

Algorithmic Analysis of Channel Machines Using Small Models

Jonathan Sharyari

11th April 2015

Abstract

Verification of infinite-state systems is in general an undecidable problem, but nevertheless, solid correctness results are important in many real-life applications. It is commonly the case that such algorithms rely on unbounded buffers for their operation, communication protocols being a typical example. Building upon abstract interpretation techniques, this project presents a verification algorithm capable of verifying the correctness of algorithms relying on unbounded *lossy* buffers.

We have implemented our approach and used it to verify a number of well-known communication protocols. The experimental results are mixed, but in most cases comparable to that of other existing tools, justifying further research on the topic.

Contents

1 Introduction

Today's society grows more and more dependent on computer applications. Often they are used directly, for example the task of paying bills online. In other cases, applications are aiding us in a more abstract manner, e.g. controlling the elevator or planning a train schedule. The common factor between the online bank, the elevator relay and the train scheduler is that the correctness of these programs is of utter importance, where program failure could have devastating results on the economy, the infrastructure or even cause harm.

This has motivated research on various techniques to find and correct potential faults, particularly in safety-critical systems. The most common technique is that of *testing*, i.e. observing the system behaviour on a variety of likely or even unlikely scenarios. The widespread use of testing is well-motivated, but there are several scenarios where testing by itself is insufficient, as testing does not provide any guarantee of correctness.

Another technique used for verification is the process of *simulation*. In comparison to testing, simulation can be done in an earlier stage of the development. Rather than first implementing an algorithm, one may simulate an abstracted model of the algorithm which may help in ensuring its correctness or find a fault in the algorithm before development has begun. An important note is that simulation techniques are not intended to be used *instead* of testing, but rather in combination with testing, as an abstract model of a system can never fully represent the system as a whole.

The goal of *model checking* is to formally verify the correctness of concurrent programs with respect to a given specification. In general, given a model of a system and a specification of its intended properties, the task is to decide whether the model meets its specification or not.

Different representations of models and properties have been proposed, as well as techniques to perform the verification. One of the most successful and common methods is that of *temporal logic model checking*. Traditionally, the model is expressed as a finite state machine and the properties as propositional logic formulae. Several verification methods for such models have been proposed[?] and although these methods have been applied to infinite models[?], the focus has in large been on the verification of finite models.

A trend in today's computing is that applications become concurrent or distributed. Such programs are inherently difficult to verify, as although processes themselves have finite models, the results of the asynchronous behaviour of processes may be infinite. This is the case for example when the composition of a possibly infinite number of processes is observed, a common scenario when verifying concurrent and distributed programs. Also, we are often not interested in performing verification of a *specific* composition of concurrent programs, but rather in verifying that it works for *all* compositions.

Related to this is the necessity for distributed and concurrent programs to communicate, and to do so accurately. In general, the underlying systems that we use for our communication are unreliable, in that message loss or message corruption may occur. This happens due to a variety of reasons, may that

be errors in the communication links, relays or the communicating parties themselves. To overcome this problem, communication protocols are designed to be resistant to such faults, and ensuring the correctness of these protocols is paramount when ensuring reliable communication. Even when the number of communicating processes is finite, communication protocols commonly result in infinite models, as the number of sent messages may be unbounded, so there could be an infinite number of messages in the buffer. The verification of systems relying asynchronous unbounded buffers, is the focus of this thesis.

Such *channel systems* are common in communication protocols using channels and in distributed computing[?]. Channels systems may also represent other types of programs, such as cache coherence protocols and sensor systems[?]. An important note is that channel systems using *perfect channels*, i.e. channels without message loss, are Turing powerful, and all non-trivial problems are therefore undecidable. However it has been proven that verification of *safety properties* of channel systems over *lossy channels*, i.e. channels that may non-deterministically lose messages, is decidable[?][?]. Nevertheless, the problem is difficult to verify, having high computational complexity.

The main problem when verifying such systems is to find a way to construct a finite approximation of the infinite system. In order to solve this problem, we find inspiration in [?], where the verification of *parameterized systems* is attempted. *Parameterized systems* are systems composed of a set of processes, where the number of processes is itself a parameter of the system – this is often the case when discussing concurrent and distributed programs. Although an undecidable problem, there are methods that provide good approximation techniques which consist in reducing the verification task to the case of finite state systems.

In [?], the authors take advantage of the fact that parameterized systems often enjoy a *small model property*, meaning that the verification of small instances of the system is enough, to capture the reachability of bad configurations. An important contribution of [?] is that they show that this property holds for any *well-structured transition systems*[?] (i.e. transitions systems monotonic with respect to a well-quasi ordering).

Building upon the work in [?], we explore the possibility of adapting the verification algorithm proposed in [?], in order to verify systems with unbounded lossy channels.

The verification algorithm is based on an enumerative exploration of all the finite approximations by bounding the size of the channels. To verify each bounded instance of the system (let us assume that the size of the buffers is bounded by $k \in \mathbb{N}$) we use a standard forward reachability algorithm. If the reachability analysis returns a counter-example, then this a real counter-example of our system and the analysis procedure terminates. Otherwise, if the analysis procedure declares the finite approximation as safe, then we proceed to a second verification step. This extra verification step uses abstract interpretation techniques[?][?], with the goal to check if k is a *cut-off* point which means that there is no need to verify any larger instance and we can claim that the program is safe. If the second step determines that the algorithm is

safe, then the algorithm is truly safe for that instance and all larger instances. If, on the otherhand, a counter-example is found, this means that the reachability analysis must be repeated, with the buffers bounded to size $k + 1$.

As lossy channel systems are well-structured, the small model property holds for the classes of systems being considered in this thesis, thus a cut-off point will eventually be found, leaving a termination guarantee for the algorithm.

The verification technique was implemented and tested for some common communication protocols. The results were compared to that of two other verification techniques for the same classes of systems; the MPass[?] verifier translates verification problems to satisfiability problems, solvable using third party SAT-solvers, and a *backward reachability analysis* as described in [?]. The backward analysis algorithm was implemented within the scope of this project for the purpose of comparison. The experimental results confirm the correctness of the results, and show that the verification times are comparable or faster than the alternative methods for most of the verified protocols.

Reading this paper. Section 2 contains formal definitions to some of the key concepts – these are previously known concepts, asides from their adaption to the specific context of this thesis. Section 3 introduces the concepts of small models and abstract interpretation, and relates these to buffer channels to create the theoretical model for this paper. In section ??, some abstractions and techniques are explained that allow for an efficient implementation of the verification algorithm. Further a protocol specification language is explained, that allows a user to define and use the verification tool without knowledge of the intricacies of the internal model. The results of the verifier when applied to a number of well-known communication algorithms is presented in section ??, as well as some comparisons against the results of other verification tools.

2 Formal Model for Lossy Channel Systems

In this chapter we will give the formal definition of a channel system. First we define some necessary terminology, such as alphabets and words, before giving the syntax and semantics of a channel system. Then we illustrate these ideas by applying them to a well-known communication protocol, the *alternating bit protocol*. Finally, we state the formal definition of the verification problem we are investigating.

2.1 Preliminaries

2.1.1 Words and Alphabet

A word $w = a_1a_2 \dots a_n$ is a finite sequence of letters from an alphabet Σ , where a_i is in Σ for all i in $\{1 \dots n\}$. We use ϵ to denote the empty word. We define the length of a word w to be the number of letters appearing in it (i.e., the length of the word $w = a_1a_2 \dots a_n$, with $a_1, a_2, \dots, a_n \in \Sigma$, is n). We use $|w|$ to denote the length of the word w . Observe that $|\epsilon| = 0$. We use Σ^* (resp. Σ^+) to denote the set of all words (resp. non-empty words) over the alphabet Σ . Let k be a natural number. We use Σ_k^* (resp. Σ_k^+) to denote the set of all words (resp. non-empty words) of length at most k . We use the symbol \bullet to emphasize the concatenation of two words, i.e. $w_1w_2w_3$ can be written as $w_1 \bullet w_2 \bullet w_3$.

Let $\sigma : \Sigma^* \rightarrow \Sigma^*$ be a mapping between words, s.t. $\sigma(a_1 \dots a_n) = \tau(a_1) \dots \tau(a_n)$, where $\tau(a_i)$ is either a_i or ϵ , $0 \leq i \leq n$. We call $\sigma(w) = w'$ a *subword* of w , denoted $w' \sqsubseteq w$.

As an example, if $w=abc$, then the set of subwords of w is $abc, ab, ac, bc, a, b, c, \epsilon$.

