Fixpoint Approximation of Strategic Abilities under Imperfect Information

Wojciech Jamroga
Institute of Computer Science,
Polish Academy of Sciences
w.jamroga@ipipan.waw.pl

Michał Knapik
Institute of Computer Science,
Polish Academy of Sciences
michal.knapik@ipipan.waw.pl

Damian Kurpiewski
Institute of Computer Science,
Polish Academy of Sciences
damian.kurpiewski@ipipan.waw.pl

ABSTRACT

Model checking of strategic ability under imperfect information is known to be hard. In this paper, we propose translations of ATL

variables that provide lower and upper bounds for their truth values, and are cheaper to verify than the original specifications. Most interestingly, the lower approximation is provided by a fixpoint expression that uses a nonstandard variant of the next-step ability operator. We show the correctness of the translations, establish their computational complexity, and validate the approach by experiments with a scalable scenario of Bridge play.

Keywords

strategic ability, alternating-time temporal logic, imperfect information, model checking, alternating mu-calculus

1. INTRODUCTION

There is a growing number of works that study the syntactic and semantic variants of the strategic logic ATL for agents with imperfect information [2]. The contributions are mainly theoretical, and include results concerning the conceptual soundness of a given semantics [29, 19, 1, 21, 10, 15, 2], meta-logical properties [16, 7], and the complexity of model checking [29, 20, 16, 30, 13, 5]. However, there is relatively little research on the use of the logics, in particular on practical algorithms for reasoning and/or verification in scenarios where agents have a limited view of the world.

This is somewhat easy to understand, since model checking of ATL variants with imperfect information has been proved \(\Delta^P_2\)-to-PSPACE-complete for agents playing memoryless strategies [29, 20, 5] and EXPTIME-complete to undecidable for agents with perfect recall of the past [13, 16]. Moreover, the imperfect information semantics of ATL does not admit alternation-free fixpoint characterizations [6, 11, 12], which makes incremental synthesis of strategies impossible, or at least difficult to achieve. Some early attempts at verification of imperfect information strategies made their way into the MCMAS model-checker [25, 28, 23, 24], but the issue was never at the heart of the tool. More dedicated attempts began to emerge only recently [26, 8, 17, 9]. Up until now, experimental results confirm that the initial intuition was right: model checking of strategic modalities for imperfect information is hard, and dealing with it requires innovative algorithms and verification techniques.

In this paper, we propose that in some instances, instead of the exact model checking, it suffices to provide an upper and/or lower bound for the output. The intuition for the upper bound is straightforward: instead of checking existence of an imperfect information strategy, we can look for a perfect information strategy that obtains the same goal. If the latter is false, the former must be false too. Finding a reasonable lower bound is nontrivial, but we construct one by means of a fixpoint expression in alternating epistemic mu-calculus. We begin by showing that the straightforward fixpoint approach does not work. Then, we propose how it can be modified to obtain guaranteed lower bounds. To this end, we alter the next-step operator in such a way that traversing the appropriate epistemic neighborhood is seen as an atomic activity. We show the correctness of the translations, establish their computational complexity, and validate the approach by experiments with some scalable scenarios.

2. VERIFYING STRATEGIC ABILITY

In this section we provide an overview of the relevant variants of ATL. We refer the to [3, 31, 29, 6, 19] for details.

2.1 Models, Strategies, Outcomes

A concurrent epistemic game structure or CEGS is given by \(M = (\text{agt}, S, \text{Props}, V, \text{Act}, d, o, \{\sim_a\ | \ a \in \text{agt}\})\) which includes a nonempty finite set of all agents \(\text{agt} = \{1, \ldots, k\}\), a nonempty set of states \(S\), a set of atomic propositions \(\text{Props}\) and their valuation \(V : \text{Props} \rightarrow 2^{\text{Act}}\), and a nonempty finite set of (atomic) actions \(\text{Act}\). Function \(d : \text{agt} \times S \rightarrow 2^{\text{Act}}\) defines nonempty sets of actions available to agents at each state, and \(o\) is a (deterministic) transition function that assigns the outcome state \(q' = o(q, \alpha_1, \ldots, \alpha_k)\) to state \(q\) and a tuple of actions \(\langle \alpha_1, \ldots, \alpha_k \rangle\) that can be executed by \(\text{agt}\) in \(q\). We write \(d_a(q)\) instead of \(d(a, q)\). Every \(\sim_a \subseteq S \times S\) is an epistemic equivalence relation. The CEGS is assumed to be uniform, in the sense that \(q \sim_a q'\) implies \(d_a(q) = d_a(q')\).

EXAMPLE 1. Consider a very simple voting scenario with two agents: the voter \(v\) and the coercer \(c\). The voter casts a vote for a selected candidate \(i \in \{1, \ldots, n\}\) (action vote\(_i\)). Upon exit from the polling station, the voter can hand in a proof of how she voted to the coercer (action give) or refuse to hand in the proof (action np). The proof may be a certified receipt from the election authorities, a picture of the ballot taken with a smartphone, etc. After that, the coercer can either punish the voter (pun) or not punish (np).


Copyright © 2017, International Foundation for Autonomous Agents and Multiagent Systems (www.ifaamas.org). All rights reserved.
Formally, a state γ denotes states where voter has already voted for candidate $v$. This voting can be represented by a function $v: St \rightarrow Act$ satisfying $s(q) = d_0(q)$ for each $q \in St$. An imperfect information memoryless strategy additionally satisfies that $s(q) = s(q')$ whenever $q \sim_A q'$. Following [29], we refer to the former as ir-strategies, and to the latter as ir-strategies.

