11 says that the application of Construction 4.8 to an initial template state of  $\mathcal{G}_N$  constructs an initial template state of  $\mathcal{G}_2$ .
- (2) Lemmas 5.12 and 5.13 say that Construction 4.8 preserves the process transition relation.
- (3) Proposition 5.14 says that the application of Construction 4.9 to an initial global configuration of  $\mathcal{G}_N$  constructs an initial global configuration of  $\mathcal{G}_2$ .
- (4) Propositions 5.15 and 5.16 say Construction 4.9 preserves the global transition relation. Proposition 5.15 captures internal transitions. Proposition 5.16 captures round transitions.

*Proof of Lemma 4.10.* It is easy to check that Lemma 4.10 holds by Propositions 5.11, 5.13, 5.14, 5.15, and 5.16. The detailed proofs of these propositions are given below.

**Proposition 5.11.** *Let  $\mathcal{A}$  be an arbitrary symmetric point-to-point algorithm. Let  $\mathcal{U}_N = (Q_N, Tr_N, Rel_N, q_N^0), \mathcal{U}_2 = (Q_2, Tr_2, Rel_2, q_2^0)$  be two process templates of  $\mathcal{A}$  for some  $N \geq 2$ . It follows that  $q_2^0$  is the index projection of  $q_N^0$  on indexes  $\{1, 2\}$ .*

*Proof.* It follows by Construction 4.8 and the definition of  $q_2^0$  in Section 3.1.  $\square$

**Proposition 5.12.** *Let  $\mathcal{A}$  be an arbitrary symmetric point-to-point algorithm, and  $\mathcal{U}_2$  and  $\mathcal{U}_N$  be process templates of  $\mathcal{A}$ . Let  $\rho_0$  and  $\rho_1$  be template states in  $\mathcal{U}_N$  such that  $\rho_0 \xrightarrow{crev(S_1, \dots, S_N)} \rho_1$  for some sets  $S_1, \dots, S_N$  of messages. Let  $\rho'_0$  and  $\rho'_1$  be template states of  $\mathcal{U}_2$  such that they are constructed with Construction 4.9 and based on configurations  $\rho_0$  and  $\rho_1$  and indexes  $\{1, 2\}$ . It follows  $\rho'_0 \xrightarrow{rcv(S_1, S_2)} \rho'_1$ .*

*Proof.* We prove that all Constraints (a)–(c) for the transition  $csnd$  defined in Section 3.1 hold. First, we focus on Constraint (a). We have  $pc(\alpha_Q(\rho_1)) = pc(\rho_1)$  by Definition 4.3. We have  $pc(\rho_1) = nextLoc(pc(\rho_0))$  by the semantics of  $crev(S_1, \dots, S_N)$  in Section 3.1. We have  $nextLoc(pc(\rho_0)) = nextLoc(pc(\rho'_0))$  by Definition 4.3. Hence, it follows  $pc(\alpha_Q(\rho_1)) = nextLoc(pc(\alpha_Q(\rho_0)))$ . Moreover, we have  $\emptyset = genMsg(pc(\rho_0))$  by the semantics of  $crev$  in Section 3.1. By Construction 4.8, we have  $genMsg(pc(\rho_0)) = genMsg(pc(\rho'_0))$ . It follows that  $genMsg(pc(\rho'_0)) = \emptyset$ . Constraint (a) holds.

We now check components related to received messages (Constraint (b)). Let  $i$  be an arbitrary index in 1..2. It follows

$$\begin{aligned}
& rvd(\rho'_1, i) \\
&= rvd(\rho_1, i) \quad (\text{by Construction 4.8}) \\
&= rvd(\rho_0, i) \cup S_i \quad (\text{by the semantics of } crev(S_1, \dots, S_N) \text{ in Section 3.1}) \\
&= rvd(\rho'_0, i) \cup S_i \quad (\text{by Construction 4.8})
\end{aligned}$$

Hence, we have  $\forall i \in 1..2: rvd(\rho'_1, i) = rvd(\rho'_0, i) \cup S_i$ . Constraint (b) holds. Moreover, by similar arguments in the proof of Proposition 5.3, we have

$$\forall i \in 1..2: lvar(\rho'_1, i) = nextVal(pc(\rho'_0), S_i, lvar(\rho'_0, i))$$

Constraint (c) holds. It follows  $\rho'_0 \xrightarrow{rcv(S_1, S_2)} \rho'_1$ .  $\square$

**Proposition 5.13.** *Let  $\mathcal{A}$  be an arbitrary symmetric point-to-point algorithm, and  $\mathcal{U}_2$  and  $\mathcal{U}_N$  be process templates of  $\mathcal{A}$ . Let  $tr \in Tr_N$  be a transition such that it is one of send, computation, crash or stuttering transitions. Let  $\rho_0$  and  $\rho_1$  be template states in  $\mathcal{U}_N$  such that  $\rho_0 \xrightarrow{tr} \rho_1$ . Let  $\rho'_0$  and  $\rho'_1$  be states of  $\mathcal{U}_2$  such that they are the index projection of  $\rho_0$  and  $\rho_1$  on indexes  $\{1, 2\}$ , respectively. Then,  $\rho'_0 \xrightarrow{tr} \rho'_1$ .*

*Proof.* By similar arguments in the proof of Lemma 5.12.  $\square$

Now we turn to properties of global configurations under Constructions 4.9.

**Proposition 5.14.** *Let  $\mathcal{A}$  be an arbitrary symmetric point-to-point algorithm. Let  $\mathcal{G}_N = (\mathcal{C}_N, Tr_N, R_N, g_N^0)$  and  $\mathcal{G}_2 = (\mathcal{C}_2, Tr_2, R_2, g_2^0)$  be two transition systems of two instances of  $\mathcal{A}$  for some  $N \geq 2$ . It follows that  $g_2^0$  is the index projection of  $g_N^0$  on indexes  $\{1, 2\}$ .*

*Proof.* It immediately follows by Construction 4.9 and the definition of  $g_N^0$ .  $\square$

**Proposition 5.15.** *Let  $\mathcal{A}$  be an arbitrary symmetric point-to-point algorithm. Let  $\mathcal{G}_2 = (\mathcal{C}_2, Tr_2, R_2, g_2^0)$  and  $\mathcal{G}_N = (\mathcal{C}_N, Tr_N, R_N, g_N^0)$  be global transition systems such that all processes in  $\mathcal{G}_2$  and  $\mathcal{G}_N$  follow the same algorithm  $\mathcal{A}$  for some  $N \geq 2$ . Let  $\kappa_0$  and  $\kappa_1$  be global configurations in  $\mathcal{G}_N$  such that  $\kappa_0 \xrightarrow{tr} \kappa_1$  where  $tr$  is an internal transition. Let  $\kappa'_0$  and  $\kappa'_1$  be the index projection of  $\kappa_0$  and  $\kappa_1$  on a set  $\{1, 2\}$  of indexes, respectively. It follows that  $\kappa'_0 \xrightarrow{tr} \kappa'_1$ .*

*Proof.* First, by Proposition 5.10, both  $\rho'_0$  and  $\rho'_1$  are configurations in  $\mathcal{G}_2$ . We prove Proposition 5.15 by case distinction. Here we provide detailed proofs only of two sub-rounds Schedule and Send. The proofs of other sub-rounds are similar.

- *Sub-round Schedule.* We prove that all Constraints (a)–(c) hold in  $\kappa'_0$  and  $\kappa'_1$ . We now focus on Constraint (a). We have  $active(\kappa'_0, 1) = active(\kappa_0, 1)$  and  $active(\kappa_0, 2) = active(\kappa_0, 2)$  by Construction 4.9. By the semantics of the sub-round Schedule in Section 3.2, we have  $\neg active(\kappa_0, 1) \wedge \neg active(\kappa_0, 2)$ . Hence, it follows  $\neg active(\kappa'_0, 1) \wedge \neg active(\kappa'_0, 2)$ . Hence, the sub-round Schedule can start with a configuration  $\kappa'_0$ . Constraint (a) holds. By Proposition 5.13, Constraint (b) holds. Constraint (c) holds by Construction 4.9. Now we focus on incoming message buffers to correct processes to prove Constraint (d). Let  $r$  be an index in  $1..N$  such that  $pc(lstate(\kappa'_1, r)) \neq \ell_{crash}$ . By Construction 4.9, for every  $s \in 1..2$ , we have  $buf(\kappa'_1, s, r) = buf(\kappa_1, s, r)$  and  $buf(\kappa_0, s, r) = buf(\kappa'_0, s, r)$ . By the semantics of the sub-round Schedule in Section 3.2, we have  $buf(\kappa_1, s, r) = buf(\kappa_0, s, r)$  for every  $s \in 1..2$ . It follows  $buf(\kappa'_1, s, r) = buf(\kappa'_0, s, r)$  for every  $s \in 1..2$ . Constraint (d) holds. Now we focus on message buffers to crashed processes to prove Constraint (d). Let  $r$  be an index in  $1..N$  such that  $pc(lstate(\kappa'_1, r)) = \ell_{crash}$ . By Construction 4.9, for every  $s \in 1..2$ , we have  $buf(\kappa'_1, s, r) = buf(\kappa_1, s, r)$ . By the semantics of the sub-round Schedule in Section 3.2, we have  $buf(\kappa_1, s, r) = \emptyset$  for every  $s \in 1..2$ . It follows  $buf(\kappa'_1, s, r) = \emptyset$  for every  $s \in 1..2$ . Constraint (e) holds. It implies that  $\kappa'_0 \xrightarrow{Sched} \kappa'_1$ .
- *Sub-round Send.* We have  $active(\kappa'_0, 1) = active(\kappa_0, 1)$  and  $active(\kappa_0, 2) = active(\kappa_0, 2)$  for every  $k \in 1..2$ . Hence, if a process  $p_i^N$  in  $\mathcal{G}_N$  is enabled in this sub-round, a corresponding process  $p_i^2$  in  $\mathcal{G}_2$  is also for every  $i \in 1..2$ . We prove that all Constraints (a)–(c) between  $\kappa'_0$  and  $\kappa'_1$  for the sub-round Send defined in Section 3.2 hold. By similar arguments in the proof of Proposition 5.15, Constraint (a) holds. Now we focus on enable processes to prove Constraints (b) and (c).

Assume that a process  $p_i^N$  in  $\mathcal{G}_N$  has sent a message  $m$  in this sub-round, we show that a process  $p_i^2$  in  $\mathcal{G}_2$  has also sent the message  $m$  in this sub-round where  $i \in 1..2$ .

By Proposition 5.13, it follows that  $lstate(\kappa'_0, i) \xrightarrow{csnd(m)} lstate(\kappa'_1, i)$ . Now we show that the message  $m$  is new in buffers  $buf(\kappa'_1, i, 1)$  and  $buf(\kappa'_1, i, 2)$ . By Construction 4.9, we have  $buf(\kappa'_1, i, \ell) = buf(\kappa_1, i, \ell)$  and  $buf(\kappa'_0, i, \ell) = buf(\kappa_0, i, \ell)$  for every  $\ell \in 1..2$ . By the semantics of the sub-round Send in Section 3.2, we have  $buf(\kappa_1, i, \ell) = \{m\} \cup buf(\kappa_0, i, \ell)$ . It follows  $buf(\kappa'_1, i, \ell) = \{m\} \cup buf(\kappa'_0, i, \ell)$  for every  $\ell \in 1..2$ . Moreover, since  $m \notin buf(\kappa_0, i, \ell)$  for every  $\ell \in 1..2$ , we have  $m \notin buf(\kappa'_0, i, \ell)$ . Therefore, the message  $m$  is new in a buffer  $buf(\kappa'_1, i, \ell)$  for every  $\ell \in 1..2$ . Constraint (b) holds. Moreover, by Construction 4.9, we have  $active(\kappa_1, i) = active(\kappa'_1, i)$ . We have  $\neg active(\kappa_1, i)$  by the semantics of the sub-round Send in Section 3.2. It follows  $\neg active(\kappa'_1, i)$ . Constraint (e) holds. It follows that  $\kappa'_0 \xrightarrow{Snd} \kappa'_1$ .

- *Sub-rounds Receive and Computation.* Similar.

Therefore, Proposition 5.15 holds.  $\square$

**Proposition 5.16.** *Let  $\mathcal{A}$  be an arbitrary symmetric point-to-point algorithm. Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be global transition systems of  $\mathcal{A}$  for some  $N \geq 2$ . Let  $\kappa_0$  and  $\kappa_1$  be global configurations of  $\mathcal{C}_N$  such that  $\kappa_0 \rightsquigarrow \kappa_1$ . Let  $\kappa'_0$  and  $\kappa'_1$  be the index projection of  $\kappa_0$  and  $\kappa_1$  on indexes  $\{1, 2\}$ . Then,  $\kappa'_0 \rightsquigarrow \kappa'_1$ .*

*Proof.* It immediately follows by Propositions 5.13 and 5.15.  $\square$

Now we present how to construct an admissible path of  $\mathcal{G}_N$  from a given admissible path of  $\mathcal{G}_2$  with Lemma 4.12 below. The main argument is that from an admissible sequence of configurations in  $\mathcal{G}_2$ , we can get an admissible sequence of configurations in  $\mathcal{G}_N$  by letting processes 3 to  $N$  be initially crashed. The proof of Lemma 4.12 requires the preliminary Propositions 5.17 and 5.18.

