A Three-valued Approach to Strategic Abilities under Imperfect Information
Francesco Belardinelli, Vadim Malvone

To cite this version:
Francesco Belardinelli, Vadim Malvone. A Three-valued Approach to Strategic Abilities under Imperfect Information. 17th International Conference on Principles of Knowledge Representation and Reasoning (KR 2020), Sep 2020, Rhodes, Greece. hal-03170197

HAL Id: hal-03170197
https://hal.science/hal-03170197
Submitted on 16 Mar 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
A Three-valued Approach to Strategic Abilities under Imperfect Information

Francesco Belardinelli\textsuperscript{1,2}, Vadim Malvone\textsuperscript{2}
\textsuperscript{1}Imperial College London, United Kingdom
\textsuperscript{2}Laboratoire IBISC, Université d’Evry, France
francesco.belardinelli@imperial.ac.uk, vadim.malvone@univ-evry.fr

Abstract

A major challenge for logics for strategies is represented by their verification in contexts of imperfect information. In this contribution we advance the state of the art by approximating the verification of Alternating-time Temporal Logic (ATL) under imperfect information by using perfect information and a three-valued semantics. In particular, we develop novel automata-theoretic techniques for the linear-time logic \(LTL\), then apply these to finding “failure” states, where the ATL specification to be model checked is undefined. Such failure states can then be fed into a refinement procedure, thus providing a sound, albeit partial, verification procedure.

1 Introduction

Logic-based languages to reason about the strategic abilities of agents are a thriving area of research in the applications of formal methods to knowledge reasoning and representation (Jamroga 2018; Fagin et al. 1995). Over the years, several logics for strategies have been introduced, including Alternating-time Temporal Logic (Alur et al. 2002), Coalition Logic (Pauly 2002), Strategy Logic (Chatterjee et al. 2007; Mogavero et al. 2014), which has also led to the development of model checking tools (Alur et al. 1998; Lomuscio et al. 2017; Kurpiewski et al. 2019).

A key challenge for these logics for strategies is represented by their verification in contexts of imperfect information. Indeed, the model checking problem for the Alternating-time Temporal Logic \(ATL\) under the assumption of perfect information is known to be \(\text{PTIME}\)-complete (Alur et al. 2002). However, under imperfect information it ranges between \(\Delta^2_0\)-complete to undecidable, depending on the underlying assumption on memory (Jamroga and Dix 2006; Dima and Tiplea 2011). Unfortunately, when reasoning about knowledge, the assumption of perfect information is either unrealistic or computationally costly. Thus, if logics for strategies are to be deployed in concrete multi-agent scenarios, it is crucial to develop even partial verification methods capable of tackling contexts of imperfect information. To this end, several proposals have been put forward, focusing on how the information is shared amongst agents (Berthon et al. 2017; Belardinelli et al. 2017a), or developing notions of constructive knowledge (Âgotnes et al. 2015) and bounded recall (Belardinelli et al. 2018), or again approximating strategy operators by using the \(\mu\)-calculus (Bulling and Jamroga 2011) (see Section 6 for an in-depth comparison with related work).

In this contribution we advance the state of the art in reasoning about strategic abilities under imperfect information. More precisely, we develop further the line initiated in (Belardinelli et al. 2019), whereby imperfect information is approximated (or abstracted) by using perfect information and a three-valued semantics; thus leading to a sound, albeit partial, verification procedure for the logic \(ATL^\ast\) under imperfect information and perfect recall. The verification procedure there outlined is partial, as it can return the undefined truth value \(uu\) for some specifications, in some states in the system. In those cases, we would like to use such “failure” states to refine the abstract model. However, a key question left open in (Belardinelli et al. 2019) concerns how to find such failure states. In (Ball and Kupferman 2006) such a procedure was provided but only for the Alternating \(\mu\)-calculus (\(AMC\)) under perfect information. Here we consider the arguably more complex case of full \(ATL^\ast\) under imperfect information, whose model checking problem is undecidable in general, differently from \(AMC\). Moreover, we prove novel results on automata-theoretic techniques for linear-time temporal logic (\(LTL\)) interpreted on a three-valued semantics, that we deem of independent interest.

The contribution is structured as follows. In Sec. 2 we present the syntax of \(ATL^\ast\), as well as its semantics given on concurrent game structures with imperfect information (iCGS). In Sec. 3 we recall the knowledge-based abstraction in (Belardinelli et al. 2019) and the related three-valued semantics. Then, in Sec. 4 we develop novel automata-theoretic techniques for three-valued \(LTL\). Specifically, we show how to construct Büchi automata accepting all traces making an \(LTL\) formula undefined and then consider the related non-emptiness problem. These results are used in Sec. 5 to find failure states, which can then be fed into the refinement algorithm in (Belardinelli et al. 2019). We conclude in Sec. 6 by discussing related literature and pointing to future work.

2 Classic Imperfect Information

In this section we introduce the classic two-valued semantics for the Alternating-time Temporal Logic \(ATL^\ast\) under imperfect information and perfect recall. We assume sets
$Ag = \{1, \ldots, m\}$ of agents and $AP$ of atoms. Given a set $U$, $\cup$ denotes its complement. We denote the length of a tuple $v$ as $|v|$, and its $i$-th element as $v_i$. Then, $last(v) = v_{|v|}$ is the last element in $v$. For $i \leq |v|$, let $v_{[i]}$ be the suffix $v_i, \ldots, v_{|v|}$ of $v$ starting at $v_i$ and $v_{\prec i}$ its prefix $v_1, \ldots, v_{i-1}$.

We start by introducing concurrent game structures with imperfect information as models for multi-agent systems (Alur et al. 2002; Jamroga and van der Hoek 2004).

**Definition 1 (iCGS).** Given sets $Ag$ of agents and $AP$ of atoms, a concurrent game structure with imperfect information is a tuple $M = (S, s_0, \{Ag\}_i \in Ag, \{\sim_i\}_i \in Ag, d, \delta, V)$ such that:

- $S \neq \emptyset$ is a finite set of states, with initial state $s_0 \in S$.
- For every agent $i \in Ag$, $\sim_i$ is a nonempty, finite set of actions. Then, let $Act = \bigcup_{i \in Ag} Act_i$ be the set of all actions, and $ACT = \prod_{i \in Ag} Act_i$ the set of all joint actions.
- For every agent $i \in Ag$, $\sim_i$ is the indistinguishability relation between states: for every $s, s' \in S$, $s \sim_i s'$ iff states $s$ and $s'$ are observationally indistinguishable for agent $i$.
- The protocol function $d : Ag \times S \rightarrow (2^{Act} \setminus \emptyset)$ defines the availability of actions so that for every $i \in Ag$, $s \in S$,
  - (i) $d(i, s) \subseteq Act_i$, and
  - (ii) $s \sim_i s'$ implies $d(i, s) = d(i, s')$.
- The transition function $\delta : S \times ACT \rightarrow S$ returns a successor $s' = \delta(s, a)$ to every state $s \in S$ and joint action $a \in ACT$ such that $a_i = d(i, s)$ for every $i \in Ag$.
- $V : S \times AP \rightarrow \{tt, ff\}$ is the two-valued labelling function.

By Def. 1 an iCGS represents the interactions of a group $Ag$ of agents, from the initial state $s_0 \in S$, according to the transition function $\delta$, as constrained by protocol $d$. Moreover, every agent $i$ has imperfect information as regards the state of the system: in any state $s$, $i$ considers possible all states $s'$ that are $i$-indistinguishable from $s$ (Fagin et al. 1995). When every $\sim_i$ is the identity relation, we obtain a standard CGS with perfect information (Alur et al. 2002).