2.1.2 Fixpoints

Let A be a set. We use 2^A to denote the set of all the subsets of A . Let F be a function with 2^A as its domain and co-domain. We say that F is a *monotonic function* if and only if for every subset $X, Y \subseteq A$, if $X \subseteq Y$ then $F(X) \subseteq F(Y)$. We say that X is a *fixpoint* of F iff $F(X) = X$. We use $\mu X.F(X)$ to denote the least fixpoint of F with respect to the subset relation (i.e., $\mu X.F(X)$ denotes the smallest set $D \subseteq A$, such that D is a fixpoint of F). From the Knaster-Tarski theorem [?], we know that the least-fix point for a monotonic function exists. Furthermore, if A is finite, then the sequence $X_0 = I, X_{i+1} = f(A_{n-1})$ for all $i \geq 0$, converges in finitely many iterations to the least-fixpoint of F .

2.2 Lossy Channel Systems

2.2.1 Syntax

We present here the syntax of a finite-state system with unbounded channels. Such a system can be seen as two parts, a *control part* and a *channel part*. The

channel part is a set of *channels*, each containing a word. The control part is a labeled finite-state transition system.

Formally, a lossy channel system LCS is a tuple $(S, s^0, A, Ch, \Sigma, \delta)$, where

- S is a finite set of control states
- s^0 is the initial control state
- A is a set of labeled actions
- Ch is a finite set of channels,
- Σ is a finite alphabet,
- δ is a finite set of transitions, each of which is a triple of the form (s, op, s') , where $s, s' \in S$ are control states, and op is a label of one of the forms
 - $ch!m$, where $ch \in Ch$ and $m \in M$
 - $ch?m$, where $ch \in Ch$ and $m \in M$
 - $a \in A$

where M denotes the set of finite words over Σ . We use the notation $s \xrightarrow{op} s'$ to describe (s, op, s') .

The finite-state control part of LCS is the set of states S , with the initial state s^0 , labeled actions A and transitions δ . The channel part is represented by the set Ch of channels, which contain words over M . The set A denotes the set of internal transitions, which only alter the control state of the system, whereas δ may either be an action from A , or an action where

$(s, ch!m, s')$ represents a change of state from $s \in S$ to $s' \in S$ while appending the message $m \in M$ to the tail of channel $ch \in Ch$.

$(s, ch?m, s')$ represents a change of state from $s \in S$ to $s' \in S$ while removing the message $m \in M$ from the head of channel $ch \in Ch$

2.2.2 Configurations

Let $\xi : Ch \rightarrow \Sigma^*$ be a function that maps the content of each channel $ch \in Ch$ to a word w over Σ , then we will call w the *evaluation* of the channel ch , and we call ξ a *channel evaluation*. We define a *configuration* to be a tuple $c = (s, \xi)$, such that $s \in S$ is a global control state and ξ is a channel evaluation.

Let $c = (s, \xi)$ be a configuration. We use $state(c)$ and $eval(c)$ to denote the state and the evaluation in c , respectively and use the shorthand $c_S = state(c)$ and $c_E = eval(c)$ for a configuration c .

Let ξ^0 denote the empty channel evaluation such that for each channel $ch \in Ch$, we $\xi^0(ch) = \epsilon$. We define c^0 to be the initial configuration (s^0, ξ^0) , i.e. the configuration with all processes in their initial state and all channel evaluations being the empty word.

We define the size of a configuration $c = (s, \xi)$ to be the length of the longest word in the channels, i.e., $\text{size}(c) = \max\{|\xi(ch)|, ch \in Ch\}$.

Finally, we extend the subword relation to the configuration of the lossy channel system as follows: Let $c = (s, \xi)$ and $c' = (s', \xi')$ be two configurations of the lossy channel system. We say that c is a sub-configuration of c' (denoted $c \sqsubseteq c'$) if and only if $s = s'$ and for every channel $ch \in Ch$, we have $\xi(ch)$ is a subword of $\xi'(ch)$.

2.3 Semantics

In the following section, we explain the semantics of a lossy channel system, which describes the behaviour of the system. The operational behaviour of LCS induces the infinite-state transition system $LTS = (C, \rightarrow)$ where C is a set of configurations and $\rightarrow \subseteq (C \times C)$ is the smallest transition relation defined as follows:

- For each transition $(s, a, s') \in \delta$ and each channel evaluation ξ , $(s, \xi) \xrightarrow{a} (s', \xi)$. This means that the control state changes with the action a .
- For each transmission transition $(s, ch!m, s')$ in δ and channel evaluations ξ and ξ' , $(s, \xi) \xrightarrow{ch!m} (s', \xi')$, $\xi'(ch) = \xi(ch) \bullet m$, and $\xi'(ch') = \xi(ch')$ for all $ch' \in Ch \setminus ch$. This means that the control state and the evaluation of the configuration change, so that the message m is appended to the content of the channel ch .
- For each reception transition $(s, ch?m, s)$ in δ and channel evaluations ξ and ξ' , $(s, \xi) \xrightarrow{ch!m} (s', \xi')$ such that $\xi(ch) = m \bullet \xi'(ch)$ and $\xi'(ch') = \xi(ch')$ for all $ch' \in Ch \setminus ch$. This means that the control state and the evaluation of the configuration change, so that the message m is removed from the content of the channel ch .
- For each state $s \in S$ and channel evaluations ξ and ξ' , $(s, \xi) \xrightarrow{*} (s, \xi')$ such that $\xi'(ch)$ is a subword of $\xi(ch)$ for all $ch \in Ch$. This means that any message can be lost at any time.

Notations for configurations Depending on the context, different notations to describe a configuration $c \in C$ may be used. For example, $c = (s, \xi)$ can be denoted as $c = (s, w_1, w_2, \dots, w_n)$ when the set of channels is ordered (e.g., $Ch = \{ch_1, ch_2, \dots, ch_n\}$).

We refer to the act of taking a transition $c' \xrightarrow{r} c$, as *firing* the transition $r = (s, \tau, s')$ from c to c' such that $\text{state}(c) = s$ and $\text{state}(c') = s'$.

2.4 Alternating Bit Protocol

Here we present a simple protocol, the *alternating bit protocol* [?]. This protocol will serve as a running example of the theoretical concepts in this and following sections.

The Alternating Bit Protocol (ABP)[?] is a distributed protocol for transmitting data from a *sender* to a *receiver* in a network. The protocol uses two unbounded channels, ch_M used to transmit messages and ch_A to transmit *acknowledgements* of received messages. The sender sends data with a sequence number $x \in \{0,1\}$ to the receiver over channel ch_M , who upon reception sends an acknowledgement with the same sequence number over channel ch_A . Both the sender and the receiver may send the same message (with the same sequence number) repeatedly. When the sender receives an acknowledgement from the receiver, the next message can be sent using the sequence number $1 - x$, hence the name Alternating Bit Protocol. The behaviour of the sender and receiver process are illustrated in figures 1a and 1b, and the pseudo-code for this algorithm is given below.

Algorithm 1 ABP Sender

```

1: b := False                                ▷ Initially False
2: for True do
3:   msg.send(data, b);                      ▷ Send the message
4:   while ack.receive().b != b do          ▷ Wait until ack has the correct ID
5:     msg.send(data, b);                    ▷ Re-send the message
6:   end while
7:   b := !b                                ▷ Alternate the bit
8: end for

```

Algorithm 2 ABP Receiver

```

1: b := False                                ▷ Initially False
2: for True do
3:   while msg.receive().b != b do          ▷ Wait until msg has the correct ID
4:     ack.send(b);                          ▷ (Re-)transmit the acknowledgement
5:   end while
6:   b := !b                                ▷ Alternate the bit
7: end for

```

In the pseudo-code above, both the sender and receiver have an internal Boolean variable b , which at any time has the value of the sequence number (ID) they expect the next message to have, which may either be False (0) or True (1). The sender will repeatedly send a messages with the current value of b as sequence number, until it receives an acknowledgement from the receiver with the same sequence number, at which point it alternates the value of b . The receiver behaves in the same manner, sending acknowledgements for the last received message until a new message is received.

