Verifying Belief-based Programs via Symbolic Dynamic Programming

Citation for published version:

Digital Object Identifier (DOI):
10.3233/FAIA230429

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Publisher's PDF, also known as Version of record

Published In:
Proceedings of the 26th European Conference on Artificial Intelligence

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
Verifying Belief-Based Programs via Symbolic Dynamic Programming

Daxin Liu\textsuperscript{a,b,*}, Qinfei Huang\textsuperscript{b}, Vaishak Belle\textsuperscript{a} and Gerhard Lakemeyer\textsuperscript{b}

\textsuperscript{a}University of Edinburgh, the United Kingdom
\textsuperscript{b}RWTH-Aachen University, Germany

Abstract. Belief-based programming is a probabilistic extension of the Golog programming language family, where every action and sensing could be noisy and every test refers to the subjective beliefs of the agent. Such characteristics make it rather suitable for robot control in a partially-observable uncertain environment. Recently, efforts have been made in providing formal semantics for belief programs and investigating the hardness of verifying belief programs. Nevertheless, a general algorithm that actually conducts the verification is missing. In this paper, we propose an algorithm based on symbolic dynamic programming to verify belief programs, an approach that generalizes the dynamic programming technique for solving (partially observable) Markov decision processes, i.e. (PO)MDP, by exploiting the symbolic structure in the solution of first-order (PO)MDPs induced by belief program execution.

1 Introduction

The action programming language GOLOG [26], short for alGOl in LOGic, is a powerful tool to express high-level agent behavior. GOLOG is based on the situation calculus [34], a first-order language to model how the world changes as a result of actions. Belief programs, introduced by Belle and Levesque [8] in the ALLEGRO system, are probabilistic extensions of the GOLOG programs where every action and sensing could be noisy and tests refer to the agent's subjective degree of belief. These characteristics, amongst others, make belief programs rather suitable for robot control in a partially observable uncertain environment.

Before deployment, it is desirable to verify if a program meets certain properties. As a running example of a belief program, consider a variant of the coffee robot from [31, 28]. The robot in a one-dimensional world tries to search the coffee. Initially, the horizontal position $h$ of the robot is 0 and coffee is at 2. The robot has a knowledge base about her location (usually a belief distribution). The robot might perform sensing $sencfe$ to detect if the coffee is at her current position and action $east$ to move a unit east. Note both $sencfe$ and $east$ could be noisy. E.g. $east$ might end up moving 1 or 2 units with, respectively, likelihood 0.8 and 0.2. A possible belief program is as follows:

\begin{verbatim}
1 while \(B(h = 2) < 1\) do
2   east|sencfe;
3 endWhile
\end{verbatim}

To perform verification, Liu and Lakemeyer [31, 28] reconsider the proposal by Belle and Levesque [8] based on a probabilistic modal logic of belief and actions, called $DSp$ [29]. Amongst others, their proposal allows specifying the properties of programs in a variant of PCTL logic [19]. For example, the above program can be expressed as $\mathbf{P}_{\leq 0.1}[BF(h = 2 : 1)]$. They also show that the verification problem is closely related to model-checking infinite horizon partially observable Markov decision process (POMDP), therefore undecidable.

Despite many theoretical results that were achieved, a general algorithm that actually conducts the verification is missing. In this paper, we propose an algorithm based on symbolic dynamic programming to verify belief programs. Symbolic dynamic programming (SDP) [36] is a generalization of the dynamic programming technique for solving (partially observable) Markov decision processes, i.e. (PO)MDP, that exploits the symbolic structure in the solution of relational and first-order (FO) logical MDPs. Such a technique suits us well in the sense that the execution of belief programs yields multiple ground POMDPs which can be captured by a single FO-POMDP.

The rest of the paper is arranged as follows: in Section 2, we review background knowledge about the logic of belief and action, i.e. the logic $DSp$, the formal semantics of belief programs, and the verification problem. The symbolic dynamic programming algorithm is presented in Section 3. Section 4 introduces and evaluates an implementation of the algorithm. We end with a discussion on related works and future directions in Section 5.

2 Preliminary

2.1 The logic $DSp$

We use the nullary fragment of the logic $DSp$, a probabilistic modal logic of beliefs and actions, to model the agent’s subjective belief. For simplicity, we only have two sorts: $\text{number}$ and $\text{action}$, and by number, we mean algebraic real number [20] which includes irrational numbers such as $\sqrt{2}$. The language features a finite set of
nullary flunets (of type number) and a fixed countable domain with
the unique name assumption: the set of standard names \( N = \mathbb{D} \cup \mathbb{N}_a \)
where \( \mathbb{D} \) are number names and \( \mathbb{N}_a \) are action names. There is a
modal operator \( B \) to express the agent’s subjective belief.

**Syntax** Formally, the vocabulary of the language is taken from the
following. Logical symbols include equality \( = \) and
- standard names \( \{ n, n', \ldots \} \) and variables \( \{ x, y, \ldots \} \);
- rigid function symbols +, \( \times \), \( \text{east}(1) \), \( \text{sense}(1) \), etc.;
- finitely many nullary fluent functions \( \{ h_1, h_2, \ldots, h_k \} \);
- a special unary fluent \( l \) that takes an action as its argument and
returns the action’s likelihood.

