

Implementation of omega-automata minimization techniques in "Spot", a model checking library.

When "Spot" SAT-based minimization meets incremental SAT solving.

Paris, January 2017

Submitted by:
Alexandre GBAGUIDI AÏSSE
Student in second year of computer engineering
at EPITA
gbagui_a@epita.fr

Supervised by:
Alexandre Duret-Lutz
Assistant Professor at LRDE(Research and
Development Laboratory of EPITA)
adl@lrde.epita.fr



Contents

I	Report	1
1	LRDE Presentation	2
1.1	Line of business	2
1.2	The Laboratory	2
1.3	Members	3
1.4	Services	3
1.4.1	Image Processing	3
1.4.2	Finite state machine manipulation	4
1.4.3	Model checking	5
1.4.4	Speaker recognition	5
1.5	The internship in the company's work	6
2	Spot	7
2.1	Structure	7
2.2	Command-line tools	8
2.3	The Python Interface	8
2.4	Workflow	9
2.4.1	Coding conventions	9
2.4.2	Git Versionning Tool	9
2.4.3	Adding Tests	9
3	Basic concepts	10
3.1	Automata theory	10
3.1.1	Automata	11
3.1.2	Alphabet, word, language	11
3.1.3	Automaton run	11
3.1.4	Determinism (DFA, NFA)	12
3.1.5	Finite-state automata (FSA) Definition	12
3.2	About Spot	12
3.2.1	Atomic preposition	12
3.2.2	Boolean formula	12
3.2.3	ω -words	13
3.2.4	ω -automaton	13
3.2.5	Acceptance condition	14
3.3	SAT solver	15

4	Specifications	16
4.1	Overall goal	16
4.1.1	The existing minimization	16
4.1.2	Tool chain	18
4.1.3	The limits	19
4.2	Detailed explanation of the results to be obtained	19
5	Contributions to Spot	22
5.1	fastSAT	22
5.2	Satsolver C++ class	24
6	Bibliography and glossary	26
II	Appendix	i

Part I

Report

Chapter 1

LRDE Presentation

1.1 Line of business

The LRDE (Research and Development Laboratory of EPITA) is focused on fundamental research and development in computer science. Its main areas of expertise are:

- Image processing and pattern recognition
- Automata and verification
- Performance and genericity

Building on its solid scientific production and academic collaborations, the laboratory has industrial contracts, conducts internal research projects and participates in collaborative academic research projects.

Its members also give classes to students at EPITA from the first year of engineering.

1.2 The Laboratory

The LRDE (<https://www.lrde.epita.fr/wiki/Home>) was created in February 1998 to promote the research activity at EPITA and to allow students to be involved into important research projects.

The research activity at LRDE is focusing on subjects related to the school with the aim of getting recognition in the scientific domain through publications and by working together with other research centers.

One particularity of the LRDE is the will to create a bond between traditional teaching given to EPITA students and teaching through research. The point of this is to:

- participate to the production of knowledge in computer science and to promote the image of EPITA in scientific domain.
- develop LRDE student's formation through research and allow them to access a third cycle formation.

1.3 Members

The laboratory is currently composed of thirteen permanent members, including teacher-researchers, engineers and administration.

In addition to permanent staff, the LRDE also hosts PhD students. Currently, there are five of them. During the whole duration of their doctoral studies, they work with two advisor researchers, one of the LRDE and one of another university (joint supervision in partnership).

Each year, the permanent members recruit third year students from EPITA, whom will stay until the end of their studies, following a dedicated study specialisation at EPITA. Hence, the laboratory hosts two generations of students that can grow to a number between ten to fifteen.

1.4 Services

The LRDE is working on four different axis:

1.4.1 Image Processing

Olena



The Olena project (<https://olena.lrde.epita.fr>) consists of a generic image processing library. Its objective is to implement a platform of numerical scientific computations dedicated to image processing, pattern recognition and computer vision. This environment is composed of a generic and efficient library (Milena), a set of tools for shell scripts and a visual programming interface. The project aims at offering an interpreted environment like MatLab or Mathematica. It provides many ready-to-use image data structures (regular 1D, 2D, 3D images, graph-based images, etc.) and algorithms. Milena's algorithms are built upon classical entities from the image processing field (images, points/sites, domains, neighborhoods, etc.).

Each of these parts imply its own difficulties and require the development of new solutions. For example, the library, which require the entirety of low level features on which it relies on to be both efficient and generic — two objectives that are hard to meet at the same time in programmation. Fortunately, the object oriented programming eases this problem if we avoid the classical object modeling with inheritance and polymorphism. Hence, this genericity allows the development of efficient and re-usable code - i.e. developers or practitioners can easily understand, modify, develop and extend new algorithms while retaining the core traits of Milena: genericity and efficiency. The Olena platform uses this paradigm. The project already addressed the problem of the diversity of data and data structures.

Furthermore, the people working on this project were able to put in light the existence of conception models related to generic programming. Olena is an open source project under General Public License (GPL) version 2.

Climb

The Climb team of the laboratory has chosen to focus on the persistent question of performance and genericity, only from a different point of view.

The purpose of this research is to examine the solutions offered by languages other than C++, dynamic languages notably, and Lisp in particular. C++ has its drawbacks, it is a heavy language with an extremely complex and ambiguous syntax, the template system is actually a completely different language from standard C++ and finally it is a static language. This last point has significant implications on the application, insofar as it imposes a strict chain of Compilation \rightarrow Development \rightarrow Run \rightarrow Debug, making for example rapid prototyping or human-machine interfacing activities difficult. It becomes therefore essential to equip the involved projects with a third language infrastructure that is rather based on scripting languages.

The Climb project aims at investigating the same domain as Olena, but starting from an opposite view. It express the same issues following an axis of dynamic genericity and compares the performance obtained by some Common Lisp compilers with those of equivalent programs written in C or C++.

1.4.2 Finite state machine manipulation

Vcsn



The VCSN project (<https://vcsn.lrde.epita.fr>) is a finite state machine manipulation platform developed in collaboration with the ENST. Finite state machines, also called automata, are useful for language treatment and task automation. In the past, such platforms, like "FSM", were supposed to work for problems of industrial scale. Hence, for efficiency reasons, they were specialized in letter automata. On the other hand, platforms like "FSA" were based on a more abstract approach. VCSN tries to answer both of these issues by using techniques of static and generic programming in C++.

