Is There a Best Büchi Automaton for Explicit Model Checking?

František Blahoudek  
Masaryk University  
Brno, Czech Republic  
xblahoud@fi.muni.cz

Alexandre Duret-Lutz  
LRDE, EPITA  
Le Kremlin-Bicêtre, France  
adl@lrde.epita.fr

Mojmír Křetínský  
Masaryk University  
Brno, Czech Republic  
kretinsky@fi.muni.cz

Jan Strejček  
Masaryk University  
Brno, Czech Republic  
strejcek@fi.muni.cz

ABSTRACT

LTL to Büchi automata (BA) translators are traditionally optimized to produce automata with a small number of states or a small number of non-deterministic states. In this paper, we search for properties of Büchi automata that really influence the performance of explicit model checkers. We do that by manual analysis of several automata and by experiments with common LTL-to-BA translators and realistic verification tasks. As a result of these experiences, we gain a better insight into the characteristics of automata that work well with Spin.

Categories and Subject Descriptors
F.4.1 [Mathematical Logic and Formal Languages]: Mathematical Logic—temporal logic; D.2.4 [Software Engineering]: Software/Program Verification—formal methods, model checking

General Terms
Theory, Algorithms, Verification

Keywords
Linear temporal logic, Büchi automata, explicit model checking

1. INTRODUCTION

The automata-theoretic approach to explicit model checking of Linear-time Temporal Logic (LTL) [24] can be broken down into four steps: (1) build the state space, i.e., an automaton \( S \) representing all the possible executions of the system to be verified, (2) translate an LTL formula \( \varphi \) representing a desired property of the system into a Büchi Automaton (BA) \( A_{\varphi} \) that accepts all the executions of the system violating \( \varphi \), (3) build the synchronous product \( S \otimes A_{\varphi} \) of these two systems, and finally (4) check this product for emptiness. If \( S \otimes A_{\varphi} \) accepts a word, it is an execution of \( S \) that invalidates \( \varphi \), i.e., a counterexample.

In a typical explicit model checker, the construction of the state space \( S \) and its synchronous product with \( A_{\varphi} \) are done one-the-fly as needed by an emptiness check procedure. This ensures that only the part of the state space that is compatible with \( A_{\varphi} \) will be constructed. Further, the whole construction can be stopped as soon as the emptiness check finds a counterexample, i.e., a reachable cycle containing an accepting state.

Here we focus on the influence of a property automaton \( A_{\varphi} \) on the steps (3) and (4) of a model checking procedure. There are many algorithms and tools for translating an LTL formula into a Büchi automaton, yet they produce various language equivalent automata. For instance, Figure 5 shows several Büchi automata for the LTL formula \( GFPa \land GFb \). Should one be preferred over the others?

The intuition that a smaller \( A_{\varphi} \) produces a smaller synchronous product \( S \otimes A_{\varphi} \) is not always correct. More importantly, it is not quite relevant: ultimately, only the part of the product that is explored by the emptiness check does matter. Some authors of automata optimizations or LTL-to-BA translation improvements (e.g., Etessami and Holzmann [9] and Dax et al. [10]) provide also running times of a selected emptiness check executed on the product of obtained automata and either random state spaces or few realistic systems. Etessami and Holzmann [9] even complained that the relation between the size of \( A_{\varphi} \) and the running time of the model checking procedure was difficult to predict, especially in the presence of a counterexample.

In order to select an ideal automaton for expressing a formula, one should be aware of the inner workings of the emptiness check procedure that will be used. Among the various existing emptiness checks, we have decided to focus on the standard emptiness check of Spin, which is a sequential algorithm based on a Nested Depth-First Search (NDFS) [15].

We look at concrete examples of how formulae are translated differently by existing tools to gain a better insight into the characteristics of automata that work well with Spin. Our results should stimulate LTL-to-BA translation...
researchers to focus on another aspects of produced automata: not only their size and determinism.

The paper is organized as follows. The next section motivates our research by experimental results quantifying influence of property automata on the performance of the explicit model checker Spin. Section 2 describes standard approaches to automata optimization motivated by reduction of the product size. In Section 3, we discuss how property automata can affect the performance of the NDFS-based emptiness check of Spin.

