Discuss Paper

Paper# 3504: Symbolic LTLf Synthesis

Abstract LTLf synthesis is the process of finding a strategy that satisfies a linear temporal specification over finite traces. An existing solution to this problem relies on a reduction to a DFA game. In this paper, we propose a symbolic framework for LTLf synthesis based on this technique, by performing the computation over a representation of the DFA as a boolean formula rather than as an explicit graph. This approach enables strategy generation by utilizing the mechanism of boolean synthesis. We implement this symbolic synthesis method in a tool called Syft, and demonstrate by experiments on scalable benchmarks that the symbolic approach scales better than the explicit one.

Paper Type Full Paper

Keywords [Knowledge Representation, Reasoning, and Logic] Automated Reasoning and Theorem Proving, [Knowledge Representation, Reasoning, and Logic] Game Theory, [Knowledge Representation, Reasoning, and Logic] Logics for Knowledge Representation

Average Rating 7.10

Submission File

Assigned Area Chairs Sheila McIlraith (#30965) (University of Toronto) assigned by Carles Sierra

Assigned Senior PC M... Alessio Lomuscio (#27440) (Imperial College London) assigned by Carles Sierra

Assigned PC Members Marco Montali (#20899) (Free University of Bozen-Bolzano) assigned by Carles Sierra
Sasha Rubin (#21284) (University of Naples, Federico II) assigned by Carles Sierra
Julian Gutierrez (#23983) (University of Oxford) assigned by Carles Sierra

Reviews

★★★★★★★★★☆☆

Review from PC Member Marco Montali (#20899) (Created: 2017-03-26 09:40:42, Last modified: 1 week, 6 days ago)

Originality

★★★★★★★★☆☆

Technical Quality

★★★★★★☆☆☆☆

Significance

★★★★★★★★★☆

Relevance

★★★★★★★★★★

Quality of writing

★★★★★★★★☆☆

Overall Score

★★★★★★★★☆☆

Confidence on your assessment

★★★★★★★★★☆

Comments to Authors.

This is a solid contribution in the very interesting area of temporal logics over finite traces and their corresponding synthesis problem. In particular, the paper builds on recent foundational results on synthesis for LTL over finite traces using DFA games, and translates such results into actual software prototypes that are experimentally evaluated on different benchmarks. The most interesting result is about the development of a symbolic technique that solves the synthesis problem without explicitly constructing the DFA, but resorting instead to BDDs. The experimental result shows the main difficult points in tackling the synthesis problem from the practical point of view.

The contribution is interesting for a broad range of researchers in AI. Although not explicitly recalled in the paper, the proposal has the potential of impacting the area of declarative business process management, where LTLf is used to describe process constraints, and where an overall declarative process model is captured by the conjunction of all LTLf formulae for its constraints. This is inline with the experimental evaluation proposed in the paper, which insists on the importance of scalability w.r.t. conjunctions of formulae. For a reference to this area, see:

- Maja Pesic, Helen Schonenberg, Wil M. P. van der Aalst: DECLARE: Full Support for Loosely-Structured Processes. EDOC 2007: 287-300

- Giuseppe De Giacomo, Riccardo De Masellis, Marco Grasso, Fabrizio Maria Maggi, Marco Montali: Monitoring Business Metaconstraints Based on LTL and LDL for Finite Traces. BPM 2014: 1-17

There are two technical aspect that would require, in my opinion, more attention.

1) I would like to see a more explicit formal result in the paper: namely the fact that the symbolic approach, and the corresponding boolean synthesis problem,

correctly reconstruct the original LTLf synthesis problem. This can be seen from the technical treatment, but still having an explicit theorem would be preferable.

2) In Section 3.2, the authors rely on a benchmark from the literature. However, that benchmark relies on LTL, and not LTLf. While it is true that, due to their common syntax, the benchmark is readily applicable to the LTLf case, the notion of realizability is completely different in the two settings. It would be therefore important to understand whether those benchmarks are also more or less "semantically preserved" while moving from one setting to the other, or whether instead working over finite traces change them completely.

Some minor technical comments follow.

