On Verifying Timed Hyperproperties

Hsi-Ming Ho
University of Cambridge, UK
hsi-ming.ho@cl.cam.ac.uk

Ruoyu Zhou
University of Cambridge, UK
ruoyu.zhou@cl.cam.ac.uk

Timothy M. Jones
University of Cambridge, UK
timothy.jones@cl.cam.ac.uk

Abstract

We study the satisfiability and model-checking problems for timed hyperproperties specified with HyperMTL, a timed extension of HyperLTL. Depending on whether interleaving of events in different traces is allowed, two possible semantics can be defined for timed hyperproperties: synchronous and asynchronous. While the satisfiability problem can be decided similarly as for HyperLTL regardless of the choice of semantics, we show that the model-checking problem for HyperMTL, unless the specification is alternation-free, is undecidable even when very restricted timing constraints are allowed. On the positive side, we show that model checking HyperMTL with quantifier alternations is possible under certain conditions in the synchronous semantics, or when there is a fixed bound on the length of the time domain.

2012 ACM Subject Classification Theory of computation → Logic and verification

Keywords and phrases Timed Automata, Temporal Logics, Cybersecurity

Digital Object Identifier 10.4230/LIPIcs.TIME.2019.20

Related Version A full version of the paper is available at https://arxiv.org/pdf/1812.10005.

Funding This work was supported by the Engineering and Physical Sciences Research Council (EPSRC), through grant references EP/K026399/1 and EP/P020011/1.

1 Introduction

Background. One of the most popular specification formalisms for reactive systems is Linear Temporal Logic (LTL), first introduced into computer science by Pnueli [52] in the late 1970s. The success of LTL can be attributed to the fact that its satisfiability and model-checking problems are of lower complexity (PSPACE-complete, as compared with non-elementary for the equally expressive first-order logic of order) and it enjoys simple translations into automata and excellent tool support (e.g., [15,35]).

While LTL is adequate for describing features of individual execution traces, many security policies in practice are based on relations between two (or more) execution traces. A standard example of such properties is observational determinism [37,54,59]: for every pair of execution traces, if the low-security inputs agree in both execution traces, then the low-security outputs in both execution traces must agree as well. Such properties are called hyperproperties [17]: a model of the property is not a single execution trace but a set of execution traces. HyperLTL [16], obtained from LTL by adding trace quantifiers, has been proposed as a specification formalism to express hyperproperties. For example, operational determinism can be expressed as the HyperLTL formula:

$$\forall \pi_a \forall \pi_b \ G(I_a = I_b) \Rightarrow G(O_a = O_b).$$

HyperLTL inherits almost all the benefits of LTL; in particular, tools that support HyperLTL verification can be built by leveraging existing tools for LTL.
For many applications, however, in addition to the occurrences and orders of events, timing has to be accounted for as well. For example, one may want to verify that in every execution trace of the system, whenever a request \( \text{req} \) is issued, the corresponding acknowledgement \( \text{ack} \) is received within the next 5 time units. Timed automata [4] and timed logics [5,9,39] are introduced exactly for this purpose. In the context of security, timing anomalies caused by different high-security inputs is a realistic attack vector that can be exploited to obtain sensitive information; this kind of timing side-channel attacks also play significant roles in high-profile exploits like Meltdown [45] and Spectre [38]. In order to detect such undesired characteristics of systems, one needs to reason about timed hyperproperties.

\[ \text{Example 1 ([55])}. \] A piece of C code that selects between two variables \( x \) and \( y \) based on a secret selection bit \( b \) (i.e. the user gets the output – either \( x \) or \( y \) – but does not know which one was actually selected) may be written as follows:

```c
uint32_t select_u32(uint32_t b, uint32_t x, uint32_t y)
{
    return b ? x : y;
}
```

This straightforward implementation, however, may result in a timing side channel – depending on what compiler optimisations are applied, the execution time can depend on which of \( x \) and \( y \) is returned. In sensitive applications like cryptography libraries and embedded smart-card software, such code snippets are usually replaced by obfuscated, functional-equivalent versions, with the hope of eliminating the potential leakage of secret information. In this case, one such version is as follows:

```c
uint32_t ct_select_u32(uint32_t b, uint32_t x, uint32_t y)
{
    signed bit = 0 - b;
    return (x & bit) | (y & ~bit);
}
```

Nevertheless, such attempts of obfuscation can easily be wiped out by more agressive code optimisations. For instance, after compilation by clang 3.3 (-O2), the C code above results in the following assembly code, which contains a jump instruction and may still reveal the truth value of \( b \) via differences in execution times due to branch prediction. The issue can, however, be detected by an analysis based on suitable instruction-level timing models.

```assembly
ct_select_u32:
    mov 0x4(%esp),%al
    test %al,%al
    jne L
    lea 0xc(%esp),%eax
    mov (%eax),%eax
    ret
L:
    lea 0x8(%esp),%eax
    mov (%eax),%eax
    ret
```

Given the highly-sophisticated cache hierarchies, pipeline stalls, etc. in contemporary real machines, the timing side channel in the example above may be difficult to realise and exploit in an actual attack; but such issues may also manifest themselves at lower levels (e.g., RTL), as illustrated by the following example.

\[ \text{Example 2 ([44])}. \] An AND gate with two inputs \( A, B \) and an output \( C \) and respective delays \( T_A, T_B, \) and \( T_C \) can be modelled as the timed automaton with two clocks \( x, y \) in Figure 1 where \( x = T_A \) checks if the value of clock \( x \) is \( T_A \), \( y := 0 \) resets clock \( y \) to 0, etc.
Figure 1 A timed automaton modelling an AND gate with inputs $A$, $B$ and output $C$ with respective delays $T_A$, $T_B$, and $T_C$.

(suppose that $T_A < T_B$ and $T_B - T_A < T_C$). Intuitively, the truth values of $A$ and $B$ are obtained after $T_A$ and $T_B$ respectively, and the output $C = A \land B$ has a delay of $T_C$ from the point when its value is confirmed. Of course, once $A$ turned out to be 0 (i.e. $A^0$ has happened), the output $C$ must be 0 as well. But the time $C^0$ happens (assuming $C = 0$) also depends on the truth value of $A$. In other words, when $C = 0$, a low-security user (to whom $A^0$ and $A^1$ are non-observable), provided that he/she can measure time, can also infer the truth value of $A$ while he/she should not be able to. The pair of traces with $C = 0$ that reveals $A$ is depicted in Figure 2 and Figure 3. In this simple example, however, the timing side channel can be removed by adding $y := 0$ on the self-loop on the lower-right location.

Figure 2 A trace $\rho_1$ with $A = 1$, $B = 0$, and $C = 0$.

Figure 3 A trace $\rho_2$ with $A = 0$, $B = 0$, and $C = 0$.

Contributions. We propose HyperMTL, obtained by adding trace quantifiers to Metric Temporal Logic (MTL) [39], as a specification formalism for timed hyperproperties. We consider systems modelled as timed automata, and thus system behaviours are sequences of events that happen at different instants in time; this gives two possible pointwise semantics of HyperMTL: asynchronous and synchronous (this is in contrast to HyperLTL, for which a synchronous semantics is sufficient). We show that, as far as satisfiability is concerned, HyperMTL is similar to HyperLTL, i.e. satisfiability is decidable for fragments not containing $\forall \exists$, regardless of which semantics is assumed. However, in contrast with HyperLTL (whose model-checking problem is decidable), model checking HyperMTL is undecidable if there is at least one quantifier alternation in the specification, even when the timing constraints used in either the system or the specification are very restricted. Still, the alternation-free fragment of HyperMTL, which is arguably sufficient to capture many timed hyperproperties of practical interest, has a decidable model-checking problem. Finally, we identify several
subcases where HyperMTL model checking is decidable for larger fragments, such as when
the synchronous semantics is assumed, the model is untimed, and the specification belongs
to a certain subclass of one-clock timed automata, or when the time domain is bounded \(a \textit{ priori} \) by some \( N \in \mathbb{N} \).