**Proposition 5.17.** *Let  $\mathcal{A}$  be an arbitrary symmetric point-to-point algorithm. Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be global transition systems of  $\mathcal{A}$  for some  $N \geq 2$ . Let  $\kappa^2$  be a configuration in  $\mathcal{G}_2$ . There exists a configuration  $\kappa^N$  in  $\mathcal{G}_N$  such that the following properties hold:*

- $\kappa^2$  is the index projection of  $\kappa^N$  on indexes  $\{1, 2\}$ , and
- $\forall i \in 3..N: pc(lstate(\kappa^N, i)) = \ell_{crash} \wedge \neg active(\kappa^N, i)$
- $\forall s \in 3..N, r \in 1..N: buf(\kappa, s, r) = \emptyset$
- $\forall s \in 3..N, r \in 1..2: rcvd(lstate(\kappa^N, s), r) = \emptyset$
- $\forall s \in 1..N, r \in 3..N: buf(\kappa, s, r) = \emptyset$

*Proof.* Proposition 5.17 is true since our construction simply adds  $N - 2$  crashed processes that have not sent any messages in the global system. The last two constraints requires that processes 1 and 2 have not received any messages from crashes processes and the message buffers to crashed processes are empty. Other components are arbitrary.  $\square$

**Proposition 5.18.** *Let  $\mathcal{A}$  be an arbitrary symmetric point-to-point algorithm. Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be global transition systems of  $\mathcal{A}$  for some  $N \geq 2$ . Let  $\kappa_0^2$  and  $\kappa_1^2$  be configurations in  $\mathcal{G}_2$  such that  $\kappa_0^2 \xrightarrow{tr} \kappa_1^2$  where  $tr$  is an internal transition. There exists two configurations  $\kappa_0^N$  and  $\kappa_1^N$  in  $\mathcal{G}_N$  such that*

- (1)  $\kappa_0^2$  and  $\kappa_1^2$  are respectively the index projection of  $\kappa_0^N$  and  $\kappa_1^N$  on a set  $\{1, 2\}$  of indexes, and
- (2)  $\kappa_0^N \xrightarrow{tr} \kappa_1^N$ .

*Proof.* By Proposition 5.17, there exists a configuration  $\kappa_0^N$  in  $\mathcal{G}_N$  such that (i)  $\kappa_0^2$  is the index projection of  $\kappa_0^N$  on indexes  $\{1, 2\}$ , and (ii) all processes with indexes in  $3..N$  are crashed and inactive in  $\kappa_0^N$ , and (iii) every process  $p_i$  has not received any messages from a process  $p_j$  where  $i \in \{1, 2\}, j \in 3..N$  (as the configuration construction in the proof of Proposition 5.17).

We construct  $\kappa_1^N$  as the following. Intuitively, this construction keeps process  $3..N$  crashed, and two processes 1 and 2 in  $\mathcal{G}_N$  make similar transitions with processes 1 and 2 in  $\mathcal{G}_2$ .

- (1)  $\forall i \in 3..N: lstate(\kappa_1^N, i) = lstate(\kappa_0^N, i) \wedge \neg active(\kappa_1^N, i)$ .
- (2)  $\forall s \in 1..N, r \in 3..N: buf(\kappa_1^N, s, r) = \emptyset$
- (3)  $\forall i \in \{1, 2\}: active(\kappa_1^N, i) = active(\kappa_1^2, i)$
- (4)  $\forall s \in 3..N, r \in 1..N: rcvd(lstate(\kappa_1^N, s), r) = \emptyset$
- (5)  $\forall s, r \in \{1, 2\}: buf(\kappa_1^N, s, r) = buf(\kappa_1^2, s, r)$
- (6) For every  $s \in \{1, 2\}$ , we have: If  $lstate(\kappa_0^2, s) \xrightarrow{csnd(m)} lstate(\kappa_1^2, s)$  for some  $m \in \text{Msg}$ , then  $buf(\kappa_1^N, s, r) = \{m\} \cup buf(\kappa_0^N, s, r)$  for every  $3 \leq r \leq N$ . Otherwise,  $buf(\kappa_1^N, s, r) = buf(\kappa_0^N, s, r)$ .
- (7) For every  $i \in \{1, 2\}$ , the configurations of processes with index  $i$  is updated as following:
  - $pc(lstate(\kappa_1^N, i)) = pc(lstate(\kappa_1^2, i))$
  - $\forall j \in \{1, 2\}: rcvd(lstate(\kappa_1^N, i), j) = rcvd(lstate(\kappa_1^2, i), j)$
  - $\forall j \in \{1, 2\}: lvar(lstate(\kappa_1^N, i), j) = lvar(lstate(\kappa_1^2, i), j)$
  - $\forall j \in 3..N: rcvd(lstate(\kappa_1^N, i), j) = rcvd(lstate(\kappa_0^N, i), j) = \emptyset$
  - $\forall j \in 3..N: lvar(lstate(\kappa_1^N, i), j) = nextVal(pc(lstate(\kappa_0^N, i)), \emptyset, lvar(lstate(\kappa_0^N, i), j))$

By the construction of  $\kappa_1^N$ , it follows that  $\kappa_1^N$  is a configuration in  $\mathcal{G}_N$ . Moreover, we have  $lstate(\kappa_0^N, i) \xrightarrow{stutter} lstate(\kappa_1^N, i)$  and  $lstate(\kappa_0^N, i)$  is crashed for every  $i \in 3..N$ . Moreover, no message from a process  $p_i$  has been sent or received for every  $i \in 3..N$ .

By the above construction, it immediately follows that  $\kappa_1^2$  is the index projection  $\kappa_1^N$  on indexes  $\{1, 2\}$ . Hence, point 1 in Proposition 5.18 holds. We prove point 2 in Proposition 5.18 by case distinction.

- *Sub-round Schedule.* By similar arguments in the proof of Proposition 5.15 and the construction of  $\kappa_1^N$ , we have  $\kappa_1^N \xrightarrow{stutter} c_2^N$ .
- *Sub-round Send.* By construction of  $\kappa_0^N$  and  $\kappa_1^N$ , we know that every process  $p_i$  is crashed, and its state is not updated, and every outgoing message buffer from  $p_i$  is always empty for every  $i \in 3..N$ . Therefore, in the following, we focus on only two processes  $p_1$  and  $p_2$ . For every  $i \in 1..2$ , if  $\neg Enabled(c_0^N, c_1^N, Loc_{snd})$ , it follows  $Frozen_S(\kappa_0^N, \kappa_1^N, i)$  by the construction of configurations  $\kappa_0^N$  and  $\kappa_1^N$ . Constraint (a) holds. We now focus on enabled processes in this sub-round. Let  $i$  be an index in  $1..2$  such that  $Enabled(c_0^N, c_1^N, Loc_{snd})$ . By the semantics of the sub-round Send in Section 3.1, we have  $lstate(\kappa_0, i) \xrightarrow{csnd(m)} lstate(\kappa_1, i)$ . We prove that  $lstate(\kappa_0^N, i) \xrightarrow{csnd(m)} lstate(\kappa_1^N, i)$  as follows. By the construction of  $\kappa_0^N$ , we have that  $pc(lstate(\kappa_0^N, i)) = pc(lstate(\kappa_0, i))$ . By the construction of  $\kappa_1^N$ , we have that  $pc(lstate(\kappa_1^N, i)) = pc(lstate(\kappa_1, i))$ . By the semantics of the transition  $csnd(m)$  in Section 3.1, we have  $pc(lstate(\kappa_1, i)) = nextLoc(pc(lstate(\kappa_0, i)))$ . It follows that

$$pc(lstate(\kappa_1^N, i)) = nextLoc(pc(lstate(\kappa_0^N, i)))$$

By similar arguments, it follows  $\{m\} = \text{genMsg}(pc(\text{lstate}(\kappa_0^N, i)))$ . Now we focus on received messages of a process  $p_i$ . By the semantics of the transtion  $\text{csnd}(m)$  in Section 3.1, we have  $\text{rcvd}(\text{lstate}(\kappa_1^2, i), j) = \text{rcvd}(\text{lstate}(\kappa_0^2, i), j)$ . For every  $j \in \{1, 2\}$ , we have

$$\begin{aligned} & \text{rcvd}(\text{lstate}(\kappa_1^N, i), j) \\ &= \text{rcvd}(\text{lstate}(\kappa_1, i), j) \quad (\text{by the construction of } \kappa_1^N) \\ &= \text{rcvd}(\text{lstate}(\kappa_0, i), j) \quad (\text{by the semantics of } \text{csnd}(m) \text{ in Section 3.1}) \\ &= \text{rcvd}(\text{lstate}(\kappa_0^N, i), j) \quad (\text{by the construction of } \kappa_0^N) \end{aligned}$$

For every  $j \in 3..N$ , we have

$$\begin{aligned} \text{rcvd}(\text{lstate}(\kappa_1^N, i), j) &= \emptyset && (\text{by the construction of } \kappa_1^N) \\ &= \text{rcvd}(\text{lstate}(\kappa_0^N, i), j) && (\text{by the construction of } \kappa_0^N) \end{aligned}$$

Hence, a process  $p_i$  does not receive any message when taking a step from  $\kappa_0^N$  to  $\kappa_1^N$ . By the construction of  $\kappa_1^N$ , it follows

$$\begin{aligned} & \text{lvar}(\text{lstate}(\kappa_1^N, i), j) \\ &= \text{nextVal}(pc(\text{lstate}(\kappa_0^N, i)), \emptyset, \text{lvar}(\text{lstate}(\kappa_0^N, i), j)) \end{aligned}$$

for every  $j \in 1..N$ . Hence, it follows  $\text{lstate}(\kappa_0^N, i) \xrightarrow{\text{csnd}(m)} \text{lstate}(\kappa_1^N, i)$ . Now we focus on outgoing message buffers from  $p_i$ . It is easy to see that the message  $m$  is new in every message buffer  $\text{buf}(\kappa_1^2, i, j)$ . By construction of  $\kappa_0^N$  and  $\kappa_1^N$ , it follows that  $m \notin \text{buf}(\kappa_0^N, i, j)$  and  $m \in \text{buf}(\kappa_1^N, i, j)$ . By similar arguments, we have  $\text{buf}(\kappa_0^N, i, j) = \{m\} \cup \text{buf}(\kappa_1^N, i, j)$ . Hence, Constraint (b) between  $\kappa_0^N$  and  $\kappa_1^N$  in the sub-round Send in Section 3.2 hold. Moreover, by the construction of  $\kappa_1^N$ , we have  $\text{active}(\kappa_1^N, i) = \text{active}(\kappa_1, i)$ . By the semantics of the sub-round Send in Section 3.2, we have  $\neg \text{active}(\kappa_1, i)$ . It follows  $\neg \text{active}(\kappa_1^N, i)$ . Constraint (c) between  $\kappa_0^N$  and  $\kappa_1^N$  in the sub-round Send in Section 3.2 holds. Therefore, it follows  $\kappa_0^N \xrightarrow{\text{Snd}} \kappa_1^N$ .

- *Case*  $\kappa_0 \xrightarrow{\text{Rcv}} \kappa_1$ . It follows by similar arguments of the sub-round Send, except that if  $\text{lstate}(\kappa_0, i) \xrightarrow{\text{rcv}(S_1, S_2)} \text{lstate}(\kappa_1, i)$ , then

$$\text{lstate}(\kappa_0^N, i) \xrightarrow{\text{rcv}(S_1, S_2, \emptyset, \dots, \emptyset)} \text{lstate}(\kappa_1^N, i)$$

- *Case*  $\kappa_0 \xrightarrow{\text{Comp}} \kappa_1$ . By similar arguments in the case of the sub-round Send. Then, Proposition 5.18 holds. □

Notice that in Proposition 5.18, if both  $p_1^N$  and  $p_2^N$  take a stuttering step from  $\kappa_0^N$  to  $\kappa_1^N$ , then  $\kappa_0^N = \kappa_1^N$ .

**Lemma 4.12.** *Let  $\mathcal{A}$  be an arbitrary symmetric point-to-point algorithm. Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be global transition systems of  $\mathcal{A}$  for some  $N \geq 2$ . Let  $\pi^2 = \kappa_0^2 \kappa_1^2 \dots$  be an admissible sequence of configurations in  $\mathcal{G}_2$ . There exists an admissible sequence  $\pi^N = \kappa_0^N \kappa_1^N \dots$  of configurations in  $\mathcal{G}_N$  such that  $\kappa_i^2$  is the index projection of  $\kappa_i^N$  on indexes  $\{1, 2\}$  for every  $i \geq 0$ .*

*Proof.* We prove Lemma 4.12 by inductively constructing  $\kappa_k^N$ .

*Base case.* Since  $\pi^2$  and  $\pi^N$  are admissible sequences, it follows  $\kappa_0^2 = g_2^0$  and  $\kappa_0^N = g_N^0$ . By Proposition 5.14, we have that  $\kappa_0^2$  is the index projection of  $\kappa_0^N$  on indexes  $\{1, 2\}$ . We construct  $\kappa_1^N$  by scheduling that all processes  $3..N$  crash in  $\kappa_1^N$ . Formally, we have:

- (1)  $\forall i \in 3..N: pc(lstate(\kappa_1^N, i)) = \ell_{crash} \wedge \neg active(\kappa_1^N, i)$ .
- (2)  $\forall i \in \{1, 2\}: active(\kappa_1^N, i) = active(\kappa_1^2, i) \wedge pc(lstate(\kappa_1^N, i)) = pc(lstate(\kappa_1^2, i))$
- (3)  $\forall s, r \in 1..N: buf(\kappa_1^N, s, r) = buf(\kappa_0^N, s, r)$
- (4)  $\forall s, r \in 1..N: rcvd(lstate(\kappa_1^N, s), r) = rcvd(lstate(\kappa_0^N, s), r)$
- (5)  $\forall s, r \in 1..N: lvar(lstate(\kappa_1^N, s), r) = lvar(lstate(\kappa_0^N, s), r)$

The above constraints ensure that  $\kappa_0^N \xrightarrow{\text{Sched}} \kappa_1^N$ .

*Induction step.* It immediately follows by Proposition 5.18.

Hence, Lemma 4.12 holds.  $\square$

**Lemma 4.13.** *Let  $\mathcal{A}$  be a symmetric point-to-point algorithm. Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be its instances for some  $N \geq 2$ . Let  $AP_{\{1,2\}}$  be a set of predicates that take one of the forms:  $P_1(1)$ ,  $P_2(2)$ ,  $P_3(1,2)$  or  $P_4(2,1)$ . It follows that  $\mathcal{G}_2$  and  $\mathcal{G}_N$  are trace equivalent under  $AP_{\{1,2\}}$ .*

*Proof.* It immediately follows by Definition 4.11, Lemma 4.10 and Lemma 4.12.  $\square$

**5.4. Trace Equivalence of  $\mathcal{G}_1$  and  $\mathcal{G}_N$  under  $AP_{\{1\}}$ .** Lemma 5.21 says that two global transition systems  $\mathcal{G}_1$  and  $\mathcal{G}_N$  whose processes follow an arbitrary symmetric point-to-point algorithm are trace equivalent under a set  $AP_{\{1\}}$  of predicates which inspect only variables whose index is 1. The proof of Lemma 5.21 is similar to one of Lemma 5.21, but applies Constructions 5.19 and 5.20. Constructions 5.19 and 5.20 are respectively similar to Constructions 4.8 and 4.9, but focus on only an index 1. Constructions 5.19 and 5.20 are used in the proof of Lemma 5.21.