We assume familiarity with LTL and Büchi automata.

2. MOTIVATION BY EMPIRICAL DATA

First of all, we present experimental results showing how important the impact of Büchi automata on Spin’s performance can be. We use the following benchmark, software, and hardware.

Benchmark. The considered benchmark set is based on the set of realistic model checking tasks BEEM [17]. Out of the original 735 pairs of a model in Promela and a corresponding specification formula, we have removed 12 pairs with formulae containing the string active in the name of some atomic proposition as Spin fails to run these tasks (it is a reserved keyword). To each model describing some mutual exclusion algorithm (altogether 22 instances of parametric models called anderson, peterson, and bakery), we add three formulae:

1. \( \text{GF}(P_0@\text{CS}) \rightarrow \text{GF}(P_0@\text{NCS}) \) meaning that if a process \( P_0 \) spends infinitely many steps in a critical section, then it also spends infinitely many steps in a non-critical section,

2. \( \text{GF}(P_0@\text{NCS}) \rightarrow \text{GF}(P_0@\text{CS}) \) meaning that if a process \( P_0 \) spends infinitely many steps in a non-critical section, then it also spends infinitely many steps in a critical section,

3. \( \text{FG}¬((P_0@\text{CS} \land P_1@\text{CS}) \lor (P_0@\text{CS} \land P_2@\text{CS}) \lor (P_1@\text{CS} \land P_2@\text{CS})) \) meaning that after finitely many steps, it never happens that two of the processes \( P_0, P_1, \) and \( P_2 \) are in a critical section at the same time.

To sum up, we consider \( 735 - 12 + 3 \cdot 22 = 789 \) verification tasks. All the benchmarks and measurements presented in this section are available at http://fi.muni.cz/~xblahoud/spin2014.tar.gz

Software. We use five LTL-to-BA translators presented in Table 1. Spin and LT2BA are well established and popular translators, MoDeLLa was the first translator focusing on determinism of produced automata, and LT3BA and Spot represent contemporary translators. The last two translators are used in several settings: the settings denoted by LT3BA (det) and Spot (det) aim to produce more deterministic automata, while the setting called Spot (no jump) is explained in Section 3. The same version of Spin (with its default settings) is also used in all our experiments to perform all model checking steps except the LTL-to-BA translation. In particular, the partial-order reduction, which severely limits the exploration of the state-space, is enabled.

Hardware. All computations are performed on an HP DL980 G7 server with 8 eight-core 64-bit processors Intel Xeon X7560 2.26GHz and 448 GiB DDR3 RAM. Each execution of Spin has been restricted by 30 minutes timeout and a memory limit of 20GiB.

Originally, we have measured the impact of Büchi automata on Spin by its running time. Unfortunately, our computation server is shared with other users and its variable workload has led to enormous dispersion of measured running times. We have observed a running time difference over 300% on the same input. Hence, instead on running times, we focus on the count of visited transitions, which is a stable statistic produced directly by Spin. The number of visited transitions accumulates the numbers of product transitions explored in depth-first searches executed during a run of the NDFS algorithm (see Section 1 for a brief description of NDFS). Hence, the number of visited transitions should be proportional to the running time on a dedicated machine.

For each of the 789 considered verification tasks, we translate the negation of the formula by all the mentioned translators and we run Spin on the model with each of the obtained automata. For 778 tasks, Spin successfully finishes the computation within the given limits at least for two automata obtained by different translation tools. For each such a verification task, we find the maximal and the minimal numbers of visited transitions and we compute their ratio. Intuitively, the ratio represents how many times slower Spin can be if we choose the worst of the produced automata compared to the best of those.

Out of the 778 tasks, the ratio is exactly 1 only in 30 cases. In other words, in more than 96% of the considered verification tasks, the choice of an LTL-to-BA translator has an influence on running time of Spin.

Table 1: Considered LTL-to-BA translators, for reference.