Given a coalition $\Gamma \subseteq Ag$ and a joint action $a \in ACT$, let $a_{\Gamma}$ (resp. $\bar{a}_{\Gamma}$) be the restricted tuple of actions for the agents in $\Gamma$ (resp. $\bar{\Gamma}$) only. Finally, for $a$ and $b$ in $ACT$, $(a_{\Gamma}, \bar{b}_{\bar{\Gamma}})$ denotes the joint action where the actions for the agents in $\Gamma$ (resp. $\bar{\Gamma}$) are taken from $a$ (resp. $\bar{b}$).

A history $h \in S^+$ is a finite (non-empty) sequence of states. The indistinguishability relations are extended to histories in a synchronous, pointwise manner, i.e., histories $h, h' \in S^+$ are indistinguishable for agent $i \in Ag$, or $h \sim_i h'$ iff (i) $|h| = |h'|$ and (ii) for all $j \leq |h|$, $h_j \sim_i h'_j$.

We now introduce the Alternating-time Temporal Logic $ATL^*$ (Alur et al. 2002) to reason about strategic abilities.

**Definition 2 (ATL*).** State ($\varphi$) and path ($\psi$) formulas in $ATL^*$ are defined as follows, where $q \in AP$ and $\Gamma \subseteq Ag$:

\[
\varphi ::= q \mid \neg \varphi \mid \varphi \land \psi \mid \langle \Gamma \rangle \psi \\
\psi ::= \varphi \mid \psi \lor \psi \land \psi \mid X\psi \mid (\psi\psi)\psi
\]

Formulas in $ATL^*$ are all and only the state formulas.

A formula $\langle \Gamma \rangle \psi$ is read as “coalition $\Gamma$ has a strategy to achieve goal $\psi$”. The meaning of linear-time operators next $X$ and until $U$ is standard; whereas operators $[\Gamma]$ release $R$, finally $F$, and globally $G$ can be introduced as usual (Baier and Katoen 2008). In particular, the language of the linear-time logic $LTL$ corresponds to the path formulas in $ATL^*$ built from atoms only. Hereafter we also consider the fragment of $\Gamma$-formulas, i.e., formulas in which the strategic operator $\langle \Gamma \rangle$ ranges only over a given coalition $\Gamma \subseteq Ag$.

We interpret formulas in $ATL^*$ by using uniform strategies (Jamroga and van der Hoek 2004).

**Definition 3 (Strategy).** A uniform strategy with perfect recall for agent $i \in Ag$ is a function $f_i : S^+ \rightarrow Act_i$ such that for all histories $h, h' \in S^+$, (i) $f_i(h) \in d(i, last(h))$; and (ii) if $h \sim_i h'$ then $f_i(h) = f_i(h')$.

By Def. 3, item (i), any strategy for agent $i$ returns actions available to $i$; and by (ii), the same action is returned, whenever histories are indistinguishable for $i$.

Given an iCGS $M$, a path $p \in S^\omega$ of states such that, for every $j \geq 1$, $s_{j+1} = \delta(s_j, \hat{a})$ for some joint action $\hat{a} \in ACT$. Given a joint strategy $F_1 = \{f_i \mid i \in \Gamma\}$, a path $p$ is $F_1$-compatible iff for every $j \geq 1$, $p_{j+1} = \delta(p_j, \hat{a})$ for some joint action $\hat{a} \in ACT$ such that for every $i \in \Gamma$, $a_i = f_i(p_{j+1})$. Let out$(s, F_1)$ be the set of all $F_1$-compatible paths from $s$.

We now interpret $ATL^*$ formulas on iCGS according to a semantics with two truth values: $\mathbb{F}$ and $\mathbb{T}$.

**Definition 4 (Satisfaction).** The two-valued satisfaction relation $\models^2$ for an iCGS $M$, state $s \in S$, path $p \in S^\omega$, atom $q \in AP$, and $ATL^*$ formula $\phi$ is defined as follows (clauses for Boolean connectives are immediate and thus omitted):

\[
\begin{align*}
(M, s) &\models^2 q \iff V(s, q) = tt \\
(M, s) &\models^2 \langle \Gamma \rangle \psi \iff \text{for some joint strategy } F_\Gamma, \\
(M, p) &\models^2 X\psi \iff \text{for all paths } p' \in \text{out}(s, F_\Gamma), (M, p) \models^2 \psi \\
(M, p) &\models^2 \psi \psi' \iff \text{for some } k \geq 1, (M, p_{k+1}) \models^2 \psi' \text{, and} \\
(M, p) &\models^2 \psi \psi' \iff \text{for all } j, 1 \leq j < k \Rightarrow (M, p_{j+1}) \models^2 \psi'
\end{align*}
\]

A formula $\varphi$ is true in $M$, or $M \models^2 \varphi$, iff $\phi(M, s_0) \models^2 \varphi$.

We now state the model checking problem for the classic, two-valued semantics.

**Definition 5 (Model Checking Problem).** Given an iCGS $M$ and a formula $\phi$, determine whether $M \models^2 \phi$.

It is well-known that model checking formulas in $ATL^*$ on iCGS with imperfect information and perfect recall is undecidable in general (Dima and Tiplea 2011). In the rest of the paper we describe a partial decision procedure; but first we illustrate the formal machine with a toy example.

**Example 1.** In Fig. 1 we present a coordination game played by two trains $t_1$ and $t_2$, and a controller $c$ at a junction. Train $t_1$ (resp. $t_2$) and $c$ need to coordinate and select the same direction, left (L) or right (R), to move from the initial state $s_1$. After this first step, the controller can still change her mind. Specifically, she can either change arbitrarily the selection (E), request a new selection to the trains (A), or execute it (O). Further, train $t_1$ cannot observe the
the iCGS in Fig. 1 symmetric we only need to add only on the side of the coordination between idle (I) and full (F) from such abstractions to the original iCGS (Theorem 1). Then, let

\[ \text{Definition 6 (Abstract CGS). Given an iCGS } M = (S, s_0, \{Act_i\}_{i \in Ag}, \{\sim_i\}_{i \in Ag}, \delta, V) \text{ and coalition } \Gamma \subseteq Ag, \text{ the abstraction } M_{\Gamma} = (\langle S \rangle_{\Gamma}, [s_0]_{\Gamma}, \{\text{Act}_i\}_{i \in Ag}, \delta^{\text{may}}_{\Gamma}, \delta^{\text{must}}_{\Gamma}, \delta^{\text{equiv}}_{\Gamma}, V_{\Gamma}^{\text{equiv}}) \text{ is such that:} \]

- \[ S_{\Gamma} = \{[s]_{\Gamma} \mid s \in S\} \text{ is the set of equivalence classes for all states } s \in S, \text{ with initial state } [s_0]_{\Gamma}; \]
- for every \( t, t' \in S_{\Gamma} \) and joint action \( a, \) (i) \( t' \in \delta^{\text{may}}_{\Gamma}(t, a) \) iff \( \delta(s, a) = s' \) for some \( s, s' \in t, t' \); (ii) \( t' \in \delta^{\text{must}}_{\Gamma}(t, a) \) iff for all \( s \in t, \) there is \( s' \in t' \) such that \( \delta(s, a) = s' ; \)
- for \( t \in S_{\Gamma} \) and \( i \in Ag, \) \( \delta^{\text{must}}_{\Gamma}(t, i) = \{ a_i \in \text{Act}_i \mid \text{for all } s \in t, a_i \in \delta(t, s) \}; \) and \( \delta^{\text{equiv}}_{\Gamma}(t, i) = \{ a_i \in \text{Act}_i \mid \delta^{\text{equiv}}(t, (a_i, \bar{a})) \text{ is defined for some } \bar{a} \} ; \)
- for \( v \in \{tt, ff\}, q \in AP, \) and \( t \in S_{\Gamma}, V_{\Gamma}(t, q) = v \) iff \( V(s, q) = v \) for all \( s \in t; \) otherwise, \( V_{\Gamma}(t, q) = \text{null} . \)

