Verifier: An efficient and computational tool for analysis of message passing programs
User Manual

Gaurav Saini and Subham Modi

August 25, 2013

Contents

1 Introduction

The verification problem such as reachability problem is undecidable for programs having perfect channels even if the number of states in each process are finite but it becomes decidable if we have lossy, stuttering or unordered channels [1]. However, to decide the reachability problem in later case we have high complexity obstacles. Thus in order to avoid this, one useful approach, *context bounding* [6], was proposed recently. This idea limits the number of context switches between two processes because of which we have a trade off between the extent of verification and computational complexity.

VERIFIER is a tool which works on a different approach called as *bounded-phase* reachability analysis. It verifies the reachability problem of programs or protocols having their phase bounded. Each process in such programs can perform a computation in which the number of phases is bounded by some natural number k. In each phase, a process can perform either send transitions or receive transitions (but not both). The transition consisting of no operation, but just the change of states, can be performed in either of these phases. However, this doesn't limit the number of context switches between two process but just the number of alternations between receive and send transitions.

Currently, VERIFIER can decide reachability problem for three types of channel semantics, namely *lossy, stuttering and unordered* channels. These channels allow the messages inside them to be lost, dublicated and re-arranged respectively. Details are given in section 3.

This manual provides basic knowledge about the semantics and specification of the model . Detailed information regarding the same can be found in [2].

2 Contact / Bug Report

Feedback, questions, bug reports or any other query related to VERIFIER should be directed to Subham Modi (`smodi@iitk.ac.in`), Gaurav Saini(`sgauarav@iitrpr.ac.in`)

3 Verifier Tool

VERIFIER performs two different levels of extraction in order to analyse the reachability problem for a given program.

Verification is achieved by taking the examples from [4] which are further described in [5] and [7]. Bounded Retransmission Protocol is also adapted from [3]. All `protocols` are used in the format of `xml-files` present in the Protocols directory within the tool repository. The protocols, thus, can be modified in a simple manner by changing the fields in xml-files.

3.1 Xml to Automata

The first task of Verifier is to translate the protocols defined in `xml-files` into *Non-Deterministic Finite Automata* (NFA). In order to achieve this, it takes xml-file path of the Protocol as an input and then uses C++ library of `lemon` to translate the protocol into NFA as shown below:

```
<rule id="Q0__ack1__INBOUND">
  <pre>
    <current_state>Q0</current_state>
    <received_message>ack1</received_message>
    <channel>c1</channel>
  </pre>
  <post>
    <send_message>mesg0</send_message>
    <next_state>Q1</next_state>
    <channel>c1</channel>
  </post>
</rule>
```

Figure 1: An example of xml code for ABP Protocol

The above rule adds two transitions from the state `Q0` to the state `Q1`. First transition defines the rule of receiving the message `ack1` from the channel `c1` whereas second transition defines the rule of sending the message `mesg0` into the channel `c0`. Each process in a protocol contain one or more such rules which in together defines the automata for that process within that protocol.

Now, since the protocols have their phase bounded and each phase contain either send or receive transitions (but not both), therefore we make two automata for each process, one containing all except the receive transitions (send copy of that process) and the other containing all except the send transitions (receive copy of that process).
In this way, we have constructed *2*Number of Process* automata for the given protocol.

3.2 Automata to Constraint Generation

Verification of protocol for reachability problem is analysed by generating *Presburger Formula* from the automata constructed as shown in `figure 1` and then using the help of modern SMT solver namely *Z3 theorem prover*. Detailed information regarding the framework showing the translation of reachability for *bounded-phase-automata* into the satisfiability of *quantifier-free Presburger formulas* can be found in [2].

In order to generate quantifier-free Presburger formula, certains variables of a particular *sort* have to be defined and thus, for all the transitions present within each automata, we'll introduce a number of variables as shown below:

Variable name	Variable code
Index-variable	i-var
Occurence-variable	o-var
Match-variable	m-var

Table 1: Variables associated with each transitions

Variable declaration and defination are explained briefly in [2].

For taking *bounded-phase-automata* into account, VERIFIER generates variables for both send and receive copy of each process and then duplicates them k times (where k is some natural number denoting the bound for that computation) which are then further used to generate Presburger formulas.
If the result of *Z3 theorem prover* for these set of formulas (one of them being displayed in `figure 2`) is satisfiable, then the *Bad State* is reachable.

$$(\mathtt{occ}\,(t) = 1) \wedge (\mathtt{occ}\,(t') = 1) \wedge (\mathtt{index}\,(t) < \mathtt{index}\,(t')) \Longrightarrow (\mathtt{match}\,(t) < \mathtt{match}\,(t')).$$

Figure 2: An example of a *quantifier-free Presburger formulas*

4 Installation

Verifier Tool can be compiled and installed on Unix-like system.