Syntax. The alternating bit protocol can be described by a channel system $CS = (S, s^0, A, Ch, \Sigma, \delta)$ such that $S = \{(s_i, r_i)\}$ with $i \in \{1 \dots 4\}$, s^0 is the initial state (s_1, r_1) , $A = \{Snd, Rcv\}$, $Ch = \{ch_M, ch_A\}$, $\Sigma = \{1, 0\}$. The set δ of transitions is, for $1 \leq i \leq 4$ the set of transitions:

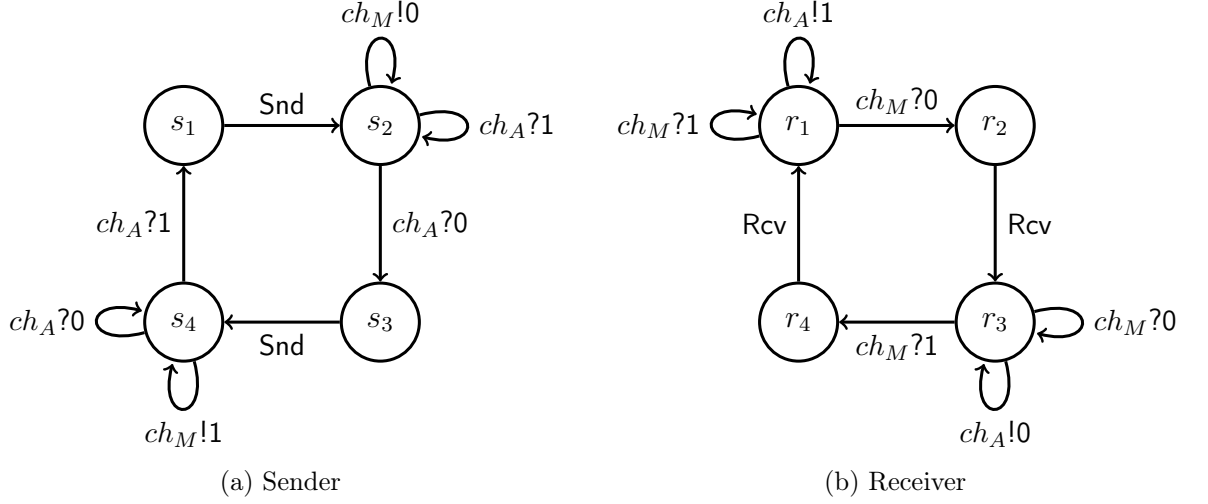


Figure 1: Program graphs of sender and receiver in the ABP protocol.

$$\begin{aligned}
(s_i, r_i) &\xrightarrow{Snd} (s_2, r_1) \xrightarrow{ch_A!1} (s_i, r_1) \\
(s_2, r_i) &\xrightarrow{ch_M!0} (s_2, r_1) \xrightarrow{ch_M?1} (s_i, r_1) \\
(s_2, r_i) &\xrightarrow{ch_A?1} (s_2, r_1) \xrightarrow{ch_M?0} (s_i, r_2) \\
(s_2, r_i) &\xrightarrow{ch_A?0} (s_3, r_2) \xrightarrow{Rcv} (s_i, r_3) \\
(s_3, r_i) &\xrightarrow{Snd} (s_4, r_3) \xrightarrow{ch_A!1} (s_i, r_3) \\
(s_4, r_i) &\xrightarrow{ch_M!1} (s_4, r_3) \xrightarrow{ch_M?0} (s_i, r_3) \\
(s_4, r_i) &\xrightarrow{ch_A?1} (s_i, r_3) \xrightarrow{ch_M?1} (s_i, r_4) \\
(s_4, r_i) &\xrightarrow{ch_A?0} (s_4, r_4) \xrightarrow{Rcv} (s_i, r_1)
\end{aligned}$$

Notations Let $c = (s, \xi)$ be a configuration of the alternating bit protocol, with the channels ch_M and ch_A containing the words 01 and 10 respectively. If the channel ch_M is ordered before ch_A in Ch , then c may also be denoted as $c = (s, 01, 10)$. There are finitely many control states in this system (precisely 16), but an infinite set of channel evaluations. The initial configuration $c^0 = ((s_1, r_1), \xi^0)$.

Although the channel system has a finite number of transitions (listed above) between states, the transition system has an infinite number of transitions between configurations, as these depend also on the evaluations. An example of such a transition $(s_2, r_1, 01, 10), ch_M!1, (s_2, r_1, 011, 10))$.

2.4.1 The Verification Problem

A channel system can potentially reach a *bad* state, i.e. a state representing unintended behaviour. Suppose *Bad* is a set of bad configurations of a lossy transition system *LTS*, as defined in 2.3. We call a sequence $t = c_0 c_1 \dots c_n$ of configurations a *trace*, if $c_i \rightarrow c_{i+1}, 0 \leq i \leq (n-1)$ and we say that c_n is

reachable from c_0 . We call a trace a *bad trace* if there exists $c^{bad} \in Bad$ such that c^{bad} is a sub-configuration of c_n . If t is the shortest bad trace in the system, we call it a *minimal bad trace*.

A configuration c is said to be *reachable* in LTS , if there is a trace from the initial configuration c^0 such that c is reachable. Let \mathcal{R} denote the set of all reachable configurations. The verification problem is to determine, for a channel transition system LTS with an initial configuration c^0 and a set $Bad \subseteq C$ of bad configurations, whether a system is safe, that is, does not have any reachable bad configurations. More precisely, this means determining if $\mathcal{R} \cap Bad = \emptyset$.

3 Verification of Lossy Channel Systems

The goal of this chapter is to formalize the use of *small models* for the verification of lossy channel systems, as is done in [?]. The technique is based on the use of *abstract interpretation* techniques, first formalized by Cousot and Cousot[?]. Abstract interpretation techniques are techniques for approximating programs. Using information about the control and data flow, i.e. the semantics of a system, an overapproximation of the possible configurations of a system can be created, which may result in an infinite set of configurations. In [?] the authors show that such an infinite set of configurations can be safely bounded to a finite set of configurations, by finding a *cut-off* point for the maximum size of the evaluations.

3.1 Views

We define a *view* $v = (s, \xi)$ to be a minimal representation of a set of configurations C_v , such that for any $c \in C_v$, $v \sqsubseteq c$. Note that a view is itself a configuration, as they have the same representation, and we use the same terminology and notation for them, for example $|v|$ to denote the size. The difference is that a configuration is a single entity, whereas the view is an abstract representation of a larger set of configurations.

Example. Let the view $v = ((s_1, r_1), ab, cd)$, then the set C_v is an infinite set, s.t. $((s_1, r_1), ab, cd) \in C_v$, $((s_1, r_1), abab, cdcd) \in C_v$ but $((s_1, r_1), ab, \epsilon) \notin C_v$

3.2 Abstraction function

For a given parameter $k \in \mathbb{N}$, we use C and V to denote sets of configurations and views respectively, and C_k and V_k to denote the set of all configurations and views respectively of size up to k .

The abstraction function $\alpha_k : C \rightarrow 2^{V_k}$ maps a configuration c into a set V' of views of size up to k , such that for each $v \in V'$, $v \sqsubseteq c$ and $size(v) \leq k$.

Example. Suppose c is a configuration (s, ab, cd) . The configuration is of size 2 and $\alpha_2(c)$ is the set

$$\begin{array}{ccccc} (s, ab, cd) & (s, a, cd) & (s, a, c) & (s, a, d) & (s, a, \epsilon) \\ & (s, b, cd) & (s, b, c) & (s, b, d) & (s, b, \epsilon) \\ & (s, \epsilon, cd) & (s, \epsilon, c) & (s, \epsilon, d) & (s, \epsilon, \epsilon) \end{array}$$

3.3 Concretization function

The concretization function $\gamma_k : 2^{V_k} \rightarrow 2^C$ returns, for a given set of views V , the set of configurations that can be reconstructed from the views in V , in other words, $\gamma_k(V) = \{c \in C \mid \alpha_k(c) \subseteq V\}$

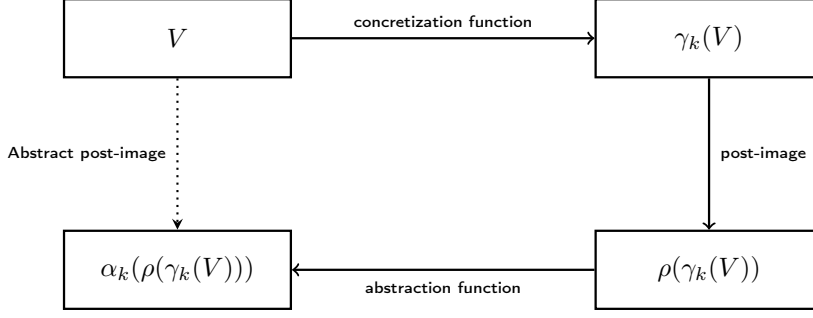


Figure 2: The application order of the α , ρ and γ

In general $\gamma_k(V)$ is an infinite set of configurations. We define $\gamma_k^l(V) := \gamma_k(V) \cap C_l$ for some $l \geq 0$. The intuitive meaning is that $\gamma_k^l(V)$ is the set of configurations of size at most l for which all views of length at most k are in V .

3.4 Post-Image

For a configuration $c \in C$ of a lossy transition system $LTS = (C, \rightarrow)$, we define the *post-image* of c denoted $\rho(c) = \{c' \mid c \rightarrow c'\}$. Intuitively, the post-image of a configuration is the configuration obtained by firing the transitions of the transition system.

For a *set* of configurations V we define the post-image of the set $\rho(V) = \{c' \mid c \rightarrow c', c \in V\}$. This means that the post-image of a set V of configurations is the set $\rho(V)$ containing the post-images of each configurations $c \in V$.