\textbf{Related work.} Since the pioneering work of Clarkson and Schneider [17], there has been great
interest in specifying and verifying hyperproperties in the past few years. The framework based
on HyperLTL [16] is possibly the most popular for this purpose, thanks to its expressiveness,
flexibility, and relative ease of implementation. In addition to satisfiability [23,24] and model
checking [16,28], tools for monitoring HyperLTL also exist [3,25,26]. Notably, the complexity
of monitoring HyperLTL, as well as model checking HyperLTL on restricted (tree-shaped or
acyclic) Kripke structures, are studied in [12] and shown to be much lower than those of the
general satisfiability and model-checking problems. These results, however, do not apply in
the current timed setting – we will see in Section 4 that our main undecidability result holds
even with these structural restrictions on the system.

Our formulation of HyperMTL is very closely related to HyperSTL [47] originally proposed
in the context of quality assurance of cyber-physical systems. While [47] focusses on testing,
we are concerned with the decidability of verification problems. On the other hand, the
semantics of HyperSTL is defined over sets of continuous signals, i.e. state-based; as noted
in [47], however, the price to pay for the extra generality is that implementing a model checker
for HyperSTL is very difficult, especially for systems modelled in proprietary frameworks
(such as Simulink®). Practical reasoning of HyperMTL, by contrast, can be carried out easily
with existing highly optimised timed automata verification back ends, e.g., UPPAAL [43].1

Indeed, a prototype model checker based on UPPAAL for the synchronous semantics of
HyperMTL (with some restrictions) is reported in [32], although it does not consider the
decidability of verification problems. Another relevant work [30], also based on UPPAAL,
checks noninterference in systems modelled as timed automata (similar to Example 4; see
below). Their approach, however, is specifically tailored to noninterference and does not
generalise. Some similar (but different) notions of noninterference for timed automata have
been considered in [29,58].

It is also possible to extend hyperlogics in other quantitative dimensions orthogonal to time.
HyperPCTL [2] can express probabilistic hyperproperties, e.g., the probability distribution
of the low-security outputs are independent of the high-security inputs. In [27], specialised
algorithms are developed for verifying quantitative hyperproperties, e.g., there is a bound on
the number of traces with the same low-security inputs but different low-level outputs. The
current paper is complementary to these works.

\section{Timed hyperproperties}

\textbf{Timed words.} A \textit{timed word} (or a \textit{trace}) over a finite alphabet \( \Sigma \) is a finite sequence of
events \( (\sigma_1, \tau_1) \ldots (\sigma_n, \tau_n) \in (\Sigma \times \mathbb{R}_{\geq 0})^n \) with \( \tau_1 \ldots \tau_n \) an increasing sequence of non-negative
real numbers ("timestamps"), i.e. \( \tau_i < \tau_{i+1} \) for all \( i, 1 \leq i < n \).

1 For more detailed accounts of the state-based and event-based semantics for timed automata and logics,
see, e.g., [7,51].

2 To simplify the exposition, we focus on finite timed words in this paper (this assumption does not
make the verification problems easier in general; e.g., HyperLTL satisfiability remains undecidable). All
of our technical results carry over to the case of infinite timed words with some simple modifications.
For example, in Section 3, suitable subformulae can be added to rule out the runs that get stuck in
self-loops labelled with \( \{p^*\} \).
word $\rho = (\sigma_1, \tau_1) \ldots (\sigma_n, \tau_n)$, we write $t \in \rho$ iff $t = \tau_i$ for some $i$, $1 \leq i \leq n$. We denote by $T\Sigma^*$ the set of all timed words over $\Sigma$. A timed language (or a trace property) is a subset of $T\Sigma^*$.

Timed automata. Let $X$ be a finite set of clocks ($\mathbb{R}_{\geq 0}$-valued variables). A valuation $v$ for $X$ maps each clock $x \in X$ to a value in $\mathbb{R}_{\geq 0}$. The set $G(X)$ of clock constraints (guards) $g$ over $X$ is generated by $g := \top \mid g \land g \mid x \vartriangleleft c$ where $\vartriangleleft \in \{\leq, <, \geq, >\}$, $x \in X$, and $c \in \mathbb{N}_{\geq 0}$. The satisfaction of a guard $g$ by a valuation $v$ (written $v \models g$) is defined in the usual way. For $t \in \mathbb{R}_{\geq 0}$, we let $v + t$ be the valuation defined by $(v + t)(x) = v(x) + t$ for all $x \in X$. For $\lambda \subseteq X$, we let $v[\lambda \leftarrow 0]$ be the valuation defined by $(v[\lambda \leftarrow 0])(x) = 0$ if $x \in \lambda$, and $(v[\lambda \leftarrow 0])(x) = v(x)$ otherwise.

A timed automaton (TA) over $\Sigma$ is a tuple $\mathcal{A} = (\Sigma, S, s_0, X, \Delta, F)$ where $S$ is a finite set of locations, $s_0 \in S$ is the initial location, $X$ is a finite set of clocks, $\Delta \subseteq S \times \Sigma \times G(X) \times 2^X \times S$ is the transition relation, and $F$ is the set of accepting locations. We say that $\mathcal{A}$ is deterministic iff for each $s \in S$ and $\sigma \in \Sigma$ and every distinct pair of transitions $(s, \sigma, g_1, \lambda_1, s_1) \in \Delta$ and $(s, \sigma, g_2, \lambda_2, s_2) \in \Delta$, $g_1 \land g_2$ is not satisfiable. A state of $\mathcal{A}$ is a pair $(s, v)$ of a location $s \in S$ and a valuation $v$ for $X$. A run of $\mathcal{A}$ on a timed word $(\sigma_1, \tau_1) \ldots (\sigma_n, \tau_n) \in T\Sigma^*$ is a sequence of states $(s_0, v_0) \ldots (s_n, v_n)$ where (i) $v_0(x) = 0$ for all $x \in X$ and (ii) for each $i$, $0 \leq i < n$, there is a transition $(s_i, \sigma_{i+1}, g, \lambda, s_{i+1})$ such that $v_i + (\tau_{i+1} - \tau_i) \models g$ (let $\tau_0 = 0$) and $v_{i+1} = (v_i + (\tau_{i+1} - \tau_i))[\lambda \leftarrow 0]$. A run of $\mathcal{A}$ is accepting iff it ends in a state $(s, v)$ with $s \in F$. A timed word is accepted by $\mathcal{A}$ iff $\mathcal{A}$ has an accepting run on it. We denote by $[\mathcal{A}]$ the timed language of $\mathcal{A}$, i.e., the set of all timed words accepted by $\mathcal{A}$. Two fundamental results on TAs are that the emptiness problem is decidable (PSPACE-complete), but the universality problem is undecidable [4].