Intuitively, \textit{must}-transitions in the abstract CGS are under-approximations of the transitions in the original iCGS; whereas \textit{may}-transitions can be interpreted as over-approximations. The undefined value \textit{null} can be thought of as unknown, unspecified, or inconsistent. This is standard in multi-valued abstraction-based methods (Shoham and Grumberg 2004; Ball and Kupferman 2006) and we do not discuss this further. A truth value \( \tau \) is defined if \( \tau \neq \text{null} . \)

To interpret formulas in ATL\(^*\) on three-valued abstractions, we introduce \textit{must-} and \textit{may}-strategies. In what follows, for \( x = \{\text{may}, \text{must}\} \), \( \bar{x} = \{\text{must}, \text{may}\} \).

\[ \text{Definition 7. For } x \in \{\text{may}, \text{must}\}, \text{ a } x \text{-strategy with perfect recall for agent } i \in Ag \text{ is a function } f_i^x : S^+ \rightarrow \text{Act}_i \text{ such that for every history } h \in S^+, f_i^x(h) \in \delta^{\tau}(i, \text{last}(h)). \]

For \( x \in \{\text{may}, \text{must}\} \) and joint strategy \( F_{\Gamma}^x = \{ f_i^x \mid i \in \Gamma \} \), a path \( p \in S^{\tau} \) is \( F_{\Gamma}^x \)-compatible iff for every \( j \geq 1, p_{j+1} \in \delta^x(p_j, \bar{a}) \) for some joint action \( \bar{a} \) such that for every \( i \in \Gamma, a_i \neq f_i^x(p_{\leq j}) \). As in (Belardinelli et al. 2019), when we consider a \textit{may} (resp. \textit{must}) strategy for coalition \( \Gamma \), we need to consider \textit{must} (resp. \textit{may}) transitions in the model. Then, \( \text{out}(s, F_{\Gamma}^x) \) be the set of all \( F_{\Gamma}^x \)-compatible paths starting from state \( s \).

Finally, we define the three-valued, perfect information semantics for ATL\(^*\) on abstractions as follows.

\[ \text{Definition 8 (Satisfaction). The three-valued satisfaction relation } \models_{\text{33}} \text{ for abstraction } M_{\Gamma}, \text{ state } s \in S, \text{ path } p \in S^{\omega}, \text{ atom } q \in AP, \text{ and } v \in \{tt, ff\}, \text{ and } \Gamma \text{-formula } \phi \text{ is defined as in Table 1. In all other cases the value of } \phi \text{ is } \text{null.} \]

\[ \text{Then, } (M_{\Gamma} \models_{\text{33}} \phi) = \text{tt} \text{ (resp. ff) iff } ((M_{\Gamma}, s_0) \models_{\text{33}} \phi) = \text{tt} \text{ (resp. ff). Otherwise, } (M_{\Gamma} \models_{\text{33}} \phi) = \text{null.} \]

In the clauses for strategy operators \( \langle \Gamma \rangle \), \textit{must}-strategies are used to check for truth, while \textit{may}-strategies appear in the clauses for falsehood.

We now recall the preservation result from abstraction \( M_{\Gamma} \) to the original iCGS M.}

---

1Note that, for simplicity, we considered imperfect information only on the side of the coordination between \( t_1 \) and \( c \). To make the iCGS in Fig. 1 symmetric we only need to add \( s_1 \sim_{t_2} s_6, s_4 \sim_{t_2} s_7 \), and \( s_6 \sim_c s_7 \).
\((M_T, s) \models^3 \varphi = v\) iff \(V_\Gamma(s, q) = v\)
\((M_T, s) \models^3 (\Gamma)\psi) = \text{tt}\) iff for some \(F^\text{must} \) for all \(p \in \text{out}(s, F^\text{must})\), \((M_T, p) \models^3 \psi = \text{tt}\)
\((M_T, s) \models^3 (\Gamma)\psi) = \text{ff}\) iff for every \(F^\text{may} \) for some \(p \in \text{out}(s, F^\text{may})\), \((M_T, p) \models^3 \psi = \text{ff}\)
\((M_T, p) \models^3 \varphi = v\) iff \((M_T, p_1) \models^3 \varphi) = v\)
\((M_T, p) \models^3 X\psi) = \text{v}\) iff \((M_T, p_{\geq 2}) \models^3 \psi) = v\)
\((M_T, p) \models^3 \psi U \psi') = \text{tt}\) iff for some \(k \geq 1\), \((M_T, p_{\geq k}) \models^3 \psi') = \text{tt}\), and for all \(1 \leq j < k \Rightarrow ((M_T, p_{\geq j}) \models^3 \psi) = \text{tt}\)
\((M_T, p) \models^3 \psi U \psi') = \text{ff}\) iff for all \(k \geq 1\), either \((M_T, p_{\geq k}) \models^3 \psi') = \text{ff}\) or for some \(j < k\), \((M_T, p_{\geq j}) \models^3 \psi) = \text{ff}\).

Table 1: The three-valued, perfect information satisfaction relation for \(ATL^*\). Boolean operators are interpreted as in Kleene’s three-valued logic and therefore the corresponding clauses are omitted.

**Theorem 1** ((Belardinelli et al. 2019)). Given an iCGS \(M\), state \(s\), and coalition \(\Gamma \subseteq A_g\), for every \(\Gamma\)-formula \(\varphi\),
\((M_T, s;_\Gamma) \models^3 \varphi = \text{tt} \Rightarrow (M, s) \models^2 \varphi\)
\((M_T, s;_\Gamma) \models^3 \varphi = \text{ff} \Rightarrow (M, s) \models^2 \varphi\)

Further, for abstract CGS we recall the decidability of the corresponding model checking problem.

**Theorem 2** ((Belardinelli et al. 2019)). The model checking problem for \(ATL^*\) on abstract CGS (with perfect information) is \(2\text{EXPTIME}\)-complete.

By combining Theorem 1 and 2 we can outline a method to verify the strategic abilities of agents under imperfect information and perfect recall. Given an iCGS \(M\) and a \(\Gamma\)-formula \(\varphi\) in \(ATL^*\), we first build the abstract, three-valued CGS \(M_T\) according to Def. 6. We can model check \(\varphi\) on \(M_T\), as the corresponding decision problem is decidable by Theorem 2, and then transfer any defined answer to the original iCGS \(M\) in virtue of Theorem 1. Unfortunately, if undefined \((\text{uu})\) is returned, then no conclusive answer can be drawn. In (Belardinelli et al. 2019) a procedure is provided to refine the abstraction in a conservative way. However, this refinement procedure assumes the existence of a “fail-ure” state in which the truth value of the relevant formula is undefined, but no algorithm is given for finding such failure states.

In Sec. 5 we describe such an algorithm, but first we prove some general results on automata for three-valued \(LTL\) in Sec. 4. To conclude, we illustrate the abstraction procedure with our coordination game in Example 1.