VCSN can then support the entirety of automata with multiplicity in any kind of semiring. Thanks to generic programming techniques, it is not necessary to code a single algorithm once for each type of automata anymore. A single abstract version is sufficient, and this without losing efficiency. It is not necessary to handle C++ perfectly to be able to use the platform thanks to an interpreter conceived to highlight all of the system's potential. This environment should allow researchers

to experiment their ideas and beginners to practice with an intuitive interface.

VCSN is an open source project under GPL license.

1.4.3 Model checking

Spot



Spot (<https://spot.lrde.epita.fr/>) is a library of algorithms for "model checking", which is a way to check that every possible behavior of a system satisfy its given properties. Spot allows to express those properties using linear-time temporal logic (LTL). It corresponds to classical propositional calculus (with its "or", "and" and "not" operators) equipped with temporal operators to express things such as "in a future time" or "anytime since now". Spot also supports arbitrary acceptance condition, transition-based acceptance and four different representation formats of ω -automata (HOA, never claims, LBTT, DSTAR). All those terms will be explained in the 'basic concepts' section.

Such formulas seen above (LTL formulas) can be translated to automata (Spot implements different algorithms), such that verifying that the behavior of a model satisfy a formula can be reduced to operations between two automata (here again Spot implements different algorithms). This approach can be applied to different kind of systems: communication protocols, electronic circuits, programs...

This project was born in the MoVe team at LIP6, but since 2007 it is mainly developed by the LRDE, with some occasional collaborations with LIP6. It is distributed under a GNU GPL version 3 license.

1.4.4 Speaker recognition

Speaker ID

The Speaker Recognition team is working on Machine Learning solutions applied to Speaker Recognition tasks. They propose statistical representations of speech signal which are more robust to the problem of session and channel variabilities.

A speaker must always be identified, whether he is ill, suffering from sore throats, or his current emotions bring change to his voice. To do this, all the characteristics of a voice that can change depending on any external parameter must be ignored. This is one of the issues the Speaker ID team is facing.

They participated in the evaluation campaign of speaker verification systems organized by NIST (the National Institute of Standards and Technology) which organizes competitions in various fields, both to stimulate research and to define new

standards since the beginning of the project.

The work of LRDE Speaker ID team is conducted in collaboration with the Spoken Language Systems Group of the MIT Computer Science and Artificial Intelligence Laboratory (<http://groups.csail.mit.edu/sls/>).

1.5 The internship in the company's work

This internship took place within the team of model checking. It was essentially focused on the improvement of the SAT-based minimization of ω -automata. It covers one of the many features of the Spot library.

Chapter 2

Spot

Spot was first presented in 2004 [10]. It was purely a library until Spot 1.0 [9], when command-line tools for LTL manipulation and translation of LTL to some generalizations of Büchi Automata have started to be distributed. Today, Spot 2.0 supports more tools with arbitrary acceptance conditions as described in the Hanoi Omega Automata format (HOA) [19] and python bindings usable in interactive environments such as IPython/Jupyter [13].

2.1 Structure

The Spot project can be broken down into several parts, as shown in Figure 2.1. Orange boxes are C/C++ libraries. Red boxes are command-line program. Blue boxes are Python-related.

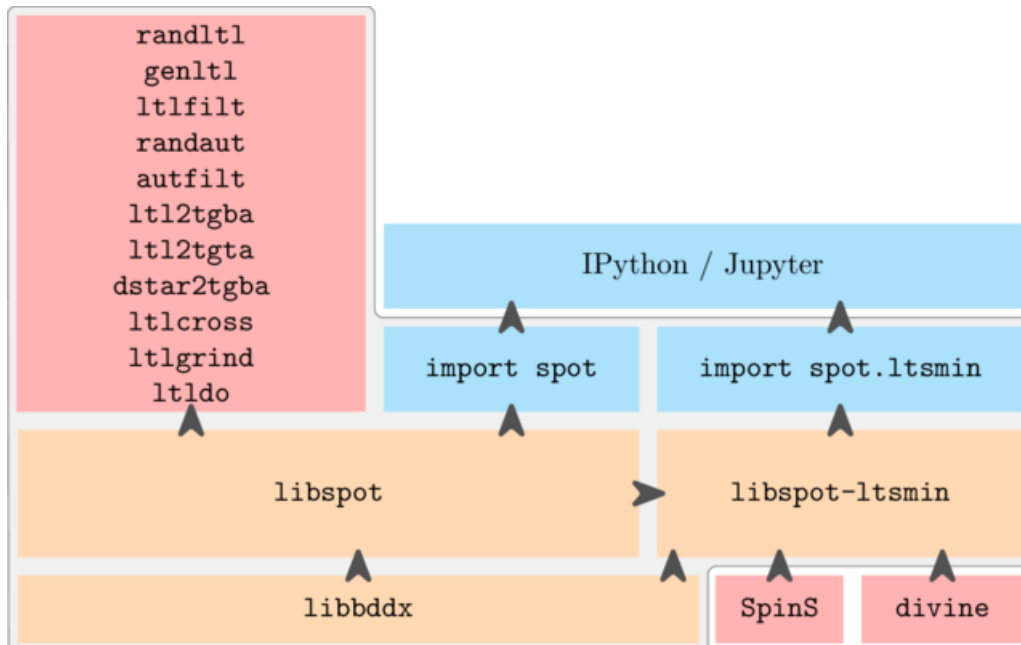


Figure 2.1: Architecture of Spot

Spot is actually split in three libraries:

- `libbddx` is a customized version of BuDDy for representing Binary Decision Diagrams which we use to label transitions in automata, and to implement a

few algorithms.

- libspot is the main library containing all data structures and algorithms.
- libspot-ltsmin contains code to interface with state-spaces generated as shared libraries by LTSmin.

2.2 Command-line tools

Spot 2.0 installs the following eleven command-line tools, that are designed to be combined as traditional Unix tools.

SPOT 1.0	randltl	Generates random LTL/PSL formulas
	genltl	Generates LTL formulas from scalable patterns
	ltlflt	Filter, converts, and transforms LTL/PSL formulas
	ltl2tgba	Translates LTL/PSL formulas into generalized Büchi automata[1], or deterministic parity automata (new in 2.0)
	ltl2tgta	Translates LTL/PSL formulas into Testing automata[2]
	ltlcross	Cross-compares LTL/PSL-to-automata translators to find bugs (works with arbitrary acceptance conditions since Spot 2.0)
	ltlgrind	mutates LTL/PSL formulas to help reproduce bugs on smaller ones
	dstar2tgba	converts ltl2dstar automata into Generalized Büchi automata[4]
	randaut	generates random ω -automata
	autfilt	filters, converts and transforms ω -automata
	ltldo	runs LTL/PSL formulas through other translators, providing uniform input and output interfaces

Figure 2.2: Spot tools description

As you see, the first six tools were introduced in Spot 1.0 [9], and have since received several updates. The other tools were introduced after.