3.5 Abstract Post-Image

The *abstract post-image* of a set $V \subseteq C_k$ is defined as $Apost_k(V) = \alpha_k(\rho(\gamma_k(V)))$. This means that the abstract post-image of a set V is the set obtained by applying γ_k , ρ and α_k in order to the set V . The procedure is illustrated in figure 2.

Note that since $V \subseteq Apost_k(V)$, $Apost_k$ is a monotonic function, thus by the Knaster-Tarski theorem, the function $Apost_k$ has a fixpoint.

3.6 Reachability Analysis

Let LTS be a lossy transition system, with an initial configuration c^0 . Then the set of reachable configurations \mathcal{R} of LTS can be computed inductively as follows: $A_0 = \{c^0\}$, $A_{i+1} = A_i \cup \rho(A_i)$. The finite set of configurations \mathcal{R}_k with size at most k can be similarly computed; $A_0 = \{c^0\}$, $A_{i+1} = A_i \cup (\rho(A_i) \cap C_k)$.

3.7 Small Models

Calculating the abstract post-image of a set of views $V \subseteq C_k$ is essential for the verification procedure. As $\gamma_k(V)$ typically is infinite, this cannot be done straightforwardly. The main result of [?] that it suffices to consider

configurations of $\gamma_k(V)$ of sizes up to $k + 1$ (i.e. γ_k^{k+1}), which is a finite set of configurations for which the abstract post-image can be computed. Formally, they show that

Lemma 1. *For any $k \in \mathbb{N}$, and $X \subseteq C_k$, $\alpha_k(\rho(\gamma_k(X))) \cup X = \alpha_k(\rho(\gamma_k^{k+1}(X))) \cup X$.*

3.7.1 Proof of lemma 1

We want to show that the set $\gamma_k^{k+1}(X)$ of views of size at most $k + 1$ is an abstract representation of the full set $\gamma_k(X)$. In order to do this, we want to show that for any configuration $c \in \rho(\gamma_k(X))$ of size $m > k + 1$ such that there is a transition $c' \xrightarrow{r} c$, then for each view $v' \in \alpha_k(c)$, the following holds: There is a configuration $d' \in \gamma_k^{k+1}(X)$ of size at most $k + 1$ and transition $d' \xrightarrow{r} d$ s.t. $v \in \alpha_k(d)$.

Note that by design (see section 2.3), transitions only change a single evaluation, therefore, although the set of evaluations may contain multiple evaluation, we direct our focus to a single evaluation in this section.

Transmissions Consider a configuration $c' = (s', x) \in \gamma_k(X)$ and a transition $r : c' \xrightarrow{ch!m} c = (s, x \bullet m)$. Any view $v = (s', y)$ of size at most k of c is on one of the following forms:

1. $y \sqsubseteq x$, $|y| \leq k$. In this case, the set $\gamma_k^{k+1}(X)$ includes all the configurations $d' = (s', y)$, as $d'_E \sqsubseteq c'_E$. Then $d' \xrightarrow{ch!m} d$ yields $d = (s, y \bullet m)$, for which $(s, y) = v$ is a view.
2. $y = z \bullet m$ with $z \sqsubseteq x$, $|z| \leq (k - 1)$. The set $\gamma_k^{k+1}(X)$ includes all the configurations $d' = (s', z)$, as $d'_E \leq c'_E$. Then $d' \xrightarrow{ch!m} d$ yields $d = (s, z \bullet m)$ which is of size at most k , meaning it is also a view, $d = v$.

Actions Consider a configuration $c' = (s', x) \in \gamma_k(X)$ and a transition $r : c' \xrightarrow{a} c = (s, x)$. Since r is an action, it can be fired regardless of the channel evaluation. Therefore, if r can be fired from the configuration c' , it may also be fired from any view $v' = (s', y)$ of size at most k of c' , resulting in a view $v = (s, y)$.

Let $\{(s', w_1), (s', w_2), \dots, (s', w_n)\}$ be the views of c' , then the transition r can be fired from each of these, resulting in a set $\{(s, w_1), (s, w_2), \dots, (s, w_n)\}$, which is the complete set of views of size at most k of c , showing that c is abstractly represented in $\gamma_k(X)$.

Receptions and Message Loss Note that receptions transitions can be seen as a special case of a message loss, where messages are lost in FIFO order, i.e. a proof of lemma 1 for message loss directly applies to the reception transitions. Consider a configuration $c' = (s', x) \in \gamma_k(X)$ and a transition $r : c' \xrightarrow{*} c = (s', y)$. Since $y \sqsubseteq x$, the set of views V of c is a subset of the set of views V' of c' .

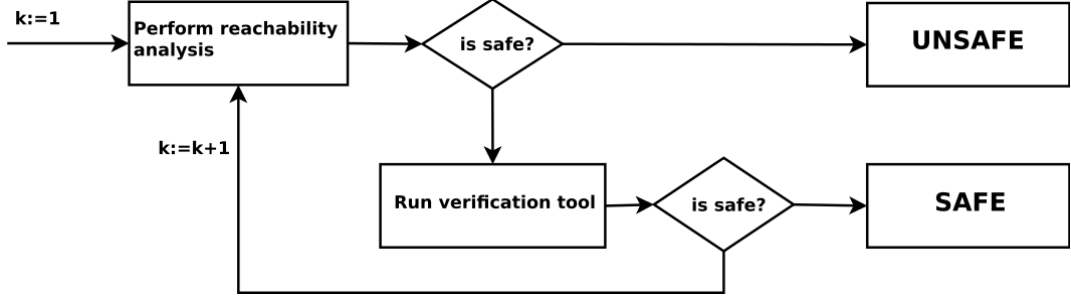


Figure 3: The general flow of the verifier.

3.8 Verification Algorithm

Suppose Bad is a set of bad states, such that $|b| = 0$ for all $b \in Bad$. As a result of lemma 1, if $\gamma_k^{k+1}(V) \cap Bad = \emptyset$ for any $k \geq 1$, then $\gamma_l^{l+1}(V) \cap Bad = \emptyset$ for any $l \geq k$. Given a set of bad states Bad , a set of initial states I and a set of transitions, verification of a system can be done with algorithm 3, which was first presented in [?].

Algorithm 3 General Verification algorithm

```

for  $k := 1$  to  $\infty$ 
  if  $\mathcal{R}_k \cap Bad \neq \emptyset$  then return Unsafe
   $V := \mu X. \alpha_k(I) \cup Apost_k(X)$ 
  if  $\gamma_k(V) \cap Bad = \emptyset$  then return Safe
  
```

The algorithm begins by performing a reachability analysis, as explained in 3.6 in order to compute \mathcal{R}_k and check for bad states. For any buffer size k , if a bad state is found to be reachable in \mathcal{R}_k , the system is unsafe and the algorithm terminates. If no such bad state was found, the algorithm continues by computing a set of configurations X , for which the set of concretizations $\gamma_k(X)$ is an *overapproximation* of reachable configurations of size k , reachable through configurations of size at most $k+1$ and checking for bad configurations. This is done by computing the fixpoint of $Apost_k$. If at this point no bad configuration has been found, the system can be said to be safe and the algorithm terminates. If on the other hand a bad state was found, the system is not necessarily unsafe, as V is an overapproximation of the reachable states in \mathcal{R}_k . The process is then repeated with a buffer size of $k+1$. This process is abstractly described in the flowchart in figure 3.

4 Naive Implementation of the Verification Method

In this chapter, we show how the algorithm in 3.8 can be implemented. The implementation is naïve, in that it strictly follows the mathematical concepts. Finally, we identify the main drawbacks of this naïve implementation and suggest an improved implementation.

Notations In this chapter, we use the terms *concretizations* and *potential concretizations*. The reason for this is that there is no straight-forward way to go from a set of views to a corresponding set of concretizations. In order to find the concretizations, we generate all of the *potential* concretizations, i.e. any extension of a view already in the set with any symbol in the alphabet. Maintaining a set V_k of views of size at most k , a view $v \in V_k$ may be extended with a symbol on one or more of its channels, yielding the potential concretization *con*. We say that *con* is *accepted*, if all the views of *con* of size up to k are in V_k , otherwise, *con* is *refuted*. Note that a concretization may be refuted in one iteration but accepted in another, as the set of views V_k may grow to include a larger set of views. We say that an accepted concretization *con* is *reached* from the view v .

4.1 Naïve implementation

A naïve way of generating configurations would be to perform the described operations in such a way that they correspond exactly to the mathematical notations described in section 3.2. This is possible to do, as most programming languages have built-in datastructures that support set operations and tuples.