Logical symbols include connectives \( \{ \land, \lor, \neg \} \). We treat \( \{ \exists, \forall, \Rightarrow \} \)
as syntactic abbreviations. For simplicity, no predicates are consid-
ered. However, we will use \( \leq \) (defined on numbers) by assuming
there is a rigid function to simulate it. Terms are the smallest set
of expressions such that: 1) every variable and standard name (or constant)
is a term; 2) if \( t_1, \ldots, t_k \) are terms and \( f \) is \( k \)-ary function symbol,
then \( f(t_1, \ldots, t_k) \) is a term. Well-formed formulas are con-
structed as usual in first-order logic with equality. They can further
be in the context of belief and action modalities. Ground terms are
terms without free variables and primitive terms \( P_t \) are terms of the
form \( f(n_1, \ldots, n_m) \), where \( n_i \in \mathbb{D} \). Additionally, we assume \( \mathbb{N}_a \)
is just the set of action primitive terms.

The logic has an epistemic operator: \( B(\alpha : x) \) is to be read as \( \alpha \) is
believed with a probability \( x \) where \( x \) is a term of the number sort.
We use \( K(\alpha) \) as abbreviation for \( B(\alpha : 1) \), read as \( \alpha \) is known.
There are two action modalities \( [a], \square \) in that if \( \alpha \) is a formula, then
so are \([a]\alpha \) (read: \( \alpha \) holds after \( a \)) and \( \Box \alpha \) (read: \( \alpha \) holds after
any sequence of actions\()\). For \( z = a_1 \cdots a_n \), we write \( [a]\alpha \) to mean
\( [a_1] \cdots [a_n] \alpha \). We use \( \Box \) to denote truth, which is taken as an
abbreviation for, say, \( \forall x(x = x) \), and \( \neg \) for its negation. For
\( \alpha \), we use \( \alpha^\gamma \) to denote the formula obtained by substituting free
variable \( x \) in \( \alpha \) with \( t \). A formula without \( B \) is called objective,
without \( [a] \), \( \Box \alpha \) outside \( B \) is called subjective.

**Semantics** The semantics is given in terms of possible worlds. In
a dynamic setting, such worlds are defined to interpret not only the
current state of affairs but also how that changes over actions. Let
\( W = \{ N_a \}^* \) be the set of all finite sequences of actions including \( \langle \rangle \),
the empty sequence. Then a world \( (x, \mathcal{W}, \mathcal{T}) \) \( x \) and \( \mathcal{W} \) are terms satisfying the rigidity constraint: if \( t \in \mathcal{T} \) is rigid, \( w[t, z] = w'[t, z'] \) for all \( w, w', z, \) and \( z' \). Additionally, \( +, \cdots \leq \) are rigid
and interpreted in the usual sense: \( \forall x(x = 1, \cdots = 2) \) for all \( w, t \). This
amounts to setting the theory of real as a background theory that
admits quantifier elimination [40].

Let \( W \) be the set of all possible worlds. The denotation of
ground terms (wrt a world \( w \), action sequence \( z \) ) is defined inductively.
If \( t \in \mathcal{T} \), then \( \| t \|_{w,z} = t \); If \( t = f(t_1, \ldots, t_m) \) \( \| t \|_{w,z} = w[f(r_1, \ldots, r_m), z] \) where \( r_i = t_i \|_{w,z} \). If \( t \) is rigid, we write \( \| t \|_{w,z} \).

An epistemic state \( e \) is a set of distributions \( d \) (weighted functions)
that maps \( W \) to \( \mathbb{R}_{\geq 0}^\mathbb{N} \). By a model, we mean a triple \( \langle e, w, z \rangle \).

**Truth for objective sentences is given as:**
- \( e, w, z \models t = t' \iff \| t \|_{w,z} = \| t' \|_{w,z} \);
- \( e, w, z \models \lnot \alpha \iff e, w, z \not\models \alpha \);
- \( e, w, z \models \alpha \land \beta \iff e, w, z \models \alpha \) and \( e, w, z \models \beta \);
- \( e, w, z \models \forall x. \alpha \iff e, w, z \models \alpha^{\forall x} \) for all \( n \in \mathcal{N} \) for the right sort;
- \( e, w, z \models [n]\alpha \iff e, w, z \models \alpha \) where \( n = \| n \|_{w,z} \);
- \( e, w, z \models \Box \alpha \iff e, w, z \models \alpha \) for all \( z' \in Z \).

To account for stochastic actions, \( DS \) uses a notion called obser-
vational indistinguishability among actions. The idea is that instead
of saying stochastic actions have non-deterministic effects, \( DS \) says
stochastic actions have non-deterministic alternatives which are mu-
tually observationally indistinguishable from the agent’s perspective
each of which has a deterministic effect. In the coffee robot ex-
ample, to express that action \( \text{east} \) might end up in moving 1 or 2
units east non-deterministically, \( DS \) uses two actions \( \text{east}(1) \) and
\( \text{east}(2) \), and they are interpreted in that the robot intends to move
a unit east but nature may select 1 or 2 as outcomes.

More formally (for simplicity, we assume actions have at most 1
argument), arguments of stochastic action \( a(y) \) are uncontrollable
and unobservable while arguments of sensing \( \text{sense}(x) \) are observ-
able yet uncontrollable to the agent. Under this convention, deter-
ministic actions are just actions without arguments. For example,
\( \text{east}(1) \), \( \text{east}(2) \) have uncontrollable and unobservable arguments 1
and 2, while \( \text{sense}(1) \) has an uncontrollable yet observable argu-
ment 1 indicating the sensor receives a reading of 1.

Besides, we define action sequence observational indistinguisha-
ility as follows:

**Definition 1** We define \( z \approx z' : 1. \langle \rangle \approx z' \iff z' \); 2. \( z, r \approx z' \iff z' \approx \cdot \cdot \cdot r \approx z \approx z' \approx \cdot \cdot \cdot r \approx z \approx z' \) and \( r \) is a deterministic action or sensing action;
3. \( z \cdot a(n) \approx z' \iff z' \approx \cdot \cdot \cdot a(n') \) for some \( n' \) and \( z \approx z' \).