**Construction 5.19.** *Let  $\mathcal{A}$  be an arbitrary symmetric point-to-point algorithm. Let  $\mathcal{U}_N$  be a process template of  $\mathcal{A}$  for some  $N \geq 2$ , and  $\rho^N$  be a template state of  $\mathcal{U}_N$ . We construct a tuple  $\rho^1 = (pc_1, rcvd_1, v_1)$  based on  $\rho^N$  and a set  $\{1\}$  of process indexes in the following way:  $pc_1 = pc(\rho^N)$ ,  $rcvd_1 = rcvd(\rho^N, 1)$ , and  $v_1 = lvar(\rho^N, 1)$ .*

**Construction 5.20.** *Let  $\mathcal{A}$  be a symmetric point-to-point algorithm. Let  $\mathcal{G}_1$  and  $\mathcal{G}_N$  be two global transitions of two instances of  $\mathcal{A}$  for some  $N \geq 1$ , and  $\kappa^N \in \mathcal{C}_N$  be a global configuration in  $\mathcal{G}_N$ . We construct a tuple  $\kappa^2 = (s_1, buf_1^1, act_1)$  based on  $\kappa^N$  and a set  $\{1\}$  in the following way:  $s_1$  is constructed from  $lstate(\kappa^N, 1)$  with Construction 5.19 and an index 1, and  $buf_1^1 = buf(\kappa^N, 1, 1)$ , and  $act_1 = active(\kappa^N, 1)$ .*

**Lemma 5.21.** *Let  $\mathcal{A}$  be a symmetric point-to-point algorithm. Let  $\mathcal{G}_1$  and  $\mathcal{G}_N$  be its instances for some  $N \geq 2$ . Let  $AP_{\{1\}}$  be a set of predicates which inspect only variables whose index is 1. It follows  $\mathcal{G}_1$  and  $\mathcal{G}_N$  are trace equivalent under  $AP_{\{1\}}$ .*

*Proof.* By applying similar arguments in the proof of Lemma 4.13 with Constructions 5.19 and 5.20.  $\square$

**5.5. Cutoff results in the unrestricted model.** In the following, we prove Propositions 5.22 and 5.23 which allows us to change positions of big conjunctions in specific formulas. Propositions 5.22 and 5.23 are used in the proof of our cutoff results, Theorems 4.1 and 4.2, respectively.

**Proposition 5.22.** *Let  $\mathcal{A}$  be a symmetric point-to-point algorithm. Let  $\mathcal{G}_N$  be instances of  $N$  processes for some  $N \geq 1$ . Let  $Path_N$  be sets of all admissible sequences of configurations in  $\mathcal{G}_N$ . Let  $\omega_{\{i\}}$  be a  $LTL \setminus X$  formula in which every predicate takes one of the forms:  $P_1(i)$  or  $P_2(i, i)$  where  $i$  is an index in  $1..N$ . Then,*

$$\left( \forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \bigwedge_{i \in 1..N} \omega_{\{i\}} \right) \quad (5.1)$$

$$\Leftrightarrow \left( \bigwedge_{i \in 1..N} (\forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \omega_{\{i\}}) \right) \quad (5.2)$$

*Proof.* ( $\Rightarrow$ ) Let  $\pi_N$  be an arbitrary admissible sequence of configurations in  $Path_N$  such that  $\mathcal{G}_N, \pi_N \models \bigwedge_{i \in 1..N} \omega_{\{i\}}$ . Let  $i_0$  be an arbitrary index in  $1..N$ , we have  $\mathcal{G}_N, \pi_N \models \omega_{\{i_0\}}$ . Hence, for every  $\pi_N \in Path_N$ , for every  $i_0 \in 1..N$ , it follows  $\mathcal{G}_N, \pi_N \models \omega_{\{i_0\}}$ . Therefore, Formula 5.1 implies: for every  $i_0 \in 1..N$ , for every  $\pi_N \in Path_N$ , it follows  $\mathcal{G}_N, \pi_N \models \omega_{\{i_0\}}$ . It follows that: for every  $i_0 \in 1..N$ ,  $\forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \omega_{\{i_0\}}$ . Now, we have that Formula 5.1 implies Formula 5.2.

( $\Leftarrow$ ) By applying similar arguments.  $\square$

**Proposition 5.23.** *Let  $\mathcal{A}$  be a symmetric point-to-point algorithm. Let  $\mathcal{G}_N$  be instances of  $N$  processes respectively for some  $N \geq 1$ . Let  $Path_N$  be sets of all admissible sequences of configurations in  $\mathcal{G}_N$ . Let  $\psi_{\{i,j\}}$  be a  $LTL \setminus X$  formula in which every predicate takes one of the forms:  $P_1(i)$  or  $P_2(i, i)$  where  $i$  is an index in  $1..N$ . Then,*

$$\left( \forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \bigwedge_{i,j \in 1..N}^{i \neq j} \psi_{\{i,j\}} \right) \quad (5.3)$$

$$\Leftrightarrow \left( \bigwedge_{i,j \in 1..N}^{i \neq j} (\forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \psi_{\{i,j\}}) \right) \quad (5.4)$$

*Proof.* ( $\Rightarrow$ ) Let  $\pi_N$  be an arbitrary admissible sequence of configurations in  $Path_N$  such that  $\mathcal{G}_N, \pi_N \models \bigwedge_{i,j \in 1..N}^{i \neq j} \psi_{\{i,j\}}$ . Let  $i_0$  and  $j_0$  be arbitrary indexes in  $1..N$  such that  $i_0 \neq j_0$ , we have that  $\mathcal{G}_N, \pi_N \models \psi_{\{i_0,j_0\}}$ . Hence, for every  $\pi_N \in Path_N$ , for every  $i_0 \in 1..N$ , for every  $j_0 \in 1..N$  such that  $i_0 \neq j_0$ , it follows that  $\mathcal{G}_N, \pi_N \models \psi_{\{i_0,j_0\}}$ . Therefore, Formula 5.3 implies: for every  $i_0 \in 1..N$ , for every  $j_0 \in 1..N$  such that  $i_0 \neq j_0$ , for every  $\pi_N \in Path_N$ , it follows  $\mathcal{G}_N, \pi_N \models \psi_{\{i_0,j_0\}}$ . It follows that: for every  $i_0 \in 1..N$ , for every  $j_0 \in 1..N$  such that  $i_0 \neq j_0$ , it holds  $\forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \psi_{\{i_0,j_0\}}$ . Therefore, Formula 5.3 implies Formula 5.4.

( $\Leftarrow$ ) By applying similar arguments.  $\square$

**Theorem 4.1.** *Let  $\mathcal{A}$  be a symmetric point-to-point algorithm under the unrestricted model. Let  $\mathcal{G}_1$  and  $\mathcal{G}_N$  be instances of 1 and  $N$  processes respectively for some  $N \geq 1$ . Let  $Path_1$  and  $Path_N$  be sets of all admissible sequences of configurations in  $\mathcal{G}_1$  and in  $\mathcal{G}_N$ , respectively. Let  $\omega_{\{i\}}$  be a  $LTL \setminus X$  formula in which every predicate takes one of the forms:*

$P_1(i)$  or  $P_2(i, i)$  where  $i$  is an index in  $1..N$ . Then, it follows that:

$$\left( \forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \bigwedge_{i \in 1..N} \omega_{\{i\}} \right) \Leftrightarrow \left( \forall \pi_1 \in Path_1: \mathcal{G}_1, \pi_1 \models \omega_{\{1\}} \right)$$

*Proof.* By Proposition 5.22, we have

$$\left( \forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \bigwedge_{i \in 1..N} \omega_{\{i\}} \right) \Leftrightarrow \left( \bigwedge_{i \in 1..N} \left( \forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \omega_{\{i\}} \right) \right)$$

Let  $i$  be an index in a set  $1..N$ . Hence,  $\alpha = (i \leftrightarrow 1)$  is a transposition on  $1..N$  (\*). By Lemma 4.7, we have: (i)  $\psi_{\{\alpha(i)}} = \psi_{\{1\}}$ , and (ii)  $\alpha(\mathcal{G}_N) = \mathcal{G}_N$ , and (iii)  $\alpha(g_N^0) = g_N^0$ .

Since  $\omega_{\{i}}$  is an LTL\X formula,  $\mathbf{A} \omega_{\{i}}$  is a LTL\X formula where  $\mathbf{A}$  is a path operator in LTL\X (see [CJGK<sup>+</sup>18]). By the semantics of the operator  $\mathbf{A}$ , it follows that  $\forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \omega_{\{i}}$  if and only if  $\mathcal{G}_N, g_N^0 \models \mathbf{A} \omega_{\{1\}}$ . By point (\*), it follows  $\mathcal{G}_N, g_N^0 \models \mathbf{A} \omega_{\{i}}$  if and only if  $\mathcal{G}_N, g_N^0 \models \mathbf{A} \omega_{\{1\}}$ . Since an index  $i$  is arbitrary, we have  $\mathcal{G}_N, g_N^0 \models \bigwedge_{i \in 1..N} \mathbf{A} \omega_{\{i}}$  if and only if  $\mathcal{G}_N, g_N^0 \models \mathbf{A} \omega_{\{i}}$ .

We have that  $\mathcal{G}_N, g_N^0 \models \mathbf{A} \omega_{\{i}}$  if and only if  $\forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \omega_{\{i}}$  by the semantics of the operator  $\mathbf{A}$ . It follows  $\forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \omega_{\{i}}$  if and only if  $\forall \pi_2 \in Path_2: \mathcal{G}_2, \pi_2 \models \omega_{\{1\}}$  by Lemma 5.21. Then, Theorem 4.1 holds.  $\square$

**Theorem 4.2.** *Let  $\mathcal{A}$  be a symmetric point-to-point algorithm under the unrestricted model. Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be instances of 2 and  $N$  processes respectively for some  $N \geq 2$ . Let  $Path_2$  and  $Path_N$  be sets of all admissible sequences of configurations in  $\mathcal{G}_2$  and in  $\mathcal{G}_N$ , respectively. Let  $\psi_{\{i,j\}}$  be an LTL\X formula in which every predicate takes one of the forms:  $P_1(i)$ , or  $P_2(j)$ , or  $P_3(i, j)$ , or  $P_4(j, i)$  where  $i$  and  $j$  are different indexes in  $1..N$ . It follows that:*

$$\left( \forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \bigwedge_{\substack{i \neq j \\ i, j \in 1..N}} \psi_{\{i,j\}} \right) \Leftrightarrow \left( \forall \pi_2 \in Path_2: \mathcal{G}_2, \pi_2 \models \psi_{\{1,2\}} \right)$$

*Proof.* By similar arguments in the proof of Theorem 4.1.  $\square$

**5.6. Verification of the Failure Detector of [CT96] with the Cutoffs.** In the following, we present Lemmas 5.25 which explains why the cutoff result 4.2 allows us to verify the strong completeness property of the failure detector of [CT96] under synchrony by model checking instances of size 2.

**Proposition 5.24.** *Let  $\mathcal{G}_N = (\mathcal{C}_N, Tr_N, R_N, g_N^0)$  be a global transition system of a symmetric point-to-point algorithm under the unrestricted model. Its indexes are  $1..N$  for some  $N \geq 1$ . Let  $i$  and  $j$  be two indexes in the set  $1..N$ . Let  $\mu_{\{i,j\}}$  be a first-order formula in which every predicate takes one of the forms:  $Q_1(i)$ , or  $Q_2(j)$ , or  $Q_3(i, j)$ , or  $Q_4(j, i)$ . The following conditions hold:*

- (1)  $\mathbf{F G} \bigwedge_{i,j \in 1..N} \mu_{\{i,j\}}$  be an LTL\X formula.
- (2)  $\bigwedge_{i,j \in 1..N} \mathbf{F G} \mu_{\{i,j\}}$  be an LTL\X formula.
- (3) Let  $\pi = \kappa_0 \kappa_1 \dots$  be an admissible sequence of configurations in  $\mathcal{G}_N$ . It follows  $\mathcal{G}_N, \pi \models \mathbf{F G} \bigwedge_{i,j \in 1..N} \mu_{\{i,j\}}$  if and only if  $\mathcal{G}_N, \pi \models \bigwedge_{i,j \in 1..N} \mathbf{F G} \mu_{\{i,j\}}$ .



*Proof.* Points (1) and (2) hold by the definition of  $\text{LTL}\setminus\text{X}$  (see [CJGK<sup>+</sup>18]). We prove Point (3) as follows.

( $\Rightarrow$ ) Since  $\mathcal{G}_N, \pi \models \mathbf{F}\mathbf{G} \bigwedge_{i,j \in 1..N} \mu_{\{i,j\}}$ , there exists  $\ell_0 \geq 0$  such that for every  $\ell \geq \ell_0$ , we have  $\kappa_\ell \models \bigwedge_{i,j \in 1..N} \mu_{\{i,j\}}$ . Let  $i_0$  and  $j_0$  be two indexes in  $1..N$ . We have  $\kappa_\ell \models \mu_{\{i_0,j_0\}}$  for every  $\ell \geq \ell_0$ . Hence, it follows  $\mathcal{G}_N, \pi \models \mathbf{F}\mathbf{G} \mu_{\{i_0,j_0\}}$ . Because  $i_0$  and  $j_0$  are arbitrary indexes in  $1..N$ , it follows that  $\mathcal{G}_N, \pi \models \bigwedge_{i,j \in 1..N} \mathbf{F}\mathbf{G} \mu_{\{i,j\}}$ .