**Example 2.** In Fig. 2 we show the abstract CGS obtained from the iCGS in Example 1 by considering formula \(\varphi = (\Gamma)F(l_1 \land \neg B U g)\) for \(\Gamma = \{t_1, c\}\). Specifically, abstraction \(M_T\) includes five abstract states according to the equivalence relation \(\sim^C_{\{t_1, c\}}\). Notice that formula \(\varphi\) is undefined in \(M_T\) due to the undefined value of atom \(l_1\) in state \(a_2\).

### 4 Automata for Three-valued \(LTL\)

In this section we introduce an automata-theoretic approach to the verification of the three-valued linear-time logic \(LTL\). We refer to (Baier and Katoen 2008) for a detailed presentation of \(LTL\); here we observe that the syntax of \(LTL\) can be obtained from Def. 2 by considering as state formulas atoms only (i.e., \(\varphi ::= q\)). Then, the three-valued semantics for \(LTL\) follows from Table 1 by considering only the conditions concerning the operators in the syntax of \(LTL\).

These results will be used in Sec. 5, in procedure \(\text{FailureState}()\) to find failure states. To this end, we build upon the standard, two-valued, automata-theoretic approach to the verification of \(LTL\) (Vardi 1995; Baier and Katoen 2008). We start by recalling that the syntax of \(LTL\) can be obtained by considering the path formulas in Def. 2, where state formulas \(\varphi\) are atoms \(q\) only. Then, the three-valued semantics of \(LTL\) is as in Def. 8, where again state formulas are atoms only.

Now, we recall the definition of generalized non-deterministic Büchi automaton (GNBA).

**Definition 9.** A GNBA is a tuple \(A = (Q, Q_0, \Sigma, \delta, F)\) where (i) \(Q\) is a finite set of states with \(Q_0 \subseteq Q\) as the set of initial states; (ii) \(\Sigma\) is an alphabet; (iii) \(\delta : Q \times \Sigma \rightarrow 2^Q\) is the transition relation; (iv) \(F\) is a (possibly empty) subset of \(2^Q\). The elements in \(F\) are called acceptance sets.

The accepted language \(L(A)\) consists of all infinite words \(w \in \Sigma^\omega\) for which there exists at least one infinite run \(q_0q_1q_2 \ldots \in Q^\omega\) such that for each acceptance set \(F \in F\) there are infinitely many indices \(i\) with \(q_i \in F\).

We now show that for every \(LTL\) formula \(\psi\), there exists an automaton \(A_{\psi, \text{uu}}\) that accepts exactly the infinite paths that evaluate \(\psi\) to undefined \((\text{uu})\). We first provide some definitions necessary for the construction.

**Definition 10** (Closure and Elementarity). The closure \(\text{cl}(\psi)\) of an \(LTL\) formula \(\psi\) is the set consisting of all subformulas \(\phi\) of \(\psi\) as well as their negation \(\neg \phi\).

Let \(B \subseteq \text{cl}(\psi)\). Set \(B\) is consistent w.r.t. propositional logic iff for all \(\psi_1 \land \psi_2, \neg \phi \in \text{cl}(\psi)\): (i) \(\psi_1 \land \psi_2 \in B\) iff \(\psi_1 \in B\) and \(\psi_2 \in B\); (ii) if \(\phi \in B\) then \(\neg \phi \notin B\); (iii) \(\neg \phi \in B\) iff \(\phi \in B\); (iv) if \(tt \in \text{cl}(\psi)\) then \(tt \in B\).
Further, $B$ is locally consistent w.r.t. the until operator iff for all $\psi_i U \psi_j \in cl(\psi)$: (i) if $\psi_j \in B$ then $\psi_i U \psi_j \in B$; (ii) if $\neg (\psi_i U \psi_j) \in B$ then $\neg \psi_j \in B$; (iii) if $\psi_i U \psi_j \in B$ and $\psi_j \not\in B$ then $\psi_i \not\in B$; (iv) if $\neg \psi_i \not\in B$ then $\neg (\psi_i U \psi_j) \not\in B$.

Finally, $B$ is elementary iff it is both consistent and locally consistent.

Notice that, differently from the standard construction for two-valued LTL (Baier and Katoen 2008), here we do not require elementary sets to be maximal, but we do require extra conditions (iii) on consistency, and (ii) and (iv) on local consistency. Hereafter $L_{\text{it}} = AP \cup \{q \mid q \in AP\}$ is the set of literals.

**Definition 11.** Let $\psi$ be a formula in LTL. We define the automaton $A_{\psi,uu} = \langle Q, Q_0, 2^{L_{\text{it}}}, \delta, F \rangle$ as follows:

- $Q$ is the set of all elementary sets $B \subseteq cl(\psi)$ with $Q_0 = \{B \in Q \mid \psi \not\in B \text{ and } \neg \psi \not\in B\}$.
- The transition relation $\delta$ is given by: if $A \not\in B \setminus Q\text{, then } \delta(A, B) = \emptyset$; otherwise $\delta(A, B)$ is the set of all elementary sets $B'$ of formulas such that for every $X_0 \cdot \psi_i U \psi_j \in cl(\psi)$: (i) $X_0 \in B' \iff \psi \in \mathcal{B}';$ (ii) $X_0 \not\in B \iff \psi \in B$; (iii) $\psi_i U \psi_j \in B \iff \psi_j \in B \text{ or, } \psi_i \in B \text{ and } \psi_i U \psi_j \not\in B$; (iv) $\neg (X_0 \cdot \psi_i U \psi_j) \in B \iff \neg \psi_j \in B \text{ and } \neg \psi_i \not\in B$.
- $F = \{F_1 \cdot U, F_2 \cdot U, F_3 \cdot U \mid \psi_i U \psi_j \in \text{cl}(\psi)\}$, where $F_1 \cdot U = \{B \in Q \mid \psi_i \not\in B \text{ and } \psi_j \in B\}$ and $F_2 \cdot U = \{B \in Q \mid \psi_j \in B \text{ and } \psi_i \not\in B\}$.

By Def. 11 the transition relation works as follows: if the automaton reads a set $A$ of literals that do not appear in the state, then the transition is not defined. Otherwise, the automaton checks the transitions enabled w.r.t. the semantics of the LTL operators. Notice that in Def. 11 we need to provide conditions on negated formulas as well, as elementary sets are not necessarily maximal. Moreover, we can define automata $A_{\psi,tt}$ and $A_{\psi,tt}$ by setting $Q_0 = \{B \in Q \mid \psi \in B \text{ and } \neg \psi \not\in B\}$ and $Q_0 = \{B \in Q \mid \psi \not\in B \text{ and } \neg \psi \in B\}$ respectively. For both automata we can prove results similar to Theorem 3 below.

We now prove that the paths that evaluate $\psi$ as undefined are exactly those included in the language of $A_{\psi,uu}$. To prove this result, we make use of the following lemma.

**Lemma 1.** Let run $B = B_1 B_2 \ldots$ in $A_{\psi,uu}$ and path $p = p_1 p_2 \ldots$ in $(2^{L_{\text{it}}})^\omega$ satisfy (i) $B_{i+1} = \delta(B_i, p_i)$, for all $i \geq 0$; and (ii) for all $F \in F$, there exist infinitely many $j \geq 0$ such that $B_j \in F$. Then, for all $\phi$, $\neg \phi \in cl(\psi)$, (a) $\phi \in B_i$ iff $\langle p \mid \phi \rangle = tt$; and (b) $\neg \phi \in B_i$ iff $\langle p \mid \phi \rangle = ff$.