<table>
<thead>
<tr>
<th>tool</th>
<th>version command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spin</td>
<td>6.2.5 spin -f</td>
</tr>
<tr>
<td>LTL2BA</td>
<td>1.1 lt12ba -f</td>
</tr>
<tr>
<td>MoDeLLa [19]</td>
<td>1.5.9 mod2spin -f</td>
</tr>
<tr>
<td>LT3BA [1]</td>
<td>1.0.2 lt3ba -S -f</td>
</tr>
<tr>
<td>LT3BA (det)</td>
<td>lt3ba -S -M -f</td>
</tr>
<tr>
<td>Spot [7]</td>
<td>1.2.3a lt12tgba -s</td>
</tr>
<tr>
<td>Spot (det)</td>
<td>lt12tgba -s -D</td>
</tr>
<tr>
<td>Spot (no jump)</td>
<td>lt12tgba -s -x degen-lskip=Q</td>
</tr>
</tbody>
</table>

In fact, the ratios significantly differ for verification tasks where the model satisfies a given formula and for those with a counterexample. Out of the 778 tasks, 696 tasks contain counterexamples while 82 tasks do not. The ratios for these two sets are presented by box-plots in Figure 1. One can clearly see that the selection of a Büchi automaton has a bigger impact on the verification tasks with counterexamples (median ratio is over 5.7) than on the tasks without counterexamples (median ratio is 1.4). Both sets contain extreme cases where the ratios exceed 10^6.

Spin also provides stored states, which is the total count of constructed and stored product states and should be proportional to the memory consumed by Spin. If we compute ratios of maximal and minimal numbers of stored states, we get the ratio 1 in 63 out of the 778 tasks. Figure 2 presents...
box-plots of the ratios for tasks with and without counterexamples. One can see that the situation is analogous to ratios of visited transitions, but the ratios of stored states are slightly lower.

To sum up, the choice of a Büchi automaton is an important issue substantially affecting both running time and memory needed for the explicit model checking process implemented in Spin.

3. STANDARD APPROACH TO OPTIMIZATION: HELPING THE PRODUCT

Most of the work on optimizing the translation of LTL formulae to Büchi automata has focused on building Büchi automata with the smallest possible number of states [e.g. 4 10 20 13 22]. This is motivated by the observation that the synchronous product of a Büchi automaton $A$ with a state space $S$ can have the same number of states as their Cartesian product in the worst case: $|S \otimes A| \leq |S| \times |A|$. Therefore, decreasing $|A|$ lowers the upper bound on $|S \otimes A|$.

However it is possible to build contrived examples where a smaller $|A|$ yields a larger product. For instance, removing one state in the automaton $A_1$ of Figure 3 doubles the size of its product with the state space $S$ of the same figure from 3 to 6 states. Of course, if $S$ was a similar cycle of 2 states, the smaller automaton $A_2$ would give a smaller product.

Hence, one cannot hope to build an optimal property automaton $A$ without a priori knowledge of the system $S$.

With the introduction of LBTT [21], a tool that checks the output of different LTL-to-BA translators by doing many cross-comparisons, including some products with random state spaces, tool designers started to evaluate not only the size of the produced automata, but also the size of their products with random state spaces [e.g. 13 8]. A recent clone of LBTT called ltlcross [16] computes multiple products with random state spaces to lessen the luck factor. Sebastiani and Tonetta [19] used this “product with a random state space” measurement to benchmark their translator MoDelLa against other available translators to support the claim that producing “more deterministic” Büchi automata might be more important than producing small Büchi automata.

Benchmarks based on the size of products may look like Table 2. The table shows that MoDelLa generates automata that are slightly bigger than LTL2BA (its competitor in 2003) but when looking at the product, MoDelLa causes fewer transitions to be built. If the number of transitions is proportional to the running time of a model checker and the number of states is proportional to its memory consumption, MoDelLa has effectively traded memory for speed.