Timed logics. The set of MTL formulae over a finite set of atomic propositions AP is generated by

$$\psi := \top \mid p \mid \psi_1 \land \psi_2 \mid \neg \psi \mid \psi_1 \mathsf{U} \psi_2 \mid \psi_1 \mathsf{F} \psi_2 \mid \psi_1 \mathsf{\bar{U}} \psi_2$$

where $p \in \text{AP}$ and $I \subseteq \mathbb{R}_{\geq 0}$ is a non-singular interval with endpoints in $\mathbb{N}_{\geq 0} \cup \{\infty\}$.\footnote{In the literature, this logic (with the requirement that constraining intervals must be non-singular) is usually referred to as MITL [5], but we simply call it MTL in this paper for notational simplicity. Also note that our undecidability results carry over to the fragment with only future operators.} We omit the subscript $I$ when $I = [0, \infty)$ and sometimes write pseudo-arithmetic expressions for constraining intervals, e.g., ‘$< 3$’ for $[0, 3)$. The other Boolean operators are defined as usual: $\bot \equiv \neg \top$ and $\psi_1 \lor \psi_2 \equiv \neg(\neg \psi_1 \land \neg \psi_2)$. We also define the dual temporal operators $\psi_1 \mathsf{U} \psi_2 \equiv \neg((\neg \psi_1) \mathsf{F} \psi_2)$ and $\psi_1 \mathsf{\bar{U}} \psi_2 \equiv \neg((\neg \psi_1) \mathsf{\bar{U}} \psi_2)$. Using these operators, every MTL formula $\psi$ can be transformed into an MTL formula in negative normal form, i.e., $\neg$ is only applied to atomic propositions. To ease the presentation, we will also use the usual shortcuts like $\mathsf{F} I \psi \equiv \top \mathsf{U} I \psi$, $\mathsf{G} I \psi \equiv \neg \mathsf{F} I \neg \psi$, $\mathsf{X} I \psi \equiv \bot \mathsf{U} I \psi$, and “weak-future” variants of temporal operators, e.g., $\mathsf{F} \psi \equiv \psi \lor \mathsf{F} \psi$. Given an MTL formula $\psi$ over AP in negative normal form, a timed word $\rho = (\sigma_1, \tau_1) \ldots (\sigma_n, \tau_n)$ over $\Sigma_{\text{AP}} = 2^\text{AP}$, and $t \in \mathbb{R}_{\geq 0}$, we define the MTL satisfaction relation $\models$ as follows:\footnote{The formulation of the pointwise semantics of MTL here deviates slightly from the standard one (cf. [8, 50]) to enable a formal treatment of interleaving of events in different traces.}
On Verifying Timed Hyperproperties

- \((\rho, t) \models \top\) if and only if \(t \in \rho\);
- \((\rho, t) \models \bot\) if and only if \(t \not\in \rho\);
- \((\rho, t) \models \sigma\) if and only if \(t \in \rho\) and \(p \in \sigma\);
- \((\rho, t) \models \lnot\psi\) if and only if \(t \in \rho\) and \(p \not\in \sigma\);
- \((\rho, t) \models \psi_1 \land \psi_2\) if \((\rho, t) \models \psi_1\) and \((\rho, t) \models \psi_2\);
- \((\rho, t) \models \psi_1 \lor \psi_2\) if \((\rho, t) \models \psi_1\) or \((\rho, t) \models \psi_2\);
- \((\rho, t) \models \psi_1 \bigcup I \psi_2\) if there exists \(t' > t\) such that \(t' - t \in I\), \((\rho, t') \models \top\), \((\rho, t') \models \psi_2\), and \((\rho, t'') \models \psi_1\) for all \(t''\) such that \(t'' > t\) and \((\rho, t'') \models \top\);
- \((\rho, t) \models \psi_1 \bigcap I \psi_2\) if for all \(t' > t\) such that \(t' - t \in I\) and \((\rho, t') \models \top\), either \((\rho, t') \models \psi_2\) or \((\rho, t'') \models \psi_1\) for some \(t''\) such that \(t'' < t\) and \((\rho, t'') \models \top\);
- \((\rho, t) \models \psi_1 \bigcap I \psi_2\) if there exists \(t', 0 \leq t' < t\) such that \(t - t' \in I\), \((\rho, t') \models \top\), \((\rho, t') \models \psi_2\), and \((\rho, t'') \models \psi_1\) for all \(t''\) such that \(t'' > t\) and \((\rho, t'') \models \top\);
- \((\rho, t) \models \psi_1 \bigcap I \psi_2\) if for all \(t', 0 \leq t' < t\) such that \(t - t' \in I\) and \((\rho, t') \models \top\), either \((\rho, t') \models \psi_2\) or \((\rho, t'') \models \psi_1\) for some \(t''\) such that \(t'' < t\) and \((\rho, t'') \models \top\).

We say that \(\rho\) satisfies \(\psi\) (\(\rho \models \psi\)) if \((\rho, 0) \models \psi\), and we write \(\llbracket \psi \rrbracket\) for the timed language of \(\psi\), i.e., the set of all timed words satisfying \(\psi\). It is well known that any MTL formula can be translated into a TA accepting the same timed language [6]; this implies that the satisfiability and model-checking problems for MTL are decidable (EXPTIME-complete).

Adding trace quantifiers. Let \(V\) be an infinite supply of trace variables, the set of HyperMTL formulae over AP are generated by

\[
\varphi := \exists \pi \varphi \mid \forall \pi \varphi \mid \psi \\
\psi := \top \mid \tau \mid p_{\pi} \mid \psi_1 \land \psi_2 \mid \neg \psi \mid \psi_1 \bigcup I \psi_2 \mid \psi_1 \bigcap I \psi_2
\]

where \(\pi \in V\), \(p \in AP\), and \(I \subseteq \mathbb{R}_{\geq 0}\) is a non-singular interval with endpoints in \(\mathbb{N}_{\geq 0} \cup \{\infty\}\) (to ease the notation, we will usually write, e.g., \(p_{\pi}\) for \(p_{\pi_{\pi}}\)). Without loss of generality we forbid the reuse of trace variables, i.e., each trace quantifier must use a fresh trace variable. Syntactic sugar is defined as in MTL, e.g., \(F_I \psi \equiv \top \bigcup_{i} \psi\). A HyperMTL formula is closed if it does not have free occurrences of trace variables. Following [22], we refer to fragments of HyperMTL by their quantifier patterns, e.g., \(\exists^{+} \forall^{*}\)-HyperMTL. Finally, note that trace quantifiers can be added to TAs in the same manner (in this case, quantified TAs operate over “stacked” traces; see the semantics for HyperMTL below).

In contrast with TAs and MTL formulae, which define trace properties, HyperMTL formulae define (timed) hyperproperties, i.e., sets of trace properties. Depending on whether one requires timestamps in quantified traces to match exactly (i.e., all quantified traces must synchronise), two possible semantics can be defined accordingly.

Asynchronous semantics. A trace assignment over \(\Sigma\) is a partial mapping from \(V\) to \(\Gamma\Sigma^*\). We write \(\Pi_{\emptyset}\) for the empty trace assignment and \(\Pi[\pi \mapsto \rho]\) for the trace assignment that maps \(\pi\) to \(\rho\) and \(\pi' \mapsto \Pi[\pi' \mapsto \rho]\) for all \(\pi' \neq \pi\). Given a HyperMTL formula \(\varphi\) over AP whose quantifier-free part is in negative normal form, a trace set \(T\) over \(\Sigma_{AP}\), a trace assignment \(\Pi\) over \(\Sigma_{AP}\), and \(t \in \mathbb{R}_{\geq 0}\), we define the HyperMTL asynchronous satisfaction relation \(\models\) as follows (we omit the cases where the definitions are obvious or exactly similar):
We say that $\Sigma = \{ (T,t) \mid (T,t) \models \Pi \}$ if $t \in \rho$ for some $\rho \in \text{range}(\Pi)$;\footnote{Note the dependency of the interpretation of $\top$ on $\Pi$; in particular, it is possible for a trace set with out-of-sync traces to satisfy $\forall p \in \rho \models \top$ but not $\forall p \in \rho \models \top$.}

$\Pi$ is the past version of $\Pi$. The asynchronous semantics for HyperMTL is (arguably) the most natural choice of semantics for the current event-based setting. As the examples below illustrate, allowing explicit interleaving of events may simplify the specification even when no quantitative timing constraint is involved.

