Strategy logic with simple goals: Tractable reasoning about strategies
Francesco Belardinelli, Wojciech Jamroga, Vadim Malvone, Aniello Murano

To cite this version:

HAL Id: hal-02377403
https://hal.science/hal-02377403
Submitted on 23 Nov 2019

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.
Strategy Logic with Simple Goals: Tractable Reasoning about Strategies

Francesco Belardinelli\textsuperscript{1,2}, Wojciech Jamroga\textsuperscript{3,4}, Damian Kurpiewski\textsuperscript{3}, Vadim Malvone\textsuperscript{2} and Aniello Murano\textsuperscript{5}

\textsuperscript{1} Imperial College London, UK
\textsuperscript{2} Université d’Evry, France
\textsuperscript{3} Institute of Computer Science, Polish Academy of Sciences, Warsaw, Poland
\textsuperscript{4} Interdisciplinary Centre for Security, Reliability, and Trust, SnT, University of Luxembourg
\textsuperscript{5} Università degli studi di Napoli “Federico II”, Italy

francesco.belardinelli@imperial.ac.uk, w.jamroga@ipipan.waw.pl, d.kurpiewski@ipipan.waw.pl, vadim.malvone@univ-evry.fr, murano@na.infn.it

Abstract

In this paper we introduce Strategy Logic with Simple Goals (SL[SG]), a fragment of Strategy Logic that strictly extends Alternating-time Temporal Logic ATL by introducing arbitrary quantification over the agents’ strategies. Our motivation comes from game-theoretic applications, such as expressing Stackelberg equilibria in games, coercion in voting protocols, as well as module checking for simple goals. We prove that model checking SL[SG] is \(\mathbb{P}\)-complete, the same as ATL. Thus, the extra expressive power comes at no computational cost as far as verification is concerned.

1 Introduction

Formal verification of multi-agent systems (MAS) has been a thriving area of investigation in the last two decades, which has led to a wealth of logics to specify the temporal, epistemic, and strategic capabilities of agents, including Alternating-time Temporal Logic [Alur et al., 2002], possibly enriched with strategy contexts [Laroussinie and Markey, 2015], irrevocable strategies [Ágotnes et al., 2007], or operators for individual and group knowledge [Jamroga and van der Hoek, 2004; Hoek and Wooldridge, 2003]; Coalition Logic [Pauly, 2002]; and Strategy Logic [Chatterjee et al., 2010; Mogavero et al., 2014].Besides theoretical results, some model checking tools have also been developed [Alur et al., 2001; Cimatti et al., 2002; Kacprzak et al., 2008; Huang and van der Meyden, 2014; Lomuscio et al., 2015; Cermák et al., 2015; Cermák et al., 2018].

The verification of MAS generates a tension between two conflicting demands. On the one hand, we need an expressive language to capture subtle temporal, epistemic, and game-theoretic notions such as reachability, common and distributed knowledge, and solution concepts in games. On the other hand, we need formalisms with a tractable model checking problem, for which efficient verification algorithms can be implemented. The same tension appears in the seminal paper [Alur et al., 2002] that introduced Alternating-time Temporal Logic. Two variants of the logic are presented: ATL* is rather expressive, but with \(2\text{EXPTIME}\) verification complexity. Its fragment ATL has less expressivity, but allows to model check strategic properties in polynomial time. This leads to a nice balance of expressivity and computational complexity – indeed, ATL model checking is supported by a number of tools [Alur et al., 2001; Kacprzak et al., 2008; Lomuscio et al., 2015]. The question is: can we use a language that is more expressive than ATL, and still retains its polynomial-time complexity of model checking? We answer the question affirmatively in this paper.

Our starting point is Strategy Logic (SL) [Mogavero et al., 2014], an expressive extension of \(\text{ATL}^*\) that allows to characterize sophisticated game-theoretic solution concepts, e.g., Nash equilibria, dominant strategies, subgame-perfect equilibria, etc. Unfortunately, its model checking complexity is non-elementary, and hence highly unlikely to enable efficient implementation. Even restricted variants of SL, such as SL with memoryless strategies [Cermák et al., 2014], non-elementary, and hence highly unlikely to enable efficient implementation. Even restricted variants of SL, such as SL with memoryless strategies [Cermák et al., 2014], do not help much, as their model checking problems range from \(2\text{EXPTIME}\)-complete to non-elementary [Mogavero et al., 2014; Bouyer et al., 2015; Gardy et al., 2018].