For example, \( \text{east}(1) \cdot \text{east}(2) \approx \text{east}(3) \cdot \text{east}(2) \). Lastly, we define the
likelihood of action sequences in a world:

**Definition 2** We define \( l^* : W \times Z \rightarrow \mathbb{R}_{\geq 0}^\mathbb{N} ;
- l^*(w, \langle \rangle) = 1 \) for all \( w \in \mathbb{Y} ;
- l^*(w, z \cdot r) = l^*(w, z) \times n \) where \( w[t, z](r) = n \).

Given \( e, w, z \) and formula \( \alpha \), let \( \| \alpha \|_{e, w, z} = \{ \{ w', z' \} : z' \approx z, e, w, z' \models \alpha \} \). \( \| \alpha \|_{e, w, z} \) is the set of all alternative worlds and actions that might result in \( \alpha \). For a distribution \( d \), we de-
finite \( \text{Norm}(d, \| \alpha \|_{e, w, z}, n) \) if \( n = 1 \times \sum e, w, z \models \alpha \| \alpha \|_{e, w, z} d(w') \times
l^*(w', z') \), where \( n \) is a normalizer with the same expression as the
numerator but replacing \( \alpha \) True. Namely, the set of pairs of worlds and
actions that result in \( \alpha \) has proportioned summed weights (or probability) \( n \). Now, we are ready to give truth for \( B \). Supposing \( r \)
is a rigid term,

**Basic action theory** To infer belief after actions, \( DS \) encom-
passes an action theory \( DS_{\alpha} \), including successor state axioms
that incorporate Reiter’s solution to the frame problem [34] and likeli-
hood axioms, to specify the dynamics of a domain.

- **Successor state axioms (SSAs):** There is one such axiom for each
  fluent \( h \) : \( \{ h \} \models h = x \iff \Phi(a, x) \) where \( \Phi(a, x) \) is a formula with
  free variables among \( a, x \).

1 Since \( W \) is uncountable, \( N \) just requires the sum here to be "well-
defined". See also [6] for details.
2 Free variables are implicitly universally quantified. The \( \{ \} \) has lower
  syntactic precedence than the connectives, and \( \cdot \) has the highest priority.
• Likelihood axioms (LAs): We assume there are only finitely many action symbols, and finitely many such axioms, one for each action symbol. Particularly, LAs are of the form (respectively for stochastic actions and sensing)
\[ \Box(a(y)) = q \equiv \bigvee_{i} y = n_{i} \land q = n_{i}^{*} \]
\[ \Box(\text{senf}(x)) = q \equiv \bigvee_{i,j} x = n_{i}^{*} \land \phi_{j} \land q = n_{i,j}^{*} \]
where \( \phi_{j} \) are mutually exclusive and complete sentences. Namely, \( \phi_{j} \models \neg \phi_{j'} \) and \( \models \bigvee_{j} \phi_{j} \equiv \text{TRUE} \). Essentially, the LAs say that both stochastic actions and sensing have finite outcomes. Moreover, the likelihood of sensing might depend on the context (\( \phi_{j} \)) but the likelihood of stochastic actions is fixed. 4 Besides, all actions have finitely many outcomes with non-zero likelihood.

Example 1 In the robot example, we might have SSAs and LAs as:
\[ \Box[a]h = x \equiv \exists y.a = \text{east}(y) \land x = y + h \]
\[ \lor \forall y.a \neq \text{east}(y) \land x = h \]
\[ \Box(\text{east}(y)) = x' \equiv y = 1 \land x' = 0.8 \lor y = 2 \land x' = 0.2 \]
\[ \lor y \notin \{1, 2\} \land x' = 0 \]
\[ \Box(\text{senf}(x)) = x' \equiv x = 1 \land h = 2 \land x' = 1 \]
\[ \lor x = 0 \land h \neq 2 \land x' = 0 \]
\[ x = 1 \land h \neq 2 \land x' = 0 \]
\[ \lor x = 0 \land h \neq 2 \land x' = 0 \]
That is, the robot’s new location \( x \) is determined by its current location \( h \) and the actual moved distance \( y \). Stochastic action \( \text{east}(y) \) might end up moving \( 1 \) (0.8 likelihood) or \( 2 \) (0.2 likelihood). Besides, sensing action \( \text{senf} \) is accurate: if the robot is at the coffee’s position, i.e. \( h = 2 \), executing \( \text{senf} \) receives a reading 1 with 100% likelihood and a reading 0 with zero likelihood.

Regression & progression The regression of a formula \( \alpha \) through an action \( a \) is another \( \alpha' \) that holds prior to \( a \). \( \alpha \) being performed iff \( [a] \alpha \) holds. The idea is to recursively replace formulas of the form \( [t]h = n \) by the RHS of \( h \)’s SSA with substitutions. E.g. \( R((\text{east}(2))h = 2, D_{\text{dyn}}) := (\exists y.\text{cast}(2) = \text{east}(y)).2 = y + h \land \forall y.a \neq \text{east}(y) \land x = h) \equiv h, \) given \( D_{\text{dyn}} \) as Example 1.