A collective x-strategy $s_A$, for $A \subseteq \text{Agnt}$ and $x \in (Ir, ir)$, is a tuple of individual x-strategies, one per agent from A. The set of all such strategies is denoted by $\Sigma_A$. By $s_A[i]$ we denote the strategy of agent $a \in A$ selected from $s_A$.

Given two partial functions $f, f': X \rightarrow Y$, we say that $f'$ extends $f$ (denoted $f \subseteq f'$) if, whenever $f(x)$ is defined, we have $f(x) = f'(x)$. A partial function $s'_a: St \rightarrow Act$ is a partial x-strategy for $a$ if $s'_a$ is extended by some strategy $s_a \in \Sigma_A$. A collective partial x-strategy $s_A$ is a tuple of partial x-strategies, one per agent from $A$.

A path $\lambda = q_0, q_1, \ldots$ is an infinite sequence of states such that there is a transition between each $q_i, q_{i+1}$. We use $\lambda[i]$ to denote the $i$th position on path $\lambda$ (starting from $i = 0$). Function $out(q, s_A)$ returns the set of all paths that can result from the execution of strategy $s_A$ from state $q$. We will sometimes write $out^M(q, s_A)$ instead of $out(q, s_A)$. Moreover, function $out^N(q, s_A) = \bigcup_{i \leq N} \bigcup_{\sim_{q'} q} out(q', s_A)$ collects all the outcome paths that start from states that are indistinguishable from $q$ to at least one agent in $A$.

### 2.2 Alternating-Time Temporal Logic

We use a variant of ATL that explicitly distinguishes between perfect and imperfect information abilities. Formally, the syntax is defined by the following grammar:

$$\varphi ::= p | \neg \varphi | \varphi \land \varphi | \langle\langle A \rangle\rangle_x \varphi | \langle\langle A \rangle\rangle_x G \varphi | \langle\langle A \rangle\rangle_x \varphi U \varphi,$$

where $x \in \{Ir, ir\}$, $p \in \text{Props}$ and $A \subseteq \text{Agnt}$. We read $\angle\langle A \rangle\rangle_x \varphi$ as “A can identify and execute a strategy that enforces $\varphi$,” $G$ as “in the next state,” and $U$ as “until.” $\angle\langle A \rangle\rangle_x \varphi$ can be read as “A might be able to bring about $\varphi$ if allowed to make guesses along the way.” We focus on the kind of ability expressed by $\langle\langle A \rangle\rangle_{ir} \varphi$. The other strategic modality (i.e., $\langle\langle A \rangle\rangle_{Ir}$) will prove useful when approximating $\langle\langle A \rangle\rangle_{ir} \varphi$.

The semantics of $\text{ATL}_{ir}$ can be defined as follows:

- $M, q \models p$ iff $q \in V(p)$,
- $M, q \models \neg \varphi$ iff $M, q \not\models \varphi$,
- $M, q \models \varphi \land \psi$ iff $M, q \models \varphi$ and $M, q \models \psi$,
- $M, q \models \langle\langle A \rangle\rangle_x \varphi$ iff there exists $s_A \in \Sigma_A$ such that for all $\lambda \in out(q, s_A) M, \lambda[1] \models \varphi$,
- $M, q \models \langle\langle A \rangle\rangle_x G \varphi$ iff there exists $s_A \in \Sigma_A$ such that for all $\lambda \in out(q, s_A)$ and $i \in N$ we have $M, \lambda[i] \models \varphi$,
- $M, q \models \langle\langle A \rangle\rangle_x \varphi U \psi$ if there exists $s_A \in \Sigma_A$ such that for all $\lambda \in out(q, s_A)$ there is $i \in N$ for which $M, \lambda[i] \models \varphi$ and $M, \lambda[j] \models \psi$ for all $0 \leq j < i$.

We will often write $\langle\langle A \rangle\rangle_x \varphi$ instead of $\langle\langle A \rangle\rangle_{Ir} \varphi$ to express one-step abilities under imperfect information. Additionally, we define “now or sometime in the future” as $F \varphi \equiv \top U \varphi$.

**Example 2.** Consider model $M_{vote}$ from Example 1. The following formula expresses that the coerker can ensure that the voter will eventually either have voted for candidate $i$ (presumably chosen by the coerker for the voter to vote for) or be punished: $\langle\langle c \rangle\rangle_{Ir} F (\neg \text{pun} \rightarrow v)$. We note that it holds in $M_{vote}, q_0$ for any $i = 1, 2$. A strategy for $c$ that validates the property is $s_c(q_0) = np, s_c(q_4) = s_c(q_2) = s_c(q_6) = q_6$ for $i = 1$, and symmetrically for $i = 2$.

Consequently, the formula $\langle\langle c \rangle\rangle_{Ir} (\neg \text{pun} \land \neg v)$ saying that the voter can avoid voting for candidate $i$ and being punished, is false in $M_{vote}, q_0$ for all $i = 1, 2$.

We refer to the syntactic fragment containing only $\langle\langle A \rangle\rangle_{Ir}$ modality as $\text{ATL}_{ir}$, and to the one containing only $\langle\langle A \rangle\rangle_{Ir}$ modalities as $\text{ATL}_{ir}$.

**Proposition 1.** ([3, 29, 20]). Model checking $\text{ATL}_{ir}$ is $\text{P}$-complete and can be done in time $O(|M| \cdot |\varphi|)$ where $|M|$ is the number of transitions in the model and $|\varphi|$ is the length of the formula.

Model checking $\text{ATL}_{ir}$ is $\Delta^P_2$-complete wrt $|M|$ and $|\varphi|$.