2.3 The Python Interface

Similar tasks can be performed in a more "algorithm-friendly" environment using the Python interface. Combined with the IPython/Jupyter notebook [13] (a web application for interactive programming), this provides a nice environment for experiments, where automata and formulas are automatically displayed.

2.4 Workflow

Working on any project of the LRDE implies to follow some rules. That allows a better integration of each member. Once a patch is ready, any member of the model checking team can re-read the patch and make suggestions.

2.4.1 Coding conventions

As Spot is a free software, uniformity of the code matters a lot. Some coding conventions are used so that the code looks homogeneous. Here are some points:

- UTF-8 is used for non-ASCII characters.
- tabs are not used for indentation in c++ files, only spaces, in order to prevent issues with people assuming different tab widths.
- `#include` with angle-brackets refers to public Spot headers (i.e those that will be installed, or system headers that are already installed).
- `#include` with double quotes refer to private headers that are distributed with Spot.
- ... (see <https://gitlab.lrde.epita.fr/spot/spot/blob/master/HACKING> for more details)

2.4.2 Git Versionning Tool

The versionning tool used in Spot is Git. All development branches except 'master' and 'next' follows a particular naming convention: `{initials}/{subject of work}`. This allows a quick glance to identify who works on which branch and on what.

Concerning commits, large commits introducing a feature are preferred to many small commits covering the same feature. Suppose that a new feature must be implemented and needs 3 key steps. Even if each step is done in many commits during the development, at the end, it's better to squash commits so as to have only 3 large commits representing the 3 key steps.

Also, if at any moment it turns out that a previous work could have been done otherwise, any update must be applied directly to the commit concerned - each commit must actually insert code in its final form.

2.4.3 Adding Tests

Any implementation done must be tested. For the purpose on one hand to avoid regression and on the other hand to ensure the code runs as expected. All tests are located in the 'tests' folders. Most of them are written in Python (using the python bindings) or shell script.

Chapter 3

Basic concepts

Spot essentially manipulates ω -automata which is a variation of finite-state automata (FSA) that runs on infinite, rather than finite. It is important to have a good understanding of automata theory, not only to understand this report but because automata crop up pretty much everywhere in computer science. In logic design, natural language processing, system analysis, regular expressions, etc. The next two sections introduce the basics of automata theory and some concepts used in Spot.

3.1 Automata theory

Automata theory [3] is the study of abstract machines and automata, as well as the computational problems that can be solved using them.

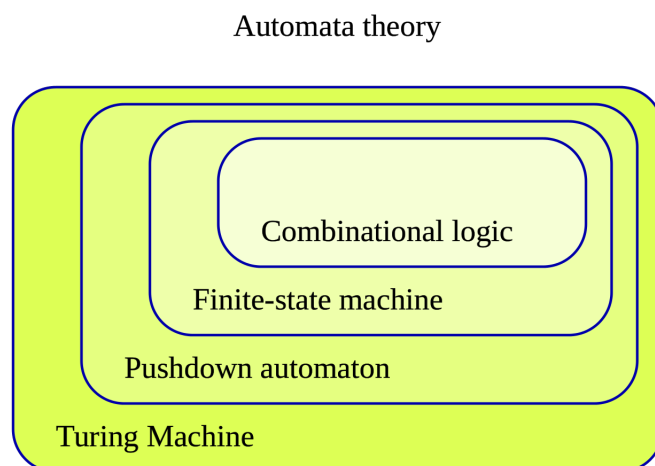


Figure 3.1: Classes of automata [3]

There are different classes of automata. The finite state machine has less computational power than some other models of computation such as the Turing machine [20]. The computational power distinction means there are computational tasks that a Turing machine can do but a finite-state automaton (FSA) can not.

From now on, the acronym FSA will be used instead of final-state automaton {a, on}.

Only FSA will be concisely described in this section as (again) ω -automata used in Spot are a variation of FSA.

3.1.1 Automata

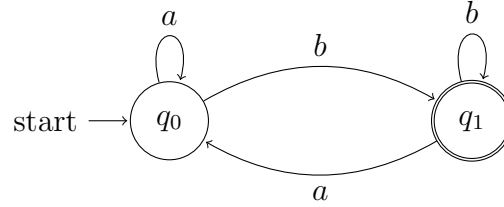


Figure 3.2: A finite-state automaton represented using a graph

The figure (3.2) shows how an automaton looks like. It consists of:

- a set of states (represented in the figure by circles). Among them we can distinguish the *initial state* **q0** (the one pointed by **start**) and an *accepting state* **q1** (the one doubly encircled).
- a transition relation (represented in the figure by arrows). This relation indicates for each state which state could be next according to the next symbol to read.

Before giving a regular definition, some points need clarification.

3.1.2 Alphabet, word, language

An alphabet is a finite set of symbols. It is commonly denoted by Σ . Edges of automata are labeled by those symbols. The alphabet used by the automaton of figure 3.2 is $\{a, b\}$.

A word is a finite sequence of symbols. $a, b, ab, aaaa, abbba, ababababbbaaabbaba$ are some words defined on the alphabet $\{a, b\}$. Automata recognizes words. In Spot, ω -automata recognizes ω -words, which are infinite rather than finite.

A language is a set of words defined on the same alphabet. The automata of figure 3.2 accepts or recognizes the set of words ending with b . **q1** is the only one accepting state and the only way to come in **q1** is to read b .

3.1.3 Automaton run

Well, an automaton run can be described as follows:

- it starts in the initial state and waits for the first character (of the word) to read.
- At each step, it reads the next symbol (character) and determine the next state using the transition relation.
- It stops when all the character chain has been read. The word is accepted if the automaton is in one of the accepting states.

3.1.4 Determinism (DFA, NFA)

A *deterministic* FSA is a final state machine where for each pair of state and input (symbols) there is one and only one transition to a next state. The figure 3.2 introduced before is actually a *deterministic* FSA or *deterministic* finite-state automaton (DFA).

A *non deterministic* FSA or *Nondeterministic* finite-state automaton (NFA) allows:

- many transitions labeled by the same symbol and outgoing from the same state,
- transitions labeled by the *empty word* ε ,
- transitions labeled by more than one symbol.