In this naïve approach, each configuration is uniquely stored in a *set* V_k . For each element c of the set V_k , the concretization, post-image and abstraction functions are applied in that sequence, until V_k reaches a *fix-point*, i.e. continuing the process does not result in any more configurations being found. Assuming that a set of channel symbols and a set of rules R describing the transitions are known, the algorithm uses the following functions:

1. **Concretization function:**

Generate a set γ_k^{k+1} : For each configuration $c \in V_k$, generate all potential concretizations *con*. For any such potential concretization *con*, remove those for which $\alpha_k(c') \not\subseteq V_k$.

2. **Post-image:**

Generate the set $post(\gamma(V_k))$: For every $con \in \gamma(V_k)$, $r \in \delta$, compute $r(con)$.

3. **Abstraction Function:**

Generate $Apost(V_k)$: For each element $p \in post(\gamma(V_k))$, compute the set V' of views of size at most k . If $V' \cup V_k = V_k$, a fixpoint has been reached, otherwise repeat the process with $V_k := V_k \cup V'$.

4. Reachable configurations

Computing the set \mathcal{R}_k can be done in a multitude of ways, the simplest being to iteratively calculate the post-image of each configuration in the set. That is, \mathcal{R}_k is initially (s^0, ξ^0) , then for each $c \in \mathcal{R}_k^i$, $c \in \mathcal{R}_k^{i+1}$ and for each $r \in \delta$, $r(c) \in \mathcal{R}_k^{i+1}$ if $\text{size}(r(c)) \leq k$.

The pseudo-code implementing algorithm 3 can be seen in listing 4.

Algorithm 4 Pseudo-code for algorithm 3.

```

1: Verifier (V, Rules, Bad):
2:  $V := \{(s_0, \xi^0)\}$ 
3:  $V' := \emptyset$ 
4: for True do
5:   if  $\mathcal{R}_k \cap \text{Bad} \neq \emptyset$  then
6:     return Unsafe
7:   end if
8:   while  $(V \neq V \cup V')$ 
9:      $V' := \alpha_k(\text{post}(\gamma_k^{k+1}(V)))$ 
10:  if  $V \cap \text{Bad} = \emptyset$  then
11:    return Safe
12:  end if
13:   $k := k+1$ 
14: end for

```

4.2 Improving the Implementation

Evaluating the procedure described above, we find that the bottle-neck lies the concretization function. In order to find all the concretizations of the set V_k , it first creates all potential concretizations of the set V_k , by testing all extensions of the views $v \in V_k$, i.e. all combinations of channel evaluations where at least one of the channels is of a larger size than in v . For each of these potential concretizations, all its views are created in order to determine whether the concretization should be accepted or not.

Although this method is correct, there is significant overlap of concretizations being considered; it is often possible to create the same concretization *con* in several ways, and each time the abstract post-image must be calculated. We will show that all concretizations can be found, while considering only a subset of the potential concretizations. Furthermore, it is possible to determine whether a concretization should be accepted or not, examining only a subset of its views.

Simplified Subword Relation Using the fact that the verification algorithm is recursive, ending first when no new configurations can be found, we can re-define the subword relation such that not all views are created at a certain time, but still guaranteeing that all views are found eventually. We redefine

the subword relation in section 2.1.1, such that a word $w' \sqsubseteq w = a_1a_2 \dots a_n$ if $w' = a_i a_{i+1} \dots a_j$ for some $0 \leq i \leq n$, $0 \leq j \leq n$. As an example, if $w = abc$, then the set of subwords of w is $abc, ab, bc, a, b, c, \varepsilon$.

Proof. Consider a subword of $w = a_1a_2 \dots a_n$ that is a subword according to the original definition of the subword relation, but not by the simplified subword relation, $w' = a_i a_{i+1} \dots a_j a_l a_{l+1} \dots a_m$, $l > j + 1$. If a view v' with the word w' on one of its channels should be accepted, then the set V_k of views necessarily also contains views v'_1, v'_2, \dots with the words $a_i a_{i+1} \dots a_j$, $a_i a_{i+1} \dots a_j a_l$, $a_i a_{i+1} \dots a_j a_l a_{l+1} \dots a_{m-1}$ on the channel respectively.

The view v'_1 with the word $a_i a_{i+1} \dots a_j$ would be created with the simplified subword relation, as it is an unbroken sequence of messages. Then the view v'_2 with the word $a_i a_{i+1} \dots a_j a_l$ is a potential concretization of v'_1 , which would be accepted. The view v'_3 with the word $a_i a_{i+1} \dots a_j a_l a_{l+1}$ on the channel is in turn a potential concretization of v'_2 , which would again be accepted. Continuing in this way, the view with the word w' on the channel will eventually be created and accepted. \square

Reducing the number of Concretizations. Given a configuration c , with channel evaluations ξ such that $size(c) \leq k$, a potential concretization of c is any configuration con such that con can be created from c by appending at least one message to at least one of the channels of c .

Let con be a concretization reached from v , where n channels have been extended by a symbol. If such a potential concretization is accepted, any view v' where $n' < n$ channels have been modified in a similar way will also be a valid concretization, since $v' \sqsubseteq v$. Therefore, con will eventually be considered also when only one channel is extended in each iteration, but n iterations are required in order to reach it.

This reduces the number of potential concretizations being inspected in each iteration significantly. If we let s denote the size of the alphabet, t the number of channels and $n = size(V_k)$ in a certain iteration we can create upper limits on the number of potential concretizations that are considered. In the naïve version, a potential concretization is created for each combination of symbols s that can be added to a channel (up to s^k combinations), each combination of such extensions on the t different channels. As this must be done for each of the n existing views, the result is a worst case of $O(n * (s^k)^t)$ potential concretizations that may be considered in a single iteration. Using the suggested abstraction, the number of potential concretizations is reduced such that each of the n views is extended with at most 1 symbol on each of its channels, resulting in a worst case of $O(n * s * t)$ potential concretizations.

Reducing the number of views. Another limitation of the naïve approach is that in order to determine whether a potential concretization should be refuted or accepted, as a potential concretization is accepted only if all its views are already in the set V_k . If potential concretizations are generated as suggested above, the number of views that need be created can be considerably

reduced, using the fact that the potential concretization differs from some already existing view by a single symbol on a single channel. Suppose we want to determine whether a potential concretization con , generated from a view v should be accepted or refuted. We know that con has been generated from v by adding a single symbol m on one of the channels of v , whereas the state of con and v are the same, as is the content of the other channels.

Lemma 2. *Say $con = (s, w_1, \dots, w_n)$ was created by extending some view $v = (s, w'_1, \dots, w'_n) \in V_k$ by adding a single message to a single channel such that $w_p = w'_p \bullet m$ for some $p \leq n$ and $w_i = w'_i$ for all $i \neq p$. Then, if $w_p = m_1, m_2 \dots m$, it suffices to check whether there is a view $v' = (s, w_1, \dots, w_n) \in V_k$ such that $w_p = m_2 \dots m$, in order to determine if con can be accepted or not.*

Proof. Using the simplified subword relation, the views of con either contain the new symbol m in the word w_p , or they do not. Any view of con not containing the symbol m in w_p is also a view of v , and must exist in V_k . Any view containing m in the word w_p does so with m as its last symbol, i.e. there is a prefix of size at most k followed by the message m . Any such word is a subword of the largest possible view containing the message m , i.e. $m_2 \dots m$. \square

Example. Suppose we want to determine whether the potential concretization $con = (s, abc, de)$ created from the view $v = (s, ab, de)$ is an element of V_2 . It is then sufficient to check that $v' = (s, bc, de)$ is an element of V_k .

5 Improved Implementation

Using the results of the last chapter, the computational complexity of the verifier is greatly reduced, but there are yet several ways to optimize the procedure. The bottle-neck with the procedure at its current state is the choice of a *Set* as lone data structure to store configurations. We expect the number of configurations to grow rather large, due to state-space explotion which cannot be avoided automatically (in certain cases, it could be reduced by further abstraction of the model under testing or by removing unnecessary redundancy in the model). Assuming the *Set* is ordered, inserting an element to the set and finding an element in the set is done in $O(\log n)$ where n is the number of elements in the set. As a consequence, the function *alpha* which determines whether the views of a certain configuration are in the set has complexity $O(p \cdot \log n)$ where $p = |\alpha_k(c)|$. We observe that by definition, a view (and a configuration) is of type $(S \times \xi)$. For any configuration $c = (s)\xi$, it's views will be of the type $(s)\xi'$, i.e., the configuration and its views have identical control-parts. It is therefore reasonable to divide the single *Set* into a *Set of Sets*, where each *Set* corresponds to a specific control-state. With such a division, it is sufficient to check whether the views of a configuration reside in the *Set* that corresponds to its control-state.