**Proof.** The proof is by mutual induction on the structure of $\phi$, $\neg \phi$, where the induction hypothesis is that for all $i \geq 0$, $\phi \in B_i$ iff $\langle p_{i+1} \ldots \mid \phi \rangle = tt$ and $\neg \phi \in B_i$ iff $\langle p_{i+1} \ldots \mid \phi \rangle = ff$. Due to limited space, we prove only (a), as (b) is proved by induction similarly. Notice that by construction, $\delta(B_i, p_i)$ is defined iff $p_i = B_i \cap Lit$.

**Base case:** The statement for $\phi = q \in AP$ follows directly from the fact that $(p_{i+1} \ldots \mid \phi) = tt$ iff $q \in p_i = B_i \cap Lit$, iff $q \in B_i$.

**Inductive steps:** based on the induction hypothesis that the claim holds for formulas $\phi',$ $\psi_j \in cl(\psi)$, we need to prove that it also holds for $\phi = X \phi,$ $\phi = \neg \phi,$ and $\phi = \psi_i U \psi_j \in cl(\psi)$. For reasons of space we provide details only for $\phi = \psi_i U \psi_j$. Let $p = p_{i+1} \ldots \in (2^{L_{\text{it}}})^\omega$ and $B_i B_{i+1} \ldots \in Q^\omega$ satisfy conditions (i) and (ii), we then show that $\phi \in B_i$ iff $\langle p_{i+1} \ldots \mid \phi \rangle = tt$.

($\Rightarrow$) Suppose that $\psi_i U \psi_j \in B_i$. Since $B_i$ is elementary, then either $\psi_i \in B_i$ or $\psi_j \in B_i$. If $\psi_i \in B_i$, then $\psi_i U \psi_j \in B_i$ for any $i \leq k < j$. By the induction hypothesis applied to $\psi_i$ and $\psi_j$, it follows that $\psi_i U \psi_j \in B_k$ for all $i \leq j < k$. Thus, if $B_i$ is elementary, $\psi_i U \psi_j \in B_i$ as well. Further, by definition of $\delta$, we obtain that $\psi_i U \psi_j \in B_i$ for all $i \leq k < j$. In particular, $\psi_i U \psi_j \in B_i$.

($\Leftarrow$) Suppose that $\psi_i U \psi_j \in B_i$. For every $B_i$, there exist infinitely many $i \geq j$. Further, since $B_i B_{i+1} \ldots$ satisfies constraint (ii), we have $B_i \in F_1 \psi_i U \psi_j$ for infinitely many $i \geq j$. By the induction hypothesis applied to $\psi_i$ and $\psi_j$, it follows $\langle p_{i+1} \ldots \mid \psi_i \rangle = tt$ and $\langle p_{i+1} \ldots \mid \psi_j \rangle = tt$ for all $i \leq j$. Hence, $\psi_i U \psi_j \in B_i$.

Finally, we prove the main theoretical result in this section. Hereafter, $\text{Paths}(\psi, uu)$ is the set of paths $p \in (2^{L_{\text{it}}})^\omega$ such that $\langle p \mid \psi \rangle = uu$.

**Theorem 3.** For every LTL formula $\psi$ there exists a GNL $A_{\psi,uu}$ (given as in Def. 11) s.t. $L(A_{\psi,uu}) = \text{Paths}(\psi, uu)$. Moreover, the size of $A_{\psi,uu}$ is exponential in the size of $\psi$.

**Proof.** Clearly, by Def. 11 the size of $A_{\psi,uu}$ in terms of number of states is exponential in the size of $\psi$.

Then, we prove the set inclusions in both directions.

(1) Let $p = p_1 p_2 \ldots \in \text{Paths}(\psi, uu)$. For $i \geq 0$, define sets $B_i$ of formulas as $\{\phi \in cl(\psi) \mid \langle p_{i+1} \ldots \mid \phi \rangle = tt\} \cup \{\phi \in cl(\psi) \mid \langle p_{i+1} \ldots \mid \phi \rangle = ff\}$. Notice that every $B_i$ is elementary, i.e., $B_i \in Q$. Now, we prove that $B_i B_{i+1} \ldots$ is an accepting run for $p$. Observe that $B_{i+1} \in \delta(B_i, p_i)$, since for all $i > 0$:

- $p_i = B_i \cap Lit$.
- $X \phi \in cl(\psi)$, we have $X \phi \in B_i$ iff $\langle p_{i+1} \ldots \mid X \phi \rangle = tt$, iff $\langle p_{i+1} \ldots \mid \phi \rangle = tt$, iff $\phi \in B_{i+1}$.
- Similarly, $X \phi \in B_i$ iff $\langle p_{i+1} \ldots \mid X \phi \rangle = ff$, iff $\langle p_{i+1} \ldots \mid \phi \rangle = ff$, iff $\phi \in B_{i+1}$.
- For $\psi_i U \psi_j \in cl(\psi)$, we have $\psi_i U \psi_j \in B_i$ iff $\langle p_{i+1} \ldots \mid \psi_i \psi_j \rangle = tt$, iff $\langle p_{i+1} \ldots \mid \psi_i \rangle = tt$, and $\langle p_{i+1} \ldots \mid \psi_j \rangle = tt$, iff $\psi_j \in B_i$ or, $\psi_j \in B_i$ and $\psi_i U \psi_j \in B_{i+1}$.
Similarly, $\neg(\psi_1 U \psi_2) \in B_i$ if $(p_ip_{i+1} \ldots \models \psi_1 U \psi_2) = \text{ff}$ iff $(p_ip_{i+1} \ldots \models \psi_2) = \text{ff}$ and, $(p_ip_{i+1} \ldots \models \psi_1) = \text{ff}$ or $(p_{i+1}p_{i+2} \ldots \models \psi_1 U \psi_2) = \text{ff}$ iff $\neg \psi_2 \in B_i$ and, $\neg \psi_1 \in B_i$ or $\neg(\psi_1 U \psi_2) \in B_{i+1}$.

The above shows that $B_1B_2 \ldots$ is a run in $A_{\psi, uu}$. Now, we need to prove that it is accepting, i.e., for each subformula $\psi_1 U \psi_2 \in cl(B_s)$, $B_s \in F_s$ for infinitely many $i$ and for each subformula $\neg(\psi_1 U \psi_2) \in cl(B_s)$, $B_s \in F_s$ for infinitely many $i$. We prove this point by contradiction. Consider there are finitely many $i$ such that $B_i \notin F_s$ for all $F_s \in F$ or $\psi_2 \notin B_i$. By considering how $B_i$ is constructed, we have that $(p_ip_{i+1} \ldots \models \psi_1 U \psi_2) = \text{tt}$ and $(p_ip_{i+1} \ldots \models \psi_2) = \text{tt}$. In particular, for some $k > i$ we have $(p_k \ldots \models \psi_2) = \text{tt}$. By the definition of $B_k$, it follows that $\psi_2 \in B_k$, and by definition of $F_i$, $B_k \notin F_i$. So, if $B_i \notin F_i$ for infinitely many $i$, then $B_i \notin \psi_2$ for infinitely many $i$, which is a contradiction. The case for subformulas $\neg(\psi_1 U \psi_2) \in cl(B_s)$ is proved similarly.