3.1.5 Finite-state automata (FSA) Definition

More formally, a finite-state automaton is defined by a quintuplet $M = (Q, \Sigma, X, s, F)$ where:

- Q is a set of states,
- Σ is an alphabet,
- X can be either a transition function $\delta : Q \times \Sigma \rightarrow Q$ (if the automaton is deterministic) or a transition relation $\Delta \subset (Q \times \Sigma^* \times Q)$ (if it is not deterministic),
- $s \in Q$ is the initial state,
- $F \subseteq Q$ is a set of accepting states.

3.2 About Spot

This section consists essentially of Spot's **concept** web page excerpts[6]. Feel free to have a look on that web page for further details.

3.2.1 Atomic proposition

An *atomic proposition* is a named Boolean variable that represents a simple property that must be true or false. It usually represents some property of a system. They are used to construct temporal logic formulas[15] to specify properties of the system.

3.2.2 Boolean formula

A Boolean formula is formed from *atomic proposition*, the Boolean constants true and false, and standard Boolean operators like and, or, implies, xor, etc.

3.2.3 ω -words

An ω -word as said before is a word of infinite length. In our context, each letter is used to describe the state of a system at a given time, and the sequence of letters shows the evolution of the system as the (discrete) time is incremented.

If the set \mathbf{AP} of atomic propositions is fixed, an ω -word over \mathbf{AP} is an infinite sequence of subsets of \mathbf{AP} . In other words, there are $2^{|\mathbf{AP}|}$ possible letters to choose from, and these letters denote the set of atomic propositions that are true at a given instant.

For instance if $\mathbf{AP} = \{a, b, c\}$, the infinite sequence $\{a, b\}; \{a\}; \{a, b\}; \{a\}; \{a, b\}; \{a\}; \dots$ is an example of ω -word over \mathbf{AP} . This particular ω -word can be interpreted as the following scenario: atomic proposition a is always true, b is true at each other instant, and c is always false.

3.2.4 ω -automaton

An ω -automaton is used to represent sets of ω -word.

Those look like the classical NFA in the sense that they also have states and transitions. However ω -automata recognize ω -words instead of finite words. In this context, the notion of final state makes no sense, and is replaced by the notion of acceptance condition: a run of the automaton (i.e., an infinite sequence alternating states and edges in a way that is compatible with the structure of the automaton) is accepting if it satisfies the constraint given by the acceptance condition.

In Spot, ω -automata have their edges labeled by Boolean formulas. An ω -word is accepted by an ω -automaton if there exists an accepting run whose labels (those Boolean formulas) are compatible with the minterms [16] used as letters in the word.

The language of an ω -automaton is the set of ω -words it accepts.

There are many kinds of ω -automata and they mostly differ by their acceptance condition. The different types of acceptance condition, and whether the automata are deterministic or not can affect their expressive power.

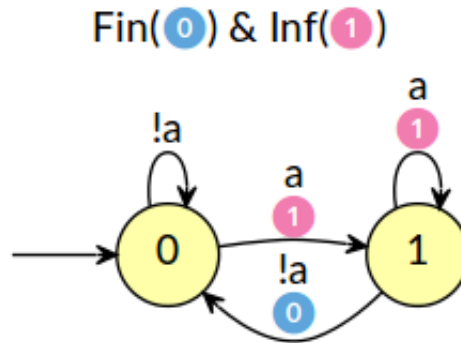


Figure 3.3: ω -automaton representing formula $\mathbf{FG}a$

3.2.5 Acceptance condition

An acceptance condition actually consists of two pieces: some acceptance sets, and a formula that tells how to use these acceptance sets.

Acceptance formulas are positive Boolean formula over atoms of the form t , f , $Inf(n)$, or $Fin(n)$, where n is a non-negative integer denoting an acceptance set.

- **t** denotes the true acceptance condition: any run is accepting
- **f** denotes the false acceptance condition: no run is accepting
- **Inf(n)** means that a run is accepting if it visits infinitely often the acceptance set n
- **Fin(n)** means that a run is accepting if it visits finitely often the acceptance set n

The above atoms can be combined using only the operator $\&$ and $|$ (also known as \wedge and \vee), and parentheses for grouping. Note that there is no negation, but an acceptance condition can be negated swapping t and f , \wedge and \vee , and $Fin(n)$ and $Inf(n)$.

The following table gives an overview of how some classical acceptance condition are encoded. The first column gives a name that is more human readable (those names are defined in the HOA [19] format and are also recognized by Spot). The second column give the encoding as a formula. Everything here is case-sensitive.

none	f
all	t
Buchi	Inf(0)
generalized-Buchi 2	Inf(0)&Inf(1)
generalized-Buchi 3	Inf(0)&Inf(1)&Inf(2)
co-Buchi	Fin(0)
generalized-co-Buchi 2	Fin(0) Fin(1)
generalized-co-Buchi 3	Fin(0) Fin(1) Fin(2)
Rabin 1	Fin(0) & Inf(1)
Rabin 2	(Fin(0) & Inf(1)) (Fin(2) & Inf(3))
Rabin 3	(Fin(0) & Inf(1)) (Fin(2) & Inf(3)) (Fin(4) & Inf(5))
Streett 1	Fin(0) Inf(1)
Streett 2	(Fin(0) Inf(1)) & (Fin(2) Inf(3))
Streett 3	(Fin(0) Inf(1)) & (Fin(2) Inf(3)) & (Fin(4) Inf(5))
generalized-Rabin 3 1 0 2	(Fin(0) & Inf(1)) Fin(2) (Fin(3) & (Inf(4)&Inf(5)))
parity min odd 5	Fin(0) & (Inf(1) (Fin(2) & (Inf(3) Fin(4))))
parity max even 5	Inf(4) (Fin(3) & (Inf(2) (Fin(1) & Inf(0))))

Figure 3.4: ω -automata acceptance conditions [6]

3.3 SAT solver

Satisfiability problem is a classic of computer science.

The purpose of SAT solving is to assign each variables of a propositional formula in such a way that the formula evaluates to true. It is the canonical NP-complete problem. SAT solvers are used to solve many practical problems and this is also the case in Spot, they are used to minimize ω -automata.

For more details, **SAT-solving in practice** [18] is a good introduction to SAT solvers.

Chapter 4

Specifications

This chapter tries to shed light on what was before this internship and why all the achieved work was needed.

4.1 Overall goal

The principal purpose of this internship is to improve an algorithm already implemented and used to minimize *deterministic* ω -automaton. The source code associated is the result of two papers:

- **SAT-based Minimization of Deterministic ω -Automata**[5] and
- **Mechanizing the Minimization of Deterministic Generalized Büchi Automata**[4].