We then propose to take one-goal SL, and further restrict goals to simple LTL formulas of type \(\exists \phi \left( \text{next } \phi \right)\), \(\phi \cup \phi'\) (\(\phi \text{ until } \phi'\)), and \(\phi_R \phi'\) (\(\phi \text{ releases } \phi'\)), similarly to the restriction of \(\text{ATL}^*\) to ATL in [Alur et al., 2002]. The result, Strategy Logic with simple goals (SL[SG]), can also be seen as the extension of ATL to arbitrary quantification on the agents’ strategies. We use SL[SG] to capture Stackelberg equilibria in games, express coercion-resistance in voting protocols [Tabatabaei et al., 2016], and characterize module checking for simple goals [Jamroga and Murano, 2014]. These are all relevant agent-related concepts, that cannot be expressed in ATL. Hence, SL[SG] is provably more expressive than ATL. Most importantly, we show that reasoning about SL[SG] is no more complex as ATL, as it also enjoys polynomial-time model checking. This is achieved by generalising the fixed-point procedures for ATL model checking. In consequence, Strategy Logic with simple goals offers an arguably better balance between expressivity and complexity than ATL. We further show the advantages by means of a case study, based on a simple voting scenario.
2 Logics for Strategies

We begin by recalling Strategy Logic (SL) [Mogavero et al., 2014], as well as its relevant syntactic fragments. Then, we provide an interpretation to these languages by means of concurrent game structures (CGS), as it is customary.

**Strategy Logic.** Fix an infinite set $AP$ of atomic propositions (atoms), a finite set $Ag$ of agents, and an infinite set $Var$ of variables $x_0, x_1, \ldots$ for strategies. *Formulas in Strategy Logic* are defined as follows, for $p \in AP$, $x \in Var$, $a \in Ag$:

$$
\varphi ::= p \mid \neg \varphi \mid \varphi \land \varphi \mid X \varphi \mid \varphi U \varphi \mid \exists x \varphi \mid (x, a) \varphi
$$

Next $X$ and until $U$ are temporal operators. The strategy quantifier $\exists x$ reads as “for some strategy $x, \ldots$”, and the binding operator $(x, a)$ intuitively means that “by using strategy $x$, agent $a$ can achieve ...”. Hereafter we use standard abbreviations, e.g., $\forall x \varphi$ for $\neg \exists x \neg \varphi$, as well as temporal operators $\text{releases} R$, $\text{globally} G$, and $\text{eventually} F$. We assume the standard definition of set $\text{free}(\varphi)$ of free agents and variables appearing in a formula $\varphi$ [Mogavero et al., 2014]. Moreover, $\text{shr}(x, \varphi)$ denotes the set of agents that use strategy $x$ in the evaluation of formula $\varphi$.

**Models.** Given sets $Ag$ of agents and $AP$ of atoms, a concurrent game structure (CGS) is a tuple $G = \langle S, s_0, \{Act_a\}_{a \in Ag}, \tau, L \rangle$ such that: $S$ is a non-empty finite set of states and $s_0 \in S$ is the initial state of $G$; for every agent $a \in Ag$, $Act_a$ is a finite set of non-empty actions; and $ACT = \prod_{a \in Ag} \text{Act}_a$ is the set of joint actions; $\tau : S \times ACT \rightarrow S$ is the transition function; finally, $L : S \rightarrow 2^{AP}$ is the labelling. A path is a (finite or infinite) sequence $\pi \in S^* \cup S^\omega$ such that for every $j \geq 1$, $\pi_{j+1} = \tau(\pi_j, \bar{a}_j)$ for some joint action $\bar{a}_j \in ACT$. We distinguish between finite paths, or histories, and infinite paths, or computations. For a path $\pi$ and $j \geq 1$, $\pi_{\leq j}$ denotes the initial history of length $j$, and last($h$) is last element in history $h$.

**Strategies.** A memoryfull strategy for an agent $a \in Ag$, or $a$-strategy, is a function $\sigma : S^+ \rightarrow ACT_a$. The set of all strategies, for all agents, is denoted as $\Sigma(G)$. A joint strategy $\sigma_{Ag}$ assigns a strategy for every agent $a \in Ag$. By the above definitions, given a strategy $\sigma$ for an agent $a$, a different agent $b$ is such that the range of strategy $\sigma$ is a subset of $ACT_b$ (i.e., $\text{ran}(\sigma) \subseteq ACT_b$), then intuitively also agent $b$ can use strategy $\sigma$. Finally, an assignment is a function $\chi : Var \cup Ag \rightarrow \Sigma(G)$ such that for every agent $a \in Ag$, $\chi(a)$ is a strategy for $a$. For $z \in Var \cup Ag$ and $\sigma \in \Sigma(G)$, the variant $\chi^z_\sigma$ is the assignment that maps $z$ to $\sigma$ and coincides with $\chi$ on all other variables and agents. Given a history $h \in S^+$, an assignment $\chi$ defines a unique computation $\lambda(h, \chi) = h \langle (\chi(a))_{a \in Ag} s_1 \mid (\chi(a))_{a \in Ag} s_2 \mid \ldots \rangle$ starting with $h$ and consistent with $\chi$.