**Remark 2.** The semantics of $\langle\langle A \rangle\rangle_{ir} \gamma$ encodes the notion of “subjective” ability [29, 21]: the agents must have a successful strategy from all the states that they consider possible when the system is in state $q$. Then, they know that the strategy indeed obtains $\gamma$. The alternative notion of “objective” ability [7] requires a winning strategy from state $q$ alone. We focus on the subjective interpretation, as it is more standard in ATL and more relevant in game solving (think of a card game, such as poker or bridge: the challenge is to find a strategy that wins for all possible hands of the opponents).

Note that if $[q]_{Ir} = \{q\}$ and $\gamma$ contains no nested strategic modalities, then the subjective and objective semantics of $\langle\langle A \rangle\rangle_{ir} \gamma$ at $q$ coincide. Moreover, model checking $\langle\langle A \rangle\rangle_{ir} p_1 U p_2$
and $[A]_p \mathbf{G}_p$ in $M,q$ according to the objective semantics can be easily reduced to the subjective case by adding a spurious initial state $q'$, with transitions to all states in $[q]$, controlled by a “dummy” agent outside $A$ [27].

### 2.3 Reasoning about Knowledge

Having indistinguishability relations in the models, we can interpret knowledge modalities $K_a$ in the standard way:

- $M,q \models K_a \varphi$ iff $M,q' \models \varphi$ for all $q$ such that $q \sim_a q'$.

The semantics of “everybody knows” ($E_a$) and common knowledge ($C_a$) is defined analogously by assuming the relation $\sim_a = \bigcup_{a \in A} \sim_a$ to aggregate individual uncertainty in $A$, and $\sim_a^C = \text{the transitive closure of } \sim_a^C$. Additionally, we take $\sim_a^C$ to be the minimal reflexive relation. We also use $[q]_R = \{ q' | q R q' \}$ to denote the image of $q$ wrt relation $R$.

**Example 3.** The following formulae hold in $M_{vote, q_0}$ for any $i = 1, 2$ by virtue of strategy $s_i$ presented in Example 2:

- $\langle \langle q \rangle \rangle_i \mathbf{G} (\neg K_{Ir,vote} \rightarrow \mathbf{p})$: The coercer has a strategy so that, eventually, the voter is punished unless the coercer has learnt that the voter voted as instructed;

- $\langle \langle q \rangle \rangle_i \mathbf{F} (K_{Ir,vote} \rightarrow \neg \mathbf{p})$: Moreover, the coercer can guarantee that if he learns that the voter obeyed, then the voter will not be punished.

### 2.4 Alternating Epistemic Mu-Calculus

It is well known that the modalities in $\mathbf{ATL}_a$ have simple fixpoint characterizations [3], and hence $\mathbf{ATL}_a$ can be embedded in a variant of $\mu$-calculus with $\langle \langle A \rangle \rangle_x X$ as the basic modality. At the same time, the analogous variant of $\mu$-calculus for imperfect information has incomparable expressive power to $\mathbf{ATL}_a$ [6], which suggests that, under imperfect information, $\mathbf{ATL}$ and fixpoint specifications provide different views of strategic ability.

Formally, alternating epistemic $\mu$-calculus ($\mathbf{AE}_\mu \mathbf{C}$) takes the next-time fragment of $\mathbf{ATL}_a$, possibly with epistemic modalities, and adds the least fixpoint operator $\mu$. The greatest fixpoint operator $\nu$ is defined as dual. Let $\text{Vars}$ be a set of second-order variables ranging over $2^\mathbb{N}$. The language of $\mathbf{AE}_\mu \mathbf{C}$ is defined by the following grammar:

$$\varphi ::= p \mid Z \mid \neg \varphi \mid \varphi \lor \psi \mid (A) \varphi \mid \mu Z(\varphi) \mid K_a,$$

where $p \in \text{Props}$, $Z \in \text{Vars}$, $a \in \text{Agnt}$, $A \subseteq \text{Agnt}$, and the formulae are $Z$-positive, i.e., each free occurrence of $Z$ is in the scope of an even number of negations. We define $\nu Z(\varphi(Z)) \equiv \neg \mu \varphi(\neg Z)$.

A formula of $\mathbf{AE}_\mu \mathbf{C}$ is alternation-free if in its negation normal form it contains no occurrences of $\nu$ (resp. $\mu$) on any syntactic path from an occurrence of $\mu Z$ (resp. $\nu Z$) to a bound occurrence of $Z$.

The denotational semantics of $\mu$-$\mathbf{AE}_\mu \mathbf{C}$ (i.e., the alternation-free fragment of $\mathbf{AE}_\mu \mathbf{C}$) assigns to each formula $\varphi$ of $\mathbf{AE}_\mu \mathbf{C}$ a set of states $[\varphi]_M^\nu$, where $\varphi$ is true under the valuation $V \in \text{Vals}$:

- $[p]_M^\nu = V(p)$,
- $[Z]_M^\nu = V(Z)$,
- $[\neg \varphi]_M^\nu = \neg [\varphi]_M^\nu$,
- $[\varphi \lor \psi]_M^\nu = [\varphi]_M^\nu \lor [\psi]_M^\nu$,
- $[(A) \varphi]_M^\nu = \{ q \in St \mid \exists s_A \in A \forall \lambda \in \text{out}_{M,q}(s_A) \lambda[1] \in [\varphi]_M^\nu \}$,
- $[\mu Z(\varphi)]_M^\nu = \{ q \in St \mid [\varphi]_{M,q}^{\nu Z,=q} \subseteq Q \}$,
- $[K_a \varphi]_M^\nu = \{ q \in St \mid \forall q' \sim_a q \text{ implies } q \in [\varphi]_M^\nu \}$.

If $\varphi$ contains no free variables, then its validity does not depend on $V$, and we write $M,q \models \varphi$ instead of $\varphi \in [\varphi]_M^\nu$.