Those two papers written by *Souheib baarir* and *Alexandre Duret-Lutz* are themselves a generalization of **Ehlers SAT'** based procedure [11]. Note that the first paper[5] is an extension of the second[4] which is restricted to generalized-Büchi acceptance.

4.1.1 The existing minimization

These previous work introduced a tool that can read any *deterministic* ω -automaton and synthesize (if it exists) an equivalent *deterministic* ω -automaton with a given number of states and arbitrary acceptance condition.

This tool, called $\text{SYNTHETIZEDTGBA}(R, n, m)$ works this way, It:

- inputs a complete DTGBA R , two target numbers of state (n) and arbitrary acceptance condition (m),
- produces a DIMACS file [8] with all the above clauses,
- calls a SAT solver to solve this problem,
- builds the resulting DTGBA C if it exists.

Using this tool, two minimization algorithms have been implemented:

Algorithm 1 A naive algorithm that calls $\text{SYNTHETIZEDTGBA}(R, n, m)$ in a loop, with a decreasing number of states, and returns the last successfully built automaton.

```

1: procedure REDUCESTATESDTGBA( $R, m = R.\text{NB\_ACC\_SETS}()$ )
2:   repeat:
3:      $n \leftarrow R.\text{nb\_states}()$ 
4:      $C \leftarrow \text{SYNTHETIZEDTGBA}(R, n - 1, m)$ 
5:     if  $C$  does not exists then return  $R$ 
6:      $R \leftarrow C$ 

```

Algorithm 2 This also calls $\text{SYNTHETIZEDTGBA}(R, n, m)$ in a loop, but attempting to find the minimum number of states using a binary search.

```

1: procedure DICHOTOMYDTGBA( $R, m = R.\text{NB\_ACC\_SETS}()$ )
2:    $\text{max\_states} \leftarrow R.\text{nb\_states}() - 1$ 
3:    $\text{min\_states} \leftarrow 1$ 
4:    $S \leftarrow \text{null}$ 
5:   while  $\text{min\_states} \leq \text{max\_states}$  do
6:      $\text{target} \leftarrow (\text{max\_states} + \text{min\_states})/2$ 
7:      $C \leftarrow \text{SYNTHETIZEDTGBA}(R, \text{target}, m)$ 
8:     if  $C$  does not exists then
9:        $\text{min\_states} \leftarrow \text{target} + 1$ 
10:    else
11:       $S \leftarrow C$ 
12:       $\text{max\_states} \leftarrow R.\text{nb\_states}() - 1$ 
13:   $R \leftarrow S$ 

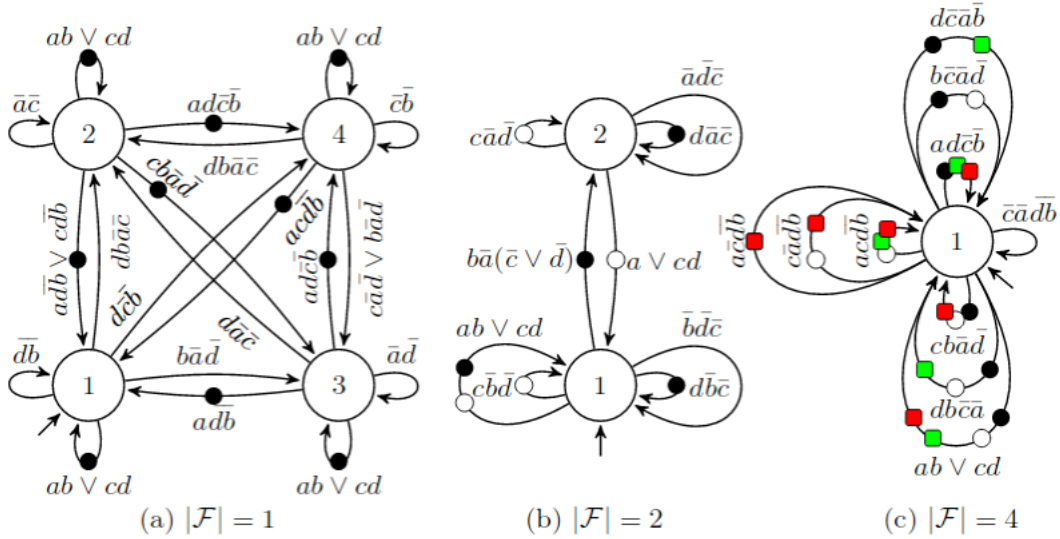
```

Until this internship, Algorithm 3 was used by default. There are no real reasons for that except that the second algorithm was implemented later in a completely different context and has never been benchmarked and compared to the first one.

ω -Automata minimization can be seen in two ways:

- **Reduction of the number of states:** This is typically the algorithm 3 that keeps by default the same number of acceptance sets (m) and decreases n at each $\text{SYNTHETIZEDTGBA}(R, n, m)$ call. The algorithm 2 has also the same perception. It knows the minimal automaton is between 1 (obviously, a smaller one does not exists) and $n - 1$ so instead of checking each number of states it performs a binary search with the will to be faster.
- **Rise of the accepting sets number:** This can be interpreted as the converse of a degeneralization: instead of augmenting the number of states to reduce the number of acceptance sets, we augment the number of acceptance sets in an attempt to reduce the number of states.

The figure below (4.1) is a great example from the first paper [4] that shows how smaller an automaton can become if the acceptance sets number is increased. Note that $|\mathcal{F}|$ here is m (the number of accepting sets).


 Figure 4.1: Examples of minimal DTGBA recognizing $(GFa \wedge GFb) \vee (GFc \wedge GFd)$

Finding the smallest m such that no smaller equivalent DTGBA with a larger m can be found is still an opened problem.