[30] also proposed a regression operator for belief formulas such as \( \text{east}(1) \) \( B(h = 2; 0.2) \) if an initial belief distribution is given. A belief distribution is a formula of the form \( \forall x.B(h = x; f(x)) \equiv \bigwedge_{h} B(h = n_{j} \implies r_{j}) \). For example, a possible initial belief distribution for the robot coffee could be \( B(0) \equiv B(h = 0: 1) \). Namely, the robot believes she is at location 0. With an initial belief distribution, the regression of beliefs is defined as the evaluation against the initial beliefs. For example:
\[ R((\text{east}(2))B(h = 2; 0.2), D_{\text{dyn}}, B(0)) \]
\[ := \sum_{n_{j}} \sum_{n_{i}} r_{j} \times \Box(\text{east}(n_{j})) \begin{cases} 1 & h = n_{i} \lor R((\text{east}(n_{i}))h = 2) \\
\text{o.w.} & \end{cases} \]
\[ \equiv 0.2 \times 1 \times 0.2 \]
which is then evaluated to \( \text{TRUE} \).

The inverse of regression is progression, which takes a formula \( \psi \) and action \( a \) and represents logical consequences in a static formula \( \psi' \) (formula without \( [a] \) and \( \Box \)). Unlike regression, restrictions must be imposed to ensure \( \psi' \) is first-order [27]. Nevertheless, [29] showed that if the input is a belief distribution \( B' \), then the progression is always first-order and in the form of another belief distribution \( B'' \), i.e. \( B' \land KD_{\text{dyn}} \models [a](B'' \land KD_{\text{dyn}}) \). For example, the progression of \( B'(0) \) wrt action \( \text{east}(1) \) is \( B'(0) \), and the progression of \( B'(1) \) wrt action \( \text{senf}(1) \) is \( B'(2) \), where \( f_{1}(x) = f_{2}(x) = \begin{cases} 0.8 & x = 1 \\
0.2 & x = 2 \text{ and } f_{2}(x) = \begin{cases} 1 & x = 2 \\
0 & \text{o.w.} \end{cases} \end{cases} \)

We comment that both of these results are significant improvements and advancements over classical regression and progression [34] as well as the epistemic non-probabilistic regression and progression by Scherl and Levesque [37] or Liu and Wen [32].

2.2 Verification of belief programs

Belief programs are probabilistic extensions of GOLOG, where every action and sensing could be noisy, and every test is referring to the agent’s subjective beliefs.

Belief program The basic ingredient of belief programs is the so-called primitive programs which are actions that suppress their uncontrollable parameters. For example, for the action \( \text{senf}(1) \) and \( \text{east}(2) \), their respective primitive programs are \( \text{senf} \) and \( \text{east} \). A primitive program \( \varphi \) is instantiated by a ground action \( t_{a} \), i.e. \( a \rightarrow t_{a} \). If \( \models \exists y.a = \varphi[y] \), then \( \varphi \) is the action that restores its suppressed parameters by \( y \).

A program expression can be a primitive program \( \varphi \), a test \( \alpha \), where \( \alpha \) is a static subjective formula, a sequence \( \delta, \delta' \), a non-deterministic choice \( (\delta|\delta') \), and a non-deterministic iteration \( \delta^{*} \) of programs. Formally, the program expression can be defined as:
\[ \delta := \varphi[\alpha]|(\delta|\delta')|\delta^{*} \]
The if-statements and while-loops are then defined as abbreviations:
\[ \text{if } \alpha \text{ then } \delta_{1} \text{ else } \delta_{2} \text{ while } \alpha \text{ do } \delta \text{ endwhile} := [\alpha?; \delta_{1}];[\neg \alpha?; \delta_{2}] \]

An example is the coffee robot program \( \delta_{\text{cfe}} \) in the introduction. Given a set of formulas without modality \( D_{0} \) that describes the initial world state, an initial belief distribution \( B^{0} \), a BAT \( D_{\text{dyn}} \), and a program expression \( \delta \), a belief program \( BP \) is a pair of the form:
\[ BP = (D_{0} \cup D_{\text{dyn}} \cup B^{0} \cup KD_{\text{dyn}}, \delta) \]
For the coffee robot, a belief program could be
\[ BP_{\text{cfe}} = ([h < 0] \cup D_{\text{dyn}} \cup B^{0} \cup KD_{\text{dyn}}, \delta_{\text{cfe}}) \]
where \( D_{\text{dyn}} \) is as in Example 1. Namely, the robot initially is at a non-positive position \( h \leq 0 \). Yet she fully believes that she is at position 0, i.e. \( B^{0} \). To handle termination and failure, we reserve two nullary fluents \( \text{Final} \) and \( \text{Fail} \). Moreover, \( [a] \text{Final} = u \equiv a = \epsilon \land u = 1 \lor \text{Final} = u \) (likewise for \( \text{Fail} \) with action \( f \)) are implicitly assumed to be part of \( D_{\text{dyn}} \). Additionally, \( D_{0} \models \text{Final} = 0 \land \text{Fail} = 0 \), and actions \( \epsilon, f \) do not occur in \( \delta \).

Program semantics & the verification problem A configuration \( (z, \delta) \) of a program consists of an action sequence \( z \) and a program expression \( \delta \), where \( z \) is an action history and \( \delta \) is the remaining program to be executed. Given \( BP = (D_{0} \cup D_{\text{dyn}} \cup B^{0} \cup KD_{\text{dyn}}, \delta) \), the transition relation \( \rightarrow \) among configurations given \( e \) is defined inductively as:(See [31, 28] for a full list):

---

3 It is possible to allow likelihood of stochastic actions to vary as well, for simplicity, we only consider rigid likelihood.