(2) Let $p = p_{i+1} \ldots \in L(A_{\psi, uu})$, i.e., there is an accepting run $B_1B_2 \ldots$ for $p$ in $A_{\psi, uu}$. By the definition of $A_{\psi, uu}$, we have that $\delta_i(A, i) = \emptyset$ for all pairs $(A, i)$ with $A \neq B \cap Lit$. Then, it follows that $p_i = B_i \cap Lit$ for all $i \geq 0$. Thus, $p = (B_1 \cap Lit)(B_2 \cap Lit) \ldots$ and we need to prove that $((B_1 \cap Lit)(B_2 \cap Lit) \ldots \models \psi) = \text{uu}$. But, this follows by Lemma 1 and the fact that neither $\psi$ nor $\neg \psi$ belong to $B_1$.

We conclude by recalling that to obtain a GNBA accepting all paths that make true (resp. false) a given $LTL$ formula, it suffices to modify the set of initial states to $Q_0^\text{it} = \{B \in Q \mid \psi \in B\}$ (resp. $Q_0^\text{it} = \{B \in Q \mid \neg \psi \in B\}$).

5 Finding Failure States

In Sec. 3 we mentioned that the refinement procedure in (Belardinelli et al. 2019) takes as input a “failure” state $s_f$ in which some subformula of the specification to be checked is undefined. However, no hint is given as to how to find such state $s_f$. Hereafter we tackle this problem, but first we recall the notion of failure state from (Ball and Kupferman 2006).

Definition 12 (Failure State). A state $s$ is a failure state with respect to formula $\varphi$ iff $\langle (M, s) \models \varphi \rangle = \text{uu}$ and, either $\varphi = q \in AP$, or $\varphi = (\langle \Gamma \rangle U \psi)$ and $\langle (M, p) \models \psi \rangle \in \{\text{tt, ff}\}$ for every path $p$ starting from $s$.

Intuitively, $s$ is a failure state with respect to $\varphi$ iff $\langle (M, s) \models \varphi \rangle = \text{uu}$ even though $M$ has definite truth values for all subformulas of $\varphi$ in the relevant states.

To introduce the procedure to find failure states, we first define the product between abstract CGS and GNBA.

Definition 13 (Product). Given an abstract CGS $M = \langle S, \delta_0, A_{\text{Act}}, d^{\text{may}}, d^{\text{must}}, \delta^{\text{may}}, \delta^{\text{must}}, V \rangle$ and a GNBA $A = \langle Q, \Sigma, \delta, Q_0, F \rangle$, their product $M \otimes A = \langle S \times Q, S_0, A_{\text{Act}}, d^{\text{may}}, d^{\text{must}}, \delta^{\text{may}}, \delta^{\text{must}}, V \rangle$ is s.t. for $s, t \in S, q, q' \in Q, q_0 \in Q_0$, and $x \in \{\text{may, must}\}$,

- $S_0 = \{ (s, q) \mid q \in \delta(q_0, V(s)) \}$;
- $d^{\text{ct}}(s, q) = d^a(s)$;
- $\delta^{\text{ct}}(s, q, \alpha) = (t, q')$ iff $d^{\text{ct}}(s, \alpha) = t$ & $q' \in \delta(q, V(t))$;
- $V(s, q) = q$;

The procedure $\text{FailureState}(s, \varphi)$ to find failure states and relevant subformulas is depicted in Algorithm 1: $\text{FailureState}(s, \varphi)$ takes as input a state $s$ and a formula $\varphi$ (with at most one strategic operator) such that $\langle (M, s) \models \varphi \rangle = \text{uu}$ and returns state $s'$ and subformula $\varphi'$ of $\varphi$.

We can check that the procedure $\text{FailureState}(s, \varphi)$ is sound.

Proposition 1. Suppose that $\langle (M, s) \models \varphi \rangle = \text{uu}$. If $\text{FailureState}(s, \varphi) = (s', \varphi')$ then $s'$ is a failure state.

Proof. We prove the soundness of $\text{FailureState}(s, \varphi)$ by induction. Given a model $M$, state $s$, and formula $\varphi$ with no nested strategy operators, the algorithm $\text{FailureState}(s, \varphi)$ starts by considering the base case in which $\varphi$ is an atom (lines 1-2). Here, $\varphi$ is a failure state since the atom $q$ is undefined on it. For the inductive step, we have the following cases. In the case of Boolean operators (lines 3-6), the pro-
procedure propagates over subformulas. To deal with the strategic operator (lines 7-11), the algorithm checks whether there is a path in the product $M \otimes A_{\psi, uu}$ (Def. 13). The product between model $M$ and automaton $A_{\psi, uu}$ accepts all paths in $M$ that make the subformula $\psi$ undefined. If there is no such path, then the procedure returns the current state and formula. Otherwise, procedure $\text{FailurePath}(p, \varphi)$ in Algorithm 2 is called, where $p$ is a path consistent with the product of $M$ and $A_{\psi, uu}$, i.e., $p \in \text{Paths}(M \otimes A_{\psi, uu})$.

In procedure $\text{FailurePath}(p, \varphi)$ the base case for state formulas (lines 1-2) returns to $\text{FailureState}$ by taking as input the first state of path $p$. In lines 3-6 $\text{FailurePath}()$ handles the Boolean operators, and in lines 7-8 solves the next operator in accordance with its semantics. The main point of interest is the until operator in accordance with its semantics. The main point of interest is the until operator (lines 9-20). To prove that the while loop on line 11 terminates, we make use of Lemma 2 below, whereby we can show that the case of the until operator $\Gamma$ in procedure $\text{FailurePath}()$ terminates after a finite number of steps.

**Lemma 2.** Consider an abstract CGS $M$, path $p$, and formula $\varphi = \psi U \psi'$. If $((M, p) \models^3 \varphi) = \text{tt}$ then for some $i \geq 0$, either $((M, p_{2i}) \models^3 \psi) = \text{tt}$ or $((M, p_{2i}) \models^3 \psi') = \text{tt}$.

**Proof.** We prove the lemma by contradiction. Suppose that $((M, p) \models^3 \varphi) = \text{tt}$ and for all $i \geq 0$, for some $v, v' \in \{\text{tt}, \text{ff}\}$, $((M, p_{2i}) \models^3 \psi) = v$ and $((M, p_{2i}) \models^3 \psi') = v'$. We then consider the following cases:

1. If $((M, p_{2i}) \models^3 \psi') = \text{ff}$ (resp. tt) for all $i \geq 0$, then by the three-valued semantics we have $((M, p) \models^3 \varphi) = \text{ff}$ (resp. tt), which is a contradiction.

2. If (1) is not the case, then formula $\psi'$ is sometimes true and sometimes false, but always defined by assumption. Consider the smallest $i \geq 0$ such that $((M, p_{2i}) \models^3 \psi') = \text{tt}$. Then, we can only have one of the following:
   (a) If for all $1 \leq j < i$, $((M, p_{2j}) \models^3 \psi) = \text{tt}$, then by the three-valued semantics we have $((M, p) \models^3 \varphi) = \text{tt}$, which is a contradiction.
   (b) Otherwise, there exists $1 \leq j < i$ such that $((M, p_{2j}) \models^3 \psi) = \text{ff}$. Since we assumed that $i$ is the smallest natural number for which $\psi'$ is true, then for all $1 \leq k < j$ we have $((M, p_{2k}) \models^3 \psi') = \text{ff}$. Hence, by the three-valued semantics it follows that $((M, p) \models^3 \varphi) = \text{ff}$, which is again a contradiction.