MoDelLa’s results do not appear to hold today: more recent translators such as LTL3BA or the translator of Spot

![Figure 1: Impact of Büchi automata on visited transitions.](image1)

![Figure 2: Impact of Büchi automata on visited states.](image2)

![Figure 3: Two BA for GFa and a state space. $A_1 \otimes S$ has 3 states whereas $A_2 \otimes S$ has 6. Note that edges in the automata are labelled by Boolean formulae over atomic propositions, where $\bar{a}$ means $\neg a$, $\top$ stands for true, and $ab$ used later means $a \land \neg b$. Formally, an edge labelled with a formula $\rho$ represents all the transitions that are labelled with a subset $M$ of atomic propositions such that $M \models \rho$.](image3)
Table 2: Translation of 178 formulae from the literature using different LTL-to-BA translators, with a timeout of 60 seconds. Column n indicates how many translations are successful within the allocated time. The automata columns show accumulated values of standard automata characteristics for all successful translations. Column ndst gives the number of non-deterministic states in the automata. All produced automata are synchronized with the same 100 random systems, and the median number of states and transitions of these products is kept. The products columns represent the medians accumulated over all successful translations. The right-most part of the table counts the number of formulae for which the translator on the row produces an automaton with higher median number of transitions in the products that the translator of the column.

<table>
<thead>
<tr>
<th>n states</th>
<th>ndst</th>
<th>edges</th>
<th>trans</th>
<th>states</th>
<th>trans</th>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
<th>(5)</th>
<th>(6)</th>
<th>(7)</th>
<th>(8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Spin</td>
<td>161</td>
<td>1739</td>
<td>1474</td>
<td>9318</td>
<td>46252</td>
<td>260934</td>
<td>8892105</td>
<td>0</td>
<td>102</td>
<td>143</td>
<td>107</td>
<td>150</td>
<td>150</td>
</tr>
<tr>
<td>(2) LTL3BA</td>
<td>178</td>
<td>1003</td>
<td>802</td>
<td>3360</td>
<td>30159</td>
<td>191608</td>
<td>5556159</td>
<td>5</td>
<td>0</td>
<td>137</td>
<td>49</td>
<td>161</td>
<td>157</td>
</tr>
<tr>
<td>(3) MoDeLLa</td>
<td>178</td>
<td>1297</td>
<td>647</td>
<td>4311</td>
<td>23874</td>
<td>216038</td>
<td>4193567</td>
<td>15</td>
<td>33</td>
<td>0</td>
<td>41</td>
<td>110</td>
<td>116</td>
</tr>
<tr>
<td>(4) LTL3BA</td>
<td>178</td>
<td>795</td>
<td>595</td>
<td>2209</td>
<td>21240</td>
<td>151373</td>
<td>3273646</td>
<td>0</td>
<td>23</td>
<td>126</td>
<td>0</td>
<td>149</td>
<td>153</td>
</tr>
<tr>
<td>(5) LTL3BA (det)</td>
<td>178</td>
<td>830</td>
<td>326</td>
<td>2405</td>
<td>14414</td>
<td>155716</td>
<td>2901474</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>5</td>
<td>76</td>
<td>75</td>
</tr>
<tr>
<td>(6) Spot</td>
<td>178</td>
<td>657</td>
<td>94</td>
<td>1615</td>
<td>10304</td>
<td>127792</td>
<td>2326271</td>
<td>1</td>
<td>6</td>
<td>15</td>
<td>5</td>
<td>30</td>
<td>0</td>
</tr>
<tr>
<td>(7) Spot (det)</td>
<td>178</td>
<td>662</td>
<td>88</td>
<td>1639</td>
<td>10414</td>
<td>128178</td>
<td>2328422</td>
<td>1</td>
<td>7</td>
<td>17</td>
<td>6</td>
<td>33</td>
<td>4</td>
</tr>
<tr>
<td>(8) Spot (no jump)</td>
<td>178</td>
<td>785</td>
<td>104</td>
<td>1874</td>
<td>12273</td>
<td>152592</td>
<td>2719360</td>
<td>12</td>
<td>28</td>
<td>40</td>
<td>27</td>
<td>61</td>
<td>57</td>
</tr>
</tbody>
</table>

4. ANOTHER VIEW TO OPTIMIZATION: HELPING THE EMPTINESS CHECK

We omitted their tool from our benchmark because (1) it only supports a subset of LTL, and (2) their optimization is implemented in Spot and both tools would therefore return the same automata. Besides, the subset of LTL does not include the formulae studied in Sections 4.3 and 4.5.