Intro

Our synthesis framework employs ... -> this sentence is quite convoluted

Section 2

i.e. LTLf -> i.e., LTLf

It would be beneficial to briefly mention that, although the syntax of LTLf and LTL are the same, the notion of weak next is peculiar to the finite-trace setting.

Definition 1. I would strongly suggest to add an intuitive explanation for the definition. It is in fact quite counterintuitive to see the synthesis problem as something that starts from an infinite sequence of propositional interpretations, instead of something that explicitly tackles a finite prefix and shows the next move to be done.

Please intuitively explain why the DFA for DFA games has alphabet 2^{\mathcal{X} \cup \mathcal{Y}}, and not simply \mathcal{X} \cup \mathcal{Y}. Again, nothing technical wrong here, just need for intuition for the average reader.

Rebuttal #4628 (Created: 1 week, 1 day ago, Last modified: 1 week, 1 day ago)

Rebuttal

Formal statements of correctness and complexity of the symbolic synthesis algorithm are indeed missing. We will add those to the revised version (adding a page to the paper if necessary). Regarding the LTL benchmarks, the semantics of LTL formulas is not, in general preserved, when moving to the finite-trace setting. While individual operators retain more or less their semantics, nesting of temporal operators can produce different meaning. For example, GFp and FGp both mean that p holds at the final point of the trace. In terms of intuitive explanations, in Definition 1, LTLf synthesis can be seen as computing a strategy for a game against the environment, which

is played until the system can reach a winning condition. Therefore, there is no a priori limit on the length of the environmental trace. Also, the alphabet of the DFA represents an interpretation of the propositional variables, which can be seen as a description of the state of the world. Each player assigns a truth value to the variables that they control. We will make these two intuitions clearer.

Assessment from Sasha Rubin (#7291) (Created: 1 day, 15 hours ago, Last modified: 1 day, 15 hours ago)

Review assessment. Only visible to Area Chairs.

★ ★ ★ ★ ★ ★ ☆ ☆ ☆ ☆

[Optional] Assessment comments. Only visible to Area Chairs.

★ ★ ★ ★ ★ ★ ☆ ☆ ☆ ☆

Review from PC Member Sasha Rubin (#21284) (Created: 2017-04-02 10:31:01, Last modified: 6 days, 1 hour ago)

Originality

★ ★ ★ ★ ★ ★ ★ ★ ☆ ☆

Technical Quality

★ ★ ★ ★ ★ ★ ★ ☆ ☆ ☆

Significance

★ ★ ★ ★ ★ ★ ★ ★ ☆ ☆

Relevance

★ ★ ★ ★ ★ ★ ★ ★ ☆ ☆

Quality of writing

★ ★ ★ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Overall Score

★ ★ ★ ★ ★ ★ ☆ ☆ ☆ ☆

Confidence on your assessment

★ ★ ★ ★ ★ ★ ☆ ☆ ☆ ☆

Comments to Authors.

SUMMARY
This paper is about synthesising finite-state strategies that realise specifications written in LTL_f, i.e., LTL over finite traces.

LTL_f has recently come to the fore as an appropriate alternative to LTL (which is over infinite traces), especially for AI applications.

The main claim in these recent papers is that algorithms for LTL_f are much easier to implement (and understand) than for the LTL case. Indeed, the algorithm proceeds as follows:
- convert LTL_f formula phi into a DFA that accepts the models of phi
- solve the reachability game over the DFA using a fixpoint computation.

In this paper, the authors implement, for the first time, explicit and symbolic versions of this algorithm.

The paper compares the two approaches and finds that the symbolic version scales better. The paper does not compare the symbolic approach for LTL_f synthesis to any existing tool for LTL synthesis.

JUSTIFICATION FOR SCORES

Originality

This seems to be the first implementation of realisability and synthesis solvers for LTL_f. The implementation uses standard ideas and existing libraries and tools.

Technical Quality
The authors compare the explicit and symbolic approaches to LTL_f synthesis. However, the authors do not compare their approach to LTL synthesis tools. Thus, it does not address the question of whether LTL_f synthesis can be done faster or better than LTL synthesis.

Significance
The paper addresses an important problem, in so far as it helps to justify claims that LTL_f synthesis is amenable to implementation.