**Semantics.** Given a CGS $G$, we inductively define the satisfaction relation $(G, h, \chi) \models \varphi$ where $h$ is a history, $\varphi$ is a formula, and $\chi$ is an assignment such that for every $x \in Var$, $\chi(x)$ is a strategy for all agents in $\text{shr}(x, \varphi)$ (we omit the standard clauses for Boolean operators):

$$(G, h, \chi) \models p \iff p \in L(\text{last}(h))$$

$$(G, h, \chi) \models X \varphi \iff (G, \lambda(h, \chi)_{\leq |h|+1}, \chi) \models \varphi$$

![Figure 1: A simple model of voting and coercion](image)

(We will formally introduce both notions in the next section.)
3 Strategy Logic with Simple Goals

Inspired by the relationship between the Alternating-time Temporal Logics ATL and ATL*, we introduce a novel restriction of SL[1G] to “simple” goals.

3.1 The Formal Language

We begin with some terminology. A binding prefix over sets $A \subseteq Ag$ of agents and $V \subseteq Var$ of variables is a finite sequence $b \in \{ (a, x) \mid a \in A \text{ and } x \in V \}^{\mid A \mid}$ of length $|b| = |A|$, such that every agent $a \in A$ occurs exactly once in $b$. In contrast, the same variable $x \in V$ can occur several times in $b$, i.e., intuitively, the same strategy denoted by $x$ can be used by several agents in $A$. A quantification prefix over a set $V \subseteq Var$ of variables is a finite sequence $\phi \in \{ \exists x, \forall x \mid x \in V \}^{\mid V \mid}$ of length $|\phi| = |V|$ such that every variable $x \in V$ occurs exactly once in $\phi$. Then, $\text{Qnt}(V) \subset \{ \exists x, \forall x \mid x \in V \}^{\mid V \mid}$ and $\text{Bnd}(A) \subset \{ (a, x) \mid a \in A \text{ and } x \in Var \}^{\mid A \mid}$ denote the sets of all quantification and binding prefixes over variables in $V$ and $A$.

Definition 2 (SL[SG]) The formulas in Strategy Logic with simple goals are defined in BNF as follows, where $b \in \text{Bnd}(Ag)$, $\phi \in \text{Qnt}(\text{free}(\phi))$:

$$\phi ::= p \mid \neg \phi \mid \phi \land \phi \mid \phi \Box \phi \mid \phi (\phi \lor \phi)$$

By Def. 2, SL[SG] restricts SL[1G] to simple ATL objectives of type $X \phi$, $\phi U \phi$, and $\phi R \phi'$ (the latter can be introduced by using $U$ and dual quantification). We also consider the fragment SL$^\rightarrow [SG]$, for which Def. 2 is restricted to binding prefixes $b$ where every variable occurs at most once. That is, one cannot bind different agents with the same strategy. Further, we define fragments SL$^\rightarrow [SG]$, for which quantification prefixes $\phi$ are restricted to at most $n$ alternations of existential and universal quantifiers. Finally, we introduce fragments SL$^\rightarrow n [SG]$ as the intersection of SL$^\rightarrow [SG]$ and each SL$^\rightarrow [SG]$.

Example 3 Clearly, the formula in Example 1 is a formula of SL[$SG$, more precisely of SL$^\rightarrow 2 [SG$].

In Fig. 2 we summarize the main syntactic inclusions between our fragments. We also remark that ATL can be thought of as the fragment of SL[SG] in which the clauses for formulas of type $\phi X \phi$ and $\phi \Box (\phi \lor \phi)$ are restricted to quantification prefixes $\phi$ with at most one alternation, as well as being binding prefixes $b$ where every variable occurs at most once. The coronet notation for the syntax is also given in the figure.

3.2 Expressiveness

An important observation that formally justifies our study is that SL[SG] is less expressive than ATL. That is, SL[SG] allows to characterize all the properties expressible in ATL, but not vice versa. We also show that SL[SG], SL$^\rightarrow [SG]$, and SL$^\rightarrow n [SG]$ all differ with respect to their expressiveness.