4.1 Emptiness Checks with Nested DFS

To check the emptiness of $S \otimes \mathcal{A}_\varphi$, one should search for a cycle that is reachable from the initial state and that contains at least one accepting state. The emptiness check procedure used in Spin by default is based on two nested depth-first searches [13]: the main DFS, which we shall call blue, explores the product (on-the-fly) and every time it would backtrack from an accepting state $s$ (i.e., all successors of $s$ have been explored by the blue DFS) it starts a second, red DFS from $s$. If the red DFS reaches any state on the blue DFS search stack then a reachable and accepting cycle is found (since $s$ is reachable from all states on the blue DFS search stack) and the algorithm reports it as a counterexample. Otherwise, the red DFS terminates and the blue DFS can continue. The two DFS always ignore states that have been completely explored by an instance of the red DFS, so a non-accepting strongly connected component is never visited more than twice.

When a counterexample exists in the product, the emptiness check may report it more or less rapidly depending on the order in which it has explored the transitions of the product. With any luck, the first transition selected at each step of the DFS will lead to an accepting cycle. Conversely, the first transitions followed might lead to a huge component of the product that just turns out to be a dead-end and from which the emptiness check has to backtrack before finding the counterexample. As the selected transition order in $S \otimes \mathcal{A}_\varphi$ depends on the order of the transitions in the property automaton $\mathcal{A}_\varphi$, this explains some of the huge differences noticed in Figure 1 and 2. Note that previous attempts to explore reordering of the transitions of $\mathcal{A}$ to help the emptiness check have been inconclusive [12], so we did not pursue this direction. (Furthermore the swarm-avoiding techniques [10] used nowadays makes this topic even less attractive.)

As an extra optimization, if the blue DFS hits its own search stack by following a transition that is either going to or coming from an accepting state [11][15], then an accepting cycle can be reported without even starting any red DFS.
4.2 Weak Automata

The last optimization, which can be effectively applied only on products with an accepting cycle, suggests that of the two automata of Figure 3, \(B_2\) should be preferred. Indeed when the blue DFS reaches a state of its search stack in the product \(S \otimes B_2\), it is guaranteed to come from (and go to) an accepting state, detecting the accepting cycle without starting a red DFS. In the product \(S \otimes B_1\) we might be less lucky if we close the cycle with the transition at the bottom time by the red DFS.

This example actually illustrates the distinction between weak automata and inherently weak automata. An inherently weak automaton is an automaton in which strongly connected components (SCCs) cannot mix accepting cycles with non-accepting cycles. A weak automaton, is an inherently weak automaton in which the states of each SCC are either all accepting or all non-accepting. Any inherently weak automaton can evidently be transformed into an equivalent weak automaton [2].

Having more accepting states is not necessarily good from the point of view of the NDFS since a red DFS is started every time the blue DFS backtrack from an accepting state. However if an entire SCC is non-accepting, the first red DFS will cover it fully, and all the successive red DFS will immediately return because they attempt to process states that have already been seen by a previous red DFS.

4.3 Automata for GF\(a \land GFb\)

Figure 5 shows six different Büchi automata for the formula GF\(a \land GFb\) produced by the considered tools. Note that if you ignore the exchange of \(a\) and \(b\) (which have symmetric purpose in the original formula), automata \(C_1\) and \(C_5\) differ only in the initial state and thus cannot be distinguished by any determinism-based or size-based metrics.

Table 3 captures data about Spin’s runs on a model of bakery mutual exclusion protocol taken from BEEM and the property automata of Figure 5. The propositions \(a\) and \(b\) describe situations that (different) pairs of processes are in the critical section at the same time. The protocol prevents such situation so neither \(a\) nor \(b\) is ever true in the model. We observe that in case of products with automata \(C_5\) and \(C_6\) (both produced by Spot), Spin explores each product twice because it triggers the red DFS from the initial state of the product. It is not the case for the other automata. This yields in the following hypothesis: When we suppose that there is no accepting cycle in the product, the automaton should keep its accepting states as far as possible from the initial state. The further they are, the more chance we have that the product will never reach the state, and therefore no red DFS will be triggered.