Relevance
The paper will be of interest to the verification/synthesis community and the planning community at IJCAI.

Quality of writing
There are a number of diagrams that help one understand what is going on.

However, the paper is not very well organised.
1. There is no description of the symbolic approach --- one has to read the whole paper to get an outline of the approach.
2. Some parts are very short on details.

- the start of sections simply "jump in" to the details without giving an idea what is about to happen, or putting that section in context.
- More than once it says "for more details see [...]". In principle this is fine, but we should be told what part of [...] is relevant for the current paper.
- It hardly describes the data structures used (e.g., there is only a very vague description of a Shared Multi-terminal BDD (ShMTBDD)).
- Some of the steps are only sketched via example, e.g., the splitting of MTBDD into BDDs. If this is standard then a citation could be given. If this is new then more details should be discussed.

3. Some parts seem to contain extraneous material:
- I do not understand the point of having the section "From ShMTBDD to Explicit DFA."
- Although section 3.2 on the reasons for choosing MONA over SPOT are interesting and an important part of the research process, perhaps it could have been summarised? Otherwise, what is the point of having all this detail? How does this section serve the message of the paper?

Also:

pg 2 col 2
Strategy g for the controller is a winning strategy, if the initial state s 0 is a wining state.

This is not a correct definition of winning strategy. Just because s_0 is a winning state, doesn't mean that g (which may be defined arbitrarily) is a winning strategy.

Definition 3
This definition should be called something like "winning deterministic finite transducer".

In the preliminaries you should probably state the theorem that solving the DFA game over DFA D_phi (where D_phi is a DFA for phi) is equivalent to solving the realisability problem for phi.

After Definition 4
"For more details on boolean synthesis we refer to [Fried et al., 2016]" This sentence is not useful. Tell us what other details we might find there to be useful for reading the present paper.

pg 65, col 1:
The description of delta' is confusing. Why is the range S? Why is the base of the logarithm z?

Comments after Response

If the paper is accepted I strongly recommend that the authors add a sketch of

correctness (and asymptotic complexity), as well as a comparison with state of the art LTL synthesis tools.

Regarding the latter, I suggest considering the following translation from LTL_f synthesis to LTL synthesis, based on the notation from [Theorem 1, De Giacomo and Vardi, 2013]: add a new atom "tail" controlled by the environment, and translate an LTL_f formula \phi into the LTL formula "(tail \land tail \until \always \neg tail) \limp t(\phi)".

Moreover, the authors could also consider comparing their tool to tools for universality of LTL_f formulas (i.e., is it the case that every finite string satisfies the given formula). Indeed, universality is a special case of realisability (i.e., when the agent does not control any variables).

Rebuttal #4640 (Created: 1 week, 1 day ago, Last modified: 1 week, 1 day ago)

Rebuttal

A comparison with LTL tools would be interesting. Currently, the reduction from LTLf to LTL described in Section 3.1 preserves only satisfiability, but we will look for a reduction preserving realizability and report on the results in the final draft. We will also give an overall description of the symbolic approach, as well as theorems stating the correctness and complexity of the algorithm. Regarding the material on the explicit method, we note that using symbolic methods is a heuristic, which doesn't change the complexity of LTLf synthesis. Thus each method should be evaluated for a fair comparison. Thank you for pointing out the errors in the definition of the winning strategy and delta'. The definition of g should be: "A strategy g is a winning strategy if for every infinite sequence \lambda etc". In the description of delta', the number of new variables should be "\lceil \log_2|S| \rceil". Lastly, we will clarify what the relevant details are for each citation. In particular, [Fried, et al., 2016] presents a more detailed description of boolean synthesis and algorithms for the problem.

★★★★★★★★☆☆☆

Review from PC Member Julian Gutierrez (#23983) (Created: 2017-04-04 13:50:50, Last modified: 3 days, 21 hours ago)

Originality

★★★★★★★★☆☆☆

Technical Quality

★★★★★★★★☆☆☆

Significance

★★★★★★★★☆☆☆

Relevance

★★★★★★★★★☆☆

Quality of writing

★★★★★★★★★☆☆

Overall Score

★★★★★★★★☆☆☆

Confidence on your assessment

★★★★★★★★★☆☆

Comments to Authors.