4 The assumption that only finite action outcomes have non-zero likelihood and finite values of random variables have a non-zero degree of belief ensures summation here is finite and hence can be replaced by a finite plus.
1. \(\langle z, \emptyset \rangle \xrightarrow{z} \langle z \cdot t, \emptyset \rangle\), if \(g \rightarrow t\);
2. \(\langle z, \delta; \emptyset \rangle \xrightarrow{z} \langle z \cdot t', \delta' \rangle\), if \((z, \delta) \xrightarrow{z} \langle z \cdot t, \delta' \rangle\);
3. \(\langle z, \emptyset^* \rangle \xrightarrow{z} \langle z \cdot t, \delta^* \rangle\), if \((z, \delta) \xrightarrow{z} \langle z \cdot t, \delta^* \rangle\).

The set of final configurations w.r.t \(e\), i.e. \(\text{Fin}(e)\), is defined as the smallest set such that:

1. \(\langle z, \emptyset \rangle \in \text{Fin}(e)\) \(\in \text{Fin}(e)\);
2. \(\langle z, \alpha! \rangle \in \text{Fin}(e)\) if \(e, w, z \models \alpha\);
3. \(\langle z, \delta; \emptyset \rangle \in \text{Fin}(e)\) if \((z, \delta) \in \text{Fin}(e)\) and \((z, \delta) \in \text{Fin}(e)\);
4. \(\langle z, \delta^* \rangle \in \text{Fin}(e)\) if \((z, \delta) \in \text{Fin}(e)\) or \((z, \delta^*) \in \text{Fin}(e)\);

The set of failing configuration is given by: 
\[\text{Fail}(e) = \{\langle z, \delta \rangle | (z, \delta) \notin \text{Fin}(e), \exists \exists \exists \langle z \cdot t, \delta' \rangle, (z, \delta) \xrightarrow{z} \langle z \cdot t, \delta' \rangle\}\].

The execution of a belief program \(P\) in a pair \(e, w\) such that \(e, w \models D_0 \cup D_{\text{dyn}} \cup B^I \cup K D_{\text{dyn}}\) yields a countably infinite partially observable Markov decision process (POMDP) \(M^\delta_{e,w} = (S, A, P, O, \Omega, s_0)\) as follows:

- \(S\): the set of configurations reachable from \(s_0\) under \(\xrightarrow{\cdot}\) (transitive and reflexive closure of \(\xrightarrow{\cdot}\));
- \(A\): the finite set of primitive programs in \(\delta\);
- \(s_0\): the initial state \(\langle \cdot, \cdot \rangle\);
- \(O\): the observations are the reachable belief distributions \(B'\) from \(B'\).
- \(\Omega: S \rightarrow O\) a deterministic observation mapping as (suppose \(s = (z, \delta)\) and \(\Omega(s) = B'\) if \(B' \models D_{\text{dyn}} \models \models \models \models \emptyset B'\)).
- \(P\): \(S \times A \times S \rightarrow \mathbb{R}\) the transition probability \(P((z, \delta), g, \{z \cdot t\}, \delta')\) given by:

\[
P(\cdot) =
\begin{cases}
  n & \text{if } g \rightarrow t, w, z \models l(t_0) = n, (z, \delta) \xrightarrow{z} (z \cdot t, \delta') \\
  1 & \text{if } (z, \delta) \in \text{Fin}(e) \text{ and } g = t = \delta' = \epsilon \\
  0 & \text{otherwise}.
\end{cases}
\]

We comment that it is a POMDP rather than MDP because we are interested in the set of possible strategies that the robot can perform. The fact that the set of observations is just the set of reachable beliefs distribution means that the robot can only act according to its beliefs about the environment rather than the actual world state, leading to a partially observable setting.

The non-determinism of programs is resolved by a policy, which is an action-selection strategy that maps each state to an action, i.e., \(\sigma : S \rightarrow A\). We will only focus on the observation-based policies \(\Sigma_{\text{obs}}\); a policy \(\sigma : S \rightarrow A\) is observation-based iff for all \(s, s' \in S\), if \(\Omega(s) = \Omega(s')\) then \(\sigma(s) = \sigma(s')\). An infinite path of the form \(\pi = s_0 \xrightarrow{a_0} s_1 \xrightarrow{a_1} s_2 \cdots\) is called a \(\sigma\)-path if \(\sigma(s_j) = a_j\), for all \(j \geq 0\). The \(j\)-th state of any such path is denoted by \(\pi[j]\). The set of all \(\sigma\)-paths starting in \(s\) is denoted by Path\(^\sigma\)(\(s, M^\delta_{e,w}\)).

Every policy \(\sigma\) induces a probability space \(P_{\sigma}^e\) on the set of infinite paths starting in the state \(s\), using the cylinder set construction [42]. For any finite path prefix \(\pi_{\text{fin}} = s_0 \xrightarrow{a_1} s_1 \cdots s_n\), the probability measure is defined as: \(P_{\sigma|\text{fin}}^e = P(s_0, a_1, s_1) \cdots P(s_{n-1}, a_n, s_n)\). This extends to a unique measure \(P_{\sigma}^e\).