For instance, if we ignore the renaming of atomic propositions, the automaton \(C_3\) could be obtained from \(C_6\) by unrolling the accepting cycle by one step, so that the cycle is entered on a non-accepting state, and the accepting state is actually the last one visited on the cycle. This superficial initial state only makes a negligible difference on the product, and does not incur any noticeable difference for Spin compared to \(C_1\), \(C_2\), or \(C_4\).

Similarly, if we do not expect an accepting cycle in the product, the inherently weak automaton \(B_1\) could be changed by letting the right-most state be accepting instead of the middle one.

4.4 Translation Differences

Most LTL-to-BA translators follow a multi-steps procedure where they first translate a given LTL formula into a generalized Büchi automaton, often with transition-based acceptance (TGBA), such as those of Figure 6. Translators then degeneralize these automata to obtain a BA. Other simplification procedures may be applied to these automata, but it turns out that the last three automata of Figure 6 were all obtained by degeneralizing \(G_1\), and their differences are due to choices made in the degeneralization procedure.

When degeneralizing a TGBA \(G\) with \(m\) acceptance sets \(F_1,\ldots,F_m\) (the \(\bullet\) and \(\odot\) on the Figure 6), the structure of \(G\) is cloned \(m + 1\) times. Let us call each of these clones a level. For each state of level \(i \leq m\), all transitions that were originally in \(F_i\) have their destination redirected to the next level, the destination of all transitions in level \(m + 1\) are redirected to level 1. Finally, all the states of the level \(m + 1\) are made accepting. The initial state can be put on any level.

This procedure ensures that words accepted by the degeneralized automaton correspond to words recognized by runs of \(G\) that visit all acceptance sets infinitely often. Accepting cycles in products involving these degeneralized automata will always involve at least \(m + 1\) states.

The degeneralization applied to \(G_1\) with the initial state on the last level and the acceptance sets ordered as \(\odot\), then \(\bullet\), produces the automaton \(C_6\) of Figure 5. Recall that the edge labelled with \(\top\) corresponds to the four edges labelled by \(ab\), \(\bar{a}b\), \(ab\), and \(ab\) in the original automaton \(G_1\).

An optimization introduced by Gastin and Oddoux [10] consists in jumping levels. If a transition of a level \(i \leq m\) belongs to \(F_1 \cap \ldots \cap F_i\), its destination can be redirected directly to the level \(j + 1\). Similarly, if a transition from the level \(m + 1\) is in \(F_1 \cap \ldots \cap F_i\), it can be redirected to the level \(j + 1\). Implementing this optimization gives automaton \(C_6\).

Changing the degeneralization order to \(\bullet\), then \(\odot\), and
Table 3: Statistics about generated automata and Spin’s run on model bakery.7.pm and formula $GFa \land GFB$ where $a$ and $b$ never occurs in the model. The corresponding automata are shown in Fig. 5.

<table>
<thead>
<tr>
<th>automaton size</th>
<th>statistics from Spin’s execution</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>states</td>
</tr>
<tr>
<td>$C_1$ Spin</td>
<td>3</td>
</tr>
<tr>
<td>$C_2$ LTL2BA &amp; LTL3BA</td>
<td>3</td>
</tr>
<tr>
<td>$C_3$ MoDeLLa</td>
<td>4</td>
</tr>
<tr>
<td>$C_4$ LTL3BA (det)</td>
<td>3</td>
</tr>
<tr>
<td>$C_5$ Spot &amp; Spot (det)</td>
<td>3</td>
</tr>
<tr>
<td>$C_6$ Spot (no jump)</td>
<td>3</td>
</tr>
</tbody>
</table>

putting the initial states on the first level would give automaton $C_4$.