4.1.2 Tool chain

The figure 4.2 (from the FORTE'14 paper [4]) gives an overview of the processing chains that can be used to turn an LTL formula [15] into minimal DBA, DTBA or DTGBA. The blue area at the top describes:

Listing 4.1: bash command-line to translate a formula using `ltl2tgba`

```
ltl2tgba -D -x sat-minimize
```

while the purple area at the bottom corresponds to:

Listing 4.2: bash command-line to translate a formula using `dstar2tgba`

```
dstar2tgba -D -x stat-minimize
```

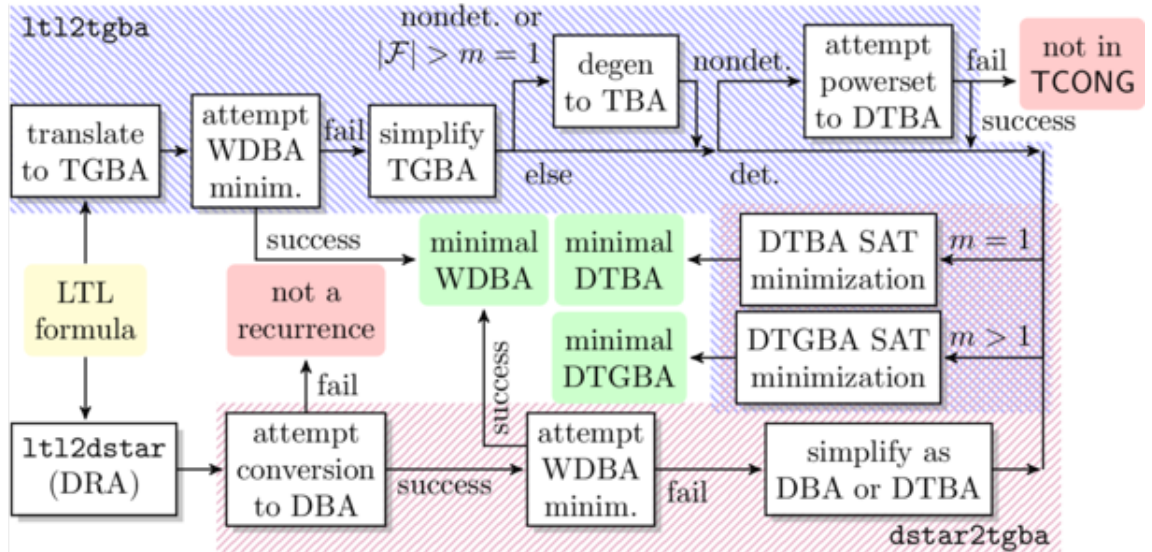


Figure 4.2: Two tool chain used to convert an LTL formula

As the SAT-based minimization only takes DTBA or DTGBA, the input automaton undergoes some transformations. In each tool, a Weak-DBA minimization is attempted. If that succeed, a minimal weak DBA is outputted (looking for transition-based or generalized acceptance will not reduce it further). For further details, please read the FORTE'14 paper [4].

4.1.3 The limits

Consider again the default algorithm (3). At each iteration, this algorithm re-encodes the research of a smaller automaton from scratch. Iterations after iterations (from n to $n - 1$, $n - 1$ to $n - 2$, etc.) the clauses encoded are almost the same. Therefore, it is a shame that nothing is retained, learned at each iteration. This is where incremental sat solving comes in mind.

Incremental solving is one of the recent directions in SAT solver research. This is based on an observation that in many applications of SAT solvers, the problems being solved consist of several calls to SAT solver on a sequence of SAT problem. Typically, the problems in the sequence share a large common part, making them highly interrelated. This is exactly our case! The purpose of incremental SAT solving is to recycle the work done in solving a previous problem in the sequence to solve the subsequent problems.

In order to use an incremental approach with SAT solver, it is no more possible to use DIMACS file [8]. Therefore, Spot needs to be linked to a SAT solving library. Let's remember that until now Spot requires a SAT solver to be installed on the same machine and provides a way to set it (through SPOT_SATSOLVER environment variable). obviously, being linked to a SAT solver and make calls to its functions will be more efficient than making Input/Output operations and executing another binary.

The memory consumption is also another problem. The larger the automaton is, the more variables there are. With some automata, the memory usage could grow over 150 Go which is uncommon for most users. The figure 4.3 helps to see memory usage peaks during a benchmark realized the end of September 2016.

4.2 Detailed explanation of the results to be obtained

As said before, the purpose of this internship is to improve the current SAT-based minimization technique. This minimization is wanted to be more fast and less greedy in memory consumption. If you look at the tool chain section above, this internship intervenes in the two SAT minimization rectangles (for $m = 1$ and $m > 1$).

The idea of testing an incremental approach for SAT-based minimization has already been raised by the Spot team. *Alexandre Duret-Lutz* had a clear idea of how to do it and I had been assigned the task of testing this idea. The objective

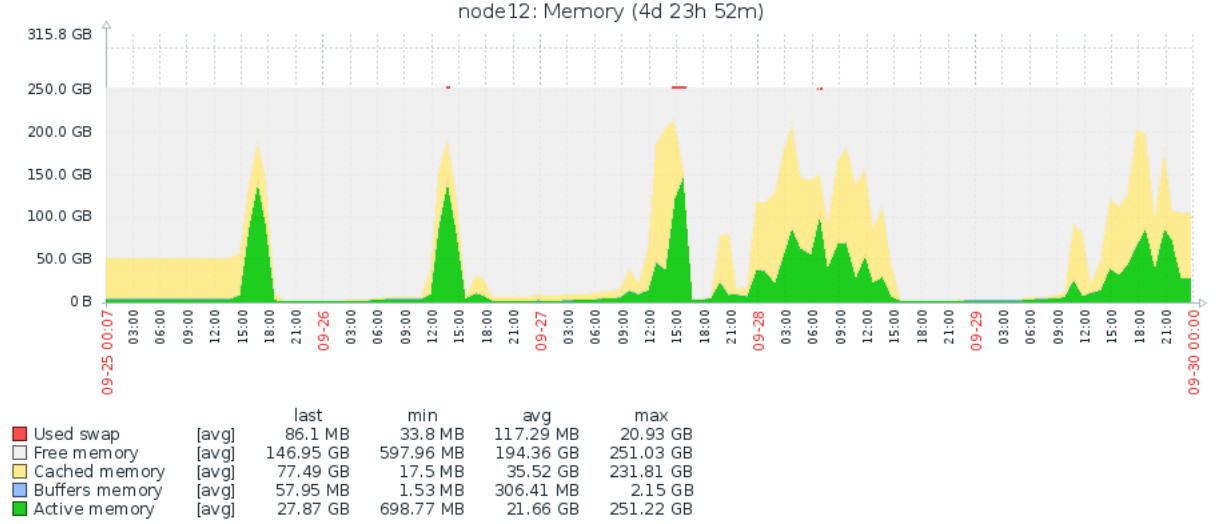


Figure 4.3: A graph showing memory usage during a benchmark realized at the beginning of the internship

being to improve it as much as possible, the internship is not limited to that. It is a line of approach as many others and the results to obtain can lead to new reflections.