Example 3. Consider again the system in Example 2 and a low-security user $u_L$ who can observe $\{B^0, B^1, C^0, C^1\}$ but not $\{A^0, A^1\}$. The property “if $B^0$ occurs in both $\pi_a$ and $\pi_b$, then the corresponding $C^0$’s must occur simultaneously in both $\pi_a$ and $\pi_b$” (a variant of noninference [46]) can be specified with the following HyperMTL formula in the asynchronous semantics:

$$\varphi_1 = \forall \pi_a \forall \pi_b \left( F B^0_a \land F B^0_b \Rightarrow F (C^0_a \land C^0_b) \right).$$

In particular, $C^0_a \land C^0_b$ holds only when the two $\{C^0\}$-events occur simultaneously in $\pi_a$ and $\pi_b$. It is clear that the system does not satisfy $\varphi_1$, as there are two traces of the system where $B^0$ occurs in both, but the occurrences of $C^0$ are at different times; as we mentioned earlier, this allows $u_L$ to infer $A$ by timing $C^0$. If, on the other hand, the timing accuracy attainable by $u_L$ is limited and thus it can only differentiate events that are $d$ time units apart, the system can instead be checked against

$$\varphi_2 = \forall \pi_a \forall \pi_b \left( F B^0_a \land F B^0_b \Rightarrow F (C^0_a \land (F \leq d C^0_b \lor O \leq d C^0_b)) \right)$$

where $O$ is the past version of $F$. This will be satisfied if $T_B - T_A \leq d$, and since $u_L$ will not be able to infer $A$, the system may be considered secure in this case. Finally, note that in the original (synchronous) semantics for HyperLTL [16], $\varphi_1$ is satisfied by the system, as events are synchronised by their positions rather than times of occurrence.

Example 4 (Noninterference in event-based systems [31]). A system operating on sequences of commands issued by different users can be modelled as a deterministic finite automaton $A$ over $\Sigma = U \times C$ where $U$ is the set of users and $C$ is the set of commands. Additionally, let $\text{Obs}$ be the set of observations and $\text{out} : S \times U \rightarrow \text{Obs}$ be the observation function for what can be observed at each location by each user. Let there be a partition of $U$ into two disjoint sets of users $U_H \subseteq U$ and $U_L \subseteq U$. Noninterference requires that for each $w \in \Sigma^*$ where $w$ ends with a command issued by a user in $U_L$ and $A$ reaches $s$ after reading $w$, the subsequence $w'$ obtained by removing all the commands issued by the users in $U_H$ results in a location $s'$ such that the observation $\text{out}(s', u_L)$ of each user $u_L \in U_L$ is identical...
to \( out(s, u_L) \). For our purpose, we can combine \( \mathcal{A} \) and \( out \) (in the expected way) into an automaton \( \mathcal{A}' \) over \( \Sigma_{AP} \) where \( AP = (U \times C) \cup (U \times \text{Obs}) \) (atomic propositions in \( U \times \text{Obs} \) reflect the observations at the location that has just been entered). Checking noninterference then amounts to model checking \( \mathcal{A}' \) (whose locations are all accepting) against the following HyperMTL formula in the asynchronous semantics:

\[
\varphi_3 = \forall \pi_a \forall \pi_b \left( G(\top \Rightarrow \psi_b^L \land \psi_{U,C}^b) \wedge G(\top \land \bot \Rightarrow \psi_a^H) \Rightarrow G(\top \Rightarrow \psi_{out(U_L)}^b) \right)
\]

(where \( \psi_b^L \) asserts that the command in \( \pi_b \) is issued by a user in \( U_L \), \( \psi_{U,C}^b \) says that the two synchronised commands in \( \pi_a \) and \( \pi_b \) agree on \( U \) and \( C \), etc.). Specifically,

- \( G(\top \Rightarrow \psi_b^L \land \psi_{U,C}^b) \) asserts that \( \pi_b \) only contains low commands and \( \pi_a \) also contains these commands at the exactly same times;
- \( G(\top \land \bot \Rightarrow \psi_a^H) \) asserts that all the commands that are only present in \( \pi_a \) are high commands;
- \( G(\top \Rightarrow \psi_{out(U_L)}^b) \) ensures that, after each low command in \( \pi_b \), the observation of each \( u_L \in U_L \) is identical to the observation of \( u_L \) after the corresponding low command in \( \pi_a \), regardless of the high commands that occur in the preceding “gaps”.

We remark that while this example is essentially untimed, the asynchronous event-based formulation leads to a much simpler and clearer specification than the state-based one in [16].

**Synchronous semantics.** A less general semantics can be defined for HyperMTL formulae where each trace quantifier only ranges over traces that synchronise with the traces in the current trace assignment (this is the case in the original HyperLTL semantics [16]). For example, the second quantifier in \( \exists \pi_b \psi \) requires \( \pi_b \) to satisfy \( (\pi_a, t) \models \top \Leftrightarrow (\pi_b, t) \models \top \) for all \( t \in \mathbb{R}_{\geq 0} \). The HyperMTL synchronous satisfaction relation \( \models^{\text{sync}} \) can, in fact, be expressed in the asynchronous semantics by explicitly requiring newly quantified traces to synchronise in the quantifier-free part of the formula. More precisely, for a closed HyperMTL formula \( \varphi = Q \varphi' \) where \( Q \) denotes a block of quantifiers of the same type (i.e. all existential or all universal) and \( \varphi' \) is a possibly open HyperMTL formula, and a set \( V \) of trace variables, let (abusing notation slightly) \( \text{sync}(\varphi, V) = Q \left( G(\bigwedge_{x \in Q \cup V} \top) \land \text{sync}(\varphi', Q \cup V) \right) \) when \( \varphi \) are existential, \( \text{sync}(\varphi) = Q \left( G(\bigwedge_{x \in Q \cup V} \top) \Rightarrow \text{sync}(\varphi', Q \cup V) \right) \) when \( \varphi \) are universal, and \( \text{sync}(\psi, V) = \psi \) when \( \psi \) is quantifier-free. The following lemma holds subject to rewriting the formula into prenex normal form.

**Lemma 5.** For any trace set \( T \) over \( \Sigma_{AP} \) and closed HyperMTL formula \( \varphi \) over \( AP \), \( T \models^{\text{sync}} \varphi \) iff \( T \models \text{sync}(\varphi, \emptyset) \).

While the synchronous semantics may seem quite restricted (intuitively, the chance that two random traces of a timed system have exactly the same timestamps is certainly slim!), one can argue that it already suffices for many applications if stuttering steps are allowed. We will see later that for alternation-free HyperMTL, the asynchronous semantics can be emulated in the synchronous semantics using a “weak inverse” of Lemma 5.