Consider two logical systems $L_1$ and $L_2$. $L_1$ is at least as expressive as $L_2$ (written $L_2 \preceq L_1$) if every formula of $L_2$ can be equivalently translated to some formula of $L_1$. Moreover, $L_1$ is at least as distinguishing as $L_2$ ($L_2 \preceq_d L_1$) if every pair of models that can be distinguished by a formula of $L_2$ can also be distinguished by some formula of $L_1$.

Figure 2: Syntactic inclusions for fragments of SL

Theorem 4 SL$^\rightarrow [SG]$ (and thus also SL[SG]) has strictly greater expressive and distinguishing power than ATL.

Proof. The embedding of ATL into SL$^\rightarrow [SG]$ is straightforward. To show that ATL does not cover the distinguishing power (and hence also the expressive power) of SL$^\rightarrow [SG]$, we can use the counterexample from the proof of [Mogavero et al., 2014, Theorem 4.3].

Interestingly, we also have that for every $n \in \mathbb{N}$, SL$^\rightarrow n [SG]$ is strictly more expressive than SL$^\rightarrow n [SG]$. That is, being able to bind the same strategy to different agents strictly increases the expressive power of Strategy Logic with simple goals.

Figure 3: Models $M_1$ and $M_2$ in the proof of Theorem 5

Theorem 5 For every $n \geq 0$, we have:

1. $\text{SL}^\rightarrow_n [SG] \preceq \text{SL}^\rightarrow_n [SG]$, and therefore $\text{SL}^\rightarrow_n [SG] \preceq_d \text{SL}^\rightarrow_n [SG]$;
2. $\text{SL}^\rightarrow [SG] \preceq \text{SL}^\rightarrow [SG]$, and therefore $\text{SL}^\rightarrow [SG] \preceq_d \text{SL}^\rightarrow [SG]$.

Proof. We adapt the proof of [Belardinelli et al., 2018, Lemma 32.1]. Clearly, $\text{SL}^\rightarrow_n [SG] \preceq \text{SL}^\rightarrow_n [SG]$ and therefore also $\text{SL}^\rightarrow_n [SG] \preceq_d \text{SL}^\rightarrow_n [SG]$. Since $\text{SL}_0 [SG] \preceq_d \text{SL}_n [SG]$ and $\text{SL}^\rightarrow_n [SG] \preceq_d \text{SL}^\rightarrow [SG]$, to show that $\text{SL}_0 [SG] \preceq_d \text{SL}^\rightarrow [SG]$, we prove that:

$$\text{SL}_0 [SG] \preceq_d \text{SL}^\rightarrow [SG]$$

To do so, we provide two models that satisfy the same formulas in SL$^\rightarrow [SG]$ but are distinguished by a formula of SL$^\rightarrow [SG]$. Consider the CGS’s $M_1$ and $M_2$ with $Ag = \{ 1, 2 \}$, depicted in Fig. 3. Since SL$^\rightarrow [SG]$ can be shown invariant under renaming of action labels, both models satisfy the same formulas of SL$^\rightarrow [SG]$. However, $M_1$ satisfies the SL$^\rightarrow [SG]$-formula $\exists x (x, 1) \land (x, 2) X p$, while $M_2$ does not. Thus, SL$^\rightarrow [SG] \preceq_d \text{SL}^\rightarrow [SG]$ and therefore also $\text{SL}_n [SG] \preceq_d \text{SL}_n [SG]$ and $\text{SL}_n [SG] \preceq_d \text{SL}^\rightarrow [SG]$ for every $n \in \mathbb{N}$. 
As regards 2., clearly, \( SL[S\eta] \preceq_c SL[\eta] \), and therefore \( SL[S\eta] \preceq_d SL[\eta] \). Since \( SL_0[S\eta] \preceq_d SL[\eta] \) and \( SL_1[S\eta] \preceq_d SL[\eta] \) (item (1)), then \( SL[\eta] \preceq_d SL[S\eta] \). So, \( SL[S\eta] \preceq_c SL[\eta] \), and thus \( SL[\eta] \preceq_d SL[S\eta] \). □

The discussion above highlights logics \( SL_0[S\eta] \) and \( SL_1[S\eta] \) as variants of \( CTL = SL_0[S\eta] \) and \( ATL = SL_1[S\eta] \) that allow for strategy sharing. Such extensions have not been considered in the literature. Nonetheless, by Theorem 5, they are strictly more expressive than CTL and ATL respectively.