The paper studies the synthesis problem for LTL on finite traces and present some experimental results. This is a borderline paper. There is nothing wrong with it, but nothing really good about it either, so it calls for the question as to whether it should appear in IJCAI or as a tool paper in another venue instead.

On the positive side, the paper presents a working implementation, which in many cases performs better than explicit constructions. The fact that a symbolic implementation of a DFA is given also has some merit. The paper also draws a few interesting conclusions. On the negative side, the results are somewhat expected. Symbolic implementation usually outperform implicit approaches. Moreover, the techniques seem to be quite standard (use of BDDs, etc.), modulo minor differences with well known literature about symbolic implementations. Finally, and what I find most critical, is the fact that the main contribution of the paper is claimed to be the synthesis part, once a symbolic DFA has been obtained from a given temporal logic formula. However, this second step is not the one driving the complexity of the overall synthesis problem. As seen by the results presented in the paper, the bottleneck is in the translation from temporal logic specifications to a symbolic DFA. However, this part is mostly done by MONA, and the additional contribution of the paper to this part of solving the problem does not improve the performance of solving the overall synthesis problem sufficiently well. In fact, the real problem is in that translation, from temporal logic formulas to DFA, whether explicit or symbolic, rather then the solution of the synthesis problem once such an explicit or symbolic representation has been obtained.

Minor comment: I would not generally argue nowadays that a tool doing symbolic verification is interesting because it outperforms one that uses explicit representations. This is expected when moving from explicit to symbolic representations. Contrarily, you should be worried if explicit representations generally scale better than your symbolic representations and associated verification procedures.

Rebuttal #4649 (Created: 1 week, 1 day ago, Last modified: 1 week, 1 day ago)

Rebuttal

We agree that DFA construction is the bottleneck rather than synthesizing a winning strategy. Pointing this fact via detailed evaluation is one contribution of the paper. We also mentioned in the paper that constructing DFA on-the-fly is our future research topic.

Assessment from Sasha Rubin (#7291) (Created: 1 day, 15 hours ago, Last modified: 1 day, 15 hours ago)

Review assessment. Only visible to Area Chairs.

★ ★ ★ ★ ★ ★ ★ ☆ ☆ ☆

[Optional] Assessment comments. Only visible to Area Chairs.

★ ★ ★ ★ ★ ★ ★ ☆ ☆ ☆

Review from Senior PC Member Alessio Lomuscio (#27440)

(Created: 2017-04-06 11:20:17, Last modified: 2 days ago)

Originality

★ ★ ★ ★ ★ ★ ☆ ☆ ☆ ☆

Technical Quality

★ ★ ★ ★ ★ ★ ☆ ☆ ☆ ☆

Significance

★ ★ ★ ★ ★ ★ ☆ ☆ ☆ ☆

Relevance

★ ★ ★ ★ ★ ★ ★ ☆ ☆ ☆

Quality of writing

★ ★ ★ ★ ★ ★ ☆ ☆ ☆ ☆

Overall Score

★ ★ ★ ★ ★ ★ ★ ☆ ☆ ☆

Confidence on your assessment

★ ★ ★ ★ ★ ★ ☆ ☆ ☆ ☆

Comments to Authors.

The submission develops a symbolic approach to synthesizing behaviors against linear temporal specifications under the assumption of finite traces.

The work primarily consists on the technical method to solve the problem and not on the possible applications in an AI context. Nonetheless the paper clarifies and gives references to the relevance of the problem in AI, eg in planning. I find this convincing.

The method improves on the current state-of-the-art by providing a symbolic method. This is evaluated experimentally in an implementation, whose details were not released, that appears to show improvements on the previous solution in the literature. The paper presents both the underlying algorithms based on symbolic structures as well as some details of the implementation.

The paper is at times difficult to follow possibly because it relies on sophisticated automata techniques. Other than this it appears well structured and well presented.

I have the following comments. Perhaps the authors could comment on some of these points during the feedback phase:

* The algorithms presented are quite sophisticated. No proof of soundness is given for the algorithms. Is it obvious that the algorithms presented on symbolic structures solve the original problem? Would it not be preferable for these algorithms to be presented algorithmically rather than in plain text?