4.1 Requirements

- A C++ compiler supporting C++11. For example g++ version 4.6 or higher.
- Z3 SMT 2.0 Solver. Also Z3 SMT solver should be installed in the bin directory so that it can be called using "z3 -smt2 filename" from the terminal. It can be downloaded from http://z3.codeplex.com.
- Lemon Graph Library, it can be downloaded from http://lemon.cs.elte.hu.
- To be able to generate pdf file for the results, pdflatex is required.

4.2 Installation

The VERIFIER Tool can be installed by using the following procedure.

- Copy the verifier_result folder from the Verifier directory to your home folder.
- Using terminal, go to the Verifier folder and execute the following commands.

```
$ touch NEWS README AUTHORS ChangeLog
$ autoreconf --force --install
$ ./configure
$ make
$ sudo make install
```

4.3 Installation Options

The configure script is built with GNU autotools, and should accept the usual options and environment variables.

Changing Installation Directory

The command 'sudo make install' will install Verifier Tool in the directories which are standard on your system. To override this behaviour add the switch –prefix to the './configure' command:

$ ./configure –prefix=/your/desired/install/path

5 Usage

The Verifier Tool can be called from the command line using 'verifier'. The path to the Settings file is expected as the first argument. The format of Settings file is as follows:

file	path_to_xml_file
semantics	channel_semantics
bound	bound_for_the_processes
bad	bad_process bad_state
channel_type	type_of_channel

5.1 Description of Settings File

- **file**: It refers to the location of the XML file to be verified.
- **semantics**: It refers to the semantics of the channels. It can be lossy, stuttering or unordered.
- **bound**: It refers to the number of bounds for the automata.
- **bad**: It takes pairs of values. First is the name of the process in which the reachability is to be checked and the second is the set of states for which reachability is being checked.
  NOTE: *Bad state for more one process can also be entered one after the other in the same format as diplayed in the example below.*

  Example:

  ```
  bad SENDER Q0 Q1 RECEIVER INVALID
  bad SENDER Q0 RECEIVER INVALID
  bad RECEIVER INVALID
  ```

- **channel_type**: It refers to the type of channel. It can be :

  `prefix` : For making channels based on the first alphabet of the messages.
  `process`: For making one channels for each process.
  `xml` : For making channels as specified in the xml file.

5.2 Other Optional Arguments

A pdf containing the results of the Verifier can also be generated if pdflatex is installed in the system.This can be done using `new` or `old` arguments in addition to the one which we were using before. It can be used as follows :

1. Using the new option:

A new pdf containing the results can be generated using this option. The pdf is placed in the `verifier_result/Result` folder in the home directory. It is used as follows :

```
verifier path_to_settings_file new
```

2. Using the old option:
The result for this run of the Verifier is appended to the previously genereated pdf. The pdf is placed in the `verifier_result/Result` folder in the home directory. It is used as follows :

```
verifier path_to_settings_file old
```

References

[1] P.A. Abdulla and B. Jonsson. Verifying programs with unreliable channels. In *LICS*, 1993.

[2] Parosh Aziz Abdulla, Mohamed Faouzi Atig, and Jonathan Cederberg. Analysis of message passing programs using smt-solvers. Uppsala University.

[3] Parosh Aziz Abdulla, Aurore Collomb-Annichini, Ahmed Bouajjani, and Bengt Jonsson. Using forward reachability analysis for verification of lossy channel systems. In *FMSD*, page 25(1):39–65, 2004.

[4] Abinoam P. Marques Jr., Anders Ravn, Jiri Srba, and Sallem Vighio. csv2uppaal. https://github.com/csv2uppaal.

[5] Abinoam P. Marques, Anders Peter Ravn, Jiri Srba, and Saleem Vighio. Tool supported analysis of web services protocols. In *TTCS*, pages pages 50–64, University of Oslo, 2011.

[6] S. Qadeer and J Rehof. Context-bounded model checking of concurrent software. In *TACAS*, 2005.

[7] Anders P. Ravn, Jiri Srba, and Saleem Vighio. Modelling and verification of web services business activity protocol. In *TACAS*, LNCS, pages pages 357–571. Springer, 2011.

GNU Free Documentation License

Version 1.3, 3 November 2008

Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "**Document**", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "**you**". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "**Modified Version**" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "**Secondary Section**" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "**Invariant Sections**" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "**Cover Texts**" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "**Transparent**" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "**Opaque**".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "**Title Page**" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "**publisher**" means any person or entity that distributes copies of the Document to the public.

A section "**Entitled XYZ**" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "**Acknowledgements**", "**Dedications**", "**Endorsements**", or "**History**".) To "**Preserve the Title**" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled “History” in the various original documents, forming one section Entitled “History”; likewise combine any sections Entitled “Acknowledgements”, and any sections Entitled “Dedications”. You must delete all sections Entitled “Endorsements”.

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See `http://www.gnu.org/copyleft/`.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright © YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with … Texts." line with this:

> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.