Algorithm 3 An incremental approach that does the same traditional encoding once and then tries to exclude one more state at each iteration of a loop. The encoding is never restarted.

```

1: procedure REDUCESTATESDTGBA( $R, m = R.NB\_ACC\_SETS()$ )
2:    $n \leftarrow R.nb\_states()$ 
3:    $C \leftarrow SYNTHETIZEDTGBA(R, n - 1, m)$ 
4:   if  $C$  does not exists then return  $R$ 
5:   repeat:
6:     add clauses to exclude one more state
7:      $C \leftarrow$  Try to solve the new problem and build the new automaton
8:     if  $C$  does not exists then return  $R$ 
9:    $R \leftarrow C$ 
    
```

To do so, Spot needs to be linked to a SAT solving library. The really first task is to know which. I had to find the more suitable SAT solver that fills those requirements:

- It must have a compatible licence with Spot's one. Spot is under a GNU General Public Licence 3.
- It must be simple to integrate with Spot. Simple means here that the code shall be modified as little as possible so that a future update to a newer version of that solver will be simple to achieve.
- Of course, it has to be performant. Therefore, a look to SAT solvers international competitions as well as a custom benchmark is a fundamental need.

Regarding the memory consumption, the purpose is to identify the most memory-hungry parts of the source code and come up with solutions.

The results to be obtained can not be more precise than that. There is no precise figure estimating the speed to reach for a particular formula or the exact memory consumption to reduce, etc.

It is an internship that is part of a research work. By definition, the results are often unpredictable.

Chapter 5

Contributions to Spot

This chapter presents the different things I have done on Spot during the internship. Might it be some algorithms implemented, scripts, display arrangements, benchmarks, results analyzes, etc.

All the achieved work is presented in a chronological way, to bring out the difficulties encountered, the unexpected results that had influence on the advancement of the work.

5.1 fastSAT

As a quick reminder, here are the required characteristics for the SAT solver:

- licence compatibility with Spot's one (GNU GPL v3),
- simplicity of integration for future updates,
- effectiveness.

The project **fastSAT**[12] was born to help choose the SAT solver to distribute with Spot. Until now, SAT-based minimization was performed through an external SAT solver. The default one was Glucose [14] (3.0 version). Therefore, it seems logical to consider Glucose as a possible candidate. **fastSAT**[12] compared Glucose 4.0 [14] to CryptoMiniSat 5.0.1[7] and PicoSAT 965 [17]. Note that some SAT solvers provide two versions, one parallel and one simple essentially because of the SAT competitions. In short, were compared:

- Glucose syrup (parallel) 4.0
- Glucose simple 4.0
- CryptoMiniSat parallel 5.0.1
- CryptoMiniSat simple 5.0.1
- PicoSAT 965

The next three figures (5.1, 5.2 and 5.3) show some comparisons for three formulas. About twenty formulas have been tested in two modes: by forcing the number of state and by doing the complete cycles of minimization. It has been executed

on a computer with an **Intel(R) Core(TM) i7-4710HQ CPU @ 2.50GHz** processor and a **8 GiB** system memory. The measuring tool used is the open Google Benchmark tool [17].

```
#####| F(a ∧ GFb) ∨ (Fc ∧ Fa ∧ F(c ∧ GF(!b))) |#####
Complete cycles of minimisation
glucose_static --> TIMEOUT
glucose-syrup_static --> TIMEOUT
```

Function name	Time	CPU	Iteration
picosat	1266210us	173us	1
states=4, det=1			
cryptominisat	4883985us	161us	1
states=4, det=1			
cryptominisatsimple	4751886us	153us	1
states=4, det=1			

```
Forced number of states
glucose_static --> TIMEOUT
glucose-syrup_static --> TIMEOUT
```

Function name	Time	CPU	Iteration
picosat	5290558us	179us	1
states=4, det=1			
cryptominisat	6354672us	124us	1
states=4, det=1			
cryptominisatsimple	6312870us	126us	1
states=4, det=1			

Figure 5.1: Benchmark for formula $F(a \wedge GFb) \vee (Fc \wedge Fa \wedge F(c \wedge GF(!b)))$

```
#####| X(G(!a M !b) ∨ G(a ∨ G(!a))) |#####
Complete cycles of minimisation
glucose_static --> TIMEOUT
glucose-syrup_static --> TIMEOUT
```

Function name	Time	CPU	Iteration
picosat	52401us	118us	13
states=6, det=1			
cryptominisat	95552us	135us	7
states=6, det=1			
cryptominisatsimple	93853us	136us	7
states=6, det=1			

```
Forced number of states
glucose_static --> TIMEOUT
glucose-syrup_static --> TIMEOUT
```

Function name	Time	CPU	Iteration
picosat	28382us	140us	24
states=7, det=1			
cryptominisat	44104us	141us	16
states=7, det=1			
cryptominisatsimple	43055us	138us	16
states=7, det=1			

Figure 5.2: Benchmark for formula $X(G(!a M !b) \vee G(a \vee G(!a)))$

```
#####| GF(a | b) & GF(b | c) |#####
Complete cycles of minimisation
glucose_static --> TIMEOUT
glucose-syrup_static --> TIMEOUT
```

Function name	Time	CPU	Iteration
picosat	6432us	153us	104
states=1, det=1			
cryptominisat	6424us	154us	101
states=1, det=1			
cryptominisatsimple	6569us	157us	95
states=1, det=1			

```
Forced number of states
glucose_static --> TIMEOUT
glucose-syrup_static --> TIMEOUT
```

Function name	Time	CPU	Iteration
picosat	8946us	138us	77
states=1, det=1			
cryptominisat	10802us	137us	67
states=1, det=1			
cryptominisatsimple	10165us	132us	71
states=1, det=1			

Figure 5.3: Benchmark for formula $GF(a \vee b) \wedge GF(b \vee c)$

In conclusion, among the different SAT solvers, **PicoSAT** was chosen for its strong performances. It consists of two source code files: **picosat.h** and **picosat.c** and was easily integrated and harmonised with Spot.

fastSAT[12] project is fully available and anyone can reproduce the benchmarks. Feel free to have a look.

5.2 New Satsolver class

There was already a satsolver class that is instantiated at the beginning of the SAT-based minimization procedures, formerly used to initialize a temporary **cnf file** (DIMACS [8]) and return it. The file writing was directly made by those procedures. The objective is to completely abstract the file writing. SAT-based minimization procedures will just have to instantiate a satsolver object at the beginning and make calls to its functions. Those functions will call the SAT solving library functions. But as we still want to support any external satsolver, this class must continue to handle temporary **cnf files**.

