Reducing the Size of Distinguishing Hennessy-Milner Formulae

Peter Heijstek[p.j.heijstek@student.tue.nl] and Tim A.C. Willemse[0000−0003−3049−7962]

Eindhoven University of Technology, Eindhoven, The Netherlands

Abstract. Two Labelled Transitions Systems (LTS) that are not bisimilar can be distinguished by a Hennessy-Milner formula. Often it is the case that these distinguishing formulae are hard to interpret due to their size. In this article an attempt is made to shorten these distinguishing formulae by extending the Hennessy-Milner logic with operators such as 'Invariantly' and 'Reachable'. To this end, an algorithm is introduced that can generate disinguishing formulae in the extended Hennessy-Milner Logic. A correctness proof and runtime complexity analysis are provided.

Keywords: Bisimulation · Hennessy-Milner Logic · Distinguishing formulae.

1 Introduction

2 Preliminaries

2.1 Labelled Transition Systems

A Labelled Transition System, or LTS for short, is defined as a tuple $(S, Act, \rightarrow)$ where S is a set of states, Act is a finite set of actions and $\rightarrow \subseteq S \times Act \times S$. $(s, a, t) \in \rightarrow$ is also written as $s \xrightarrow{a} t$.

Note that this definition does not prohibit multiple transitions from a single state with the same action, hence these systems can be non-deterministic.

2.2 Hennessy-Milner Logic

The syntax of the Hennessy-Milner Logic is given by:

$$\Phi = tt \mid \neg\Phi \mid \Phi_1 \wedge \Phi_2 \mid \langle Act\rangle\Phi$$

The set of all Hennessy-Milner Logic formulas is defined as F. Given an LTS $L = (S, Act, \rightarrow)$, the semantics of the HML formulas can be defined as as function $[\![]\!]_L : F \rightarrow 2^S$.

The definition of the function is:

$$[\![tt]\!]_L = S$$

$$[\![\Phi_1 \wedge \Phi_2]\!]_L = [\![\Phi_1]\!]_L \cup [\![\Phi_2]\!]_L$$

$$[\![\neg \Phi]\!]_L = S - [\![\Phi]\!]_L$$

$$[\![\langle a \rangle \Phi]\!]_L = \{s \in S : \exists t \in [\![\Phi]\!]_L : s \xrightarrow{a} t\}$$

3 Related Work

Bisimulation partition algorithm Cleavelands algorithm (1990)

Reference Jan proves that finding a minimal-size distinguishing formula is NP-hard. The size is in this case the total number of observations in the formula. However, different definitions of size allow for a polynomial-time algorithm for generating witnesses. Specifically, formulas with the smallest nesting depth of observations and formulas with the smallest negation depth can be found in polynomial time.

HLMU

Coalgebraic approach Konig et al 2020

4 Extension to the Hennessy-Milner Logic

We extend the HML with the operators Inv and $Reach$. Informally, $Inv(\Phi)$ holds in a state if Φ holds for all states reachable from that state (including itself). $Reach(\Phi)$ holds in all states that can reach a state where Φ holds. The syntax becomes

$$\Phi = tt \mid \neg \Phi \mid \Phi_1 \wedge \Phi_2 \mid \langle Act \rangle \Phi \mid Inv(\Phi) \mid Reach(\Phi)$$

To properly define the semantics, the following functions, with LTS $L = (S, Act, \rightarrow)$ as context, are introduced:

$$F_L(X) = \{s \in X \mid \forall s \xrightarrow{a} s' : s' \in X\}$$

$$G_L(X) = \{s \in S \mid \exists s \xrightarrow{a} s' : s' \in X\}$$

$F_L(X)$ and $G_L(X)$ are monotonic, hence there exists a greatest fixpoint and least fixpoint for these functions.

The semantics for these operators, given an LTS $L = (S, Act, \rightarrow)$, is

$$[\![Inv(\Phi)]\!]_L = vX.F_L(X) \cap [\![\Phi]\!]_L$$

$$[\![Reach(\Phi)]\!]_L = \mu X.G_L(X) \cup [\![\Phi]\!]_L$$

Note that these operators are each others dual: $Inv(\Phi) = \neg Reach(\neg \Phi)$.

5 Generating Distinguishing formulae in the Extended Hennessy-Milner Logic

6 Reflection

7 Conclusion

Acknowledgments. A bold run-in heading in small font size at the end of the paper is used for general acknowledgments, for example: This study was funded by X (grant number Y).

Disclosure of Interests. It is now necessary to declare any competing interests or to specifically state that the authors have no competing interests. Please place the statement with a bold run-in heading in small font size beneath the (optional) acknowledgments[1], for example: The authors have no competing interests to declare that are relevant to the content of this article. Or: Author A has received research grants from Company W. Author B has received a speaker honorarium from Company X and owns stock in Company Y. Author C is a member of committee Z.

References

1. Author, F.: Article title. Journal **2**(5), 99–110 (2016)
2. Author, F., Author, S.: Title of a proceedings paper. In: Editor, F., Editor, S. (eds.) CONFERENCE 2016, LNCS, vol. 9999, pp. 1–13. Springer, Heidelberg (2016). https://doi.org/10.10007/1234567890
3. Author, F., Author, S., Author, T.: Book title. 2nd edn. Publisher, Location (1999)
4. Author, A.-B.: Contribution title. In: 9th International Proceedings on Proceedings, pp. 1–2. Publisher, Location (2010)
5. LNCS Homepage, http://www.springer.com/lncs, last accessed 2023/10/25

[1] If EquinOCS, our proceedings submission system, is used, then the disclaimer can be provided directly in the system.