In a best-case scenario, there would be an equal number of configurations for every state in the system. The complexity of checking whether $\alpha_k(c) \in V$ is reduced to $O(p \cdot \log(n/s))$ where s denotes the number of states in the system. The gains of these modifications in terms of computational complexity is difficult to determine, as the number of configurations with a certain control-state are not necessarily well-distributed, but we anticipate that the gains in many cases will be close to the best case scenario.

5.1 Control-State Partitioning

Above it was suggested that the set V could be divided into several sets, distinguished by control-states. The number of control-states in a system is finite and unique; For a system with n processes, the number of states is $\prod_{i=1}^n |p_i|$. This makes it possible to partition the set of configurations into several smaller disjoint sets, such that all configurations in a set have equal control-state. These sets can be stored in a hashmap indexed by control-state.

5.2 Advantages of Partitioning

Using this partitioning, each node in the hashmap is a *Set* with equal-state configurations, addressed by the common control-state. Compared to the previous solution, this leads to a speed-up when inserting, retrieving and looking for the existence of elements in the sets, as the size of the sets will be smaller than before. Retrieving and inserting nodes into the hashmap is done in constant time in practice (the number of elements will be static, avoiding the need of resizing the hashmap).

Having partitioned the configurations, consider the act of applying a rule in order to create a new configuration. Recall that any rule has a state-predicate, a channel-predicate, a state-event and a channel-event. If the predicates are fulfilled, a new configuration can be created by applying the events to the current configuration.

By organizing the set of *rules* or transitions in a similar way in a hashmap of rules, we can ensure that the state-predicate is fulfilled without specifically testing for it. A state-predicate is a (possibly empty) predicate on the states of the processes in the system, requiring that one or more processes are in a specific state. It is therefore possible to generate a static hashmap of rules, addressed again by control-states.

Considering a transition t_2 with no requirements on any processes, the state-predicate will be fulfilled by any configuration, thus a corresponding rule is created in every node of the tree. Consider then instead a transition t_2 with requirements on all the processes in the system, i.e. there is only one valid control-state. Such a transition corresponds to a single rule in the node addressed by that control-state. Last, consider a transition t_3 with requirements on a true subset of the processes in the system, then the transition can be taken from a number of control-states. These control states can be generated, and the transition will correspond to a set of rules in the nodes corresponding to those control-states.

Example. Consider yet again the alternating bit protocol, as described in ???. The system has three processes *Sender*, *Receiver* and *Observer* with 4, 4 and 3 states respectively. Consider then the transition with the predicates that the sender is in state 3, the observer in state 3 and they may take the synchronized transition with the action *Snd* to states 4 and 2 respectively. This transition has no requirements on the receiver, thus it corresponds to four rules, $(3,1,3) \rightarrow (4,1,2)$, $(3,2,3) \rightarrow (4,2,2)$, $(3,3,3) \rightarrow (4,3,2)$, $(3,4,3) \rightarrow (4,4,2)$. These rules are inserted in the nodes $(3,1,3)$, $(3,2,3)$, $(3,3,3)$ and $(3,4,3)$.

There is a small one-time cost of creating the rule tree, but after creation, it is highly effective. The division by itself ensures that the state-predicate is fulfilled, if not, we never even attempt to apply the rule to a configuration. We illustrate this in figure ??

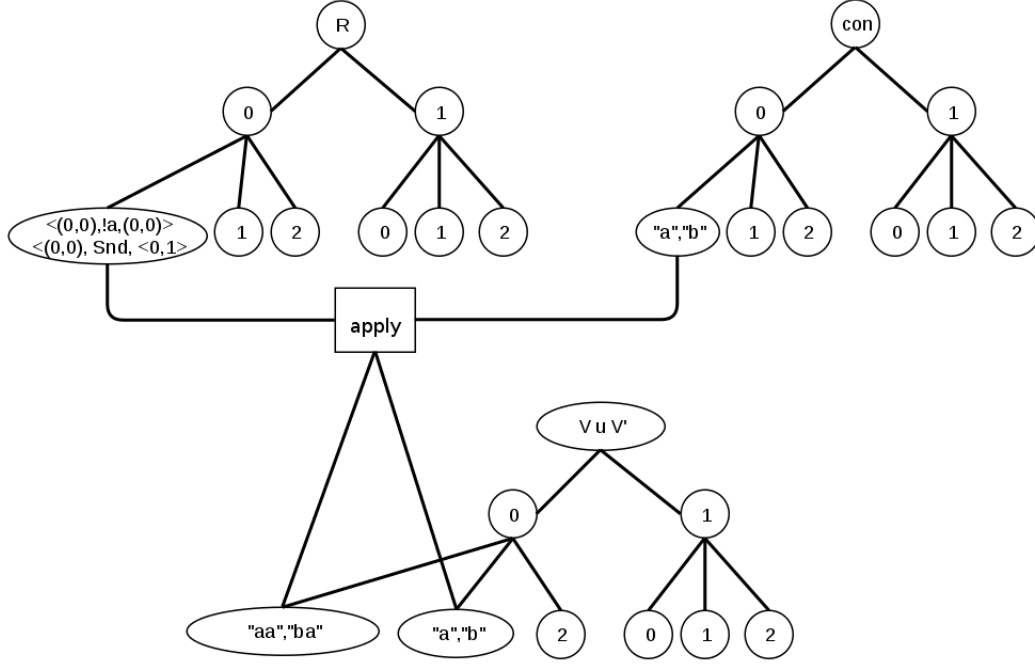


Figure 4: This picture shows the process of applying rules. For each control-state, each rules with that state are applied on each configuration with the same state. This will generate new configurations, not necessarily with the same control-state. This is visualized in a tree, rather than a hashmap, only since hashmap are less intuitive to draw.

6 Final Implementation

An efficient algorithm in this context is largely an algorithm that avoids performing unnecessary calculations. This can either be done by avoiding to create unnecessary configurations such as was done with the rule hashmap above or by avoiding re-calculating previously calculated results. The algorithm as described above reproduces its steps each iteration; if a configuration c can be extended to a concretization con at any point in the verification process, then con can and will be created in every following iteration. This includes checking whether $\alpha_k(con) \subset V$, applying a set of rules to the configuration and then adding all the views of the resulting configurations to the set. Each time the calculations are performed, the result will be duplicates and no new views are added to the system.

We solve this by maintaining another hashmap, *seen*, of configurations in parallel, containing exactly those concretization that have been accepted. If a configuration c can be extended to the concretization con , then we first check if con is an element of *seen*. If it is, we discard con , otherwise we add con to *seen* and also to the set of concretizations to be evaluated in this iteration.

Yet another source of repetition is the fact that there are multiple ways to create the same channel evaluations. Therefore, after a rule has been applied to a concretization, it may result in a configuration already in the set. Instead

Algorithm 5 The verification algorithm from section 3 in somewhat higher detail. This version includes

```

1: Gamma (V, Seen):
2:    $\text{con}' := \text{concretizations}(\text{V})$ 
3:    $\text{con} := c \mid c \in \text{con} \wedge c \notin \text{Seen}$ 
4:
5: Step (Con, Rules):
6: for  $\text{state} \in \text{nodes}(\text{V})$  do
7:    $S := r(c) \mid \forall c \in \text{con}(\text{state}) \wedge \forall r \in \text{Rules}(\text{state})$ 
8: end for
9:
10: Alpha (V, S):
11:    $V := V \cup \text{views}(C)$ 
12:
13: Verifier (V, Rules, Bad):
14: for True do
15:   if  $\mathcal{R}_k \cap \text{Bad} \neq \emptyset$  then
16:     return Unsafe
17:   end if
18:    $V := \mu\text{Alpha}(\text{Step}(\text{Gamma}(V)))$ 
19:   if  $\gamma_k(V) \cap \text{Bad} = \emptyset$  then
20:     return Safe
21:   end if
22:    $k := k+1$ 
23: end for

```

of performing the costly α -calculation, we first check if the newly created configuration is not in fact a duplicate by checking if it is already in V . If so, the configuration can again be discarded.

The final algorithm amounts to the following pseudo-code representation:

6.1 Reachability Analysis

An important step of the verification process which has yet to be covered is that of performing a reachability analysis, in order to find bad states, if any such states are reachable and find a minimal bad trace leading up to the bad state. See sections ?? and ?? for formal definitions of bad states and traces respectively.

Below, a simple technique of finding a minimal bad trace is presented, accompanied with a proof that the trace is in fact minimal.

Finding Minimal Traces When running the verification, if a bad state is found we want to produce a trace leading up to the bad state. Preferably, this would be a minimal trace that leads to the bad state.

The proposed verification method generates a finite set of reachable states

(nodes in this context), but it does not record the available transitions between the nodes (i.e. the edges). It is possible to for each node n to save all nodes n' from which an edge to n exists, and thus build the complete reachability graph of the problem. There exists efficient algorithms to solve such a problem, e.g. *dijkstra shortest path*, or even the shortest path between any two nodes, e.g. flow-network techniques. Although these algorithms are efficient, building the complete reachability graph would be costly in terms of memory space, as the number of edges may be much larger than the number of states.