The figure 5.4 shows a pseudo UML representation of the new satsolver class. It can either initialize PicoSAT or a `cnf_stream..` The idea is to let its function (`add`, `comment`, etc.) to decide if they call PicoSAT functions or write in the `cnf_stream..` That way, SAT-based minimization procedures are not aware of what's going on behind and can repeat over and over again the same algorithms.

Of course the clause counting mechanism is provided by the new satsolver class. At the end, SAT-based procedures will just have to call the `get_solution()` method.

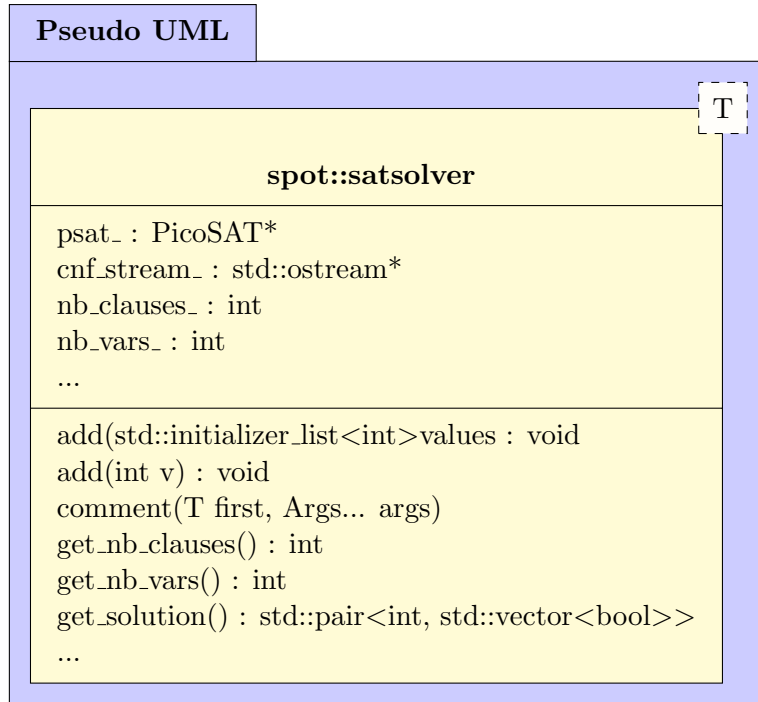


Figure 5.4: Satsolver class UML representation

Once this was done, SAT-based procedures had already gained some speed. For instance, with this command line:

Listing 5.1: bash command-line to test a formula minimization using ltl2tgba

```
time ltl2tgba -D -x sat-minimize 'G(a -> Fb) & G(c -> Fd)'
--stats='states=%s, det=%d'
```

we obtained:

Version	Result
PicoSAT as linked SAT solving library	0.29s user 0.08s system 98% cpu 0.371 total
PicoSAT as external SAT solver	0.82s user 0.09s system 98% cpu 0.925 total

Chapter 6

Bibliography and glossary

References

- [1] A.Duret-Lutz. “LTL translation improvements in Spot 1.0”. In: *Int. J. on Critical Computer-Based Systems* (2014), pp. 31–54.
- [2] A.Duret-Lutz A.E.Ben Salem and F.Kordon. “Model checking using generalized testing automata”. In: *Transactions on Petri Nets and Other Models of Concurrency (ToPNoC V1)* (2012), pp. 94–112.
- [3] *Automata Theory*. URL: https://en.wikipedia.org/wiki/Automata_theory.
- [4] Souheib Baarir and A.Duret-Lutz. “Mechanizing the Minimization of Deterministic Generalized Büchi Automata”. In: *FORTE* vol. 8461 (2014), pp. 266–283. URL: <https://www.lrde.epita.fr/~adl/dl/adl/baarir.14.forte.pdf>.
- [5] Souheib Baarir and A.Duret-Lutz. “SAT-based Minimization of Deterministic omega-Automata”. In: *LPAR* (2015). URL: <https://www.lrde.epita.fr/~adl/dl/adl/baarir.15.lpar.pdf>.
- [6] *Concepts*. URL: <https://spot.lrde.epita.fr/concepts.html>.
- [7] *CryptoMiniSat*. URL: <https://github.com/msoos/cryptominisat/releases/tag/5.0.1>.
- [8] *DIMACS format*. URL: <http://www.satcompetition.org/2009/format-benchmarks2009.html>.
- [9] A. Duret-Lutz. “Manipulating LTL formulas using Spot 1.0”. In: *ATVA* vol. 8172.13 (Springer, 2013), pp. 442–445.
- [10] A. Duret-Lutz and D.Poitrenaud. “SPOT: an Extensible Model Checking Library using Transition-based Generalized Büchi Automata”. In: *MASCOTS* 04 (2004), pp. 76–83.
- [11] Rüdiger Ehlers. *Minimising deterministic Büchi automata precisely using SAT solving*. 2010.
- [12] *fastSAT*. URL: <https://github.com/shumpaga/fastSAT>.
- [13] F.Pérez and B.E.Granger. “IPython: a system for interactive scientific computing”. In: *Computing in Science and Engineering* (21-29, 2007). URL: <http://ipython.org/>.

- [14] *Glucose*. URL: <http://www.labri.fr/perso/lsimon/glucose/>.
- [15] *Linear-time Temporal Logic (LTL)*. URL: <https://spot.lrde.epita.fr/concepts.html#ltl>.
- [16] *Minterms*. URL: https://en.wikipedia.org/wiki/Canonical_normal_form#Minterms.
- [17] *PicoSAT*. URL: <http://fmv.jku.at/picosat/>.
- [18] *SAT-solving in practice*. URL: <http://www.cse.chalmers.se/edu/year/2012/course/TDA956/Papers/satFinal.pdf>.
- [19] A.Duret-Lutz J.Klein J.Kretinskiy D.Müller D.Parker T.Babiak F.Blahoudek and J.Strejcek. "The Hanoi Omega-Automata format". In: *CAV* vol. 9206.15 (Springer, 2015). URL: <http://adl.github.io/hoaf/>.
- [20] *Turing Machine*. URL: https://en.wikipedia.org/wiki/Turing_machine.

Part II

Appendix

Contents (Appendix)

A	Company documentation	iii
B	Hardware / Software Documentation	iv
C	Gross results	v

Appendix A

Company documentation

Appendix B

Hardware / Software Documentation

Appendix C

Gross results