On Construction of Safety Signal Automata for $MITL[\mathcal{U}, \mathcal{S}]$ Using Temporal Projections

Dileep Raghunath Kini$^1$, Shankara Narayanan Krishna$^1$, and Paritosh K. Pandya$^2$

$^1$ Department of Computer Science & Engineering, IIT Bombay, Mumbai, India 400 076
{dileep,krishnas}@cse.iitb.ac.in

$^2$ School of Technology and Computer Science, Tata Institute of Fundamental Research, Mumbai, India 400 005
pandya@tcs.tifr.res.in

Abstract. Construction of automata for Metric Temporal Logics has been an active but challenging area of research. We consider here the continuous time Metric temporal logic $MITL[\mathcal{U}_I, \mathcal{S}_I]$ as well as corresponding signal automata.

In previous works by Maler, Nickovic and Pnueli, the signal automaton synthesis has mainly addressed $MITL$ under an assumption of bounded variability. In this paper, we propose a novel technique of “Temporal Projections” that allows easy synthesis of safety signal automata for continuous time $MITL[\mathcal{U}_I, \mathcal{S}_I]$ over finite signals without assuming bounded variability. Using the same technique, we also give synthesis of safety signal automata for $MITL[\mathcal{U}_I, \mathcal{S}_I]$ with bounded future operators over infinite signals. For finite signals, the Temporal Projections allow us to syntactically transform an $MITL$ formula $\phi(Q)$ over a set of propositions $Q$ to a pure past time $MITL$ formula $\psi(P, Q)$ with extended set of propositions $(P, Q)$ which is language equivalent “modulo temporal projection”, i.e. $L(\phi) = L(\exists P. \Box \psi)$. A similar such transformation over infinite signals is also formulated for $MITL[\mathcal{U}_I, \mathcal{S}_I]$ restricted to Bounded Future formulae where the Until operators use only bounded (i.e.non-infinite) intervals. It is straightforward to construct safety-signal-automaton for the transformed formula. We give complexity bounds for the resulting automaton. Our temporal projections are inspired by the use of projections by D’Souza et al for eliminating past in $MTL$.

1 Introduction

Logic automaton connection has proved to be influential in finding practical model checking technique for the verification of programs, as well as in theoretical studies on expressiveness and decidability of logics. For example, the well known Vardi-Wolper technique gives synthesis of a Buchi automaton recognizing the language of an LTL formula. By using this automaton as a synchronous monitor, the LTL formula can be model checked. This approach has been applied to several other logics too. However, extending this approach to timed logics has been challenging.

A prominent (linear) timed logic is $MITL[\mathcal{U}_I, \mathcal{S}_I]$. Here the temporal modalities $\mathcal{U}_I$ and $\mathcal{S}_I$ are time constrained using a time interval $I$ with integer end-points. The logic can be interpreted over different forms of time. For example, $MITL[\mathcal{U}_I, \mathcal{S}_I]$ over timed words gives the so called pointwise $MTL$ where as $MITL[\mathcal{U}_I, \mathcal{S}_I]$ over timed state
sequences (also called signals), gives the continuous timed MTL (see \([1]\)). Moreover, the timed behaviour may be infinite (extending up to infinity in time) or finite. In this paper, we confine ourselves to continuous timed MTL. Logics MTL over finite and infinite behaviours are respectively denoted as MTL\(_{\text{fin}}\) and MTL\(_{\text{inf}}\).

The expressiveness and decidability properties of the temporal logic vary according to the nature of time assumed, permitted operators and permitted time intervals. Full MTL\([\mathcal{U}_I, \mathcal{S}_I]\) is undecidable for both finite and infinite behaviours. Alur, Feder and Henzinger \([2]\) proposed MITL\([\mathcal{U}_I, \mathcal{S}_I]\) as a restriction of MTL\([\mathcal{U}_I, \mathcal{S}_I]\) where singular (or punctual) intervals of the form \([l, l]\) are disallowed in formulae. Alur, Feder and Henzinger established the EXPSPACE satisfiability of MITL\([\mathcal{U}_I]\) by constructing a tableaux for the formula. However, the proposed construction for MITL\([\mathcal{U}_I, \Diamond_I, \mathcal{S}, \Diamond_I]\) is complex and not very practicable. Hence, several subsequent papers have addressed simpler techniques for the construction of signal automata for various fragments of continuous time MTL\([\mathcal{U}_I, \mathcal{S}_I]\) \([6,7,8]\). Thus, Maler et al \([6]\) exhibited synthesis of deterministic signal automata for the purely past time logic MITL\(_{\text{fin}}[\mathcal{S}, \Diamond_I]\). Extending this, Maler et al \([7]\) gave a construction of a deterministic signal automaton \(A(\phi, k)\) for a bounded future formula MITL\([\mathcal{U}_I, \mathcal{S}_I]\) and a variability index \(k\). The automaton accepts exactly those \(k\)-variable signals which satisfy the formula \(\phi\). A signal is called \(k\)-variable if it does not change more than \(k\) times in any unit interval.

In this paper, we consider a novel technique for the synthesis of MITL\([\mathcal{U}_I, \Diamond_I, \mathcal{S}, \Diamond_I]\) formula automaton without any restriction of bounded variability. Note that this logic MITL\([\mathcal{U}_I, \Diamond_I, \mathcal{S}, \Diamond_I]\) is equivalent to the more traditional MITL\([\mathcal{U}_I, \mathcal{S}_I]\). Our main results are as follows.

- For MITL\(_{\text{fin}}[\mathcal{U}_I, \Diamond_I, \mathcal{S}, \Diamond_I]\) formula (over finite signals) we construct a safety signal automaton which accepts a signal iff the signal satisfies the formula.
- For BMITL (over infinite signals) which consists only of formulae with bounded future, we construct a safety signal automaton which accepts a signal iff the signal satisfies the formula.

In both cases, the automaton construction uses a novel technique called temporal projections. A formula \(\Box \phi\) holds for a behaviour if it holds at every point in the behaviour. A formula \(\phi\) over a set of propositions \(Q\) is called “equivalent modulo projection” to a formula \(\psi\) over a set of propositions \(P \cup Q\) provided \(\phi \equiv \exists P \psi\). The composite operator \(\exists P \Box\) is named temporal projection.

For finite signals, the Temporal Projections allow us to syntactically transform an MITL\(_{\text{fin}}[\mathcal{U}_I, \Diamond_I, \mathcal{S}, \Diamond_I]\) formula \(\phi(Q)\) over a set of propositions \(Q\) to a pure past time MITL\(_{\text{fin}}[\mathcal{S}, \Diamond_I]\) formula \(\psi(P, Q)\) with extended set of propositions \((P, Q)\) which is language equivalent “modulo temporal projection”, i.e. \(L(\phi) = L(\exists P \Box \psi)\). Our temporal projections are inspired by the use of projections by D’Souza et al \([3]\) for eliminating past in MTL. They allow us to state future requirements in terms of past requirements by shifting the time point of reference. A similar such transformation over infinite signals is also formulated for BMITL where the future operators use only bounded (i.e.non-infinite) intervals. Thus, temporal projections allow us to reduce MITL\([\mathcal{U}_I, \Diamond_I, \mathcal{S}, \Diamond_I]\) formulas to a purely past time formula.

In this paper, we consider timed state sequences in their full generality. We also consider the full logic MITL without any restrictions. This must be contrasted with \([6,7]\).