**Satisfiability and model checking.** Given a closed HyperMTL formula \( \varphi \) over \( AP \), the satisfiability problem asks whether there is a non-empty trace set \( T \subseteq T \Sigma_{AP}^* \) satisfying it, i.e. \( T \models \varphi \) (or \( T \models^{\text{sync}} \varphi \), if the synchronous semantics is assumed). Given a TA \( \mathcal{A} \) over \( \Sigma_{AP} \) and a closed HyperMTL formula \( \varphi \) over \( AP \), the model-checking problem asks whether \( \llbracket \mathcal{A} \rrbracket \models \varphi \) (or \( \llbracket \mathcal{A} \rrbracket \models^{\text{sync}} \varphi \)). Our focus in this paper is on the decidability of these problems, as their complexity (when they are decidable) follow straightforwardly from standard results on MTL [5] and HyperLTL [16, 22].
3 Satisfiability

To emulate interleaving of events (of a concurrent or distributed system, say) in a synchronous, state-based setting, it is natural and necessary to introduce stuttering steps. In the context of verification, it is often a desirable trait for a temporal logic to be stutter-invariant [41, 42] so that it cannot be used to differentiate traces that ought to be regarded as the same (e.g., in an iterative refinement process, an abstract component of a system may be replaced by a concrete implementation that simulates an abstract step with some additional internal actions). As a simple attempt to reconcile the asynchronous and synchronous semantics of HyperMTL, we can make use of silent events in the same spirit to enable synchronisation of interleaving traces while preserving the semantics. More precisely, let stutter(ρ) for a trace ρ ∈ TΣAP be the maximal set of traces ρ′ ∈ TΣAP, (AP = AP ∪ {p′}) such that

- for every event (σi, τi) in ρ′, either σi = {p′} or p′ ∉ σi;
- ρ can be obtained from ρ′ by deleting all the {p′}-events.

This extends to trace sets T ⊆ TΣAP in the obvious way. For a closed alternation-free HyperMTL formula ϕ = Qψ over AP, let stutter(ϕ) = Qψ′′ be the HyperMTL formula over APc obtained by replacing in ψ, e.g., all Tπ with ¬p′π, to give ψ′, and finally let ψ′′ = G(∀p′ ∈ Q ψ′) ∧ (∃p′ ∈ Q ψ′) when Q are existential and ψ′′ = G(∀p′ ∈ Q ψ′) ∧ (∃p′ ∈ Q ψ′) when Q are universal. Intuitively, ψ′′ ensures that the traces involved are well-formed (i.e. satisfy the first condition above), and its own satisfaction is insensitive to the addition of silent events. The following lemma follows from a simple structural induction.

Lemma 6. For any trace set T over ΣAP and closed alternation-free HyperMTL formula ϕ = Qψ over AP (Q is either a block of existential quantifiers or universal quantifiers and ψ is quantifier-free), T |= ϕ iff stutter(T) |=sync stutter(ϕ).

The following two lemmas follow from Lemma 6 and the fact that for alternation-free HyperMTL formulae, satisfiability in the synchronous semantics can be reduced (in the same way as HyperLTL) to MTL satisfiability.

Lemma 7. The satisfiability problem for 3∗-HyperMTL is decidable.

Lemma 8. The satisfiability problem for 4∗-HyperMTL is decidable.

Lemma 6, however, does not extend to larger fragments of HyperMTL. For example, consider T = {{p}, 1}, {{r}, 3}, {{q}, 2} and ϕ = 3π0 νπ0 (F p0 ∧ ¬F q0). Now it is obvious that T \models ϕ, but since {{p}, 1}, {{r}, 3} ∈ stutter(T), we have stutter(T) \models sync stutter(ϕ) (provided that the definition of stutter(·) is extended to general HyperMTL formulae, as in Lemma 5). Still, it is not hard to see that the crucial observation used in 3∗-HyperLTL satisfiability (if 3π0 \ldots 3πk νπ′0 \ldots νπ′k ψ is satisfiable, then it is also satisfiable by the trace set {π0, ..., πk}) extends to HyperMTL in the asynchronous semantics; the following lemma then follows from Lemma 7.

Lemma 9. The satisfiability problem for 3∗4∗-HyperMTL is decidable.

Finally, note that the undecidability of 43-HyperLTL carries over to HyperMTL: in the synchronous semantics, the reduction in [22] applies directly with some trivial modifications (as we work with finite traces); undecidability then holds for the case of asynchronous semantics as well, by Lemma 5.

Lemma 10. The satisfiability problem for 43-HyperMTL is undecidable.

Theorem 11. The satisfiability problem for HyperMTL is decidable if the formula does not contain 43.
4 Model checking

We now turn to the model-checking problem, which behaves quite differently than in the case of HyperLTL.

The alternation-free case. Without loss of generality, we consider only the case of $\exists^*\text{-HyperMTL}$ in the asynchronous semantics. By Lemma 6, checking $[A] \models \varphi$ (for a TA $A$ over $\Sigma_{AP}$ and a closed $\exists^*\text{-HyperMTL}$ formula $\varphi$ over AP) is equivalent to checking
\[ \text{stutter}([A]) \models_{\text{sync}} \text{stutter}(\varphi). \]
To this end, we define $\text{stutter}(A)$ as the TA over $\Sigma_{AP}$, obtained from $A$ by adding a self-loop labelled with $\{p_0\}$ to each location; it should be clear that $\llbracket \text{stutter}(A) \rrbracket = \text{stutter}([A])$. In this way, the problem reduces to model checking $\exists^*\text{-HyperMTL}$ in the synchronous semantics which, as the model-checking problem for $\exists^*\text{-HyperLTL}$, can be reduced to MTL model checking.

▶ Theorem 12. Model checking alternation-free HyperMTL is decidable.

The general case. Recall that the model-checking problem for HyperLTL is decidable even when the specification involves arbitrary nesting of quantifiers. This is unfortunately not the case for HyperMTL: allowing only one quantifier alternation already leads to undecidability. To see this, recall that any TA can be written as a formula $\exists X \psi$ where $X$ is a set of (new) atomic propositions and $\psi$ is an MTL formula [33, 53]. The undecidable TA universality problem – given a TA $A$ over $\Sigma$, deciding whether $[A] = T\Sigma^*$ – can thus be reduced to model checking HyperMTL: one simply checks whether there exists an $X$-labelling for every timed word over $\Sigma$ so that $\psi$ is satisfied. Here we show that model checking HyperMTL is essentially a harder problem: in the case of asynchronous semantics, model checking HyperMTL with quantifier alternations necessarily involves TAs with $\epsilon$-transitions [11], and therefore remains
undecidable even when both the model and the specification are deterministic and only one of them uses a single clock (i.e. the other is untimed); by contrast, (standard) TA universality over finite timed words is decidable when the TA uses only one clock [49].

We adapt the undecidability proof of the reactive synthesis problem for MTL in [14], which itself is by reduction from the halting problem for deterministic channel machines (DCMs), known to be undecidable [13]. Note that, in contrast to HyperMTL model checking, MTL reactive synthesis is decidable when the specification is deterministic [19]; in this sense, quantification over traces is more powerful than quantification over strategies (there is a winning strategy of the controller for all possible strategies of the environment).\footnote{Indeed, the quantifier-free part \( \psi \) in the simpler encoding mentioned above (based on labelling timed words with propositions in \( X \)) is already in \( \text{LTL}_\lhd \) and thus is deterministic.} For our purpose, we introduce the \( \lhd \) operator, in which we allow \( I \) to be singular (note that this is merely syntactic sugar and does not increase the expressiveness of MTL [33,53]):

\[
(T,t) \models \lhd \varphi \iff \exists t' \leq t \text{ such that } t-t' \in I, (T,t') \models \varphi, \text{ and } (T,t') \not\models \varphi \text{ for all } t'' \text{ such that } t'' \in (t',t) \text{ and } (T,t'') \models \top.
\]