**Example 4.** Consider the $\mathbf{AE}_\mu \mathbf{C}$ formula $\mu Z.(\neg (\neg \mathbf{p} \rightarrow \mathbf{vote}) \lor \mathbf{c} Q)$, i.e., the “naive” fixpoint translation of the formula $\langle \langle 0 \rangle \rangle \mathbf{F} (\neg \mathbf{p} \rightarrow \mathbf{vote})$ from Example 2. The fixpoint computation produces the whole set of states $St$, Thus, in particular, $M_{vote, q_0} \models \mu Z.(\neg (\neg \mathbf{p} \rightarrow \mathbf{vote}) \lor \mathbf{c} Q)$.

**Proposition 3.** [6] Model checking $\mathbf{af}-\mathbf{AE}_\mu \mathbf{C}$ with strategic modalities for up to 2 agents is P-complete and can be done in time $O(|\varphi| \cdot |\varphi|)$ where $|\varphi|$ is the size of the largest equivalence class among $\sim_1, \ldots, \sim_k$, and $|\varphi|$ is the length of the formula.

For coalitions of size at least 3, the problem is between NP and $\Delta_2^P$ wrt $|\varphi|$.

Thus, alternation-free alternating epistemic $\mu$-calculus can be an attractive alternative to $\mathbf{ATL}_a$ from the complexity point of view. Unfortunately, formulae of $\mathbf{ATL}_a$ admit no universal translations to $\mathbf{af}-\mathbf{AE}_\mu \mathbf{C}$. Formally, it was proved in [6, Proposition 6] that $\mathbf{af}-\mathbf{AE}_\mu \mathbf{C}$ does not cover the expressive power of $\mathbf{ATL}_a$. The proof uses formulae of type $\langle \langle a \rangle \rangle \mathbf{F} \varphi$, but it is easy to construct an analogous argument for $\langle \langle a \rangle \rangle \mathbf{G} \varphi$. In consequence, long-term strategic modalities of $\mathbf{ATL}_a$ do not have alternation-free fixpoint characterizations in terms of the next-step strategic modalities $\langle A \rangle$. A similar result was proved for $\mathbf{ATL}_m$ in [11, Theorem 11].

### 3. LOWER BOUNDS FOR ABILITIES

The complexity of $\mathbf{AE}_\mu \mathbf{C}$ model checking seems more attractive than that of $\mathbf{ATL}_a$. Unfortunately, the expressivity results cited in Section 2.4 imply that there is no simple fixpoint translation which captures exactly the meaning of $\mathbf{ATL}_a$ operators. It might be possible, however, to come up with a translation $tr$ that provides a lower bound of the actual strategic abilities, i.e., such that $M,q \models tr(\langle A \rangle \langle \gamma \rangle) \Rightarrow M,q \models \langle A \rangle \langle \gamma \rangle$. In other words, a translation which can only reduce, but never enhance the abilities of the coalition.

We begin by investigating the “naive” fixpoint translation that mimics the one for $\mathbf{ATL}_a$, and show that it works in some cases, but not in general. Then, we propose how to alter the semantics of the nexttime modality so that a general lower bound can be obtained. We focus first on reachability goals, expressed by formulae $\langle A \rangle \mathbf{F} \varphi$, and then move on to the other modalities.

### 3.1 Trying It Simple for Reachability Goals

We assume from now on that $\varphi$ is a formula of $\mathbf{ATL}_a$, $M$ is a CEGS, and $q$ is a state in $M$ (unless explicitly stated otherwise). We start with the simplest translation, analogous to that of [3]: $tr(\langle A \rangle \langle \gamma \rangle \mathbf{F} \varphi) = \mu Z.(\varphi \lor (A) Z)$. Unfortunately, this translation provides neither a lower nor an upper bound. For the former, use model $M_0$ in Figure 2, and observe that $M_0,q_0 \models \mu Z.(p \lor (1) Z)$ but $M_0,q_0 \not\models \langle \langle 1 \rangle \rangle \mathbf{F} p$. For the latter, take model $M$ in [6, Figure 1], and observe that $M,q_0 \models \langle \langle 1 \rangle \rangle \mathbf{F} p$ but $M,q_0 \not\models \mu Z.(p \lor (1) Z)$.

**Proposition 4.** $M,q \models \mu Z.(\varphi \lor (A) Z)$ does not imply $M,q \models \langle A \rangle \mathbf{F} \varphi$. The converse implication does not hold either.
Consider now a slightly stronger fixpoint specification:
\[ tr_2(⟨(A)⟩_{i=0} F φ) = μ Z.(E_A φ ∨ (A) Z). \]
This new translation works to an extent, as the following proposition shows.

**Proposition 5.**

1. \( M, q \models μ Z.(E_A φ ∨ (A) Z) \) iff \( M, q \models ⟨(A)⟩_{i=0} F φ \);
2. If \( |A| = 1 \), then \( M, q \models μ Z.(E_A φ ∨ (A) Z) \) implies \( M, q \models ⟨(A)⟩_{i=0} F φ \), but the converse does not hold;\(^1\)
3. If \( |A| > 1 \), then \( M, q \models μ Z.(E_A φ ∨ (A) Z) \) does not imply \( M, q \models ⟨(A)⟩_{i=0} F φ \), and vice versa.

**Proof.** **Case 1:** follows from the fact that the empty coalition the ir–reachability is equivalent to the IR–reachability, which in turn has a fixpoint characterization.