Often (but not in this example), jumping levels is a way to effectively avoid creating useless copies of some states. Another side effect of this optimization is that some accepting cycles may be shorter than $m+1$: the change effectively keeps the automaton as close to the accepting level as possible. If we are looking for counterexamples, $C_5$ appear better than $C_6$ because its accepting cycles are shorter on the average.

We recall that the initial state of a degeneralized automaton can be put on any level. For example, Giannakopoulou and Lerda [13] noticed that by changing the initial level, they could sometimes save some states, so they try to use both the first and the last level and keep the smallest automaton. In our example, $C_4$ and $C_5$ differ only by the choice of the initial level (and degeneralization order but this is negligible as $a$ and $b$ are symmetric in our problem), there is no size difference, and yet it makes a huge difference in the running time of Spin, as discussed in the previous section.

Another translation difference evidently comes from the difference between the generalized automata obtained from the LTL formula. In our case $C_4$, $C_5$, and $C_6$ were obtained from $G_1$ while $C_1$ and $C_2$ were obtained from $G_2$. (The difference with Spin ($C_1$) is that it does no level jumping from the accepting state.) The difference between $G_1$ and $G_2$ is caused by choices made during the translation to favor deterministic states in the case of $G_1$. In our example of Table 3, this improved determinism makes no difference since $a$ and $b$ are never true in the model.

4.5 Automata for $\neg(GFa \rightarrow GFB)$

We now focus on another concrete case: $\neg(GFa \rightarrow GFB)$ on mutex protocols. The formula without negation describes that if some process visits infinitely often the critical section, it infinitely often leaves it—this property holds in model Peterson.4.pm and therefore Spin has to build a whole product to find that it contains no accepting cycle.

Table 1 shows a series of experiments of verification of the model Peterson.4.pm against this formula, using different tools to obtain a Büchi automaton.

In this case, each tool produces a different automaton, as shown in the first part of Figure 4. Note again that automata $D_2$ and $D_4$ cannot be distinguished only by determinism and size metrics (see Table 1). They differ only in the target of the outgoing edge of $s_0$, yet we observe a significant difference in Spin’s behaviors.

We actually use 12 different automata for this formula. The first seven of the table are generated by the considered tools. The other are handwritten by modifying the previous automata to explore which aspects of the automata make a significant difference in Spin’s behavior as described further.

Another translation difference evidently comes from the difference between the generalized automata obtained from the LTL formula. In our case $C_4$, $C_5$, and $C_6$ were obtained from $G_1$ while $C_1$ and $C_2$ were obtained from $G_2$. (The difference with Spin ($C_1$) is that it does no level jumping from the accepting state.) The difference between $G_1$ and $G_2$ is caused by choices made during the translation to favor deterministic states in the case of $G_1$. In our example of Table 3, this improved determinism makes no difference since $a$ and $b$ are never true in the model.

Based on Table 4 we can group these automata in three categories, listed from the best to the worst with respect to Spin’s performance. Before we discuss these categories, it is important to notice that in a model where $a$ means the process is in the critical section and $b$ means the process leaves the critical section, we can expect most of the state space to be labelled by $ab$.

$D_6$, $D_7$, $D_8$, $D_0$: Automata with the smallest number of transitions. Note that the no jump version ($D_7$) and the one with a non-deterministic SCC ($D_8$) both yields a few more states and transitions in the product, but the difference is not significant. The key property of these
Figure 7: Automata for the formula $\neg (GFa \rightarrow GFb)$.

Table 4: Statistics about generated automata and Spin’s run on the empty product between model peter-son.4.pm and formula $\neg (GFa \rightarrow GFb)$. The corresponding automata are shown in Fig. 7.