### 3.3 Motivating Examples and Applications

Strategy Logic enables to address complex interaction between strategies of different players, who may pursue adversarial, collaborative, or uncorrelated goals. Also, the goals can be based on sophisticated temporal patterns. This expressivity comes at the expense of tractability, or even decidability of decision problems for SL. At the other end, we have ATL where only a single alternation is allowed in strategy quantification. Moreover, the agents’ goals can only be phrased in terms of reachability. This results in a somewhat rigid specification language, albeit one with a big advantage: the model checking problem becomes tractable.

With \( SL[S\eta] \), we extend ATL by allowing arbitrarily many alternations of strategy quantifiers. We argue that the extra expressivity is useful, i.e., it allows for specification of relevant properties of agent interaction in multi-agent systems. To this end, we propose a number of motivating examples.

**Example 6 (Stackelberg equilibria)** Stackelberg games concern scenarios where one player (the leader) exposes his strategy first, and the other player (the follower) adapts to that strategy by choosing her best response. For example, coercion in voting often has a Stackelberg structure: the coercer must lay out his coercion strategy in a believable way to force the voter to vote as requested. A desirable property in voting systems is that the voter can resist coercion, i.e., for every strategy of the coercer \((c)\) there exists a response of the voter \((v)\) such that for every run of the environment \((e)\) the voter will have voted as she intended without being punished [Tabatabaie et al., 2016]. This is captured by the following formula of \( SL[S\eta] \):

\[
\forall x_e \exists x_v \forall x_e ((x_e, c)(x_v, v) F(voted_{x,v} \land \neg\text{punished}).
\]

**Example 7 (Coercion in voting, ctld.)** A more realistic model of coercion allows the coercer to split his strategy into a public and a private part. We can simulate that by splitting the model of the coercer into two agents: cpub and cprv, each responsible for different parts of the coercion strategy. Moreover, some voting protocols include a process that can add decoy votes after the election to deceive the coercer. This can be incorporated into our specification of coercion-resistance as follows:

\[
\forall x_e \exists x_e \forall x_e \exists x_e ((x_{c1}, cpub)(x_e, v)(x_{c2}, cprv) \quad (x_{d}, d)(x_e, e) F({\text{voted}}_{x,d} \land \neg\text{punished})).
\]

This specification can intuitively be read as: for every public strategy of the coercer \((x_{c1},)\), there exists a response by the voter \((x_{c2})\) such that, no matter what the coercer does privately \((x_{c2})\), the decoy process \(d\) can use decoy votes to make sure that the voter votes as she likes without being punished.

**Example 8 (Module checking for strategic abilities)** The problem of module checking asks, for an open system embedded in a nondeterministic environment, whether the correctness specification holds for every possible strategy of the environment\(^2\). It has been proved that module checking of either temporal or strategic specifications cannot be expressed in ATL [Jamroga and Murano, 2014]. The ability of an autonomous taxi \((t)\) to serve an unbounded stream of customers \((e)\) so that no accident occurs, regardless of what the agents \(a_1, \ldots, a_k\) do, can be captured as

\[
\forall x_e \exists x_{a1} \forall x_{a2} (x_e, e)(x_{a1}, t)(x_{a1}, a_1)(x_{a2}, a_k) G \neg\text{crash}.
\]

A careful reader may notice that the results in Section 3.2 indeed apply to the above specifications. That is, the formulas in Examples 6–8 cannot be equivalently expressed in ATL.

### 4 Model Checking

Given a CGS \(G\) and a formula \(\phi\) in language \(L\), the model checking problem w.r.t. \(L\) consists in determining whether \(G \models \phi\). In this section we study model checking for Strategy Logic with simple goals and its fragments. These results are essential for applications of \(SL[S\eta]\) to the verification of multi-agent systems, including the specifications in Examples 6–8. Our main theoretical result is that verification of \(SL[S\eta]\) is tractable with respect to the size of the CGS (i.e., the number of its transitions) and the length of the formula.

We first prove that the fixed-point characterisation of ATL carry over to \(SL[S\eta]\).

**Proposition 9** The following formula is a validity in \(SL[S\eta]\):

\[
\forall \phi(\phi(\varphi_1 \cup \varphi_2)) \leftrightarrow \varphi_2 \lor (\varphi_1 \land \phi(X \phi(\varphi(\varphi_1 \cup \varphi_2)))
\]