Let \( \text{LTL}_\lhd \) be the fragment of MTL where all timed subformulæ must be of the form \( \lhd \varphi \), and all \( \varphi 's \) in such subformulæ must be “pure past” formulæ; these requirements ensure that \( \text{LTL}_\lhd \), in which we will write the quantifier-free part of the specification, translates into deterministic TAs [18]. To ease the understanding, we will first do the proof for the case of asynchronous semantics and then adapt it to the case of synchronous semantics.

\begin{theorem}
Model checking \( \exists^* \forall^* - \text{HyperMTL} \) and \( \forall^* \exists^*- \text{HyperMTL} \) are undecidable in the asynchronous semantics.
\end{theorem}

\textbf{Proof.} A DCM \( \mathcal{S} = (S,s_0,s_{\text{halt}},M,\Delta) \) can be seen as a finite automaton equipped with an unbounded fifo channel: \( S \) is a finite set of locations, \( s_0 \) is the initial location, \( s_{\text{halt}} \) is the halting location (such that \( s_{\text{halt}} \neq s_0 \)), \( M \) is a finite set of messages, and \( \Delta \subseteq S \times \{!m,?m \mid m \in M\} \times S \) is the transition relation satisfying the following determinism hypothesis: (i) \((s,q,s') \in \Delta \) and \((s,q,s'') \in \Delta \) implies \( s' = s'' \); (ii) if \((s,m!,s') \in \Delta \) then it is the only outgoing transition from \( s \). Without loss of generality, we further assume that there is no incoming transition to \( s_0 \), no outgoing transition from \( s_{\text{halt}} \), and \((s_0,q,s') \in \Delta \) implies that \( q \in \{!m \mid m \in M\} \) and \( s' \neq s_{\text{halt}} \). The semantics of \( \mathcal{S} \) can be described with a graph \( G(\mathcal{S}) \) with vertices \( \{(s,x) \mid s \in S, x \in M^*\} \) and edges defined as follows: (i) \((s,x) \rightarrow (s',xm)\) if \((s,m!,s') \in \Delta \); (ii) \((s,\text{max}) \rightarrow (s',x)\) if \((s,m!,s') \in \Delta \). In other words, \( m! \) “writes” a copy of \( m \) to the channel and \( m \) “reads” a copy of \( m \) off the channel. We say that \( \mathcal{S} \) \textit{halts} if there is a path in \( G(\mathcal{S}) \) from \((s_0,e)\) to \((s_{\text{halt}},x)\) (a halting computation of \( \mathcal{S} \)) for some \( x \in M^* \). An example DCM and its unique halting computation are depicted in Figure 4.

The idea, as in many similar proofs (e.g., [50]), is to encode a halting computation of \( \mathcal{S} \) as a trace where each \( m \) is preceded by a corresponding \( m! \) exactly 1 time unit earlier, and each \( m! \) is followed by an \( m? \) exactly 1 time unit later if \( s_{\text{halt}} \) has not been reached yet. To this end, let the model \( \mathcal{A} \) be an (untimed) finite automaton over \( \Sigma = 2^\text{AP} \) where \( \text{AP} = \{m^1, m^2 \mid m \in M\} \cup \{p^\text{begin}, p^\text{end}, p^\text{read}, p^1, q^1\} \) and whose set of locations is \( S \cup \{s_1\} \), where \( s_1 \) is a new non-accepting location. The transitions of \( \mathcal{A} \) follow \( \mathcal{S} \): for each \( m \in M \),

\[
s \xrightarrow{\{m\}} s' \text{ is a transition of } \mathcal{A} \text{ iff } (s,m?,s') \in \Delta, \text{ and similarly for } m! \text{-- except for those going out of } s_0 \text{ or going into } s_{\text{halt}}, \text{ on which we further require } p^\text{begin} \text{ or } p^\text{end} \text{ to hold, respectively. Let } s_0 \text{ be the initial location and } s_{\text{halt}} \text{ be the only accepting location, and finally add transitions } s_0 \xrightarrow{p^\text{begin}} s_{\text{halt}} \text{ and } s_0 \xrightarrow{p^1} s_1 \xrightarrow{q^1} s_{\text{halt}}. \text{ It is clear that } \mathcal{A} \text{ is deterministic and it accepts only three types of traces:}
\]
1. From $s_0$ through some other locations of $S$ and finally $s_{halt}$, i.e. those respecting the transition relation, but not necessarily the semantics, of $S$.

2. From $s_0$ to $s_{halt}$ in a single transition (on which $p^{read}$ holds).

3. From $s_0$ to $s_1$ and then $s_{halt}$.

It remains to write a specification $\varphi$ such that $[A] \models \varphi$ exactly when $A$ accepts a trace of type (1) that also respects the semantics of $S$ (one such trace that corresponds to the unique halting computation of the DCM in Figure 4 is depicted in Figure 5). This is where the traces of types (2) and (3) come into play: for example, if a trace of type (1) issues a read $m$? without a corresponding write $m!$, then a trace of type (3) can be used to “pinpoint” the error. More precisely, let $\varphi = \exists \pi_a \forall \pi_b (\psi_1 \land \psi_2 \land \psi_3 \land \psi_4)$ where

- $\psi_1 = Fp^{end}_a$ ensures that $\pi_a$ is of type (1);
- $\psi_2 = F(p^{read}_b \land \psi_R) \Rightarrow F(p^{read}_b \land \varphi_{\geq 1} p^{begin}_a)$, where $\psi_R = \bigvee \{m'_a \mid m \in M\}$, is a simple sanity check which ensures that in $\pi_a$, each $m'$ must happen at time $t \geq t + 1$ if $p^{begin}$ happens at $t$;
- $\psi_3 = \bigwedge_{m \in M} (F(q_b \land m'_a) \Rightarrow (F(p^{begin}_a \land F(p_b^1) \land F(q_b \land \varphi_{1} p^{begin}_a) \Rightarrow F(p_b^1 \land m'_a)))$ ensures that each $m'$, if it happens at $t$, is preceded by a corresponding $m'$ at $t - 1$ in $\pi_a$;
- $\psi_4 = \bigwedge_{m \in M} (F(q_b \land m'_a) \Rightarrow F(p^{end}_a \land \varphi_{\leq 1} p^{begin}_a) \land (F(q_b \land \varphi_{1} p^{begin}_a) \Rightarrow F(q_b \land m'_a)))$ ensures that each $m'$ at $t$ is followed by a corresponding $m'$ at $t + 1$ (unless $p^{end}$ happens first) in $\pi_a$.

Now observe that the only timed subformulae are $\varphi_{\leq 1} p^{begin}_a$, $\varphi_{\leq 1} p^{begin}_b$, and $\varphi_{\leq 1} p^{begin}_a$. As $p^1$ and $p^{read}$ cannot happen in the same trace ($\pi_b$), it is not hard to see that the reduction remains correct if we replace these by $\varphi_{\leq 1} (p^{begin}_a \lor p^{begin}_b)$, $\varphi_{\leq 1} (p^{begin}_a \lor p^{begin}_b)$, and $\varphi_{\leq 1} (p^{begin}_a \lor p^{begin}_b)$ (respectively) to obtain $\psi'_2$, $\psi'_3$, and $\psi'_4$. It follows that $\psi_1 \land \psi'_2 \land \psi'_3 \land \psi'_4$ can be translated into a one-clock deterministic TA. Finally, it is possible to move all the timing constraints into the model and use an untimed HyperLTL formula as the specification: in the model, ensure that $p^1$ and $q^1$ are separated by exactly 1 time unit, and add $s_0 \xrightarrow{(p^2)} s_1 \xrightarrow{(q^2)} s_{halt}$ such that $p^2$ and $q^2$ are separated by $< 1$ time unit; in the specification, use $p^2$, $q^2$ to rule out those $\pi_a's$ with some $m'$ at $< 1$ time unit from $p^{begin}$.