In Algorithm 3 we report the high-level iterative model checking procedure. Given an iCGS $M$, state $s$, and $\Gamma$-formula $\varphi$ to check, we first construct the abstract CGS $M_{\Gamma}$ based on $M$ and $\Gamma$. Then, we model check formula $\varphi$ in the abstract state $s_{\Gamma} \supseteq s$, which is decidable by Theorem 2. If a defined truth value is returned, by Theorem 1 we transfer this result to the original model checking problem. On the other hand, if $((M_{\Gamma}, s_{\Gamma}) \models^3 \varphi) = \text{tt}$ then we use a bottom-up procedure (lines 4-13). We start by checking for each state if the innermost formula having a strategic operator is undefined (line 7). If this is the case, we call procedure $\text{FailureState}(s_f, \varphi)$ to find failure state $s_f$ that "makes" the formula $\varphi$ undefined (line 7). Then, in line 9 we call the function $\text{Refinement}(M_{\Gamma}, M, s_f)$ that is a slight variant of the refinement procedure in (Belardinelli et al. 2019) with $s_f$ as input. Intuitively, we look at incoming transitions into $s_f$. For concrete states $s$ and $s'$ in $s_f$, if the $\Gamma$-component of actions ending respectively in $s$ and $s'$ are different, any uniform strategy for $\Gamma$ will visit either $s$ or $s'$ as a result, the abstract state $s_f$ can be split "safely" into an $s$- and an $s'$-component. More precisely, the procedure $\text{Refinement}()$, shown in Algorithm 4, begins by initializing as true the values of a matrix $m$ that stores the relation outlined above between the concrete states in $s_f$ (lines 1-2). Then, the algorithm calls the subroutine $\text{Check}_1(M_{\Gamma}, M, s_f, m)$, shown in Algorithm 5, which updates the values in $m$ by considering the concrete transition function $\delta$ in $M$. In particular, at each iteration $\text{Check}_1()$ considers one predecessor $t_f$ of $s_f$ (line 1). Then, two other loops (lines 2-3) consider pairs of states.

**Algorithm 3 ModelCheckingProcedure($M, s, \varphi, \Gamma$)**

1: $(M_{\Gamma}, s_{\Gamma}) = \text{Abstraction}(M, \Gamma)$
2: if $((M_{\Gamma}, s_{\Gamma}) \models^3 \varphi) = \text{uu}$ then
3: return $((M_{\Gamma}, s_{\Gamma}) \models^3 \varphi)$
4: i = 0; $\varphi_i = \text{InnermostFormula}(\varphi)$
5: while $\varphi_i \neq \varphi$ do
6: for $s_{f_i} \in S_f$ do
7: while $((M_{\Gamma}, s_{f_i}) \models^3 \varphi_i) = \text{uu} \land \text{split} = \text{true}$ do
8: $(s_f, \psi) = \text{FailureState}(s_{f_i}, \varphi_i)$
9: $(M_{\Gamma}, \text{split}) = \text{Refinement}(M_{\Gamma}, M, s_f)$
10: Add($\text{atom}_{\varphi_i}, L(s)$)
11: $M_{\Gamma} = \text{UpdateModel}(M_{\Gamma}, \text{atom}_{\varphi_i})$
12: $\varphi = \text{UpdateFormula}(\varphi, \text{atom}_{\varphi_i})$
13: if $\text{split} = \text{true}$ then
14: $(s_f, \psi) = \text{FailureState}(s_{f_i}, \varphi_i)$
15: $(M_{\Gamma}, \text{split}) = \text{Refinement}(M_{\Gamma}, M, s_f)$
16: if $\text{split} = \text{true}$ then
17: return $(M_{\Gamma}, s_{f_i}) \models^3 \varphi$
18: else
19: return "No refinement is available, $\varphi$ remains uu"
20: end

![Figure 3: The refinement for the CGS in Example 2.](image-url)
Algorithm 4 Refinement($M$, $s_f$)

1: for $s, s' \in s_f$ do
2: \textbf{if} $m[s, s'] = \text{true}$ \textbf{then}
3:   \textbf{else}
4:   \textbf{end if}
5: \textbf{end for}

Algorithm 5 Check$_1$($M$, $s_f$)

1: for $t, t' \in s_f$ do
2: \textbf{if} $m[t, t'] = \text{true}$ \textbf{then}
3: \textbf{end if}
4: \textbf{end for}

Algorithm 6 Check$_2$($M$, $s_f$)

1: for $s, s' \in s_f$ do
2: \textbf{if} $m[s, s'] = \text{true}$ \textbf{then}
3: \textbf{end if}
4: \textbf{end for}

$s$ and $s'$ in the abstract state $s_f$ and pairs of states $t$ and $t'$ in the predecessor $t_f$. If $s$ and $s'$ are indistinguishable for some agent $i \in \Gamma$ and $i$ performs the same action in the transitions from $t$ and $t'$ to $s$ and $s'$ respectively, then we update the value of the corresponding cell in $m$ to false (lines 4-7). The subroutine Check$_1$ carries out the first round of updates on $m$. Further updates in the Refinement() algorithm are performed by the subroutine Check$_2$, shown in Algorithm 6, which considers the “indirect” binding that some concrete states may have in an abstract state. Specifically, given the states $s$ and $s'$ in the abstract state $s_f$ that have true as value in $m$ (lines 2-3), we need to consider the relation that $s$ and $s'$ have with the other states in $s_f$: if the values in $m$ for both states related with some other state $t$ are false, then we update the value of cell $m[s, s']$ to false as well (lines 4-6). Subroutine Check$_2$ is called repeatedly in algorithm Refinement() as long as guard update remains true, i.e., until we have at least an update in each call of the procedure. When update becomes false, we proceed to check whether there is at least an element true in $m$ (line 8). If this is the case, we can split $s_f$. So, we assign the related concrete states $s$ and $s'$ to two different, new abstract states $v$ and $w$ (line 10). Finally, we populate the new abstract states $v$ and $w$ with the other concrete states in the old abstract state $s_f$ (which is removed) according to matrix $m$ (lines 11-15). When the loop in lines 7-9 of the ModelCheckingProcedure() concludes, we update the structure (lines 10-11) and the formula (lines 12) and continue with the new innermost formula (line 13). This part of the procedure (lines 5-13) terminates when we have $\varphi$ with a single, outermost strategic operator. So, we can check formula $\varphi$ on $s_f$. If this formula is undefined, we use a loop (lines 14-16) that calls procedure FailureState($s_f, \varphi$) to find failure state $s_f$ making formula $\varphi$ undefined. Then, in line 16 we call the refinement procedure with $s_f$ as input. When the while loop in lines 14-16 is terminated, we check the truth value of the boolean variable split that is returned by the refinement procedure (line 17). We recall that split is true if and only if the model has been refined. If this is the case, the while loop is exited, as the last refinement step made the formula $\varphi$ defined and then by Theorem 1 and 2 we transfer the defined truth value to the original model checking problem (line 18). On the other hand, if split is false, it was not possible to refine the model in a way to make the formula defined with our procedure (lines 19-20).