We show that due to the method of iteratively constructing the graph, nodes are created in such a way, that if a node n_i created in the i :th iteration is reached by a node n_{i-1} over an edge e_{i-1} , the shortest path from the initial node n_0 will necessarily be a path $e_1...e_{i-1}$.

Proof. This is proven using an induction proof. We hypothesize that, if at the point of creation of n_i , choosing the parent node n_{i-1} from which an edge e_{i-1} can be taken n_i , the path $e_1..e_i$ will be the shortest path to n_i and has length i . Note that the node n_{i-1} must have been created in the previous iteration; had it been created earlier, the edge e_i could have been taken in a previous iteration, and so n_{i+1} would already be a node in the tree.

The base case is that for any node reachable from n_0 over any edge e_0 , e_0 will be the shortest path and has length 1. This is trivially true.

Now suppose a node n_{i+1} is reachable over an edge e_i from a node n_i , and the node n_{i+1} is not yet in the system. The induction hypothesis states that the path $e_1...e_i$ is the shortest path leading up to n_i . If $e_0..e_{i-1}e_i$ would not be the shortest path to n_{i+1} , there would be a path $e'_0..e'_{k-1}$ to another node n_k with $k < i$ from which n_{i+1} can be reached. But any such node would have been created in the k :th iteration of the algorithm, which would contradict the fact that the node n_{i+1} was not already in the system.

Having shown this, we need only record the information of a single parent of a node, in order to build up a tree from which the shortest path from n_0 to any node in the system can efficiently be found.

6.2 Specification Language

In order for the verification algorithm to be easily used, a specification language is needed in which algorithms can be formally defined. We expect such a specification language to

- be expressive enough to express all algorithms that are in the scope of the verification program
- be independent of the internal representations of the verifier and to demand as little knowledge of the actual verification process as possible from the user
- to be as clear as possible in order to ensure that the model at hand in fact corresponds to the actual algorithm, the way it was intended

The specification language used is an adaption of previous works in [?]. The language simply uses XML to describe an algorithm. There are minor differences between the specification language used here, with respect to that used in by the MPass verification algorithm, and correspond to different expressiveness of the models. More specifically, the MPass verifier allows for joint reception and transmission transitions, i.e. a single transition may read a message from a channel and write a message to a channel at the same time. On the other hand, it does not allow for synchronized transitions, this has therefore been added to the language.

6.2.1 Example

We return yet again to the Alternating Bit Protocol to exemplify the specification language. Bearing in mind the formal definition in section 2.2, a model needs a set of messages, channels, actions and transitions.

We begin by specifying a new protocol, its name and that it is operating on FIFO buffers. We then specify a set of messages, a set of channels and a set of actions in a similar manner.

```

1 <protocol name="Alternating_Bit_Protocol" medium="FIFO">
2   <messages>
3     <message>ack0</message>
4     <message>ack1</message>
5     <message>mesg0</message>
6     <message>mesg1</message>
7   </messages>
8
9   <channels>
10    <channel>c1</channel>
11    <channel>c2</channel>
12  </channels>
13
14  <actions>
15    <action>Rcv</action>
16    <action>Snd</action>
17  </actions>

```

We then continue by defining the different processes in the system, i.e. the sender, receiver and observer. Such a process is defined by its states and its transitions. In the specification language, we differentiate between transitions over an action, and transitions that modify a channel. The latter type is called a *rule* in the specification language, in order to comply with the names used in the MPass specification language. This should not be confused with the word as used earlier in this section.

```

1   <role name="SENDER">
2     <states>
3       <state type="initial">Q0</state>
4       <state>Q1</state>

```

```

5      <state>Q2</state>
6      <state>Q3</state>
7  </states>
8  <action>
9      <current_state>Q0</current_state>
10     <type>Snd</type>
11     <next_state>Q1</next_state>
12 </action>
13 <rule>
14     <current_state>Q1</current_state>
15     <send_message>mesg0</send_message>
16     <next_state>Q1</next_state>
17     <channel>c1</channel>
18 </rule>

```

Last, we specify that the processes **SENDER** and **OBSERVER**, and **RECEIVER** and **OBSERVER** are to be synchronized over the actions **Snd** and **Rcv** respectively.

```

1  <synchronize>
2      <first_role>SENDER</first_role>
3      <second_role>OBSERVER</second_role>
4      <action>Snd</action>
5  </synchronize>
6  <synchronize>
7      <first_role>RECEIVER</first_role>
8      <second_role>OBSERVER</second_role>
9      <action>Rcv</action>
10 </synchronize>

```

7 Result

An implementation of this method has been written in the *Haskell* programming language (<https://www.haskell.org/haskellwiki/Haskell>). It was used to verify a number of parameterized systems, all of which are communication protocols;

ABP	The alternating bit protocol, as described in 1 with the extension suggested in ???. The Alternating Bit Protocol corresponds to the <i>Sliding Window Protocol</i> with $k=2$. Automatas for the the Sliding Window Protocol can be found in ???.
ABP_F	A purpously faulty version of the ABP.
SW3	The sliding window protocol, with $k=3$.
ABP_F	A purpously faulty version of the SW3.
SW4	The sliding window protocol, with $k=3$.
SW5	The sliding window protocol, with $k=3$.
BRP	The <i>Bounded Retransmission Protocol</i> , a variant of the alternating bit protocol.
BRP_F	A purpously faulty version of the BRP.

The **Backward** verifier uses *backward reachability* for verification, and follows the algorithm described in [?]. The algorithm was implemented as part of this project with the purpose of comparison in mind. It was therefore implemented in such a way that it accepts exactly the same specification language, as that of the verifier of this project.

The *MPass* verifier addresses the verification bounded-phase reachability problem, i.e. every process may perform only a bounded number of *phases* during a run in the system. This problem is then translated into a satisfiability formula (a quantifier-free Presburger formula to be exact) which in turn is solved by a third party SMT-solver (Z3 SMT-solver, <http://z3.codeplex.com>).

Note on the MPass verification results. The input language used in this project (see ??) was based on that of the *MPass* verifier, but does not fully coincide. The tool ships with some example protocols (ABP, ABP_F, SW3_F, BRP), which with minor changes could be adapted such that they would comply to the specification language used here. The remaining protocols were written from scratch, and use specification artifacts not comprehensible by *MPass*. Reformulating these would result in very different models, making it difficult to draw any conclusions from a comparison. For this reason, *MPass* was only used to verify a subset of the protocols mentioned above.

It should be mentioned that the time estimation for the *MPass* solver is part the time to generate an *SMT* formula, and part to verify that formula with a third party *SMT*-solver. The times generated in the latter part were approximated to full seconds, meaning the values have a measurement error up to ± 0.5 seconds.

						Backward			MPass		
	k	size(V)	Result	Time	Mem	Size V	Result	Time	Bound	Result	Time
ABP	2	108	Safe	0.00s	1MB	56	Safe	0.01s	3	Safe	1.04s
ABP_F	1	–	Fail	0.00s	1MB	–	Fail	0.01s	3	Fail	6.04s
SW3	3	4247	Safe	0.10s	3MB	270	Safe	0.17s	–	–	–
SW3_F	1	–	Fail	0.00s	1MB	–	Fail	0.10s	3	Fail	26.08s
SW4	4	98629	Safe	3.64s	36MB	840	Safe	2.03s	–	–	–
SW5	5	1834345	Safe	120.20s	924MB	2028	Safe	24.31s	–	–	–
BRP	2	45	Safe	0.02s	3MB	–	??	Timeout	3	Safe	1.23s
BRP_F	1	–	Fail	0.00	2	–	Fail	0.15	–	–	–

Table 1: Runtime and verification results for the verification method in this paper, in comparison to backward reachability and the MPass verifier.

7.1 Experimental Results

The results can be seen in ???. The table shows the size of the variable k , whether the result was safe or unsafe, the runtime and the amount of working memory used by the verifier for each of the communication protocols above. Further, the table shows the runtime and result of two other verifiers, verifying the same protocols. For these verifiers, only the runtime and the safety result is specified.

The results were generated on a 3.2GHz Intel Core i3 550 with 4GB of memory, running Debian Linux, using a single core.

7.2 Analysis of Results

The results in ?? show that the verification tool is in large efficient, yielding comparable verification times to backward reachability and faster than the *MPass* verifier for all of the protocols tested. Further, all verifiers yield the same safety results, which is to be expected as all three solvers are free from both false positives and negatives.