**Case 2:** Let us assume that \( A = \{a\} \) for some \( a \in A \).t. We define the sequence \( \{F_i\}_{i∈N} \) of \( αFpC \) formulae s.t. \( F_0 = K_φ \) and \( F_{i+1} = F_0 ∨ (a) F_i \), for all \( i ≥ 0 \). From Kleene fixed-point theorem we have \( [μ Z.(K φ ∨ (a) Z)] = \bigcup_{i=0}^∞ [F_i] \), and \( \{[F_i]\}_{i∈N} \) is a non-decreasing monotone sequence of subsets of \( S_t \). Now, we prove that for each \( j ∈ N \) there exists a partial strategy \( s_{a}^j \) s.t. \( dom(s_{a}^j) = [F_j] \), \( \forall q ∈ dom(s_{a}^j) \) \( λ ∈ out^j(q, s_{a}^j) \) \( \exists k ≤ j \) \( λ[k] = φ \), and \( s_{a}^j ⊆ s_{a}^{j+1} \). The proof is by induction on \( j \). We constructively build \( s_{a}^{j+1} \) from \( s_{a}^j \) for each \( j ∈ N \). The base case is trivial. For the inductive step, first observe that for each \( j ∈ N \) if \( q ∈ [F_j] \), then \( [q]_0 ⊆ [F_j] \). As \( α_0 \) is an equivalence relation, for each \( q ∈ [F_{j+1}] \) either \( [q]_0 ⊆ [F_j] \) or \( [q]_0 ⊆ [F_{j+1}] \ exclusive \( [F_j] \). In the first case we put \( s_{a}^{j+1}(q) = s_{a}^j(q) \). In the second case, we know that there exists a strategy \( s_{a}^j \) s.t. \( \forall λ ∈ out^j(q, s_{a}^j) \) \( λ[1] ∈ [F_j] \). We thus put \( s_{a}^{j+1}(q') = s_{a}^j(q') \) for all \( q' ∈ [q]_0 \), which concludes the inductive proof.

We finally define the partial strategy \( s_{a}^j = \bigcup_{j∈N} s_{a}^j \). For each \( q ∈ S_t \) s.t. \( M, q \models μ Z.(K φ ∨ (a) Z) \), either \( M, q \models φ \), or \( φ \) is reached along each path consistent with any extension of \( s_{a} \) to a full strategy.

For the converse implication, take model \( M \) in [6, Figure 1], and observe that \( M, q_0 \models ⟨(1)⟩_{i=0} F p \) but \( M, q_0 \not\models μ Z.(Kp ∨ (1) Z) \).

**Case 3:** Consider the CEGS \( M_1 \) presented in Figure 3. We assume that \( d_1(q) = \{a, b\} \) and \( d_2(q) = \{x, y\} \), for \( q ∈ \{q_1, q_2, q_3, q_4\} \). In the remaining states the protocols allow only one action. For clarity, we omit from the figure the transitions leaving the states \( q_1, q_2, q_3, \) and \( q_4 \), leading to state sink. Assume now \( φ ≡ p \). Note that \( M, q_0 \models μ Z.(E_{\{1, 2\}} φ ∨ (1, 2) Z) \) and \( M, q_0 \not\models ⟨(1, 2)⟩_{i=0} F φ \). For larger coalitions \( A \), we extend the model with a sufficient number of spurious (idle) agents.

For the other direction, use the counterexample from Case 2, extended with appropriately many spurious agents. □

As Propositions 4 and 5 show, translation \( tr_2 \) provides lower bounds for \( ATL_{ir} \) verification only in a limited number of instances. Also, the bound is rather loose, as the following example demonstrates.

**Example 5.** Consider the single-agent CEGS \( M_2 \) presented in Figure 4A. The sole available strategy, in which agent 1 selects always action \( a \), enforces eventually reaching \( p \), i.e., \( M_2, q_0 \models ⟨(1)⟩_{i=0} F p \). On the other hand, \( M_2, q_0 \not\models μ Z.(Kp ∨ (1) Z) \). This is because the next-step operator in \( ATL_{ir} \) requires reaching \( p \) simultaneously from all the states indistinguishable from \( q_0 \), whereas \( p \) is reached from \( q_0, q_1 \) in one and two steps, respectively.

### 3.2 Steadfast Next Step Operator

To obtain a tighter lower bound, and one that works universally, we introduce a new modality. \( (A)^* \) can be seen as a semantic variant of the next-step ability operator \( (A) \) where:

(i) agents in \( A \) look for a short-term strategy that succeeds from the “common knowledge” neighborhood of the initial state (rather than in the “everybody knows” neighborhood), and

(ii) they are allowed to “steadfastly” pursue their goal in a variable number of steps within the indistinguishability class. In this section, we propose the semantics of \( (A)^* \) and show how to revise the lower bound. Some additional insights are provided in Section 4.

We begin by defining the auxiliary function \( Reach \) so that \( q ∈ Reach_M(s_A, Q, φ) \) collects all \( q \in Q \) such that all the paths executing \( s_A \) from \( q \) eventually reach \( φ \) without leaving \( Q \), except possibly for the last step:

\[ Reach_M(s_A, Q, φ) = \{ q \in Q \mid \forall λ ∈ out(q, s_A) \] \( \exists \gamma ∈ Q \) \( (\exists j ≤ i [λ j] ∈ Q) \) \]

The **steadfast next-step operator** \( (A)^* \) is defined as follows:
Proof. The proof is similar to the proof of Proposition 5. As previously, we define a sequence \{F_j\} \subseteq \af-\mathbf{AP}_\mathbf{C}
 for all \(j \geq 0\). We also use a sequence \{H_j\}_{j \in \mathbb{N}} with \(H_j = (\langle S \rangle)^{F_j}\). From Kleene fixed-point theorem we have \([\mu \lambda\varphi. (E_A \varphi \land (\langle S \rangle)^{\varphi})] = \bigcup_{n \in \mathbb{N}} \varphi\), with the following result.