Now we consider the synchronous semantics. The corresponding result is weaker in this case, as we will see in the next section that in several subcases the problem becomes decidable. Still, the reduction above can be made to work if the model has one clock and an extra trace quantifier is allowed.

▶ Theorem 14. Model checking $\exists^* \forall^*$.HyperMTL and $\forall^* \exists^*$.HyperMTL are undecidable in the synchronous semantics.

Proof of Theorem 14. We use a modified model $A'$ whose set of locations is $S \cup \{s_1, s_2, s_3, s_4\}$; the transitions are similar to $A$ in the proof of Theorem 13, but we now use a clock $x$ in the path $s_0 \xrightarrow{(p^1)} x=0 \xrightarrow{(q^1)} x=2 \xrightarrow{(x)} x=0 \xrightarrow{(p^1)} x=0 \xrightarrow{(q^2)} x=0 \xrightarrow{(x)} x=0 \xrightarrow{(x)} s_{halt}$, the paths $s_0 \xrightarrow{(p^2)} x=0 \xrightarrow{(q^2)} x=0 \xrightarrow{(p^1)} x=0 \xrightarrow{(q^2)} x=0 \xrightarrow{(x)} x=0 \xrightarrow{(x)} s_{halt}$ are added, and $s_0 \xrightarrow{(p^{end})} s_{halt}$ is removed. Moreover, a self-loop labelled with $\{p^r\}$ is added to each of $s_0, s_1, s_2, s_3, s_4$, and $s_{halt}$. The specification is $\varphi' = \exists \pi_a \forall \pi_b \forall c \bigwedge_{1 \leq i \leq 9} \psi_i'$ where $\bigwedge_{1 \leq i \leq 9} \psi_i'$ is the following untimed LTL formula:

- $\psi'_1 = Fp^{end}_a$;
- $\psi'_2 = F(q_b^4 \land \psi_R) \Rightarrow \neg F(p_b^4 \land p^{begin}_a)$ where $\psi_R = \bigvee \{m'_a \mid m \in M\}$;
- $\psi'_3 = \bigwedge_{m \in M} (F(q_b \land q^2 \land m'_a) \land F(p_b^1 \land p_b^2 \land m'_a))$;
We conclude this section by showing that the undecidability results above can actually be obtained for trivial systems with only a single location. In particular, the structural restrictions considered in [12] have no effect on the decidability of HyperMTL model checking.

\begin{corollary}
Model checking $\exists \forall^*\text{-HyperMTL}$ and $\forall^*\exists^*\text{-HyperMTL}$ are undecidable in the asynchronous semantics for systems with only one location.
\end{corollary}

\begin{corollary}
Model checking $\exists \forall^*\text{-HyperMTL}$ and $\forall^*\exists^*\text{-HyperMTL}$ are undecidable in the synchronous semantics for systems with only one location.
\end{corollary}

\section{Decidable subcases}

While the negative results in the previous section may be disappointing, we stress again that model checking alternation-free HyperMTL is no harder than MTL model checking, and it can in fact be carried out with algorithms and tools for the latter. In any case, we now identify several subcases where model checking is decidable beyond the alternation-free fragment.

\subsection*{Untimed model + untimed specification.}
The first case we consider is when both the model and the specification are untimed, and the synchronous semantics is assumed (note that, if instead, the synchronous semantics is assumed, then this case is simply HyperLTL model checking). Our algorithm follows the lines of [16] and is essentially based on self-composition (cf. [10], and many others; see the references in [16]) of the model; the difficulty here, however, is to handle interleaving of events. Let the model $A$ be a finite automaton over $\Sigma_{AP}$ and the specification be a (untimed) closed HyperMTL formula over AP. Without loss of generality, we assume the specification to be $\phi = \exists \pi_1 \forall \pi_2 \ldots \exists \pi_{k-1} \forall \pi_k \psi$, which can be rewritten into $\exists \pi_1 \neg \exists \pi_2 \ldots \exists \pi_{k-1} \neg \exists \pi_k \neg \psi$. We start by translating $\text{stutter}(\neg \psi)$ (in which we replace all occurrences of $\neg i$ with $\neg p_i$, i.e. regarded here simply as an MTL formula over $\Sigma_{AP}$) into the equivalent finite automaton over $\Sigma_{(AP)^*}$, and take its product with (i) the automaton for $G(\bigvee_{1 \leq i \leq k} \neg p_i) \land (\bigwedge_{1 \leq i \leq k} G(p_i \Rightarrow \bigvee_{p \in \text{AP}} \neg p_i))$ and (ii) the automaton obtained from $\text{stutter}(A)$ by extending the alphabet to $\Sigma_{(AP)^*}$ and renaming all the occurrences of $p$ to $p_k$, to obtain $B$. Now let $C$ be the projection of $B$ onto $\bigvee_{1 \leq i \leq k} p_i$. By construction, $C$ accepts only traces that are well-formed in dimensions 1 to $k-1$, and so does $C$; but $C$ may accept traces containing $\{p_i^1 \mid 1 \leq i \leq k-1\}$-events. We replace these events by $\epsilon$ (the “real” silent event, which can be removed with the standard textbook constructions, e.g., [36]) to obtain $C'$. Finally, we complement $C'$ to obtain $C''$ (this step corresponds to $\neg \psi$). We can then start over by taking the product of $C''$, the automaton for
20:14 On Verifying Timed Hyperproperties

\[ G(\forall_{1 \leq i \leq k-1} \neg p_i^k) \land (\Lambda_{1 \leq i \leq k-1} G(p_i^k \Rightarrow \Lambda_{p \in AP} \neg p_i)), \] and the automaton obtained from \( \text{statter}(A) \) by extending the alphabet to \( \Sigma_{AP, \leq k-1} \) and renaming all the occurrences of \( p \) to \( p_{k-1} \); the resulting automaton is the new \( B \). We continue this process until the outermost quantifier \( \exists \) is reached, when we test the emptiness of \( B \) (at this point, it is an automaton over \( \Sigma_{AP, \leq k} \)).

**Proposition 17.** Model checking HyperMTL is decidable when the model and the specification are both untimed.

**One clock + one alternation.** The algorithm outlined in the previous case crucially depends on the fact that both \( A \) and \( \varphi \) are untimed, hence their product (in the sense detailed in the previous case) can be complemented. When the synchronous semantics is assumed and there is only one quantifier alternation in \( \varphi \), it might be the case that we do not actually need complementation. For example, if \( A \) is untimed and \( \varphi = \forall x. \exists y. \exists z. \psi \) where \( \psi \) translates into a one-clock TA, the corresponding model-checking problem clearly reduces to universality for one-clock TAs, which is decidable but non-primitive recursive [1].\(^7\) This observation applies to other cases as well, such as when \( A \) is a one-clock TA and \( \varphi = \exists x. \forall y. \psi \) where \( \psi \) is untimed; here model checking reduces to language inclusion between two one-clock TAs.