Given a POMDP \(M^\delta_{e,w}\), a policy \(\sigma\), and a static subjective formulas \(\psi_{\text{goal}}\) as goal, we say that a state \(s = (z, \delta)\) satisfies \(\psi_{\text{goal}}\), i.e., \(s \models \alpha\) if \(e, w, z \models \psi_{\text{goal}}\), an infinite path \(\pi\) satisfies \(\psi_{\text{goal}}\), i.e., \(\pi \models \psi_{\text{goal}}\), iff \(3k, \pi[k] \models \psi_{\text{goal}}\), where \(\pi[k]\) is the \(k\)-th state in \(\pi\). The reachability probability \(P_{\sigma}^e(\psi_{\text{goal}})\) is then defined \(P_{\sigma}^e(\pi | \pi \models \psi_{\text{goal}})\). Given a program \(BP\), a static subjective formula \(\alpha\), and a threshold \(\tau\), the verification problem ask if

\[
\max_{\sigma \in \Sigma_{\text{obs}}} \{P_{\sigma}^e(\psi_{\text{goal}})\} \leq \tau
\]

for all POMDPs \(M^\delta_{e,w}\) with \(e, w \models D_0 \cup D_{\text{dyn}} \cup B^I \cup K D_{\text{dyn}}\). We write \(BP \models P(\psi_{\text{goal}}) \leq \tau\) if the program satisfies the property.\(^6\)

In the coffee robot example, we might be interested in whether the maximal reachability probability for the robot to fully believe it reaches the coffee is no more than 0.1. Namely, deciding \(BP_{\text{fc}} \models P(\text{Fin} = 2) \leq 0.1\).

### 3 Verification by symbolic dynamic programming

One way to solve a POMDP is value iteration. Since the optimal policy of a POMDP might not be state-based, one has to transfer it into a continuous belief MDP so that the optimal policy of the original POMDP corresponds to the optimal state-based policy of the belief MDP [1]. The states \(B\) of the belief MDP are called belief states,\(^7\) and are distributions over states of the original POMDP.

In value iteration, every belief state \(b\) is assigned a value \(V(b)\) representing the maximal reachability probability that can achieve from the belief state \(b\), hence we are interested in the value of the initial belief state \(b_1\) with \(b_1(s_0) = 1\). The value function \(V\) is essentially the fixed-point of the Bellman backup operator and thus can be computed iteratively \([11, 39]\). \(V(b) = \max_{a \in A} \sum \{P(b, a, b') \times V(b')\}\). While the number of belief states \(B\) is infinite, it is well-known that the optimal value function for finite horizon \(H\) is piece-wise linear and convex, therefore can be approximated arbitrarily closely as the upper envelope of a finite set of “\(\alpha\)-vectors” \(V\) as \(V(b) = \max_{a \in B} b \cdot \alpha\). Hence value iteration is transformed to compute \(V\) via:

\[
\begin{align}
V^H &= \bigcup_{a \in A} V^H_a \\
V^H_{a,o} &= \{a^o, a|a \in V^H-1\} \\
\alpha_{a^o,a}(s) &= \left[\Omega(s') = 0\right] \cdot P(s, a, s') \cdot a(s')
\end{align}
\]

where \(V_1 \oplus V_2 = \{a_1 + a_2|a_1 \in V_1, a_2 \in V_2\}\), \(\llbracket x \rrbracket\) is the indicator function and returns 1 if \(x\) is true and 0 otherwise, and \(P\) is the transition function of the original POMDP.

#### 3.1 FO-POMDP for belief programs

A first-order partially observable MDP (FO-POMDP) is a compact representation of (infinite) POMDP which abstractly defines the states \(S_{\text{FO}}\), actions \(A_{\text{FO}}\), observations \(O_{\text{FO}}\), transition probability \(T_{\text{FO}}\) and observation function \(\Omega_{\text{FO}}\). It is suitable for our need to abstractly represent the underlying infinite POMDPs generated by the execution of belief programs \(M^\delta_{e,w}\).

To begin with, we need the notion of characteristic program graph \(G^\delta\) of a program \(\delta\). The nodes of \(G^\delta\) are the reachable subprograms \(Sub(\delta)\), each of which is associated with a termination condition \(\text{Fin}(\delta)\) (initial node \(v_0\) corresponds to the overall program) and

\(^6\) Here, we only consider the upper bound. A dual question is to consider the lower bound, i.e. determining if \(\tau \leq \min_{\sigma \in \Sigma_{\text{obs}}} \{P_{\sigma}^e(\psi_{\text{goal}})\}\) for all POMDPs \(M^\delta_{e,w}\) which involves policy synthesis [33]. We leave it for future.

\(^7\) This is in contrast to our model of belief \(B\). Here, belief is just a distribution over states, that is, it is a meta-linguistic notion while \(B\) is a logical notion.
an edge $\delta_1 \xrightarrow{\phi/\alpha} \delta_2$ represents a transition from $\delta_1$ to $\delta_2$ by the primitive program $\psi$ if test condition $\alpha$ holds. Moreover, failure conditions are given by Fail($\delta$) := \neg(Fin($\delta$) ∨ L($\delta$) ∨ $\phi/\alpha$). In the coffee robot program, $G_{\delta, i}$ has only one node with two self-loops.

Given a belief program $BP$, we define a FO-POMDP $M_{BP}^{FO} = (S_{FO}, A_{FO}, P_{FO}, s_0, O_{FO}, \Omega_{FO})$ in the following way:

- $S_{FO}$: the set of states are of the form $\langle \phi, \delta \rangle$, where $\phi$ is a first-order $\mathcal{DSp}$ formula. Intuitively, $\langle \phi, \delta \rangle$ represents the set of all possible worlds $w$, epistemic states $e$, and program configurations $\langle e, \delta \rangle$ such that $e, w, z \models \phi$;
- $A_{FO}$: the finite set of primitive actions in $\delta$;
- $\delta_{d, FO} = \langle \phi, \delta \rangle$: is the initial state;\footnote{The BAT and initial belief distribution $\mathcal{D}dyn \wedge B^\forall \wedge K\mathcal{D}dyn$ is implicitly included.}
- $O_{FO}$: the observations are the same as in $M_{d, w}$;
- $\Omega_{FO}$: a deterministic observation function $\Omega_{FO}(\langle \phi, \delta \rangle) = B'$ if $\phi = B'$; 
- $P_{FO}(\langle \phi, \delta \rangle)$ is given as:

$$P_{FO}(\cdot) = \begin{cases} n & \text{if } \delta_1 \xrightarrow{\phi/\alpha} \delta_2 \in G_3 \text{ for some } \beta \text{ and } \exists e, \beta \models t(e) = n \wedge \beta \\ 1 & \text{if } \phi_1 = \text{Final} = 1 \text{ and } \phi = \delta_2 = e \\ 1 & \text{if } \phi_1 = \text{Final} = 1 \text{ and } \phi = \delta_2 = f \\ 0 & \text{Otherwise} \end{cases}$$