Proposition 6. If \(M, q \models \mu \lambda\varphi. (E_A \varphi \land (\langle S \rangle)^{\varphi})\), then \(M, q \models \langle \langle S \rangle \rangle_{\mathbf{AP}} \varphi\). The converse does not universally hold.

Proof. The proof is by induction on \(j\). In the base case of \(H_0 = (\langle S \rangle)^{F_0}\) observe that if \(q \in [H_0]\) then there exists a strategy \(s_{q0}^0\) with \(\text{dom}(s_{q0}^0) = [q]_{\sim} \subseteq s_{q0}^0 \cup s_{q0}^0\). Thus, \(s_{q0}^0\) is an equivalence relation, we have for each state \(q\), if \(j \in \mathbb{N}\) such that \([q]_{\sim} \cap [H_j]\) \neq \emptyset, then \([q]_{\sim} \subseteq [H_j]\).

We prove that for each \(j \in \mathbb{N}\) there exists a partial strategy \(s_{q0}^j\) s.t. \(\text{dom}(s_{q0}^j) = [H_j]\), \(q \in [H_j]\), \(\forall q \in \text{dom}(s_{q0}^j) \in \text{out}^\mathbb{U}(q, s_{q0}^j) \exists k \in \mathbb{N}\). The converse does not universally hold.

4. DISCUSSION & PROPERTIES

Theorem 7 shows that \(tr_3(\varphi)\) provides a correct lower bound of the value of \(\varphi\) for all formulae of \(\mathbf{ATL}_\mathbf{a}\). In this section, we discuss the tightness of the approximation from the theoretical point of view. An empirical evaluation will be presented in Section 6.

4.1 Comparing \(tr_3\) and \(tr_4\) for Reachability Goals

Translation \(tr_3\) updates \(tr_2\) by replacing the standard next-step ability operator (A) with the "steadfast next-step ability" (A)*. The difference between (A) and (A)* is twofold. First, (A) looks for a winning strategy in the "everybody knows" neighborhood of a given state (i.e., [q]G), whereas (A)* looks at the "common knowledge" neighborhood (i.e., [q]G). Secondly, (A)* allows to "zig-zag" across [q]G until a state satisfying \(\varphi\) is found.

Actually, the first change would suffice to provide a universally correct lower bound for \(\mathbf{ATL}_\mathbf{a}\). The second update makes it more useful in models where agents may not see the occurrence of some action, such as \(M_2\) of Figure 4A. To see this formally, we show that \(tr_3\) provides a strictly tighter approximation than \(tr_2\) on singleton coalitions:

Proposition 8. For \(A = \{a\}\), if \(M, q \models \mu \lambda\varphi. (K_a \varphi \lor (a)^{\varphi})\), then \(M, q \models \mu \lambda\varphi. (K_a \varphi \lor (a)^{\varphi})\). The converse does not universally hold.

Proof. It suffices to observe that \(M, q \models (a)^{\varphi}\) implies \(M, q \models (a)^{\varphi}\), for any \(\varphi\) in \(\af-\mathbf{AP}_\mathbf{C}\). Note that this is true only for single-agent coalitions. For the converse, notice that in CEGS \(M_2\) from Figure 4A we have \(M_2, q_0 \models \mu \lambda\varphi. (K_1 \varphi \lor (1)^{\varphi})\) and \(M_2, q_0 \not\models \mu \lambda\varphi. (K_1 \varphi \lor (1)^{\varphi})\).

On the other hand, if agent a always sees whenever an action occurs, then \(tr_3\) and \(tr_2\) coincide for a’s abilities. Formally, let us call CEGS \(M\) lockstep for a if, whenever there is a transition from q to q’ in M, we have \(q \not\equiv q’\). The following is straightforward.

Proposition 9. If \(M\) is lockstep for a, then \(M, q \models (a)^{\varphi}\) iff \(M, q \models (a)^{\varphi}\). In consequence, \(M, q \models tr_2(\langle a \rangle \mathbf{F} \varphi)\) iff \(M, q \models tr_3(\langle a \rangle \mathbf{F} \varphi)\).
4.2 When is the Lower Bound Tight?

An interesting question is: what is the subclass of CEGS’s for which \( tr_3 \) is tight, i.e., the answer given by the approximation is exact? We address the question only partially here. In fact, we characterize a subclass of CEGS’s for which \( tr_3 \) is certainly not tight, by the necessary condition below.

Let \( \gamma \equiv G \phi \) or \( \gamma \equiv \psi_1 \cup \psi_2 \) for some \( \psi_1, \psi_2 \in ATL_2 \). We say that strategy \( s_A \in \Sigma_A^\gamma \) is winning for \( \gamma \) from \( q \) if it obtains \( \gamma \) for all paths in \( out^A(q, s_A) \). Moreover, for such \( s_A \), let \( RR(q, s_A, \gamma) \) be the relevant reachable states of \( s_A \) in the context of \( \gamma \), defined as follows: \( RR(q, s_A, \phi) = \) the set of states that occur anywhere in \( out^A(q, s_A) \); \( RR(q, s_A, \psi_1 \cup \psi_2) \) is the set of states that occur anywhere in \( out^A(q, s_A) \) before the first occurrence of \( \psi_2 \).

**Proposition 10.** Let \( M \) be a CEGS, \( q \in St_M \), and \( \phi \equiv \langle A \rangle |_{tr} \gamma \). Furthermore, suppose that \( \phi \) and \( tr_3(\phi) \) are either both true or both false in \( M, q \). Then:

1. either no strategy \( s_A \in \Sigma^\gamma_A \) is winning for \( \gamma \) from \( q \), or
2. there is a strategy \( s_A \in \Sigma^\gamma_A \) which is winning for \( \gamma \) from every \( q' \in RR(q, s_A, \gamma) \).