* Is the complexity of solving the problem symbolically the same as the original problem or could the symbolic encoding raise the worst-case complexity?

* Given that the bottleneck of the algorithm is the construction of the DFA. Would it make sense to construct symbolic encodings of this on the fly? This is standard practice in several areas and it seems puzzling to see that the implementation first builds the entire DFA and then constructs its symbolic encoding. This limits the significance of the contribution.

Confidential Comments (Not visible to the authors)

This was the best paper in my batch. Other PCs expressed the same view. In case some accepted papers are not presented other than as posters, we believe this should be presented orally.

Metareview

The paper attracted positive reviews from experts in the area. There was agreement that the limitations of the paper included a proof of correctness for the symbolic part and a more in-depth comparison symbolic LTL synthesis tools. Many reviewers commented on the lack of on-the-fly construction of the DFA. The authors are aware of this and mention this in the paper as further work.

Overall, even in view of the limitations above, it was felt the paper was significant and relevant to the IJCAI community.

Rebuttal #4652 (Created: 1 week, 1 day ago, Last modified: 1 week, 1 day ago)

Rebuttal

We will clarify the soundness and completeness of the algorithms in the final draft. Furthermore, the algorithmic details will also be shown (adding an additional page if needed). The symbolic encoding does not raise the worst-case complexity, which is doubly exponential and therefore dominates everything else. Constructing symbolic DFA on the fly is indeed one of our future works.

Assessment from Sasha Rubin (#7291) (Created: 1 day, 15 hours ago, Last modified: 1 day, 15 hours ago)

Review assessment. Only visible to Area Chairs.

★ ★ ★ ★ ★ ★ ★ ★ ☆ ☆

[Optional] Assessment comments. Only visible to Area Chairs.

Comments

Alessio Lomuscio (#27440) wrote 2 days ago:

Dear All

We are all positive on this paper and we have agreement on all the points. I find their answer convincing. I will write a metareview summarising our view and suggesting accept.

Julian, even considering the limitations discussed, I think this was also the strongest submission in my batch.

Thanks.

-A

Julian Gutierrez (#23983) wrote 3 days, 21 hours ago:

Dear everyone,

I think Sasha gives a good "executive summary" and short evaluation of the paper: thanks!

Surprisingly, this was the best paper I got -- the one with a higher score. I think the paper will be above the acceptance threshold for IJCAI this year, and therefore should be accepted. I thinks the paper is not great, but good enough. Wrt the authors response, I think it's honest and reasonable. In the case of the response to my main concern, they essentially agree, and honestly state that the improvement, to make the paper stronger,

is future work and not something they can manage to do for the final version of this paper. Anyway, I think the paper can be accepted.

Best,

Julian.

PS: currently on holiday, thus unable to discuss much further.

Sasha Rubin (#21284) wrote 6 days, 1 hour ago:

Dear Alessio et al.,

I think if the authors implement what they say they will (i.e., sketch proof of correctness, complexity of construction, comparison with symbolic LTL synthesis tools) then this paper, while light, is a reasonable contribution and probably worth publishing at IJCAI.

If the authors had also implemented an on-the-fly construction of the DFA, then this paper would have been a solid contribution (however, the authors make clear that this is left for future work).

Sasha

Alessio Lomuscio (#27440) wrote 6 days, 17 hours ago:

Dear All

Can we discuss this a little bit? I see we have all raised similar points. The conclusion I draw from all the reviews and the responses is that while this is far from a best paper winning, there is value in the paper. The topic is interesting and the method seems sound. The lack of on-the-fly construction and lack of details on the symbolic vs explicit step (perhaps inevitable in the page constraints) make evaluate this as an accept but just so.

What are your thoughts on all this?

Thanks.

-A (PS: Travelling on holiday with the family - please bear with me if I cannot immediately reply - thanks).

Alessio Lomuscio (#27440) wrote 1 week, 6 days ago:

Dear Julian

Can you please upload your review by today?

Many thanks.

Best

-A

Alessio Lomuscio (#27440) wrote 2 weeks ago:

Dear Julian and Marco

Just a courtesy reminder the deadline for all reviews is today.

Best

-A