**Untimed model + MIA specification.** The main obstacle in applying the algorithm above to larger fragments of HyperMTL, as should be clear now, is that universal quantifiers amount to complementations, which are not possible in general in the case of TAs. Moreover, we note that the usual strategy of restricting to deterministic models and specifications does not help, as the projection step in the algorithm necessarily introduces non-determinism. To make the algorithm work for larger fragments, we essentially need a class of automata that is both **closed under projection** and **complementable**. Fortunately, there is a subclass of one-clock TAs that satisfies these conditions. We consider two additional restrictions on one-clock TAs:

- Non-Singular (NS): a one-clock TA is NS if all the guards are non-singular (i.e. must be of the form \( x \in I \) where \( x \) is the single clock and \( I \) is a non-singular interval).
- Reset-on-Testing (RoT): a one-clock TA is RoT if whenever the guard of a transition is not \( \top \), \( x \) must be reset on that transition.

One-clock TAs satisfying both NS and RoT are called **metric interval automata (MIAs)**, which are determinisable [21]. Since the projection operation cannot invalidate NS and RoT, the algorithm above can be applied when the synchronous semantics is assumed, \( A \) is untimed, \( \psi \) or \( \neg \psi \) translates to a MIA, and only one complementation is involved; in this case it runs in elementary time.

**Proposition 18.** Model checking \( \forall \exists \text{-HyperMTL} \) (\( \exists \forall \text{-HyperMTL} \)) is decidable in the synchronous semantics when the model is untimed and \( \psi \) (\( \neg \psi \)) translates into a MIA in the specification \( \varphi = \forall \pi_1 \ldots \exists \pi_k \psi \) (\( \varphi = \exists \pi_1 \ldots \forall \pi_k \psi \)).

On the other hand, we can adapt the proof of Theorem 14 to show that model checking an untimed model against an \( \exists \forall \text{-HyperMTL} \) specification \( \varphi \) in the synchronous semantics, when the quantifier-free part \( \psi \) (instead of \( \neg \psi \)) translates into a MIA, remains undecidable.

\(^7\) This case is undecidable in the asynchronous semantics by Theorem 13; as explained above, the algorithm may introduce \( \epsilon \)-transitions in the asynchronous semantics, while universality for one-clock TAs with \( \epsilon \)-transitions is undecidable [1].
Proposition 19. Model checking \( \exists^* \forall^* \text{-HyperMTL} \) is undecidable in the synchronous semantics when the model is untimed and \( \psi \) in the specification \( \varphi = \exists \pi_1 \ldots \exists \pi_k \psi \) translates into a MIA.

The decidability results in the synchronous semantics are summarised in Table 1.

Table 1 Decidability of model checking untimed or one-clock TAs against (one-clock) \textsf{HyperMTL} in the synchronous semantics; NS stands for Non-Singular constraints and RoT stands for Reset-on-Testing.

<table>
<thead>
<tr>
<th>Model</th>
<th>Spec.</th>
<th>untimed</th>
<th>NS+RoT</th>
<th>NS</th>
<th>RoT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Dec. (Proposition 17)</td>
<td>Dec. for ( \forall^* \exists^* ) (Proposition 18)</td>
<td>Undec. for ( \exists \forall ) (Proposition 19)</td>
<td>Undec. for ( \exists \forall ) (Proposition 19)</td>
</tr>
<tr>
<td>untimed</td>
<td></td>
<td>Dec.</td>
<td>Undec. for ( \exists \forall ) (Theorem 14)</td>
<td>Undec.</td>
<td>Undec.</td>
</tr>
</tbody>
</table>

**Bounded time domains.** We end this section by showing that when there is an \textit{a priori} bound \( N \) (where \( N \) is a positive integer) on the length of the time domain, the model-checking problem for full \textsf{HyperMTL} becomes decidable; in fact, in the case of synchronous semantics it reduces to the satisfiability problem for \textsf{QPTL} [56]. From a practical point of view, this implies that \textit{time-bounded} \textsf{HyperMTL} verification (at least for the \( \exists^* \forall^* \)-fragment, say) can be carried out with highly efficient, off-the-shelf tools that work with \textsf{LTL} and (untimed) automatata, such as \textsf{SPOT} [20], \textsf{GOAL} [57], and \( \omega \textsf{LTL} \) [40].

We assume the asynchronous semantics. For a given \( N \), we consider all traces in which all timestamps are less than \( N \). Denote by \( [A]_{[0,N]} \) the set of all such traces in \( [A] \); the model-checking problem then becomes deciding whether \( [A]_{[0,N]} \models \varphi \). As before, we assume \( \varphi \) to be \( \exists \pi_1 \neg \exists \pi_2 \ldots \exists \pi_{k-1} \neg \exists \pi_k \neg \psi \). Following [34, 48], we can use the \textit{construction} to obtain, from the conjunction \( \psi' \) of \textit{stutter} (\( \neg \psi \)) and \( G(\bigvee_{\pi \in Q} \neg p'_{\pi}) \land (\bigwedge_{\pi \in Q} G(p'_{\pi} \Rightarrow \bigwedge_{p \in AP} \neg p_{\pi})) \), an equi-satisfiable untimed (\textsf{QPTL}) formula \( \overline{\varphi} = \exists W \overline{\psi}' \) over the stacked alphabet \( (\overline{AP})^* \cup \overline{Q} \) (where \( (\overline{AP})^* = \{ p_{i,j} \mid p \in AP, 1 \leq i \leq k, 0 \leq j < N \} \) and \( \overline{Q} = \{ q_j \mid 0 \leq j < N \} \}). We apply the following modifications to \( \overline{\varphi} \) to obtain \( \overline{\varphi}' \):

1. introduce atomic propositions \( \{ p'_{i,j} \mid 1 \leq i \leq k \} \) and add the conjunct
   \[ \land_{1 \leq i \leq k} G \left( (\land_{0 \leq j < N} (q_j \Rightarrow p'_{i,j})) \Leftrightarrow p'_{i,j} \right) ; \]

2. introduce atomic propositions \( \{ q_{i,j} \mid 1 \leq i \leq k, 0 \leq j < N \} \) and add the conjunct
   \[ \land_{1 \leq i \leq k} G \left( (\land_{0 \leq j < N} (\neg p_{i,j} \land q_j \Rightarrow q_{i,j})) \right) ; \]

3. project away \( \{ p'_{i,j} \mid 1 \leq i \leq k, 0 \leq j < N \} \) and \( \overline{Q} \);

4. replace all occurrences of \( p'_{i,j} \) by \( \bot_{i,j} \).

Now, as we mentioned earlier, we can write \( A \) as an \( \text{MSO}[<, +1] \) [48]) formula \( \varphi_A = \exists X_A \psi_A \) where \( X_A \) is a set of atomic propositions such that \( AP \cap X_A = \emptyset \) and \( \psi_A \) is an \textsf{MTL} formula over \( AP \cup X_A \). Let \( \overline{A} \) be its stacked counterpart \( \exists \overline{X} \exists \forall \overline{\psi}_A \); we translate \( \overline{\varphi}_A \) back into an untimed automaton \( \overline{A} \) over the stacked alphabet \( \overline{AP} \cup \overline{Q} \). The problem thus reduces to
20:16 On Verifying Timed Hyperproperties

untimed model checking of $A$ against $\exists \pi_1 \forall \pi_2 \ldots \exists \pi_{k-1} \forall \pi_k \varphi$ in the asynchronous semantics, which is decidable by Proposition 17 ($\varphi$ has outermost existential propositional quantifiers, but clearly the equivalent automaton can be used directly in the algorithm).

Finally, note that the proof is simpler for the case of synchronous semantics: we can simply work with a (non-stuttering) MSO[$\langle, +1\rangle$] formula in all the intermediate steps without translating it into an automaton, and then check the satisifiability of the final formula by stacking it into a QPTL formula.

\textbf{Proposition 20.} Model checking HyperMTL is decidable when the time domain is $[0, N)$, where $N$ is a given positive integer.

References