Conversely, the approximation is not tight if there are winning strategies, but each of them reaches a intermediate state \( q' \) from which no winning substrategy can be computed. This can only happen if some states in \( [q'] \cup [s_A] \) are not reachable by \( s_A \). In consequence, the agents in \( A \) forget relevant information that comes alone from the fact that they are executing \( s_A \). We will use Proposition 10 in Section 6 to show that the few benchmarks existing in the literature are not amenable to our approximations.

## 5. APPROXIMATION SEMANTICS FOR ATL

Note that \( M, q \models \langle A \rangle |_{tr} \gamma \) always implies \( M, q \models E_A \langle A \rangle |_{tr} \gamma \). Based on this, and the lower bounds established in Theorem 7, we propose the upper approximation \( TR \) and the upper approximation \( TR \) for \( ATL_2 \) as follows:

\[
\begin{align*}
tr(p) &= p, \\
\tr(\neg \phi) &= \neg \tr(\phi), \\
\tr(\phi \land \psi) &= \tr(\phi) \land \tr(\psi), \\
\tr(\langle A \rangle \phi) &= \tr(\phi), \\
\tr(\langle A \rangle \psi) &= \psi Z(C\tr(\phi) \land \langle A \rangle^* Z), \\
\tr(\langle A \rangle \psi_1 \cup \psi_2) &= \mu Z(E\tr(\phi) \lor (C\tr(\phi) \land \langle A \rangle^* Z)).
\end{align*}
\]

Approximation of abilities under perfect recall. In this paper, we focus on approximating abilities based on memoryless strategies. Approximations might be equally useful for \( ATL_R \) (i.e., the variant of \( ATL \) using uniform perfect recall strategies); we simply begin with the problem that is easier in its exact form. The high intractability of \( ATL_R \) model checking suggests that a substantial extension will be needed to come up with satisfactory approximations.

We also observe that the benchmark in Section 6.2 is a model of perfect recall, i.e., the states explicitly encode the agents’ memory of their past observations. In consequence, the memoryless and perfect recall semantics of \( ATL \) coincide. The experimental results suggest that, for such models, verification of perfect recall abilities can be much improved by using the approximations proposed here.

### 6. EXPERIMENTAL EVALUATION

Theorem 11 and Proposition 12 validate the approximations we use in the theoretical results by looking at how well the approximations work in practice. We address two issues: the performance and the accuracy of the approximations.

### 6.1 Existing Benchmarks

The only publicly available tool that provides verification of \( ATL \) with imperfect information is MCMA [25, 28, 23, 24]. We note, however, that imperfect information strategies are not really at the heart of the model-checker, the focus being on verification of CTLK and \( ATL \) with perfect information strategies. More dedicated attempts produced so far only experimental algorithms, with preliminary performance results reported in [26, 8, 17, 9, 27]. Because of that, there are few benchmarks for model checking \( ATL_2 \), and few experiments have actually been conducted.

The classes of models typically used to estimate the performance of \( ATL_2 \) model checking are \( TianJi \) [28, 8] and \( Castles \) [26]. The properties to be verified are usually reachability properties, saying that Tian Ji can achieve a win over the king (in \( TianJi \)), or that a given coalition of workers can defeat another castle (for \( Castles \)). We observe that both \( TianJi \) and \( Castles \) do not satisfy the necessary condition in Proposition 10. This is because the states of the model do not encode some relevant information about the actions that have been already played by the coalition. Thus, even one
step before winning the game, the players take into account also some (possibly losing) states that couldn’t be reached by the strategy that they are executing.

This means that the AEϕ/C approximations, proposed in this paper, are not useful for TianJi and Castles. It also means that the benchmarks arguably do not capture realistic scenarios. We usually do not want to assume agents to forget their own actions from a few steps back. In the remainder, we propose several new benchmarks that can be used to evaluate our approximation scheme.

Finally, we note that most experiments reported in the literature use very simple input formulae (no nested strategic modalities; singleton coalitions or groups of agents with identical indistinguishability relations). As the results show, verification of such formulae is complex enough – see the performance of exact model checking in the rest of this section.

6.2 Verifying the Simple Voting Scenario

For the first benchmark, we adapt the simple voting scenario from Example 1. The model consists of k + 1 agents (k voters v1, . . . , vk, 1 cooperator c). The module of voter vi implements the transition structure from Figure 1, with three modifications. First, the voter can at any state execute the “idle” action wait (this is needed to ensure uniformity of the resulting CEGS). In consequence, synchronous voting as well as interleaving of votes is allowed. Secondly, in states q3, . . . , q6, the cooperator’s action np (“no punishment”) leads to an additional final state (q′ 2, . . . , q′ 10), labeled accordingly. Thirdly, the old and new leaves in the structure (i.e., q7, . . . , q10, q′ 2, . . . , q′ 10) are labeled with an additional atomic proposition finish.

As specifications, we want to use the properties saying that: (i) the cooperator can force the voter to vote for candidate 1 or else the voter is punished, and (ii) the voter cannot avoid voting for candidate 1 and being punished (cf. Example 2). Note, however, that the model used for the experiments is an unconstrained product of the voter modules. Thus, it includes also paths that were absent in the CEGS Mvote from Example 1 (in particular, ones where a voter executes wait all the time). To deal with this, we modify the specifications from Example 2 so that they discard such paths:

1. \( \varphi_1 \equiv \langle c \rangle_0 F (finish \land \neg pun \rightarrow vote, 1) \) which always holds in the voting scenario,
2. \( \varphi_2 \equiv \langle v \rangle_0 F (finish \land \neg pun \land \neg vote, 1) \) which is always false.