<table>
<thead>
<tr>
<th>Automaton</th>
<th>States</th>
<th>Edges</th>
<th>Transitions</th>
<th>Stored States</th>
<th>Visited Transitions</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D_1$ Spin</td>
<td>3</td>
<td>2</td>
<td>6</td>
<td>12</td>
<td>1577446</td>
<td>7680k</td>
</tr>
<tr>
<td>$D_2$ LTL2BA</td>
<td>3</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>1577440</td>
<td>7684k</td>
</tr>
<tr>
<td>$D_3$ MoDeLLa</td>
<td>5</td>
<td>2</td>
<td>8</td>
<td>18</td>
<td>1580893</td>
<td>7670k</td>
</tr>
<tr>
<td>$D_4$ LTL3BA</td>
<td>3</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>2299250</td>
<td>15583k</td>
</tr>
<tr>
<td>$D_5$ LTL3BA (det)</td>
<td>4</td>
<td>1</td>
<td>7</td>
<td>14</td>
<td>2297625</td>
<td>15561k</td>
</tr>
<tr>
<td>$D_6$ Spot</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>9</td>
<td>848641</td>
<td>2853k</td>
</tr>
<tr>
<td>$D_7$ Spot (no jump)</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>9</td>
<td>852094</td>
<td>2863k</td>
</tr>
<tr>
<td>$D_8$</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>10</td>
<td>848641</td>
<td>2853k</td>
</tr>
<tr>
<td>$D_9$</td>
<td>3</td>
<td>3</td>
<td>6</td>
<td>11</td>
<td>852094</td>
<td>2878k</td>
</tr>
<tr>
<td>$D_{10}$</td>
<td>3</td>
<td>1</td>
<td>7</td>
<td>10</td>
<td>1575844</td>
<td>7658k</td>
</tr>
<tr>
<td>$D_{11}$</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>10</td>
<td>1577440</td>
<td>7657k</td>
</tr>
<tr>
<td>$D_{12}$</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>10</td>
<td>2297625</td>
<td>15561k</td>
</tr>
</tbody>
</table>
automata is that they can leave state $s_0$ only by reading $\bar{a}b$, whereas other automata are more permissive.

$D_1, D_2, D_3, D_{10}, D_{11}$ All these automata exhibit more nondeterminism on state $s_0$ and will enter the accepting state even after reading $\bar{a}b$. However when this happens, they do not reach the accepting state before $\bar{a}b$ is read, so this limits the number of red DFS.

$D_4, D_5, D_{12}$ These automata go from $s_0$ to the accepting state $s_1$ each time they read $\bar{a}b$. This both makes the product unnecessarily large, but it also force many calls to the red DFS every time a product state with property automaton state $s_1$ is backtracked. The nondeterminism in accepting SCC of $D_4$ causes it to visits only slightly more states than the other two automata.

A comparison of automata $D_6$ and $D_{11}$ and their impact to Spin’s performance show that the hypothesis of Section 13 cannot be used alone to select the best automaton. Indeed, $D_6$ outperforms $D_{11}$ even if the distance from the initial to the accepting state is shorter in $D_6$. Here the more restrictive label of transition $(s_0, s_1)$ in $D_6$ plays an important role as well.

To sum up, if we suppose that there is no accepting cycle in the product, the automaton should

1. keep accepting states as far as possible from the initial state (compare $D_{11}$ to $D_{12}$) and
2. use more restrictive labels (compare $D_6$ to $D_{12}$)

in order to make the accepting states as hard to reach as possible. Moreover, make use of more restrictive labels can also help to reduce the product.

An appropriate metric taking these two factors into account, as well as an LTL-to-BA translation reflecting these hypotheses, are topics for our future research.

5. CONCLUSION

LTL-to-BA translators have several degrees of freedom when producing automata. Some of these choices have effects on the product with a system to be verified and also to the emptiness check of the product. However, these effects are difficult to predict. So far, most authors of LTL-to-BA translation tools have measured the performance of their translators by looking at the size of the output, sometimes also by translation tools have measured the performance of their LTL-to-BA translators should tune their output according to the purpose of the BA: a BA used for bug finding need not to be the same as a BA used to prove correctness. Here we focused on the Nested DFS implementation of Spin, but many other emptiness checks exist. For instance, some emptiness checks based on the enumeration of SCCs are insensible to the location of accepting states on a cycle, so our suggestions should not be generalized blindly.

Another point that can be influenced by the property automaton is the size of the counterexample generated. The question of finding an automaton that is optimal from this point of view is left open by Gastin et al. [11].

References