( $\Leftarrow$ ) Let  $i_0$  and  $j_0$  be two indexes in  $1..N$ . Since  $\mathcal{G}_N, \pi \models \bigwedge_{i,j \in 1..N} \mathbf{F}\mathbf{G} \mu_{\{i,j\}}$ , it follows that  $\mathcal{G}_N, \pi \models \mathbf{F}\mathbf{G} \mu_{\{i_0,j_0\}}$ . Therefore, there exists  $\ell_j^i \geq 0$  such that  $\kappa_\ell \models \mu_{\{i_0,j_0\}}$  for every  $\ell \geq \ell_{j_0}^{i_0}$ . Let  $\ell = \max(\{\ell_j^i : i \in 1..N \wedge j \in 1..N\})$  where  $\max$  is a function to pick a maximum number in a finite set of natural numbers. It follows that  $\kappa_\ell \models \mu_{\{i,j\}}$  for every  $\ell \geq \ell_0$ , for every  $i, j \in 1..N$ . Therefore,  $\mathcal{G}_N, \pi \models \mathbf{F}\mathbf{G} \bigwedge_{i,j \in 1..N} \mu_{\{i,j\}}$ .  $\square$

**Lemma 5.25.** *Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be two global transition systems of a symmetric point-to-point algorithm such that:*

- (1) *These systems  $\mathcal{G}_2$  and  $\mathcal{G}_N$  have 2 and  $N$  processes respectively where  $N \geq 2$ .*
- (2) *All processes  $\mathcal{G}_2$  and  $\mathcal{G}_N$  follow Algorithm 1.*
- (3) *The model of computation of these systems is under the unrestricted model.*

*Let  $\Pi$  be a set of indexes, and  $\mu(\Pi)$  denote the strong completeness property in which the set of process indexes is  $\Pi$ , i.e.*

$$\mu(\Pi) \triangleq \mathbf{F}\mathbf{G}(\forall p, q \in \Pi : (\text{Correct}(p) \wedge \neg \text{Correct}(q)) \Rightarrow \text{Suspected}(p, q))$$

*Let  $\text{Path}_2$  and  $\text{Path}_N$  be sets of all admissible sequences of configurations in  $\mathcal{G}_2$  and in  $\mathcal{G}_N$ , respectively. Then, it holds:*

$$\begin{aligned} & \forall \pi_N \in \text{Path}_N : \mathcal{G}_N, \pi_N \models \mu(1..N) \\ \Leftrightarrow & \forall \pi_2 \in \text{Path}_2 : \mathcal{G}_2, \pi_2 \models \mu(1..2) \end{aligned}$$

*Proof.* To keep the presentation simple, let  $\nu(p, q)$  be a predicate such that  $\nu(p, q) \triangleq (\text{Correct}(p) \wedge \neg \text{Correct}(q))$ . Let  $\pi_N$  be an admissible sequence of configurations in  $\mathcal{G}_N$ . We have  $\mathcal{G}_N, \pi_N \models \mu(\Pi)$  if and only if  $\mathcal{G}_N, \pi_N \models \mathbf{F}\mathbf{G}(\forall p, q \in 1..N : \nu(p, q) \Rightarrow \text{Suspected}(p, q))$ . It follows

$$\begin{aligned} & \mathcal{G}_N, \pi_N \models \mu(1..N) \\ \Leftrightarrow & \mathcal{G}_N, \pi_N \models \mathbf{F}\mathbf{G} \left( \bigwedge_{p,q \in 1..N} \nu(p, q) \Rightarrow \text{Suspected}(p, q) \right) \\ \Leftrightarrow & \mathcal{G}_N, \pi_N \models \bigwedge_{p,q \in 1..N} \mathbf{F}\mathbf{G}(\nu(p, q) \Rightarrow \text{Suspected}(p, q)) \quad (\text{by Proposition 5.24}) \end{aligned}$$

The last formula is equivalent to

$$\begin{aligned} & \mathcal{G}_N, \pi_N \models \bigwedge_{\substack{p \neq q \\ p,q \in 1..N}} \mathbf{F}\mathbf{G}(\nu(p, q) \Rightarrow \text{Suspected}(p, q)) \\ \wedge & \mathcal{G}_N, \pi_N \models \bigwedge_{\substack{p=q \\ p,q \in 1..N}} \mathbf{F}\mathbf{G}(\nu(p, q) \Rightarrow \text{Suspected}(p, q)) \end{aligned}$$

For every  $p, q \in 1..N$ , if  $p = q$ , then  $(Correct(p) \wedge \neg Correct(q)) = \perp$  (\*). Hence, it follows that

$$\begin{aligned} \mathcal{G}_N, \pi_N &\models \bigwedge_{p, q \in 1..N} \mathbf{F G}(\nu(p, q) \Rightarrow Suspected(p, q)) \\ \Leftrightarrow \mathcal{G}_N, \pi_N &\models \bigwedge_{\substack{p \neq q \\ p, q \in 1..N}} \mathbf{F G}(\nu(p, q) \Rightarrow Suspected(p, q)) \end{aligned}$$

It follows that  $\forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \mu$  if and only if

$$\forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \bigwedge_{\substack{p \neq q \\ p, q \in 1..N}} \mathbf{F G}(\nu(p, q) \Rightarrow Suspected(p, q))$$

By Theorem 4.2, it follows

$$\begin{aligned} \forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N &\models \mu(1..N) \\ \Leftrightarrow \forall \pi_2 \in Path_2: \mathcal{G}_2, \pi_2 &\models \bigwedge_{p, q \in 1..2} \mathbf{F G}(\nu(p, q) \Rightarrow Suspected(p, q)) \end{aligned}$$

By point (\*), we have

$$\begin{aligned} \forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N &\models \mu(1..N) \\ \Leftrightarrow \forall \pi_2 \in Path_2: \mathcal{G}_2, \pi_2 &\models \bigwedge_{p, q \in 1..2} \mathbf{F G}(\nu(p, q) \Rightarrow Suspected(p, q)) \end{aligned}$$

By Proposition 5.24, it follows

$$\begin{aligned} \forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N &\models \mu(1..N) \\ \Leftrightarrow \forall \pi_2 \in Path_2: \mathcal{G}_2, \pi_2 &\models \mathbf{F G}(\bigwedge_{p, q \in 1..2} (\nu(p, q) \Rightarrow Suspected(p, q))) \\ \Leftrightarrow \forall \pi_2 \in Path_2: \mathcal{G}_2, \pi_2 &\models \mu(1..2) \end{aligned}$$

Hence, Lemma 5.25 holds. □

**Lemma 5.26.** *Let  $\mathcal{G}_1$  and  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be three global transition systems of a symmetric point-to-point algorithm such that:*

- (1) *These systems  $\mathcal{G}_1$  and  $\mathcal{G}_2$  and  $\mathcal{G}_N$  have 1, 2 and  $N$  processes respectively.*
- (2) *All processes in  $\mathcal{G}_1$  and  $\mathcal{G}_2$  and  $\mathcal{G}_N$  follow Algorithm 1.*
- (3) *Three sets  $Path_1$  and  $Path_2$  and  $Path_N$  be sets of admissible sequences of configurations in  $\mathcal{G}_1$  and  $\mathcal{G}_2$  and  $\mathcal{G}_N$ , respectively.*
- (4) *The model of computation of these systems is under the unrestricted model.*

*Let  $\Pi$  be a set of process indexes, and  $\mu(\Pi)$  denote the eventually strong accuracy property in which the set of process indexes is  $\Pi$ , i.e.,*

$$\mu(\Pi) \triangleq \mathbf{F G}(\forall p, q \in \Pi: (Correct(p) \wedge Correct(q)) \Rightarrow \neg Suspected(p, q))$$

*It follows  $\forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \mu(1..N)$  if and only if both  $\forall \pi_2 \in Path_2: \mathcal{G}_2, \pi_2 \models \mu(1..2)$  and  $\forall \pi_1 \in Path_1: \mathcal{G}_1, \pi_1 \models \mu(1..1)$ .*

*Proof.* To keep the presentation simple, we define

$$\nu(p, q) = (\text{Correct}(p) \wedge \text{Correct}(q)) \Rightarrow \neg \text{Suspected}(p, q)$$

By similar arguments in Proposition 5.25, we have  $\forall \pi_N \in \text{Path}_N: \mathcal{G}_N, \pi_N \models \mu(1..N)$  is equivalent to the following conjunction

$$\begin{aligned} & \left( \forall \pi_N \in \text{Path}_N: \mathcal{G}_N, \pi_N \models \bigwedge_{p,q \in 1..N}^{p=q} \mathbf{F G} \nu(p, q) \right) \\ & \wedge \left( \forall \pi_N \in \text{Path}_N: \mathcal{G}_N, \pi_N \models \bigwedge_{p,q \in 1..N}^{p \neq q} \mathbf{F G} \nu(p, q) \right) \end{aligned}$$

By Theorems 4.1 and 4.2, the above conjunction is equivalent to

$$\begin{aligned} & \left( \forall \pi_1 \in \text{Path}_1: \mathcal{G}_1, \pi_1 \models \bigwedge_{p,q \in 1..N}^{p=q} \mathbf{F G} \nu(1, 1) \right) \\ & \wedge \left( \forall \pi_2 \in \text{Path}_2: \mathcal{G}_2, \pi_2 \models \bigwedge_{p,q \in 1..N}^{p \neq q} \mathbf{F G} \nu(1, 2) \right) \end{aligned}$$

By Proposition 5.24, the above conjunction is equivalent to

$$\begin{aligned} & \left( \forall \pi_1 \in \text{Path}_1: \mathcal{G}_1, \pi_1 \models \mathbf{F G} \bigwedge_{p,q \in 1..N}^{p=q} \nu(1, 1) \right) \\ & \wedge \left( \forall \pi_2 \in \text{Path}_2: \mathcal{G}_2, \pi_2 \models \mathbf{F G} \bigwedge_{p,q \in 1..N}^{p \neq q} \nu(1, 2) \right) \end{aligned}$$

Therefore, Lemma 5.26 holds.  $\square$

## 6. CUTOFF RESULTS IN THE CASE OF UNKNOWN TIME BOUNDS

In this section, we extend the above cutoff results on a number of processes (see Theorems 4.1 and 4.2) for partial synchrony in case of unknown bounds  $\Delta$  and  $\Phi$ . The extended results are formalized in Theorems 6.1 and 6.2. It is straightforward to adapt our approach to other models of partial synchrony in [DLS88, CT96].

**Theorem 6.1.** *Let  $\mathcal{A}$  be a symmetric point-to-point algorithm under partial synchrony with unknown bounds  $\Delta$  and  $\Phi$ . Let  $\mathcal{G}_1$  and  $\mathcal{G}_N$  be instances of  $\mathcal{A}$  with 1 and  $N$  processes respectively for some  $N \geq 1$ . Let  $\text{Path}_1$  and  $\text{Path}_N$  be sets of all admissible sequences of configurations in  $\mathcal{G}_1$  and in  $\mathcal{G}_N$  under partial synchrony, respectively. Let  $\omega_{\{i\}}$  be a  $LTL \setminus X$  formula in which every predicate takes one of the forms:  $P_1(i)$  or  $P_2(i, i)$  where  $i$  is an index in  $1..N$ . It follows that:*

$$\left( \forall \pi_N \in \text{Path}_N: \mathcal{G}_N, \pi_N \models \bigwedge_{i \in 1..N} \omega_{\{i\}} \right) \Leftrightarrow \left( \forall \pi_1 \in \text{Path}_1: \mathcal{G}_1, \pi_1 \models \omega_{\{1\}} \right)$$

**Theorem 6.2.** *Let  $\mathcal{A}$  be a symmetric point-to-point algorithm under partial synchrony with unknown bounds  $\Delta$  and  $\Phi$ . Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be instances of  $\mathcal{A}$  with 2 and  $N$  processes respectively for some  $N \geq 2$ . Let  $Path_2$  and  $Path_N$  be sets of all admissible sequences of configurations in  $\mathcal{G}_2$  and in  $\mathcal{G}_N$  under partial synchrony, respectively. Let  $\psi_{\{i,j\}}$  be an LTL\X formula in which every predicate takes one of the forms:  $Q_1(i)$ , or  $Q_2(j)$ , or  $Q_3(i,j)$ , or  $Q_4(j,i)$  where  $i$  and  $j$  are different indexes in  $1..N$ . It follows that:*

$$(\forall \pi_N \in Path_N: \mathcal{G}_N, \pi_N \models \bigwedge_{\substack{i \neq j \\ i,j \in 1..N}} \psi_{\{i,j\}}) \Leftrightarrow (\forall \pi_2 \in Path_2: \mathcal{G}_2, \pi_2 \models \psi_{\{1,2\}})$$

Since the proofs of these theorems are similar, we here focus on only Theorem 6.2. The proof of Theorem 6.2 follows the approach in [EN95, TKW20], and is based on the following observations. Remind that Steps 1 and 2 are already proved in Section 4.

- (1) The global transition system and the desired property are symmetric.
- (2) Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be two instances of a symmetric point-to-point algorithm with 2 and  $N$  processes, respectively. We have that two instances  $\mathcal{G}_2$  and  $\mathcal{G}_N$  are trace equivalent under a set of predicates in the desired property.
- (3) We will now discuss that the constraints maintain partial synchrony. Let  $\pi_N$  be an execution in  $\mathcal{G}_N$ . By applying the index projection to  $\pi_N$ , we obtain an execution  $\pi_2$  in  $\mathcal{G}_2$ . If partial synchrony constraints (PS1) and (PS2) – defined in Section 3.3 – hold on  $\pi_N$ , these constraints also hold on  $\pi_2$ . This result is proved in Lemma 6.3.
- (4) Let  $\pi_2$  be an execution in  $\mathcal{G}_2$ . We construct an execution  $\pi_N$  in  $\mathcal{G}_N$  based on  $\pi_2$  such that all processes  $3..N$  crash from the beginning, and  $\pi_2$  is an index projection of  $\pi_N$  (defined in Section 4.2). For instance, see Figure 2. If partial synchrony constraints (PS1) and (PS2) – defined in Section 3.3 – hold on  $\pi_2$ , these constraints also hold on  $\pi_N$ . This result is proved in Lemma 6.4.

**Lemma 6.3.** *Let  $\mathcal{A}$  be a symmetric point-to-point algorithm under partial synchrony with unknown bounds  $\Delta$  and  $\Phi$ . Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be instances of  $\mathcal{A}$  with 2 and  $N$  processes, respectively, for some  $N \geq 2$ . Let  $Path_2$  and  $Path_N$  be sets of all admissible sequences of configurations in  $\mathcal{G}_2$  and in  $\mathcal{G}_N$  under partial synchrony, respectively. Let  $\pi^N = \kappa_0^N \kappa_1^N \dots$  be an admissible sequences of configurations in  $\mathcal{G}_N$ . Let  $\pi^2 = \kappa_0^2 \kappa_1^2 \dots$  be a sequence of configurations in  $\mathcal{G}_2$  such that  $\kappa_k^2$  be an index projection of  $\kappa_k^N$  on indexes  $\{1,2\}$  for every  $k \geq 0$ . It follows that*

- (a) *Constraint (PS1) on message delay holds on  $\pi^2$ .*
- (b) *Constraint (PS2) on the relative speed of processes holds on  $\pi^2$ .*

*Proof.* Recall that the index projection is defined in Section 4.2. In the following, we denote  $p^2$  and  $p^N$  two processes such that they have the same index, and  $p^2$  is a process in  $\mathcal{G}_2$ , and  $p^N$  is a process in  $\mathcal{G}_N$ . We prove Lemma 6.3 by contradiction.