The results of experiments for \( \varphi_1 \) are shown in Figure 5, and for \( \varphi_2 \) in Figure 6. The columns present the following information: parameter of the model (the number of voters k), size of the state space (#states), generation time for models (tg), and time and output of verification (tevr, result) for model checking the lower approximation TR(\( \varphi \)), and similarly for the upper approximation TR(\( \varphi \)); the percentage of cases where the bounds have matched (match), and the total running time of the exact ATL\( \text{ir} \) model checking for \( \varphi \) (tg+tv). The running times are given in seconds. Timeout indicates that the process did not terminate in 48 hours (!).

The computation of the lower and upper approximations was done with a straightforward implementation (in Python 3) of the fixpoint model checking algorithm for AEϕ/C and ATL\( \text{ir} \), respectively. We used the explicit representation of models, and the algorithms were not optimized in any way. The exact ATL\( \text{ir} \) model checking was done with MCMAS.

6.3 Bridge Endplay

We use bridge play scenarios of a type often considered in bridge handbooks and magazines. The task is to find a winning strategy for the declarer, usually depicted at the South position (S), in the k-endplay of the game, see Figure 7 for an example. The deck consists of 4n cards in total (n in each suit)\(^2\) and the initial state captures each player holding k cards in their hand, after having played n − k cards. This way we obtain a family of models, parameterized by the possible values of (n,k). A NoTrump contract is being played; the declarer wins if she takes more than k/2 tricks in the endplay.

The players’ cards are played sequentially (clockwise). S plays first at the beginning of the game. Each next trick (i.e., the set of four played cards, one per player) is opened by the player who won the latest trick. The declarer handles her own cards and the ones of the dummy (N). The opponents (W and E) handle their own hands each. The cards of the dummy are visible to everybody; the other hands are only seen by their owners. Each player remembers the cards that have already been played, including the ones that were used up before the initial state of the k-endplay. That is, the local state of a player contains: the current hand of the player, the current hand of the dummy, the cards from the deck that were already used up in the previous tricks, the status

\(^2\)In real bridge, n = 13.
of the current trick, i.e., the sequence of pairs \((\text{player}, \text{card})\) for the cards already played within the trick (alternatively, the sequence of cards already played within the trick, plus who started the trick); and the current score (which team has won how many tricks so far).

We observe the following properties of the model. First, it is turn-based (with the “idle” action \(\text{wait} \) that players use when another player is laying down a card). Secondly, players have imperfect information, since they cannot infer (except for the last round) the hands of the other players. The missing information is relevant: anybody who has ever played bridge or poker knows how much the limited knowledge of the opponents’ hands decreases one’s chances of winning the game. Thirdly, this is a model of imperfect recall. The players do not remember in which order the cards have been played so far, and who had what cards;\(^3\) formally: the model is a DAG and not a tree as there are histories \(h \not\approx_h h'\) such that \(\text{last}(h) \sim_a \text{last}(h')\). Finally, the model is lockstep (everybody sees when a transition happens), and thus \(\text{tr}_2\) and \(\text{tr}_3\) coincide on singleton coalitions.

\(\text{tr}_2\) and \(\text{tr}_3\) coincide on singleton coalitions.

Figure 8: Experimental results: solving endplay in bridge

The results of the experiments for formula \(\varphi \equiv \langle\langle S\rangle\rangle \text{W} \text{win}\) are shown in Figure 8. The columns present the following information: parameters of the model \((n, k)\), size of the state space \((\#\text{states})\), generation time for models (\(\text{tgen}\)), time and output of verification (\(\text{tverif} \), \%true) for model checking the lower approximation \(\text{tr}_2(\varphi)\), and similarly for the upper approximation \(\text{TR}(\varphi)\); the percentage of cases where the bounds have matched (match), and the total running time of the exact \text{ATL}^\text{at} model checking for \(\varphi\) (\(\text{tg}+\text{tv}\)). The times are given in seconds, except where indicated.

The experiments were run in the same environment as for the voting scenario in Section 6.2. Again, we ran the experiments for up to 48h per instance. The results in each row are averaged over 20 randomly generated instances, except for \((*)\) where only 1 instance was used.

**Discussion of results.** In the experiments, our approximations offered a dramatic speedup. Exact model checking of \(\varphi\) was infeasible except for the simplest models (hundreds of states), even with an optimized symbolic model checker like MCMAS. In contrast, the bounds were verified for models up to millions of states. Moreover, our approximations obtained an astonishing level of accuracy: the bounds matched in 100% of the analyzed instances, thus producing fully conclusive output. This was partly because we only considered endplays in relatively small decks. The gap grows for decks of more than 20 cards (we verified that by hand on selected instances from bridge literature).

\(^3\)This reflects the capabilities of middle-level bridge players: they usually remember what has been played, but not in which order and by whom. Advanced players remember also who played what, and masters remember the whole history of the play.

**7. CONCLUSIONS**

Verification of strategic properties in scenarios with imperfect information is difficult, both theoretically and in practice. In this paper we suggest that model checking of logics like \text{ATL}^\text{at} can be in some cases obtained by computing an under- and an overapproximation of the \text{ATL}^\text{at} specification, and comparing if the bounds match. In a way, our proposal is similar to the idea of may/must abstraction [14, 4, 22], only in our case the approximations are obtained by transforming formulae rather than models.

We propose such approximations, prove their correctness, and show that, for singleton coalitions, their values can be computed in polynomial time. We also propose novel benchmarks for experimental validation. Finally, we report very promising experimental results, in both performance and accuracy of the output. To our best knowledge, this is the first successful attempt at approximating strategic abilities under imperfect information by means of fixpoint methods.

**Acknowledgements.** The authors acknowledge the support of the National Centre for Research and Development (NCBR), Poland, under the PolLux project VoteVerif (POL-LUX-IV/1/2016).
REFERENCES