Examining the sliding window protocols of increasing size, i.e. ABP, SW3, SW4 and SW5, it is evident that the verifier suffers from a higher degree of exponential growth with respect to the problem size, than does the backward reachability verifier (which also suffers from exponential growth, as this is an inherent property of the model). First and foremost, it is the amount of working memory that is the bottleneck.

Increasing the size of the sliding window protocol means increasing the window size of the protocol – this not only means that the value of k for which the protocol can be found safe increases, but also that there is additional symbols to consider, and that the number of states and transitions increase (i.e. 1 compared to ??). The number of potential configurations depend on exactly these factors and due to the overapproximation configurations, we expect that a large set of these will be reachable. As the verification tool stores *all* reachable configurations, without approximation or abstraction, this leads to memory becoming a bottle-neck for this particular protocol.

8 Summary and Further Work

In this paper I have investigated the possibility of verifying systems depending on lossy channels. The approach was to model such systems as parameterized systems and to use abstract interpretation techniques in order to bound systems with otherwise infinite reachable states, to a carefully chosen finite subset of those states. This method is influenced by and builds upon previous work[?], adapting the existing verification method to work for unbounded lossy channels.

The verification method was implemented, and a protocol specification language was designed, influenced by the XML-layout used by the MPASS verification language[?]. Experimental results with the verifier, in comparison to that of the MPASS verifier and a verification algorithm based on backward reachability analysis[?], show that the method achieved comparable or better results on most of the protocols tested.

A notable weakness of the verification method is that it struggles with the space and time complexity caused by an increased number of messages, but copes relatively well with an increase of local states in the processes, because all reachable channel evaluations are explicitly stored. This is a point that could be improved, by finding a method to abstractly represent a larger number of channel evaluations more compactly, possibly by introducing further overapproximation.

In addition to this, an important theoretical issue has been largely overlooked in this paper, i.e. the fact that the verifier is not guaranteed to ever converge towards a solution. Considering that the verifier terminates for all tested protocols, it is likely that the verification algorithm could leave such a guarantee for at least some classes of problems, as is done in [?]. Identifying and formally proving such guarantee of termination would be a valuable theoretical addition worth investigation.

9 Related Work

Parameterized model checking focuses verification scenarios where the size of the problem under observation is a parameter of the system, and the size has no trivial upper bound. The goal is to verify the correctness of the system regardless of the value of the parameter. As this generally corresponds to a transition system of infinite size, research in this field of verification focuses on techniques to limit the size of the transition system.

One such method is the *invisible invariants* method[?], which similar to [?] and [?] use *cut-off* points to check invariants. Such cut-off points can be found dynamically[?] or be constant[?]. The works of Namjoshi[?] show that methods based on process invariants or cut-offs are complete for safety properties.

Small model systems have been investigated in [?], which combines it with infinite state backward coverability analysis. Such methods prevent its use on undecidable reachability problems, such as those considered in [?]. The work of [?] also show that the problem is decidable for a large class of well quasi-ordered systems, including Petri Nets[?]. Practical results indicate that these methods may be decidable for yet larger classes of systems. More on well-structured infinite transition systems can be found in [?].

Abstract interpretation techniques were first described by Cousot and Cousot[?][?]. Similar work to [?] can be found in [?, ?].

Edsger Dijkstra was the first to consider the interaction between processes communicating over channels[?][?]. In [?], the authors show that verification of perfect channels systems is undecidable, by relating it to the simulation of a Turing Machine[?]. The decidability of lossy channels has been researched in[?, ?].

Similar to this thesis, [?] make use of abstract interpretation to channel systems, applying the technique to regular model checking. MPass[?] is a verification tool for channel systems, that restates the verification problem to an equivalent first-order logic, which is then solved by an SMT solver. Its input language is roughly the same as this thesis, although the tool is more general, being applicable also on *stuttering* and unordered channels.

References

- [1] The free on-line dictionary of computing.
- [2] ABDULLA, P., HAZIZA, F., AND HOLÍK, L. All for the price of few. In *Verification, Model Checking, and Abstract Interpretation*, R. Giacobazzi, J. Berdine, and I. Mastroeni, Eds., vol. 7737 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2013, pp. 476–495.
- [3] ABDULLA, P., AND JONSSON, B. Verifying programs with unreliable channels. In *Logic in Computer Science, 1993. LICS '93., Proceedings of Eighth Annual IEEE Symposium on* (Jun 1993), pp. 160–170.
- [4] ABDULLA, P. A. Well (and better) quasi-ordered transition systems. *Bulletin of Symbolic Logic* 16, 4 (12 2010), 457–515.
- [5] ABDULLA, P. A., ATIG, M. F., CEDERBERG, J., MODI, S., REZINE, O., AND SAINI, G. Mpass: An efficient tool for the analysis of message-passing programs.
- [6] ARONS, T., PNUELI, A., RUAH, S., XU, Y., AND ZUCK, L. Parameterized verification with automatically computed inductive assertions? In *Computer Aided Verification*, G. Berry, H. Comon, and A. Finkel, Eds., vol. 2102 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2001, pp. 221–234.
- [7] BAIER, C., KATOEN, J.-P., ET AL. *Principles of model checking*, vol. 26202649. MIT press Cambridge, 2008.
- [8] BARTLETT, K. A., SCANTLEBURY, R. A., AND WILKINSON, P. T. A note on reliable full-duplex transmission over half-duplex links. *Communications of the ACM* 12, 5 (1969), 260–261.
- [9] BERTRAND, N., AND SCHNOEBELEN, P. Model checking lossy channels systems is probably decidable. In *Foundations of Software Science and Computation Structures*, A. Gordon, Ed., vol. 2620 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2003, pp. 120–135.
- [10] BRAND, D., AND ZAFIROPULO, P. On communicating finite-state machines. *Journal of the ACM (JACM)* 30, 2 (1983), 323–342.
- [11] COUSOT, P., AND COUSOT, R. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Proceedings of the 4th ACM SIGACT-SIGPLAN symposium on Principles of programming languages* (1977), ACM, pp. 238–252.
- [12] COUSOT, P., AND COUSOT, R. Systematic design of program analysis frameworks. In *Proceedings of the 6th ACM SIGACT-SIGPLAN symposium on Principles of programming languages* (1979), ACM, pp. 269–282.

- [13] DIJKSTRA, E. W. Information streams sharing a finite buffer. *Information Processing Letters* 1, 5 (1972), 179 – 180.
- [14] EMERSON, E., AND NAMJOSHI, K. On model checking for non-deterministic infinite-state systems. In *Logic in Computer Science, 1998. Proceedings. Thirteenth Annual IEEE Symposium on* (Jun 1998), pp. 70–80.
- [15] EMERSON, E. A., AND NAMJOSHI, K. S. Reasoning about rings. In *Proceedings of the 22nd ACM SIGPLAN-SIGACT symposium on Principles of programming languages* (1995), ACM, pp. 85–94.
- [16] FINKEL, A., AND SCHNOEBELEN, P. Well-structured transition systems everywhere! *Theoretical Computer Science* 256, 1 (2001), 63–92.
- [17] FREDLUND, L.-Å., AND SVENSSON, H. Mcerlang: a model checker for a distributed functional programming language. In *ACM SIGPLAN Notices* (2007), vol. 42, ACM, pp. 125–136.
- [18] GANTY, P., RASKIN, J.-F., AND VAN BEGIN, L. A complete abstract interpretation framework for coverability properties of wsts. In *Verification, Model Checking, and Abstract Interpretation* (2006), Springer, pp. 49–64.
- [19] GEERAERTS, G., RASKIN, J.-F., AND VAN BEGIN, L. Expand, enlarge, and check. In *Proceedings of MOVEP06: MOdeling and VERifying parallel processes* (2006), p. 4.
- [20] KAISER, A., KROENING, D., AND WAHL, T. Dynamic cutoff detection in parameterized concurrent programs. In *Computer Aided Verification* (2010), Springer, pp. 645–659.
- [21] LE GALL, T., JEANNET, B., AND JÉRON, T. Verification of communication protocols using abstract interpretation of fifo queues. In *Algebraic Methodology and Software Technology*. Springer, 2006, pp. 204–219.
- [22] MCMILLAN, K. L. *Symbolic model checking*. Springer, 1993.
- [23] NAMJOSHI, K. S. Symmetry and completeness in the analysis of parameterized systems. In *Verification, Model Checking, and Abstract Interpretation* (2007), Springer, pp. 299–313.
- [24] TARSKI, A., ET AL. A lattice-theoretical fixpoint theorem and its applications. *Pacific journal of Mathematics* 5, 2 (1955), 285–309.
- [25] ZUCK, L., AND PNUELI, A. Model checking and abstraction to the aid of parameterized systems (a survey). *Computer Languages, Systems & Structures* 30, 3–4 (2004), 139 – 169. Analysis and Verification.

A Automata for the Sliding Window Protocol