**Case Statement** To concisely represent $P_{FO}$ and distributions over states $S_{FO}$ of the FO-POMDP, we introduce a tabular meta-logical device called *case statement* \[35\]. A case-statement Case defines a distribution over the state $\langle \phi, \delta \rangle \in S_{FO}$ as

$$\text{Case}[\phi_1, \delta_1, t_1; \ldots; \phi_k, \delta_k, t_k] \equiv \begin{cases} \langle \phi_1, \delta_1 \rangle : t_1 \\ \vdots \\ \langle \phi_k, \delta_k \rangle : t_k \end{cases}$$

Additionally, Case = $t$ iff for $1 \leq i \leq k$, if $\phi_i$ holds and the remaining program is $\delta_i$, then $t = t_i$. We assume $t_1, \ldots, t_k$ are constants for simplicity. For example, the following case statement expresses a distribution that assigns all weights to the state that satisfies $B(h = 2)$ with $\delta_{cfe}$ as the remaining program:

$$\text{Case} := \{ K_h = 2, \delta_{cfe} : 1 \}$$

(2)

For a given program $BP$, we might wish to use some logical operator over its reachable sub-program $\text{Sub}(\delta)$ in case statements as shorthand, they are defined as

$$\text{Case}[\phi, \delta_1 \vee \delta_2, t] := \text{Case}[\phi, \delta_1, t; \phi, \delta_2, t]$$

$$\text{Case}[\phi, \neg \delta_1, t] := \text{Case}[\phi, \delta_2, t; \ldots; \phi, \delta_k, t]$$

where $\delta_2, \ldots, \delta_k$ are programs in $\text{Sub}(\delta)$ and distinct from $\delta_1$. Following this definition, we use $\delta_I$ to mean the disjunctions for all $\delta_i \in \text{Sub}(\delta)$ and $\delta_f$ for its negation.

Besides, we define sum $\oplus$ (likewise for product $\otimes$) over two case statements as (we might use a scalar value $n$ in $\oplus$ or $\otimes$, they should

Lastly, we need to compute the preimage of a case statement wrt a ground action $t_a$ in a program graph $G_3$: (supposing $\delta_{i,j} \xrightarrow{\phi/\delta_{i,j}} \delta_i \in G_3$ and $\psi \rightarrow t_a$)

$$\text{Pre} \langle \phi_i, \delta_i, t_i \rangle, G_3, t_a \rangle := \text{Case}[\delta_i, j \land t_a \phi_i, \delta_i, j, t_i]$$

If no ambiguity, we write $\text{Pre} \langle \phi_i, t_a \rangle$ or $\text{Pre} \langle \phi_i \rangle$ for short. Essentially, $\text{Pre} \langle \phi_i \rangle$ represents the conditions that prior distributions over $S_{FO}$ should satisfy in order to result in $\text{Case}$ after the action $t_a$. For example, $\langle \text{senfe}, 1 \rangle, K_h = 2, \delta_{cfe} : 1 \rangle$ is the preimage of $\text{Case}$ wrt $G_3$ and action $\text{senfe}(1)$. This is because $G_{\delta_{cfe}}$ only has self-loops, the program expression previous to the action $\text{senfe}(1)$ can only be $\delta_{cfe}$ itself.

Now we show how to represent $P_{FO}$. First, for each ground action $t_a$ according to the BAT, $l(t_a)$ can be represented by a case statement: $l(t_a) := \text{Case}[\phi_i, \delta_i, t_i]$, where $\phi_i$ is the likelihood conditions and $t_i$ is the corresponding values. In case $t_a$ is a stochastic action, $\phi_i \equiv \text{TRUE}$. Next, recall that $P_{FO}$ in $M_{BP}^{FO}$ not only depends on $l(t_a)$ but also the program graph $G_3$. Hence, given $G_3$, (supposing $\delta_i \xrightarrow{\phi/\alpha} \delta_{i,j} \in G_3$ and $\psi \rightarrow t_a$), we define:

$$P_{FO}^{G_3}(\varphi, t_a) := \text{Case}[\delta_i, j \land l(t_a), \delta_{i,j}]$$

Then, we can represent the transition probability $P_{FO}$ by a set of case statements, one for each primitive program and ground action. In the coffee robot program example, $P_{FO}$ contains the following.\footnote{We omit cases with 0 values for short.}

$$P_{FO}^{G_3}(\text{east}, \text{east}(1)) := \{ \text{TRUE}, \delta_{cfe} : 0.8 \}$$

$$P_{FO}^{G_3}(\text{east}, \text{east}(2)) := \{ \text{TRUE}, \delta_{cfe} : 0.2 \}$$

$$P_{FO}^{G_3}(\text{senfe}, \text{senfe}(1)) := \{ K_h = 2, \delta_{cfe} : 1 \}$$

$$P_{FO}^{G_3}(\text{senfe}, \text{senfe}(0)) := \{ K_h = 2, \delta_{cfe} : 1 \}$$