**Proof.** The proof makes use of the preimage function \(\text{Pre}()\) that is defined in Algorithm 2 and will be described in detail in the proof of Theorem 10. As regards the implication from left to right, suppose that \(\phi(\varphi(\varphi_1 \cup \varphi_2))\) holds in some state \(s\). Then, if \(\varphi_2\) does not hold in \(s\), \(\varphi_1\) does. Moreover, consider set \(Y \subseteq S\) such that \(s \in \text{Pre}(\varphi_1 \lor \varphi, Y, t)\), i.e., the successors of \(s\) that are consistent with the quantification and binding prefixes. Since \((G, s) \models \phi(\varphi_1 \cup \varphi_2)\) and \((G, s) \not\models \varphi_2\), for every \(s' \in Y\), we have \((G, s') \models \phi(\varphi_1 \cup \varphi_2)\): indeed every strategy \(\sigma_i\) witnessing an existential quantifier \(Q_i\) in \(\varphi\) at \(s\), also witnesses \(Q_i\) in history \(s'\). In particular, \((G, s') \models \phi(\varphi(\varphi_1 \cup \varphi_2))\), and finally, \((G, s) \models \phi(X \phi(\varphi(\varphi_1 \cup \varphi_2)))\) by the way \(s'\) was chosen.

As for the implication from right to left, if \(\varphi_2\) holds at state \(s\), then \(\phi(\varphi(\varphi_1 \cup \varphi_2))\) is also the case. On the other hand, suppose that \((G, s) \models \phi(\varphi_1 \cup \varphi_2)\). In particular, every existential quantifier \(Q_i\) in \(\varphi\) is witnessed in \(s\) by some strategy \(\sigma_{i'}\), and in every “successor” state \(s' \in Y\), \(Q_i\) is witnessed in history \(s''\) by some (possibly different) strategy \(\sigma_{i''}\). Then, define strategies \(\sigma_i''(s)\) such that \(\sigma_i''(s,h) = \sigma_i''(h)\) for all \(h \in S^+\). In particular, each \(\sigma_{i''}\) witnesses \(Q_i\) at \(s\), that is, \((G, s) \models \phi(\varphi(\varphi_1 \cup \varphi_2))\). Observe the essential use of perfect recall in the construction of strategy \(\sigma_{i''}\) from \(\sigma_i\) and \(\sigma_{i'}\).

\(^2\)Admittedly, to represent module checking properly we need CGSs with non-deterministic transitions. Nonetheless, the characterization of module checking in \(SL[S\eta]\) would remain the same.
Recall that Model checking Algorithm 1 SL the ATL S primitive operations: The procedure is inspired by the standard model checking end procedure Union, intersection, difference, and inclusion test for By using Prop. 9 we can prove the main theoretical result. As for the upper bound, Algorithm 1 shows a procedure for •

3m

s∈τ

=1

ϕ

et al.

2002

Algorithm 1 SL[SG] Model Checking

procedure MODELchecking(G, Ő)
for all Ő′ in S咄(Œ) do
  case Ő′ = p: [Õ′] := Reg(p);
  case Ő′ = ϑ: [Õ′] := S \ {ϑ};
  case Ő′ = Ő1 ∧ Ő2: [Õ′] := [Õ1] ∩ [Õ2];
  case Ő′ = ϑ X Ő: [Õ′] := Pre(Õ, ϑ, Ő, e);
  case Ő′ = ϑ(ϑ U Ő2): Y := 0; Z := [Õ2];
  while Z Y do
    Y := Y U Z;
    Z := Pre(Õ, ϑ, Y, e) \ [Õ1];
  end while
  [Õ′] := Y;
end for
return [Õ];
end procedure

By using Prop. 9 we can prove the main theoretical result.

Theorem 10 Model checking SL[SG] is P-complete.

Proof. Recall that CTL corresponds to the SL0 [SG] fragment of SL[SG]. Then, the lower bound follows immediately from the P-hardness of model checking CTL [Katoen, 2008].

As for the upper bound, Algorithm 1 shows a procedure for model checking SL[SG], which manipulates sets of states in S. The procedure is inspired by the standard model checking algorithm for ATL [Alur et al., 2002], but the preimage operator for the ATL modality ⟨A⟩X is now replaced by the Pre operator in Algorithm 2 for an arbitrary block of strategy quantifiers. Specifically, Algorithm 1 uses the following primitive operations:

- The function Sub returns a sequence of syntactic subformulas of a given formula Ő.
- The function Reg returns the set \{s ∈ S | p ∈ L(s)\} of states s ∈ S labelled with a given atom p ∈ AP.
- The function Pre, when given a quantification prefix Ő = Q_i x_1 \ldots Q_k x_k, a binding prefix b = (x_1, a_1,1) \ldots (x_1, a_1,m_1) \ldots (x_k, a_k,1) \ldots (x_k, a_k,m_k)^3, a set Y ⊆ S of states, and a tuple \vec{α} of actions for all agents a ∈ Ag such that \( (x, a) \) appears in b and x does not appear in Y, returns the set of states s ∈ S from which there exist transitions consistent with Ő, b, and \vec{α}, ending up in Y. Formally, Pre is a recursive function defined on the length of Ő. For the base case Ő = ϵ, notice that Ő is a joint action for all agents in Ag, and therefore Pre returns the set of states s ∈ S such that \( τ(s, \vec{α}) \) ∈ Y. As for the recursive step, s ∈ Pre(Õ, b, Y, Ő) iff for \( ϕ_1 = \exists \) (resp. \( ϕ_1 = \forall \)) for some (resp. every) action Ő, it is the case that s ∈ Pre(ϕ_1, b, Y, update(b, α, x, β)), where function update(b, α, x, β) given a binding b, a tuple \vec{α} of actions, variable x, and action β, returns a tuple \vec{α}′ of actions such that for every a ∈ Ag, if \( (x, a) \) appears in b then \( α_a′ = β \), otherwise \( α_a′ = α_a \). For more details on function Pre, see Algorithm 2.
- Union, intersection, difference, and inclusion test for sets of states.

Algorithm 1 works bottom-up on the structure of the formula; the cases of interest are for strategy formulas. For Ő′ = ϑ X Ő, the procedure calls function Pre to compute the set of states that are “bound” to end up in satisfaction set [Õ]. As regard Ő′ = ϑ(ϑ U Ő2), the procedure computes the least fixed-point of operator F(Z) = \([Õ2] \cup ([Õ1] \cap ϑ X ϑ(Z))\). We observe that, since F is monotone, such a fixed-point always exists. Further, Algorithm 1 runs in polynomial time in the size of the CGS and the size of the formula3. Termination of Algorithm 1 is guaranteed, as the state space S is finite. Soundness and completeness can be proved by induction on the structure of the input formula Ő by using Proposition 9 for the case Ő′ = ϑ(ϑ U Ő2).

By Theorem 10 we immediately obtain that for all fragments of SL[SG] in Fig. 2 model checking is P-complete.

5 Experimental Evaluation

With SL[SG], we propose a logic that enhances the expressivity of ATL while enjoying the same, polynomial-time complexity of model checking. Alternatively, we sacrifice some expressiveness of SL[1G] in order to reduce the verification complexity from highly intractable (2EXPTIME-complete) to tractable. In consequence, one would expect that the verification algorithm for SL[SG], presented in Section 4, should perform better than the general algorithm that handles the whole “one-goal” fragment of SL [Cermák et al., 2015].

However, theoretical complexity results rely on worst case complexity. Thus, it can be that the practical performance of SL[1G] model checking is much better than the 2EXPTIME classification suggests. In particular, one may ask if the specialized SL[SG] algorithm of the previous section performs significantly better than the general algorithm in [Cermák et al., 2015] on the formulas of SL[SG]. To answer this question, we have conducted a series of experiments with a scalable benchmark, based on the simple voting and coercion scenario of Examples 1 and 6.

We consider models ESV_k,n (Extended Simple Voting with k voters and n candidates), constructed as follows. The initial state q0 is handled by a new election authority ea, who decides whether to implement low or high anti-coercion protection. The former choice leads to a copy of the SV_k,n CGS. The latter proceeds to a modified copy of the same model, with proposition pun, satisfied only in the states where the coercer has decided to punish the voter and the voter gave him her voting receipt.

3The parameter \( m_i \) represents the number of agents assigned to variable \( x_i \), for each \( 1 \leq i \leq k \).

4Notice, however, that the number of transitions in a CGS can be exponential w.r.t. the number of agents.
Moreover, we consider the formula:

$$\exists v_0 \forall v_0 \exists v_1 \forall v_2 \ldots \forall v_k (v_0, e)(v_1, e)(v_2, e) \ldots (v_k, e)$$

expressing that the election authority can make sure that, for every strategy of the coercer, voter 1 has a strategy to eventually complete her participation in the election, having voted for candidate 1 without getting punished. Clearly, the formula is true in every model $ESV_{k,n}$ (the strategy for $e$ being high protection, and for the voter to never give away her vote). In the experiments, we have only used models with $n = 2$. Thus, the number of voters ($k$) was the sole scaling factor.

We implemented the model checking algorithm in Section 4 in Python 3, using explicit representation of states and transitions. The tool is available on-line\(^3\). For the general $SL[1G]$ algorithm, we used the MCMAS-SL[1G] extension of MCMAS [Cermák et al., 2015] and the MCMAS-SLK extension. The experiments were conducted on an Intel Core i7-6700 CPU with dynamic clock speed of $2.60$–$3.50$ GHz and $32$ GB RAM, running under 64-bit Windows 10. The timeout was set to $5$ hours. The experimental results are presented in Tab. 1. All times are given in seconds. The first two columns describe the model configuration and its size. The next two columns show the model generation time and the verification time for our algorithm. Finally, the last column presents the performance of the general $SL[1G]$ tool.