(a) Assume that Constraint (PS1) does not hold on  $\pi^2$ . Hence, there exist a time  $\ell > 0$ , and two processes  $s^2, r^2 \in 1..2$  in  $\mathcal{G}_2$  such that after  $r^2$  executes Receive at a time  $\ell$ , there exists an old message in a message buffer from process  $s^2$  to process  $r^2$ . By the definition of the index projection, for every  $k \geq 0$ , we have that:

- Let  $p^N, q^N \in \{1,2\}$  be two processes in  $\mathcal{G}_N$ , and  $p^2, q^2$  be corresponding processes in  $\mathcal{G}_2$ . For every  $k \geq 0$ , two message buffers from process  $p^2$  to process  $q^2$  in  $\kappa_k^2$ , and from process  $p^N$  to process  $q^N$  in  $\kappa_k^N$  are the same.

- Let  $p^N \in \{1, 2\}$  be a process in  $\mathcal{G}_N$ , and  $p^2$  be a corresponding process in  $\mathcal{G}_2$ . For every  $k \geq 0$ , process  $p^2$  takes an action *act* in configuration  $\kappa_k^2$  if and only if process  $p^N$  takes the same action in configuration  $\kappa_k^N$ .

It implies that process  $r^N$  in  $\mathcal{G}_N$  also executes Receive at a time  $\ell$ , and there exists an old message in a buffer from process  $s^N$  to process  $r^N$ . Contradiction.

(b) By applying similar arguments in case (a).  $\square$

**Lemma 6.4.** *Let  $\mathcal{A}$  be a symmetric point-to-point algorithm under partial synchrony with unknown bounds  $\Delta$  and  $\Phi$ . Let  $\mathcal{G}_2$  and  $\mathcal{G}_N$  be instances of  $\mathcal{A}$  with 2 and  $N$  processes, respectively, for some  $N \geq 2$ . Let  $Path_2$  and  $Path_N$  be sets of all admissible sequences of configurations in  $\mathcal{G}_2$  and in  $\mathcal{G}_N$  under partial synchrony, respectively. Let  $\pi^2 = \kappa_0^2 \kappa_1^2 \dots$  be an admissible sequences of configurations in  $\mathcal{G}_2$ . Let  $\pi^N = \kappa_0^N \kappa_1^N \dots$  be a sequence of configurations in  $\mathcal{G}_N$  such that (i) every process  $p \in 3..N$  crashes from the beginning, and (ii)  $\kappa_k^2$  be an index projection of  $\kappa_k^N$  on indexes  $\{1, 2\}$  for every  $k \geq 0$ . It follows that*

- (a) *Constraint (PS1) on message delay holds on  $\pi^N$ .*
- (b) *Constraint (PS2) on the relative speed of processes holds on  $\pi^N$ .*

*Proof.* By applying similar arguments in the proof of Lemma 6.3, and the facts that every process  $p \in 3..N$  crashes from the beginning, and that  $\kappa_k^2$  be an index projection of  $\kappa_k^N$  on indexes  $\{1, 2\}$  for every  $k \geq 0$ .  $\square$

## 7. ENCODING THE CHANDRA AND TOUEG FAILURE DETECTOR

In this section, we first discuss why it is sufficient to verify the failure detector by checking a system with only one sender and one receiver by applying the cutoffs presented in Section 6. Next, we introduce two approaches to encoding the message buffer, and an abstraction of in-transit messages that are older than  $\Delta$  time-units. Finally, we present how to encode the relative speed of processes with counters over natural numbers. These techniques allow us to tune our models to the strength of the verification tools: FAST, IVy, and model checkers for TLA<sup>+</sup>.

**7.1. The System with One Sender and One Receiver.** The cutoff results in Section 6 allow us to verify the Chandra and Toueg failure detector under partial synchrony by checking only instances with two processes. In the following, we discuss the model with two processes, and formalize the properties with two-process indexes. By process symmetry, it is sufficient to verify Strong Accuracy, Eventually Strong Accuracy, and Strong Completeness by checking the following properties.

$$\mathbf{G}((Correct(1) \wedge Correct(2)) \Rightarrow \neg Suspected(2, 1)) \quad (7.1)$$

$$\mathbf{F G}((Correct(1) \wedge Correct(2)) \Rightarrow \neg Suspected(2, 1)) \quad (7.2)$$

$$\mathbf{F G}(\neg Correct(1) \wedge Correct(2)) \Rightarrow Suspected(2, 1) \quad (7.3)$$

We can take a further step towards facilitating verification of the failure detector. First, every process typically has a local variable to store messages that it needs to send to itself, instead of using a real communication channel. Hence, we can assume that there is no delay for those messages, and that each correct process never suspects itself. Second, local variables in Algorithm 1 are arrays whose elements correspond one-to-one with a remote

process, e.g.,  $timeout[2, 1]$  and  $suspected[2, 1]$ . Third, communication between processes is point-to-point. When this is not the case, one can use cryptography to establish one-to-one communication. Hence, reasoning about Properties 7.1–7.3 requires no information about messages from process 1 to itself, local variables of process 1, and messages from process 2.

Due to the above characteristics, it is sufficient to consider process 1 as a sender, and process 2 as a receiver. In detail, the sender follows Task 1 in Algorithm 1, but does nothing in Task 2 and Task 3. The sender does not need the initialization step, and local variables  $suspected$  and  $timeout$ . In contrast, the receiver has local variables corresponding to the sender, and follows only the initialization step, and Task 2, and Task 3 in Algorithm 1. The receiver can increase its waiting time in Task 1, but does not send any message.

**7.2. Encoding the Message Buffer.** Algorithm 1 assumes unbounded message buffers between processes that produce an infinite state space. Moreover, a sent message might be in-transit for a long time before it is delivered. We first introduce two approaches to encode the message buffer based on a logical predicate, and a counter over natural numbers. The first approach works for TLA<sup>+</sup> and IVy, but not for counter automata (FAST). The latter is supported by all mentioned tools, but it is less efficient as it requires more transitions. Then, we present an abstraction of in-transit messages that are older than  $\Delta$  time-units. This technique reduces the state space, and allows us to tune our models to the strength of the verification tools.

**7.2.1. Encoding the message buffer with a predicate.** In Algorithm 1, only “alive” messages are sent, and the message delivery depends only on the age of in-transit messages. Moreover, the computation of the receiver does not depend on the contents of its received messages. Hence, we can encode a message buffer by using a logical predicate  $existsMsgOfAge(x)$ . For every  $k \geq 0$ , predicate  $existsMsgOfAge(k)$  refers to whether there exists an in-transit message that is  $k$  time-units old. The number 0 refers to the age of a fresh message in the buffer.

It is convenient to encode the message buffer's behaviors in this approach. For instance, Formulas 7.4 and 7.5 show constraints on the message buffer when a new message is sent:

$$existsMsgOfAge'(0) \tag{7.4}$$

$$\forall x \in \mathbb{N} . x > 0 \Rightarrow existsMsgOfAge'(x) = existsMsgOfAge(x) \tag{7.5}$$

where  $existsMsgOfAge'$  refers to the value of  $existsMsgOfAge$  in the next state. Formula 7.4 implies that a fresh message has been added to the message buffer. Formula 7.5 ensures that other in-transit messages are unchanged.

Another example is the relation between  $existsMsgOfAge$  and  $existsMsgOfAge'$  after the message delivery. This relation is formalized with Formulas 7.6–7.9. Formula 7.6 requires that there exists an in-transit message in  $existsMsgOfAge$  that can be delivered. Formula 7.7 ensures that no old messages are in transit after the delivery. Formula 7.8 guarantees that no message is created out of thin air. Formula 7.9 implies that at least one message is delivered.

$$\exists x \in \mathbb{N} . existsMsgOfAge(x) \tag{7.6}$$

$$\forall x \in \mathbb{N} . x \geq \Delta \Rightarrow \neg existsMsgOfAge'(x) \tag{7.7}$$

$$\forall x \in \mathbb{N} . existsMsgOfAge'(x) \Rightarrow existsMsgOfAge(x) \tag{7.8}$$

$$\exists x \in \mathbb{N} . existsMsgOfAge'(x) \neq existsMsgOfAge(x) \tag{7.9}$$



FIGURE 3. The message buffer after increasing message ages in case of `buf = 6`

This encoding works for  $\text{TLA}^+$  and IVy, but not for FAST, because the input language of FAST does not support functions.

7.2.2. *Encoding the message buffer with a counter.* In the following, we present an encoding technique for the buffer that can be applied in all tools  $\text{TLA}^+$ , IVy, and FAST. This approach encodes the message buffer with a counter `buf` over natural numbers. The  $k^{\text{th}}$  bit refers to whether there exists an in-transit message with  $k$  time-units old.

In this approach, message behaviors are formalized with operations in Presburger arithmetic. For example, assume  $\Delta > 0$ , we write `buf' = buf + 1` to add a fresh message in the buffer. Notice that the increase of `buf` by 1 turns on the  $0^{\text{th}}$  bit, and keeps the other bits unchanged.

To encode the increase of the age of every in-transit message by 1, we simply write `buf' = buf  $\times$  2`. Assume that we use the least significant bit (LSB) first encoding, and the left-most bit is the  $0^{\text{th}}$  bit. By multiplying `buf` by 2, we have updated `buf'` by shifting to the right every bit in `buf` by 1. For example, Figure 3 demonstrates the message buffer after the increase of message ages in case of `buf = 6`. We have `buf' = buf  $\times$  2 = 12`. It is easy to see that the  $1^{\text{st}}$  and  $2^{\text{nd}}$  bits in `buf` are on, and the  $2^{\text{nd}}$  and  $3^{\text{rd}}$  bits in `buf'` are on.

Recall that Presburger arithmetic does not allow one to divide by a variable. Therefore, to guarantee the constraint in Formula 7.8, we need to enumerate all constraints on possible values of `buf` and `buf'` after the message delivery. For example, assume `buf = 3`, and  $\Delta = 1$ . After the message delivery, `buf'` is either 0 or 1. If `buf = 2` and  $\Delta = 1$ , `buf'` must be 0 after the message delivery. Importantly, the number of transitions for the message delivery depends on the value of  $\Delta$ .

To avoid the enumeration of all possible cases, Formula 7.8 can be rewritten with bit-vector arithmetic. However, bit-vector arithmetic are currently not supported in all verification tools  $\text{TLA}^+$ , FAST, and IVy.

The advantage of this encoding is that when bound  $\Delta$  is fixed, every constraint in the system behaviors can be rewritten in Presburger arithmetic. Thus, we can use FAST, which accepts constraints in Presburger arithmetic. To specify cases with arbitrary  $\Delta$ , the user can use  $\text{TLA}^+$  or IVy.

7.2.3. *Abstraction of old messages.* Algorithm 1 assumes underlying unbounded message buffers between processes. Moreover, a sent message might be in transit for a long time before it is delivered. To reduce the state space, we develop an abstraction of in-transit messages that are older than  $\Delta$  time-units; we call such messages “old”. This abstraction makes the message buffer between the sender and the receiver bounded. In detail, the message buffer has a size of  $\Delta$ . Importantly, we can apply this abstraction to two above encoding techniques for the message buffer.

In partial synchrony, if process  $p$  executes Receive at some time point from the Global Stabilization Time, *every* old message sent to  $p$  will be delivered immediately. Moreover,

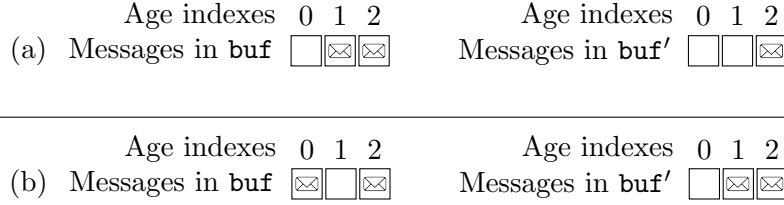


FIGURE 4. The increase of message ages with the abstraction of old messages. In the case (a), we have  $\Delta = 2$ ,  $\text{buf} = 6$ , and  $\text{buf}' = 4$ . In the case (b), we have  $\Delta = 2$ ,  $\text{buf} = 5$ , and  $\text{buf}' = 6$ .

```

1: if  $\text{buf} < 2^\Delta$  then  $\text{buf}' \leftarrow \text{buf} \times 2$ 
2: else
3:   if  $\text{buf} \geq 2^\Delta + 2^{\Delta-1}$  then  $\text{buf}' \leftarrow \text{buf} \times 2 - 2^{\Delta+1}$ 
4:   else  $\text{buf}' \leftarrow \text{buf} \times 2 - 2^{\Delta+1} + 2^\Delta$ 

```

FIGURE 5. Encoding the increase of message ages with a counter  $\text{buf}$ , and the abstraction of old messages.

the computation of a process in Algorithm 1 does not depend on the content of received messages. Hence, instead of tracking all old messages, our abstraction keeps only one old message that is  $\Delta$  time-units old, does not increase its age, and throws away other old messages.

In the following, we discuss how to integrate this abstraction into the encoding techniques of the message buffer. We demonstrate our ideas by showing the pseudo code of the increase of message ages. It is straightforward to adopt this abstraction to the message delivery, and to the sending of a new message.

Figure 4(a) presents the increase of message ages with this abstraction in a case of  $\Delta = 2$ , and  $\text{buf} = 6$ . Unlike Figure 3, there exists no in-transit message that is 3 time-units old in Figure 4(a). Moreover, the message buffer in Figure 4(a) has a size of 3. In addition,  $\text{buf}'$  has only one in-transit message that is 2 time-units old. We have  $\text{buf}' = 4$  in this case. Figure 4(b) demonstrates another case of  $\Delta = 2$ ,  $\text{buf} = 5$ , and  $\text{buf}' = 6$ .