Example 3. As an example of the application of procedure FailureState() we consider as input formula $\varphi = \langle a \rangle F (l_1 \land \neg b U g)$ and state $a_1$ in Fig. 2. In Example 2 we observed that $((M, a_1) \models^3 \varphi) = \text{un}$. Since the main operator in $\varphi$ is the strategic modality $\langle a \rangle$, procedure FailureState() goes to line 7. In particular, it constructs the automaton $A_{\varphi, uu}$ that accepts all paths where $\psi = \text{true} U (l_1 \land \neg b U g)$ is undefined. Now, the language of the product between model $M$ and $A_{\varphi, uu}$ is not empty. Hence, the procedure calls FailurePath() with input, for instance, $p = a_1 a_2 a_3 \ldots$, i.e., one of the paths in the product. Since formula $\psi$ has until $U$ as the main operator, the procedure goes to line 9. Now, $((M, p_{22}) \models^3 \psi) = \text{un}$ and we call FailurePath($p_{22}, \psi'$) with $\psi' = l_1 \land \neg b U g$. Observe that the main operator in $\psi'$ is $\land$ and therefore we go to lines 5-6. Here, $((M, p_{22}) \models^3 l_1) = ((M, p_2) \models^3 l_1) = \text{un}$, then we call FailurePath($p_{22}, l_1$), and by lines 1-2, FailureState($p_2, l_1$) finally returns failure state $a_2$ and atom $l_1$. This ends the FailureState() procedure. So, the ModelCheckingProcedure() calls the Refinement() procedure. Here, given $a_2$ as failure state, the Refinement() procedure splits state $a_2$ in new states $a_2'$ with concrete states $s_1$ and $s_2$, and $a_2''$ with concrete states $s_3$ and $s_4$ as in Fig. 3. In the new model formula $\varphi$ is defined (specifically, true) and this ends the whole procedure.

5.1 Complexity Results

We conclude this section by discussing the complexity of our model checking procedure. First, notice that ModelCheckingProcedure() does not necessarily terminate with a defined truth value. Indeed, the ATL* model checking problem in case of imperfect information and per-
fect recall is undecidable in general. This is meant to be a sound, albeit partial, verification algorithm.

**Theorem 4.** ModelCheckingProcedure() terminates in 2EXPTIME.

**Proof.** We analyze in detail Algorithm 3. The procedure of abstraction has to explore a polynomial number of states to generate the abstract model. Since the abstraction procedure returns a CGS with perfect information, the verification of $ATL^*$ formulas can be performed by using the automata-theoretic techniques in (Alur et al. 2002) for instance. This leads to a model checking procedure in 2EXPTIME. The loops in lines 5-13 explore a polynomial number of formulas (while in line 5), a polynomial number states (for in line 6), and a polynomial number of operation on the model (while in line 7). The last loop is shown to be polynomial by variable split that guarantees termination. Further, procedure FailurePath() explores a polynomial number of states and formulas and procedure FailureState() builds a formula automaton by using polynomial space. So, it appears that the refinement procedure (lines 8-9) can be performed in PSPACE. By considering the fact that in lines 14-16 we have again the refinement procedure, we can conclude that the whole complexity of our procedure is in 2EXPTIME.

By Theorem 4 the complexity of our partial model checking procedure is high. However, we claim that it is still better than the general undecidability result.

### 6 Related Work and Conclusions

Recently several approaches to the verification of $ATL^*$ under imperfect information and perfect recall have been put forward. Typically, these contributions assume restrictions either on the syntax or the semantics of the specification language, or develop abstraction and approximation methods. In the first line, decidability results have been proved for hierarchical (Aminof et al. 2012; Berthon et al. 2017) and broadcast systems (Belardinelli et al. 2017b, 2017a). In the second line, techniques to construct syntactic (Bulling and Jamroga 2011) and semantic (Belardinelli et al. 2018) approximations have been investigated. Our contribution falls in the second line, specifically semantic approximations, even though it differs from (Belardinelli et al. 2018), where memory is abstracted to achieve decidability, as here we approximate information instead.

More closely related is a series of works on three-valued abstractions for temporal and strategy logics. An abstraction-refinement framework for $CTL$ on a three-valued semantics was studied in (Shoham and Grumberg 2004), (2007), then extended to the $\mu$-calculus in (Grumberg et al. 2007). As regards $ATL$, three-valued abstractions have also been put forward in (Ball and Kupferman 2006; Lomuscio and Michaliszyn 2014), (2015; 2016). However, there are considerable differences between these approaches and the one here pursued. In fact, their methods focus on settings of perfect information, and (Lomuscio and Michaliszyn 2014),(2015; 2016) considers non-uniform strategies (Raimondi and Lomuscio 2005), whereby the corresponding model checking problem is decidable. Their aim, therefore, is to speed-up the verification task and not, as we do here, to provide a sound, albeit partial, procedure for an undecidable problem. Moreover, we consider the full language $ATL^*$, while the references above only deal with its fragment $ATL$ (Alur et al. 2002).

Regarding the multi-valued automata technique for $LTL$ used in this work, we now discuss the differences w.r.t. (Kupferman and Lustig 2007; Chechik et al. 2001; Bruns and Godefroid 2003). In particular, (Bruns and Godefroid 2003) consider a reduction from multi-valued to two-valued $LTL$, but they do not provide automata-theoretic techniques. On the other hand, (Chechik et al. 2001) present an automata-theoretic approach to general multi-valued $LTL$ following the tableau-based construction in (Gerth et al. 1995). Also (Kupferman and Lustig 2007) is devoted to general multi-valued automata. Specifically, the authors define lattices, deterministic and non-deterministic automata, as well as their extensions to Büchi acceptance conditions. As an application of their theoretical results, they provide an automata construction for multi-valued $LTL$, but only in passing, without a clear explanation of states and transitions. To sum up, differently from (Kupferman and Lustig 2007; Chechik et al. 2001; Bruns and Godefroid 2003), the approach we proposed here modifies minimally the automata-theoretic construction for two-valued $LTL$ in (Baier and Katoen 2008) and extends it to a three-valued interpretation. In this sense we claim that our contribution is novel w.r.t. the current literature. Furthermore, it is not clear how the techniques in (Kupferman and Lustig 2007; Chechik et al. 2001; Bruns and Godefroid 2003) could be used in our construction. As mentioned above, (Bruns and Godefroid 2003) does not really deal with $LTL$. The approach in (Chechik et al. 2001) is more suitable for on-the-fly verification. Finally, in (Kupferman and Lustig 2007) the authors only briefly discuss model checking, and their approach is tailored more generally for multi-valued logics.

Finally, we mentioned that the present work builds upon (Belardinelli et al. 2019), where a three-valued abstraction and refinement procedure for $ATL^*$ is presented. We observed that the refinement procedure takes a failure state as input, but in (Belardinelli et al. 2019) no method was provided to find such failure states. Here we presented such an algorithm that, differently from the state of the art (Ball and Kupferman 2006), operates on the whole $ATL^*$, under imperfect information. To this end, we developed automata-theoretic techniques for $LTL$ in a three-valued semantics, that we deem of independent interest.

As future work we intend to build a toolkit to generate abstractions and refinements automatically. Any such toolkit will require the novel implementation of the three valued semantics here described and will therefore constitute a substantial undertaking. Another interesting question that we would like to explore as future work is to find the “most promising” failure states. It might be possible to find robust heuristics to find good candidates for refinement. Finally, we plan to extend the verification techniques here developed to more expressive languages including Strategy Logic (Chatterjee et al. 2007; Mogavero et al. 2014) in the light of the recent comparison results in (Belardinelli et al. 2019).
Acknowledgments

F. Belardinelli acknowledges the support of ANR JCJC Project SVeDaS (ANR-16-CE40-0021).

References


Jamroga, W., and Dix, J. 2006. Model checking abilities under incomplete information is indeed Δ₂₀⁻complete. In EUMAS’06, 14–15.