The results show significant improvement in running time when using the specialized algorithm (by orders of magnitude). Moreover, our implementation was able to verify models of up to nearly 80,000 states, while the more general tool handled only 10 times smaller models.

## 6 Conclusions

In this paper we advanced the state of the art on tractable logics for strategic reasoning in MAS. Inspired by the restriction of the Alternating-time Temporal Logic $ATL^+$ to $ATL$, we introduced Strategy Logic with simple goals ($SL[SG]$), a fragment of Strategy Logic that only allows for simple goals of form $X \phi, \phi U \phi'$, and $\phi R \phi'$. Alternatively, $SL[SG]$ can be seen as the extension of $ATL$ to arbitrary quantification on the agents’ strategies. Such an extension is motivated by relevant specification requirements in Game Theory, voting protocols, and formal verification. In particular, we showed that subtle notions, such as Stackelberg equilibria, coercion-resistance, module checking, can all be naturally represented in $SL[SG]$.

Then, we analysed the comparative expressivity of $SL[SG]$, and introduced the family of logics $SL_n[SG]$ and $SL_n^{\leq}[SG]$, for $n \in \mathbb{N}$, inbetween $CTL$ and $SL[SG]$. We pointed out that $ATL$ is strictly less expressive than $SL[SG]$ and even $SL_n^{\leq}[SG]$ (Theorem 4). We showed that strategy binding strictly increases the expressive power of our fragments (Theorem 5). Most importantly, the enhanced expressivity of $SL[SG]$ with respect to $ATL$ comes at no extra computational cost: model checking $SL[SG]$ is $P$-complete, the same complexity as $ATL$ (Theorem 10). Because of its tractable model checking problem, $SL[SG]$ lends itself to an efficient implementation.

As an evidence, in Section 5 we presented an implementation of the proposed $SL[SG]$ model checking algorithm and conducted a series of experiments that have showed striking improvements in running time with respect to the implementation of the $SL[1G]$ algorithm in [Cermák et al., 2015].

### Related Work

Logics for strategies are a powerful tool for strategic reasoning in MAS. Their major bottleneck is the high complexity of the related decision problems. To overcome this, two main lines of research have been followed recently. One deals with semantical restrictions, mainly by limiting the number of strategies to evaluate [Chatterjee et al., 2014; Vester, 2013; Brihaye et al., 2009; Jamroga et al., 2017b; Bruyère et al., 2013]; while the other deals with the syntax, e.g., by looking at “simpler” fragments [Alur and La Torre, 2004; Pauly, 2002; Mogavero et al., 2014]. In this paper, we focused on this second line. Among such fragments, one of the most studied is $ATL^+$, a proper sublanguage of $ATL^*$ [Alur et al., 2002]. Recently, the syntactic restriction to simple goals behind the success of $ATL$ has also been investigated in the context of more powerful logics for strategic reasoning. In [Malvone et al., 2018] the authors consider the simple vanilla fragment of Graded $SL[1G]$ ($GS[1G]$), but for two agents only. Hence, their contribution is orthogonal to ours: it is more general, as they can count strategies, but also more restricted, since it only considers two agents. Further, in [Laroussinie and Markey, 2015] the authors consider the $ATL$-like restriction of $ATL^*$ with strategy contexts. However, this restriction does not reduce the expressive power nor the complexity of the related decision problems.

### Future Work

A natural direction for future work is to look for more expressive, yet tractable, formalisms. For instance, [Bulling and Jamroga, 2010] introduced $ATL^+$ that sits between $ATL$ and $ATL^*$. This fragment includes only formulas where each temporal operator is followed by a state formula, and allows cooperation modalities to be followed by a Boolean combination of path formulas. Notably, model checking $ATL^+$ is $PSPACE$-complete. We envisage an extension of $SL[SG]$ similar to $ATL^*$, hopefully with a $PSPACE$-complete model checking problem too. We also plan to release our model checking prototype as a verification tool.

### Acknowledgements

F. Belardinelli acknowledges the support of the ANR JCJC Project SVeDaS (ANR-16-CE40-0021). W. Jamroga and D. Kurpiewski acknowledge the support of the National Centre for Research and Development NCBiR, Poland, and the National Research Fund FNR, Luxembourg, under the PolLux/FNR-INTER project VoteVerif (POLLUX-IV/1/2016).
References