Formally, Figure 5 presents the pseudo code of the increase of message ages that is encoded with a counter  $\text{buf}$ , and the abstraction of old messages. There are three cases. In the first case (Line 1), there exist no old messages in  $\text{buf}$ , and we simply set  $\text{buf}' = \text{buf} \times 2$ . In other cases (Lines 3 and 4),  $\text{buf}$  contains an old message. Figure 4(a) demonstrates the second case (Line 3). We subtract  $2^{\Delta+1}$  to remove an old message with  $\Delta + 1$  time-units old from the buffer. Figure 4(b) demonstrates the third case (Line 4). In the third case, we also need to remove an old message with  $\Delta + 1$  time-units old from the buffer. Moreover, we need to put an old message with  $\Delta$  time-units old to the buffer by adding  $2^\Delta$ .

Now we discuss how to integrate the abstraction of old messages in the encoding of the message buffer with a predicate. Formulas 7.10–7.13 present the relation between  $\text{existsMsgOfAge}$  and  $\text{existsMsgOfAge}'$  when message ages are increased by 1, and this abstraction is applied. Formula 7.10 ensures that no fresh message will be added to  $\text{existsMsgOfAge}'$ . Formula 7.11 ensures that the age of every message that is until  $(\Delta - 2)$  time-units old will be increased by 1. Formulas 7.12–7.13 are introduced by this abstraction. Formula 7.12



implies that if there exists an old message or a message with  $(\Delta - 1)$  time-units old in  $\text{existsMsgOfAge}$ , there will be an old message that is  $\Delta$  time-units old in  $\text{existsMsgOfAge}'$ . Formula 7.13 ensures that there exists no message that is older than  $\Delta$  time-units old.

$$\neg \text{existsMsgOfAge}'(0) \quad (7.10)$$

$$\forall x \in \mathbb{N}. (0 \leq x \leq \Delta - 2)$$

$$\Rightarrow \text{existsMsgOfAge}'(x + 1) = \text{existsMsgOfAge}(x) \quad (7.11)$$

$$\text{existsMsgOfAge}'(\Delta) = \text{existsMsgOfAge}(\Delta) \vee \text{existsMsgOfAge}(\Delta - 1) \quad (7.12)$$

$$\forall x \in \mathbb{N}. x > \Delta \Rightarrow \text{existsMsgOfAge}'(x) = \perp \quad (7.13)$$

**7.3. Encoding the Relative Speed of Processes.** Recall that we focus on the case of unknown bounds  $\Delta$  and  $\Phi$ . In this case, every correct process must take at least one step in every contiguous time interval containing  $\Phi$  time-units [DLS88].

To maintain this constraint on executions generated by the verification tools, we introduced two additional control variables  $\text{sTimer}$  and  $\text{rTimer}$  for the sender and the receiver, respectively. These variables work as timers to keep track of how long a process has not taken a step, and when a process can take a step. Since these timers play similar roles, we here focus on  $\text{rTimer}$ . In our encoding, only the global system can update  $\text{rTimer}$ . To schedule the receiver, the global systems non-deterministically executes one of two actions in the sub-round *Schedule*: (i) resets  $\text{rTimer}$  to 0, and (ii) if  $\text{rTimer} < \Phi$ , increases  $\text{rTimer}$  by 1. In other sub-rounds, the value of  $\text{rTimer}$  is unchanged. Moreover, the receiver must take a step whenever  $\text{rTimer} = 0$ .

## 8. REDUCE LIVENESS PROPERTIES TO SAFETY PROPERTIES

To verify the liveness properties *Eventually Strong Accuracy* and *Strong Completeness* with *IVy*, we first need to reduce them to safety properties. Intuitively, these liveness properties are bounded; therefore, they become safety ones. In the following, we explain how to do that.

**8.1. Eventually Strong Accuracy.** By cutoffs discussed in Section 6, it is sufficient to verify *Eventually Strong Accuracy* on the Chandra and Toueg failure detector by checking the following property on instances with 2 processes.

$$\mathbf{F G}((\text{Correct}(1) \wedge \text{Correct}(2)) \Rightarrow \neg \text{Suspected}(2, 1)) \quad (8.1)$$

where process 1 is the sender and process 2 is the receiver.

In the following, we present how to reduce Formula 8.1 to a safety property. Our reduction is based on the following observations:

- (1) *Fairness* (Line 5 in Algorithm 1): correct processes send “alive” infinitely often.
- (2) *The reliable communication* (Constraint (TC1)): Let  $\text{rcv\_msg\_from}(2, 1)$  be a predicate that refers to whether process 2 receives a message from process 1. If processes  $p$  and  $q$  are always correct, then it holds  $\mathbf{G F rcv\_msg\_from}(2, 1)$ .

(3) Transition invariant: Let  $\psi_1(2, 1)$  be a predicate such that

$$\psi_1(2, 1) \triangleq rcv\_msg\_from(2, 1) \wedge Correct(1) \wedge Correct(2) \wedge Suspected(2, 1)$$

Then, the following property is a transition invariant.

$$\mathbf{G}(\psi_1(p, q) \Rightarrow timeout'[2, 1] = timeout[2, 1] + 1) \quad (8.2)$$

Points 1–3 implies that if  $timeout[2, 1]$  is always less than some constant in an arbitrary execution path, then Formula 8.1 holds in this path.

Now we discuss why  $timeout[2, 1]$  does not keep increasing forever if processes 1 and 2 are correct. To that end, we find a specific guard  $g$  for  $timeout[2, 1]$  such that if  $timeout[2, 1] \geq g$ <sup>5</sup> and the sender is correct, then the receiver waits for the sender in less than  $g$  time-units. Moreover, the value of  $g$  depends only on the values of  $\Delta$  and  $\Phi$ . Hence, it is sufficient to verify Formula 8.1 by checking Formula 8.3.

$$\mathbf{G}(timeout[2, 1] \geq g \Rightarrow ((Correct(1) \wedge Correct(2)) \Rightarrow \neg Suspected(2, 1))) \quad (8.3)$$

**8.2. Strong Completeness.** By cutoffs discussed in Section 6, it is sufficient to verify Strong Completeness on the Chandra and Toueg failure detector by checking the following property on instances with 2 processes.

$$\mathbf{F} \mathbf{G}((\neg Correct(1) \wedge Correct(2)) \Rightarrow Suspected(2, 1)) \quad (8.4)$$

Notice that in partial synchrony, every sent message is eventually delivered. Hence, after the sender crashes, the receiver eventually receives nothing from the sender. To reduce Formula 8.4 to a safety property, we first introduced a ghost variable **hLFSC** to measure for how long the sender has crashed. **hLFSC** is set to 0 when the sender crashes. After that, **hLFSC** is increased by 1 in every global step if the receiver has not suspected the crashed sender. Let  $\psi_2(2, 1)$  denote the constraint:  $\psi_2(2, 1) \triangleq \neg Correct(1) \wedge Correct(2) \wedge \neg Suspected(2, 1)$ . Then, the following property is a transition invariant.

$$\mathbf{G}(\psi_2(p, q) \Rightarrow \mathbf{hLFSC}' = \mathbf{hLFSC} + 1) \quad (8.5)$$

By Formula 8.5, if **hLFSC** is always less than some constant in an arbitrary execution path, then Formula 8.4 holds in this path.

Now we show that **hLFSC** cannot keep increasing forever. To that end, we find a specific guard  $g' > 0$  for **hLFSC** such that if **hLFSC** =  $g'$ , then the receiver suspects the sender. It implies that **hLFSC** is unchanged. Moreover, the value of  $g'$  depends only on the values of  $\Delta$  and  $\Phi$ . Hence, it is sufficient to verify Formula 8.4 by checking Formula 8.6.

$$\mathbf{G}(\mathbf{hLFSC} = g' \Rightarrow ((\neg Correct(1) \wedge Correct(2)) \Rightarrow Suspected(2, 1))) \quad (8.6)$$

## 9. EXPERIMENTS FOR SMALL $\Delta$ AND $\Phi$

In this section, we describe our experiments with TLA<sup>+</sup> and FAST. We ran the following experiments on a virtual machine with Core i7-6600U CPU and 8GB DDR4. Our specifications can be found at [TKW].

---

<sup>5</sup>As the default-value of  $timeout[2, 1]$  is a parameter,  $timeout[2, 1]$  might be greater than  $g$  from the initialization.

```

1:  $SSnd \stackrel{\Delta}{=} \wedge ePC = \text{"SSnd"}$ 
2:    $\wedge \text{IF } (sTimer = 0 \wedge sPC = \text{"SSnd"})$ 
3:     THEN  $buf' = buf + 1$ 
4:     ELSE UNCHANGED  $buf$ 
5:    $\wedge ePC' = \text{"RNoSnd"}$ 
6:    $\wedge$  UNCHANGED  $\langle sTimer, rTimer... \rangle$ 

```

FIGURE 6. Sending a new message in  $TLA^+$  in case of  $\Delta > 0$

**9.1. Model Checkers for  $TLA^+$ : TLC and APALACHE.** We first use  $TLA^+$  [Lam02] to specify the failure detector with both encoding techniques for the message buffer, and the abstraction in Section 7. Then, we use the model checker TLC in the  $TLA^+$  Toolbox version 1.7.1 [YML99, Mic] and the model checker APALACHE version 0.15.0 [KKT19, Sys19] to verify instances with fixed bounds  $\Delta$  and  $\Phi$ , and the GST  $T_0 = 1$ . This approach helps us to search constraints in inductive invariants in case of fixed parameters. The main reason is that counterexamples and inductive invariants in case of fixed parameters, e.g.,  $\Delta \leq 1$  and  $\Phi \leq 1$ , are simpler than in case of arbitrary parameters. Hence, if a counterexample is found, we can quickly analyze it, and change constraints in an inductive invariant candidate. We apply the counterexample-guided approach to find inductive strengthenings. After obtaining inductive invariants in small cases, we can generalize them for cases of arbitrary bounds, and check with theorem provers, e.g., IVy (Section 10).

$TLA^+$  offers a rich syntax for sets, functions, tuples, records, sequences, and control structures [Lam02]. Hence, it is straightforward to apply the encoding techniques and the abstraction presented in Section 7 in  $TLA^+$ . For example, Figure 6 represents a  $TLA^+$  action  $SSnd$  for sending a new message in case of  $\Delta > 0$ . Variables  $ePC$  and  $sPC$  are program counters for the environment and the sender, respectively. Line 1 is a precondition, and refers to that the environment is in subround Send. Lines 2–3 say that if the sender is active in subround Send, the counter  $buf'$  is increased by 1. Otherwise, two counters  $buf$  and  $buf'$  are the same (Line 4). Line 5 implies that the environment is still in the subround Send, but it is now the receiver's turn. Line 6 guarantees that other variables are unchanged in this action.

Figure 7 represents the next–state relation in  $TLA^+$ . Line 1 describes actions in sub-round Schedule. The environment schedules the Sender, schedules the Receiver, and then increases message ages. Lines 2, 3, and 4 describes actions in sub-rounds Send, Receive, and Computation, respectively. The program counter  $ePC$  of the environment is used to ensure that every action is repeated periodically and in order.

Figure 8 represents how the environment schedules the Receiver in  $TLA^+$ . Line 1 says that the current step is to schedule the Receiver, and Line 2 refers to the next action that is to increase message ages. Line 3 non-deterministically sets the Receiver active in the current global step. Lines 4–6 are to update the program counter  $rPC$  of the Receiver. The environment schedules the Sender, schedules the Receiver, and then increases message ages. Lines 7–8 non-deterministically sets the Receiver inactive in the current global step if the Receiver is not frozen in the last  $Phi - 1$  global steps. Line 9 is to keep other variables unchanged.

Now we present the experiments with TLC and APALACHE. We used these tools to verify (i) the safety property Strong Accuracy, and (ii) an inductive invariant for Strong Accuracy, and (iii) an inductive invariant for a safety property reduced from the liveness

$$\begin{aligned}
1: \text{Next} &\stackrel{\Delta}{=} \vee \text{SSched} \vee \text{RSched} \vee \text{IncMsgAge} \\
2: &\vee \text{SSnd} \vee \text{RNoSnd} \\
3: &\vee \text{RRcv} \\
4: &\vee \text{RComp}
\end{aligned}$$

FIGURE 7. The Next predicate for the next-state relation in TLA<sup>+</sup>

$$\begin{aligned}
1: \text{RSched} &\stackrel{\Delta}{=} \wedge ePC = \text{"RSched"} \\
2: &\wedge ePC' = \text{"IncMsgAge"} \\
3: &\wedge \vee \wedge rTimer' = 0 \\
4: &\wedge \vee (rPC = \text{"RNoSnd"} \wedge rPC' = \text{"RRcv"}) \\
5: &\vee (rPC = \text{"RRcv"} \wedge rPC' = \text{"RComp"}) \\
6: &\vee (rPC = \text{"RComp"} \wedge rPC' = \text{"RNoSnd"}) \\
7: &\vee \wedge rTimer < Phi - 1 \\
8: &\wedge rTimer' = rTimer + 1 \\
9: &\wedge \text{UNCHANGED } \langle \text{buf}, sTimer \dots \rangle
\end{aligned}$$

FIGURE 8. The RSched predicate for scheduling the Receiver in TLA<sup>+</sup>

property Strong Completeness in case of fixed bounds, and  $\text{GST} = 1$  (initial stabilization). The structure of the inductive invariants verified here are very close to one in case of arbitrary bounds  $\Delta$  and  $\Phi$ . While all parameters are assigned specific values in the inductive invariants of small instances, they have arbitrary values in the case of arbitrary bounds.

Table 1 shows the results in verification of Strong Accuracy in case of the initial stabilization, and fixed bounds  $\Delta$  and  $\Phi$ . Table 1 shows the experiments with the three tools TLC, APALACHE, and FAST. The column “#states” shows the number of distinct states explored by TLC. The column “#depth” shows the maximum execution length reached by TLC and APALACHE. The column “buf” shows how to encode the message buffer. The column “LOC” shows the number of lines in the specification of the system behaviors (without comments). The symbol “-” (minus) refers to that the experiments are intentionally missing since FAST does not support the encoding of the message buffer with a predicate. The abbreviation “pred” refers to the encoding of the message buffer with a predicate. The abbreviation “cntr” refers to the encoding of the message buffer with a counter. The abbreviation “TO” means a timeout of 6 hours. In these experiments, we initially set  $\text{timeout} = 6 \times \Phi + \Delta$ , and Strong Accuracy is satisfied. The experiments show that TLC finishes its tasks faster than the others, and APALACHE prefers the encoding of the message buffer with a predicate.

Table 2 summarizes the results in verification of Strong Accuracy with the tools TLC, APALACHE, and FAST in case of the initial stabilization, and small bounds  $\Delta$  and  $\Phi$ , and initially  $\text{timeout} = \Delta + 1$ . Since  $\text{timeout}$  is initialized with a too small value, there exists a case in which sent messages are delivered after the timeout expires. The tools reported an error execution where Strong Accuracy is violated. In these experiments, APALACHE is the winner. The abbreviation “TO” means a timeout of 6 hours. The meaning of other columns and abbreviations is the same as in Table 1.

Table 3 shows the results in verification of inductive invariants for Strong Accuracy and Strong Completeness with TLC and APALACHE in case of the initial stabilization, and slightly larger but fixed bounds  $\Delta$  and  $\Phi$ , e.g.,  $\Delta = 20$  and  $\Phi = 20$ . The message buffer was

TABLE 1. Showing Strong Accuracy for fixed parameters.

#	$\Delta$	$\Phi$	buf	TLC				APALACHE		FAST	
				time	#states	depth	LOC	time	depth	time	LOC
1	2	4	pred	3s	10.2K	176	190	8m	176	-	-
2			cntr	3s	10.2K	176	266	9m	176	16m	387
3	4	4	pred	3s	16.6K	183	190	12m	183	-	-
4			cntr	3s	16.6K	183	487	35m	183	TO	2103
5	4	5	pred	3s	44.7K	267	190	TO	222	-	-
6			cntr	3s	44.7K	267	487	TO	223	TO	2103

TABLE 2. Violating Strong Accuracy for fixed parameters.

#	$\Delta$	$\Phi$	buf	TLC			APALACHE		FAST
				time	#states	depth	time	depth	time
1	2	4	pred	1s	840	43	11s	42	-
2			cntr	1s	945	43	12s	42	10m
3	4	4	pred	2s	1.3K	48	15s	42	-
4			cntr	2s	2.4K	56	16s	42	TO
5	20	20	pred	TO	22.1K	77	1h15m	168	-

TABLE 3. Proving inductive invariants with TLC and APALACHE.

#	$\Delta$	$\Phi$	Property	TLC		APALACHE
				time	#states	time
1	4	40	Strong Accuracy	33m	347.3M	12s
2	4	10	Strong Completeness	44m	13.4M	17s

encoded with a predicate in these experiments. In these experiments, inductive invariants hold, and APALACHE is faster than TLC in verifying them. In our experiment, we applied the counterexample-guided approach to manually find inductive strengthenings.

As one sees from the tables, APALACHE is fast at proving inductive invariants, and at finding a counterexample when a desired safety property is violated. TLC is a better option in cases where a safety property is satisfied.

In order to prove correctness of the failure detector in cases where parameters  $\Delta$  and  $\Phi$  are arbitrary, the user can use the interactive theorem prover TLA<sup>+</sup> Proof System (TLAPS) [CDLM10]. A shortcoming of TLAPS is that it does not provide a counterexample when an inductive invariant candidate is violated. Moreover, proving the failure detector with TLAPS requires more human effort than with IVy. Therefore, we provide IVy proofs in Section 10.

**9.2. FAST.** A shortcoming of the model checkers TLC and APALACHE is that parameters  $\Delta$  and  $\Phi$  must be fixed before running these tools. FAST is a tool designed to reason about safety properties of counter systems, i.e. automata extended with unbounded integer

```

1: transition SSnd_Active := {
2:   from := incMsgAge;
3:   to := ssnd;
4:   guard := sTimer = 0;
5:   action := buf' = buf + 1; };

```

FIGURE 9. Sending a new message in FAST in case of  $\Delta > 0$

variables [BLP06]. If  $\Delta$  is fixed, and the message buffer is encoded with a counter, the failure detector becomes a counter system. We specified the failure detector in FAST, and made experiments with different parameter values to understand the limit of FAST: (i) the initial stabilization, and small bounds  $\Delta$  and  $\Phi$ , and (ii) the initial stabilization, fixed  $\Delta$ , but unknown  $\Phi$ .

Figure 9 represents a FAST transition for sending a new message in case of  $\Delta > 0$ . Line 2 describes the (symbolic) source state of the transition, and region `incMsgAge` is a set of configurations in the failure detector that is reachable from a transition for increasing message ages. Line 3 mentions the (symbolic) destination state of the transition, and region `sSnd` is a set of configurations in the failure detector that is reachable from a transition named “SSnd\_Active” for sending a new message. Line 4 represents the guard of this transition. Line 5 is an action. Every unprimed variable that is not written in Line 5 is unchanged.

The input language of FAST is based on Presburger arithmetics for both system and properties specification. Hence, we cannot apply the encoding of the message buffer with a predicate in FAST.

Tables 1 and 2 described in the previous subsection summarize the experiments with FAST, and other tools where all parameters are fixed. Moreover, we ran FAST to verify Strong Accuracy in case of the initial stabilization,  $\Delta \leq 4$ , and arbitrary  $\Phi$ . FAST is a semi-decision procedure; therefore, it does not terminate on some inputs. Unfortunately, FAST could not prove Strong Accuracy in case of arbitrary  $\Phi$ , and crashed after 30 minutes.

## 10. IVY PROOFS FOR PARAMETRIC $\Delta$ AND $\Phi$

While TLC, APALACHE, and FAST can automatically verify some instances of the failure detector with fixed parameters, these tools cannot handle cases with unknown bounds  $\Delta$  and  $\Phi$ . To overcome this problem, we specify and prove correctness of the failure detector with the interactive theorem prover IVy [MP20]. In the following, we first discuss the encoding of the failure detector, and then present the experiments with IVy.

The encoding of the message buffer with a counter requires that bound  $\Delta$  is fixed. We here focus on cases where bound  $\Delta$  is unknown. Hence, we encode the message buffer with a predicate in our IVy specifications,

In IVy, we declare `relation existsMsgOfAge( $X$  : num)`. Type `num` is interpreted as integers. Since IVy does not support primed variables, we need an additional relation `tmpExistsMsgOfAge( $X$  : num)`. Intuitively, we first compute and store the value of `existsMsgOfAge` in the next state in `tmpExistsMsgOfAge`, then copy the value of `tmpExistsMsgOfAge` back to `existsMsgOfAge`. We do not consider the requirement of `tmpExistsMsgOfAge` as a shortcoming of IVy since it is still straightforward to transform the ideas in Section 7 to IVy.

Figure 2 represents how to add a fresh message in the message buffer in IVy. Line 1 means that `tmpExistsMsgOfAge` is assigned an arbitrary value. Line 2 guarantees the appearance of a fresh message. Line 3 ensures that every in-transit message in `existsMsgOfAge` is preserved in `tmpExistsMsgOfAge`. Line 4 copies the value of `tmpExistsMsgOfAge` back to `existsMsgOfAge`.

---

**Algorithm 2** Adding a fresh message in IVy
 

---

```

1: tmpExistsMsgOfAge( $X$ ) := *;
2: assume tmpExistsMsgOfAge(0);
3: assume forall  $X$ : num .  $0 < X \rightarrow$  existsMsgOfAge( $X$ ) = tmpExistsMsgOfAge( $X$ );
4: existsMsgOfAge( $X$ ) := tmpExistsMsgOfAge( $X$ );

```

---

Importantly, our specifications are not in decidable theories supported by IVy. In Formula 7.11, the interpreted function “+” (addition) is applied to a universally quantified variable  $x$ .

The standard way to check whether a safety property *Prop* holds in an IVy specification is to find an inductive invariant *IndInv* with *Prop*, and to (interactively) prove that *IndInv* holds in the specification. To verify the liveness properties Eventually Strong Accuracy, and Strong Completeness, we reduced them into safety properties by applying a reduction technique in Section 8, and found inductive invariants containing the resulting safety properties reduced from the liveness properties. These inductive invariants are the generalization of the inductive invariants in case of fixed parameters that were found in the previous experiments.

TABLE 4. Proving inductive invariants with IVy for arbitrary  $\Delta$  and  $\Phi$ .

#	Property	timeout <sub>init</sub>	time	LOC	#line <sub>I</sub>	#strengthening steps
1	Strong Accuracy	$= 6 \times \Phi + \Delta$	4s	183	30	0
2	Eventually Strong Accuracy	$= \star$	4s	186	35	0
3	Strong Completeness	$= 6 \times \Phi + \Delta$	8s	203	111	0
4		$\geq 6 \times \Phi + \Delta$	22s	207	124	15
5		$= \star$	44s	207	129	0

Table 4 shows the experiments on verification of the failure detector with IVy in case of unknown  $\Delta$  and  $\Phi$ . The symbol  $\star$  refers to that the initial value of `timeout` is arbitrary. The column “#line<sub>I</sub>” shows the number of lines of an inductive invariant, and the column “#strengthening steps” shows the number of lines of strengthening steps that we provided for IVy. The meaning of other columns is the same as in Table 1. While our specifications are not in the decidable theories supported in IVy, our experiments show that IVy needs no user-given strengthening steps to prove most of our inductive invariants. Hence, it took us about 4 weeks to learn IVy from scratch, and to prove these inductive invariants.

The most important thing to prove a property satisfied in an IVy specification is to find an inductive invariant. Our inductive invariants use non-linear integers, quantifiers, and uninterpreted functions. (The inductive invariants in Table 4 are given in the repository [TKW].)

While IVy supports a liveness-to-safety reduction [PHL<sup>+</sup>17], this technique is not fully automated, and IVy still needs user-guided inductive invariant for reduced safety properties that may be different from those in Table 4. Moreover, IVy has not supported reasoning techniques for clocks. Therefore, we did not try the liveness-to-safety reduction of IVy.

It is straightforward to generalize the inductive invariants in Table 4 for partially synchronous models with known time bounds in [DLS88, CT96]. To reason about models with  $\text{GST} > 0$ , we need to find additional inductive strengthenings because the global system is under asynchrony before GST. Other partially synchronous models in [ABND<sup>+</sup>87] consider additional parameters, e.g., message order or point-to-point transmission that are out of scope of this paper.

## 11. RELATED WORK

**11.1. Cutoffs.** Distributed algorithms are typically parameterized in the number of participants, e.g., two-phase commit protocol [LS79] and the Chandra and Toueg failure detector in Section 2. While the general parameterized verification problem is undecidable [AK86, Suz88, BJK<sup>+</sup>15], many distributed algorithms such as mutual exclusion and cache coherence enjoy the cutoff property, which reduces the parameterized verification problem to verification of a small number of instances. In a nutshell, a cutoff for a parameterized algorithm  $\mathcal{A}$  and a property  $\phi$  is a number  $k$  such that  $\phi$  holds for every instance of  $\mathcal{A}$  if and only if  $\phi$  holds for instances with  $k$  processes [EN95, BJK<sup>+</sup>15]. In the last decades, researchers have proved the cutoff results for various models of computation: ring-based message-passing systems [EN95, EK04], purely disjunctive guards and conjunctive guards [EK00, EK03], token-based communication [CTTV04], and quorum-based algorithms [MSB17]. However, we cannot apply these results to the Chandra and Toueg failure detector because it relies on point-to-point communication and timeouts. Moreover, distributed algorithms discussed in [EN95, EK00, EK03, EK04, CTTV04, MSB17] are not in the symmetric point-to-point class.

**11.2. Formal verification for partial synchrony.** Partial synchrony is a well-known model of computation in distributed computing. To guarantee liveness properties, many practical protocols, e.g., the failure detector in Section 2 and proof-of-stake blockchains [BKM18, YMR<sup>+</sup>19], assume time constraints under partial synchrony. That is the existence of bounds  $\Delta$  on message delay and  $\Phi$  on the relative speed of processes after some time point.

While partial synchrony is important for system designers, it is challenging for verification. The mentioned constraint makes partially synchronous algorithms parametric in time bounds. Moreover, partially synchronous algorithms are typically parameterized in the number of processes.

Research papers about partially synchronous algorithms, including papers about failure detectors [LAF99, ADGFT06, ADGFT08] contain manual proofs and no formal specifications. Without these details, proving those distributed algorithms with interactive theorem provers [CDL<sup>+</sup>12, MP20] is impossible.

System designers can use timed automata [AD94] and parametric verification frameworks [LPY97, AFKS12, LRST09] to specify and verify timed systems. In the context of timed systems, we are aware of only one paper about verification of failure detectors [AMO12]. In this paper, the authors used three tools, namely UPPAAL [LPY97], mCRL2 [BGK<sup>+</sup>19],



and FDR2 [Ros10] to verify small instances of a failure detector based on a logical ring arrangement of processes. Their verification approach required that message buffers were bounded, and had restricted behaviors in the specifications. Moreover, they did not consider the bound  $\Phi$  on the relative speed of processes. In contrast, there are no restrictions on message buffers, and no ring topology in the Chandra and Toueg failure detector.

In recent years, automatic parameterized verification techniques [KLVW17a, SKWZ19, DWZ20] have been introduced for distributed systems, but they are designed for synchronous and/or asynchronous models. Interactive theorem provers have been used to prove correctness of distributed algorithms recently. For example, researchers proved safety of Tendermint consensus with Ivy [Gal].

## 12. CONCLUSION

We have presented parameterized and parametric verification of both safety and liveness of the Chandra and Toueg failure detector. To this end, we first introduce and formalize the class of symmetric point-to-point algorithms that contains the failure detector. Second, we show that the symmetric point-to-point algorithms have a cutoff, and the cutoff properties hold in three models of computation: synchrony, asynchrony, and partial synchrony.

Next, we develop the encoding techniques to efficiently specify the failure detector, and to tune our models to the strength of the verification tools: model checkers for  $\text{TLA}^+$  (TLC and APALACHE), counter automata (FAST), and the theorem prover Ivy. We verify safety in case of fixed parameters by running the tools TLC, APALACHE, and FAST. To cope with cases of arbitrary bounds  $\Delta$  and  $\Phi$ , we reduce liveness properties to safety properties, and proved inductive invariants with desired properties in Ivy. While our specifications are not in the decidable theories supported in Ivy, our experiments show that Ivy needs no additional user assistance to prove most of our inductive invariants.

Modeling the failure detector in  $\text{TLA}^+$  helped us understand and find inductive invariants in case of fixed parameters. Their structure is simpler but similar to the structure of parameterized inductive invariants. We found that the  $\text{TLA}^+$  Toolbox [KLR19] has convenient features, e.g., Profiler and Trace Exploration. A strong point of Ivy is in producing a counterexample quickly when a property is violated, even if all parameters are arbitrary. In contrast, FAST reports no counterexample in any case. Hence, debugging in FAST is very challenging.

While our specification describes executions of the Chandra and Toueg failure detector, we conjecture that many time constraints on network behaviors, correct processes, and failures in our inductive invariants can be reused to prove other algorithms under partial synchrony. We also conjecture that correctness of other partially synchronous algorithms may be proven by following the presented methodology. For future work, we would like to extend the above results for cases where GST is arbitrary. It is also interesting to investigate how to express discrete partial synchrony in timed automata [AD94], e.g., UPPAAL [LPY97].

## REFERENCES

- [ABND<sup>+</sup>87] Hagit Attiya, Amotz Bar-Noy, Danny Dolev, Daphne Koller, David Peleg, and Radiger Reischuk. Achievable cases in an asynchronous environment. In *SFCS*, pages 337–346. IEEE, 1987.
- [AD94] Rajeev Alur and David L Dill. A theory of timed automata. *Theoretical computer science*, 126(2):183–235, 1994.
- [ADGFT06] Marcos Kawazoe Aguilera, Carole Delporte-Gallet, Hugues Fauconnier, and Sam Toueg. Consensus with Byzantine failures and little system synchrony. In *DSN*, pages 147–155. IEEE, 2006.
- [ADGFT08] Marcos K Aguilera, Carole Delporte-Gallet, Hugues Fauconnier, and Sam Toueg. On implementing omega in systems with weak reliability and synchrony assumptions. *Distributed Computing*, 21(4):285–314, 2008.
- [AFKS12] Étienne André, Laurent Fribourg, Ulrich Kühne, and Romain Soulat. IMITATOR 2.5: A tool for analyzing robustness in scheduling problems. In *FM*, pages 33–36. Springer, 2012.
- [AK86] K. Apt and D. Kozen. Limits for automatic verification of finite-state concurrent systems. *Information Processing Letters*, 15:307–309, 1986.
- [AMO12] Muhammad Atif, Mohammad Reza Mousavi, and Ammar Osaiweran. Formal verification of unreliable failure detectors in partially synchronous systems. In *SAC*, pages 478–485, 2012.
- [AW04] Hagit Attiya and Jennifer Welch. *Distributed Computing: Fundamentals, Simulations and Advanced Topics, Second Edition*. John Wiley & Sons, Inc., 2004.
- [BCG20] Manuel Bravo, Gregory Chockler, and Alexey Gotsman. Making Byzantine consensus live. In *DISC*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2020.
- [BFLP08] Sébastien Bardin, Alain Finkel, Jérôme Leroux, and Laure Petrucci. Fast: acceleration from theory to practice. *International Journal on Software Tools for Technology Transfer*, 10(5):401–424, 2008.
- [BGK<sup>+</sup>19] Olav Bunte, Jan Friso Groote, Jeroen JA Keiren, Maurice Laveaux, Thomas Neele, Erik P de Vink, Wieger Wesselink, Anton Wijs, and Tim AC Willemse. The mCRL2 toolset for analysing concurrent systems. In *TACAS*, pages 21–39. Springer, 2019.
- [BJK<sup>+</sup>15] Roderick Bloem, Swen Jacobs, Ayrat Khalimov, Igor Konnov, Sasha Rubin, Helmut Veith, and Josef Widder. *Decidability of Parameterized Verification*. Synthesis Lectures on Distributed Computing Theory. Morgan & Claypool Publishers, 2015.
- [BKM18] Ethan Buchman, Jae Kwon, and Zarko Milosevic. The latest gossip on BFT consensus. *arXiv preprint arXiv:1807.04938*, 2018.
- [BLP06] Sébastien Bardin, Jérôme Leroux, and Gérald Point. Fast extended release. In *CAV*, pages 63–66, 2006.
- [CDL<sup>+</sup>12] Denis Cousineau, Damien Doligez, Leslie Lamport, Stephan Merz, Daniel Ricketts, and Hernán Vanzetto. TLA<sup>+</sup> proofs. In *FM*, pages 147–154. Springer, 2012.
- [CDLM10] Kaustuv Chaudhuri, Damien Doligez, Leslie Lamport, and Stephan Merz. The TLA<sup>+</sup> Proof System: Building a heterogeneous verification platform. In *ICTAC*, pages 44–44. Springer, 2010.
- [CJGK<sup>+</sup>18] Edmund M Clarke Jr, Orna Grumberg, Daniel Kroening, Doron Peled, and Helmut Veith. *Model checking*. MIT press, 2018.
- [CT96] Tushar Deepak Chandra and Sam Toueg. Unreliable failure detectors for reliable distributed systems. *Journal of the ACM*, 43(2):225–267, 1996.
- [CTTV04] Edmund Clarke, Muralidhar Talupur, Tayssir Touili, and Helmut Veith. Verification by network decomposition. In *CONCUR*, pages 276–291. Springer, 2004.
- [DLS88] Cynthia Dwork, Nancy Lynch, and Larry Stockmeyer. Consensus in the presence of partial synchrony. *Journal of the ACM*, 35(2):288–323, 1988.
- [DWZ20] Cezara Drăgoi, Josef Widder, and Damien Zufferey. Programming at the edge of synchrony. *Proceedings of the ACM on Programming Languages*, 4(OOPSLA):1–30, 2020.
- [EK00] E Allen Emerson and Vineet Kahlon. Reducing model checking of the many to the few. In *CADE*, pages 236–254. Springer, 2000.
- [EK03] E Allen Emerson and Vineet Kahlon. Exact and efficient verification of parameterized cache coherence protocols. In *Advanced Research Working Conference on Correct Hardware Design and Verification Methods*, pages 247–262. Springer, 2003.
- [EK04] E. Allen Emerson and Vineet Kahlon. Parameterized model checking of ring-based message passing systems. In *CSL*, volume 3210 of *LNCS*, pages 325–339. Springer, 2004.

- [EN95] E Allen Emerson and Kedar S Namjoshi. Reasoning about rings. In *POPL*, pages 85–94, 1995.
- [Gal] Inc. Galois. Ivy proofs of tendermint. URL: <https://github.com/tendermint/spec/tree/master/ivy-proofs>, accessed: December 2020.
- [Hoa80] Charles Antony Richard Hoare. A model for communicating sequential process. 1980.
- [KKT19] Igor Konnov, Jure Kukovec, and Thanh-Hai Tran. TLA<sup>+</sup> model checking made symbolic. *Proceedings of the ACM on Programming Languages*, 3(OOPSLA):1–30, 2019.
- [KLR19] Markus Alexander Kuppe, Leslie Lamport, and Daniel Ricketts. The TLA<sup>+</sup> toolbox. *arXiv preprint arXiv:1912.10633*, 2019.
- [KLVW17a] Igor Konnov, Marijana Lazic, Helmut Veith, and Josef Widder. Para<sup>2</sup>: Parameterized path reduction, acceleration, and SMT for reachability in threshold-guarded distributed algorithms. *Formal Methods in System Design*, 51(2):270–307, 2017.
- [KLVW17b] Igor Konnov, Marijana Lazić, Helmut Veith, and Josef Widder. A short counterexample property for safety and liveness verification of fault-tolerant distributed algorithms. In *POPL*, pages 719–734, 2017.
- [LAF99] Mikel Larrea, Sergio Arévalo, and Antonio Fernández. Efficient algorithms to implement unreliable failure detectors in partially synchronous systems. In *DISC*, pages 34–49. Springer, 1999.
- [Lam02] Leslie Lamport. *Specifying systems: The TLA<sup>+</sup> language and tools for hardware and software engineers*. Addison-Wesley, 2002.
- [LPY97] Kim G Larsen, Paul Pettersson, and Wang Yi. UPPAAL in a nutshell. *International Journal on Software Tools for Technology Transfer*, 1(1-2):134–152, 1997.
- [LRST09] Didier Lime, Olivier H Roux, Charlotte Seidner, and Louis-Marie Traonouez. Romeo: A parametric model-checker for Petri nets with stopwatches. In *TACAS*, pages 54–57. Springer, 2009.
- [LS79] Butler Lampson and Howard E Sturgis. Crash recovery in a distributed data storage system. 1979.
- [LT88] Nancy A Lynch and Mark R Tuttle. *An introduction to input/output automata*. Laboratory for Computer Science, Massachusetts Institute of Technology, 1988.
- [Mic] Microsoft and HP. The TLA<sup>+</sup> Toolbox. URL: [github.com/tlaplus](https://github.com/tlaplus), accessed: July 2021].
- [MP20] Kenneth L McMillan and Oded Padon. Ivy: a multi-modal verification tool for distributed algorithms. In *CAV*, pages 190–202. Springer, 2020.
- [MSB17] Ognjen Marić, Christoph Sprenger, and David Basin. Cutoff bounds for consensus algorithms. In *CAV*, pages 217–237. Springer, 2017.
- [PHL<sup>+</sup>17] Oded Padon, Jochen Hoenicke, Giuliano Losa, Andreas Podelski, Mooly Sagiv, and Sharon Shoham. Reducing liveness to safety in first-order logic. In *POPL*, pages 1–33, 2017.
- [Pnu77] Amir Pnueli. The temporal logic of programs. In *SFCS*, pages 46–57. IEEE, 1977.
- [PW97] Doron Peled and Thomas Wilke. Stutter-invariant temporal properties are expressible without the next-time operator. *Information Processing Letters*, 63(5):243–246, 1997.
- [Ros10] Andrew William Roscoe. *Understanding concurrent systems*. Springer Science & Business Media, 2010.
- [SKWZ19] Iliana Stoilkovska, Igor Konnov, Josef Widder, and Florian Zuleger. Verifying safety of synchronous fault-tolerant algorithms by bounded model checking. In *TACAS*, pages 357–374. Springer, 2019.
- [Suz88] Ichiro Suzuki. Proving properties of a ring of finite-state machines. *Information Processing Letters*, 28(4):213–214, 1988.
- [Sys19] Informal Systems. APALACHE: symbolic model checker for TLA<sup>+</sup>, 2019. URL: [github.com/informalsystems/apalache](https://github.com/informalsystems/apalache), accessed: July 2021.
- [TKW] Thanh-Hai Tran, Igor Konnov, and Josef Widder. Specifications of the Chandra and Toueg failure detector in TLA<sup>+</sup>, FAST, and Ivy. URL: <https://zenodo.org/record/4687714#.YHcBeBKxVH4>, accessed: April 2021.
- [TKW20] Thanh-Hai Tran, Igor Konnov, and Josef Widder. Cutoffs for symmetric point-to-point distributed algorithms. In *NETYS*, pages 329–346. Springer, 2020.
- [TKW21] Thanh-Hai Tran, Igor Konnov, and Josef Widder. A case study on parametric verification of failure detectors. In *FORTE*, pages 138–156. Springer, 2021.
- [YML99] Yuan Yu, Panagiotis Manolios, and Leslie Lamport. Model checking TLA<sup>+</sup> specifications. In *Correct Hardware Design and Verification Methods*, pages 54–66. Springer, 1999.

[YMR<sup>+</sup>19] Maofan Yin, Dahlia Malkhi, Michael K Reiter, Guy Golan Gueta, and Ittai Abraham. Hotstuff: BFT consensus with linearity and responsiveness. In *PODC*, pages 347–356, 2019.

## APPENDIX A. LINEAR TEMPORAL LOGIC (LTL)

The syntax of LTL formulae is given by the following syntax [Pnu77]:

$$\phi ::= \top \mid p \mid \neg\phi \mid \phi \wedge \phi \mid \mathbf{X}\phi \mid \phi \mathbf{U}\phi$$

where

- $\top$  stands for true,
- $p$  ranges over a countable set  $AP$  of atomic predicates,
- $\neg$  and  $\wedge$  are Boolean operators negation and conjunction respectively,
- $\mathbf{X}$  and  $\mathbf{U}$  are the temporal operators next and until respectively.

Other Boolean operators  $\vee$ ,  $\Rightarrow$ , and  $\Leftrightarrow$  are defined in the standard way. We also use  $\perp$  (false),  $\mathbf{F}$  (eventually),  $\mathbf{G}$  (always) to abbreviate  $\neg\top$ ,  $\top \mathbf{U}\phi$ , and  $\neg(\top \mathbf{U}\neg\phi)$  respectively.

Let us consider an LTL formula  $\phi$  over propositions in  $AP$  and a word  $w: \mathbb{N} \rightarrow 2^{AP}$ . We define the relation  $w \models \phi$  (the word  $w$  satisfies the formula  $\phi$ ) inductively as follows.

- $w \models \top$  for all  $w$
- $w \models p$  if  $p \in w[0]$
- $w \models \neg\phi$  if not  $w \models \phi$
- $w \models \phi_1 \wedge \phi_2$  if  $w \models \phi_1$  and  $w \models \phi_2$
- $w \models \mathbf{X}\phi$  if  $w[1..] \models \phi$  where  $w[k..]$  denotes the suffix  $w[k]w[k+1]\dots$
- $w \models \phi_1 \mathbf{U}\phi_2$  if there exists  $j \geq 0$  such that  $w[j..] \models \phi_2$  and for all  $0 \leq i < j$ ,  $w[i..] \models \phi_1$

Two words  $w$  and  $w'$  are stuttering equivalent if there are two infinite sequences of numbers  $0 = i_0 < i_1 < i_2 < \dots$  and  $0 = j_0 < j_1 < j_2 < \dots$  such that for every  $\ell \geq 0$ , it holds  $w_{i_\ell} = w_{i_\ell+1} = \dots = w_{i_{\ell+1}-1} = w'_{j_\ell} = w'_{j_\ell+1} = \dots = w'_{j_{\ell+1}-1}$  [CJGK<sup>+</sup>18].

In this paper, we deal with properties in  $\text{LTL} \setminus \mathbf{X}$  (LTL minus the next operator). Importantly, all LTL properties that are invariants under stuttering equivalence can be expressed without the next operator  $\mathbf{X}$  [PW97].