### 3.2 Symbolic dynamic programming

To solve the FO-POMDP for a program $BP$, we propose a *symbolic dynamic programming (SDP)* algorithm in the form of lifted $\alpha$-vectors. Lifted $\alpha$-vectors will be represented as case statements, e.g. $\alpha\text{Case}$ and the lifted POMDP value function will be represented as a maximization over a set $V^H = \{ \alpha\text{Case} \}$:

$$V^H(b) = \max_{\alpha\text{Case} \in V^H} b \otimes \alpha\text{Case}. \quad \text{(3)}$$

For a goal $\psi_{goal}$, we initialize the value $V^0$ by the single case statement $\alpha\text{Case} := \{ (\psi_{goal}, \delta_{cfe}) : 1 \}$. Intuitively, if initially $\psi_{goal}$ already holds, then the reachability would be 1 with the optimal policy saying do nothing. For example, we have $\alpha\text{Case} := \text{Case}$ as in Eq. (2) for the goal $K_h = 2$ and program $BP_{cfe}$.

We comment that an important concern in the implementation of evaluating $V^H(b)$ for a belief state $b$ or, more general, computing $\otimes$ over case statements is to reduce the number of cases by removing inconsistent cases. We achieve this by an external theorem prover. Moreover, while it is possible to eliminate $[a]$ for objective formulas by regression (wrt BAT $\mathcal{D}dyn$) in order to identify equivalent cases,
it is impossible to eliminate $B$ as regression of $B$ is essentially evaluating it against an input belief distribution $B^{t}$. Nevertheless, such a procedure requires extra effort (we defer a discussion on this to the Implementation section). For the purpose of presentation, we eliminate $[a]$ whenever possible by regression.

**Relevant observations** Another problem in value iteration for the FO-POMDP is that observations $O_{t}$ are infinite, hence it is infeasible to perform iterations as in Eq. (1a). The idea here is to identify the set of relevant observations at iterations [36]. Given a belief distribution (or observation) $B^{t}$ and a primitive program $g$, the set of relevant observations $O_{t}$ are fixed and are determined by the set of ground actions $a_{t}$ s.t. $g \rightarrow t_{a}$ (as new observations are the progressions of $B^{t}$ wrt $t_{a}$). We denote the set of all relevant observations $O_{Rel}$ as $O_{Rel} = \bigcup_{t} O^{t}$. Additionally, $O^{t} = \bigcup_{o} O^{t_{o}}$ where $g \rightarrow t_{o}$.

In our robot example, we have $O_{Rel} = O^{east} \cup O^{sencfe}$.

**Proof Sketch** [9] proves the correctness of value iteration for reachability probability in POMDPs. Hence it remains to show that the

\[ \alpha_{Case}^{E,O(1),1} \]

\[ = \begin{cases} 1 & \text{if } \langle h = 2, \delta_{cfe} \rangle : 1 \text{ and } E(1) = 1 \\ 0 & \text{otherwise} \end{cases} \]

\[ \alpha_{Case}^{S,O(1),1} \]

\[ = \begin{cases} 1 & \text{if } \langle h = 2, \delta_{cfe} \rangle : 1 \text{ and } S(1) = 1 \\ 0 & \text{otherwise} \end{cases} \]

The last equality is because $[E(1)]K_{h} = 2$ and $[E(2)]K_{h} = 2$ are logically equivalent: again the robot has no idea about the outcome of $east$. Likewise:

\[ \alpha_{Case}^{S,O(1),1} = \begin{cases} 1 & \text{if } \langle h \neq 2 \land S(0) \rangle K_{h} = 2, \delta_{cfe} : 1 \\ 0 & \text{otherwise} \end{cases} \]

The first case $\langle h < 0 \land \delta_{cfe} : 1 \rangle$ is due to that starting from $B^{10}$, after the stochastic action $east(1)$, the agent would believe $B(h = 1: 0.8)$ and $B(h = 2: 0.2)$, hence, $[E(1)]K_{h} = 2$ does not hold. Likewise $[S(1)]K_{h} = 2 \equiv \text{TRUE}$ and $[S(0)]K_{h} = 2 \equiv \text{FALSE}$. The result suggests that the maximal reachability is policies with at most 1 horizon is still 0.

For $H = 2$, observing the fact that $[east(1)]K_{h} = 2$ and $[east(0)]K_{h} = 2$ is impossible under $B^{10}$ and $D_{dyn}$, after eliminating inconsistent cases we have

\[ \text{Theorem 1 Given a belief program } BP, \text{ a goal } \psi_{goal}, \text{ a threshold } \tau, \text{ the SDP algorithm above returns } "BP \neq Pr(F_{\psi_{goal}}) \leq \tau" \text{ iff } BP \neq Pr(F_{\psi_{goal}}) \leq \tau. \]

**Proof Sketch** [9] proves the correctness of value iteration for reachability probability in POMDPs. Hence it remains to show that the
FO-POMDP for a belief program is a faithful abstraction of the underlying infinite ground POMDPs, which can be proved based on the facts that 1) every observation-based policy of the FO-POMDP is an observation-based policy of the ground POMDPs and vice versa; 2) every state \( \langle \varphi, \delta \rangle \) in FO-POMDP abstractly represents a set of program configurations (states of the ground POMDP) which satisfy \( \varphi \).

### 4 Implementation & Evaluation

The main challenge in implementation is how to implement the case statement and operations over it. For this, we exploit the idea of first-order algebraic decision diagram (FOADD) in [35]. The algebraic decision diagram (ADD) [2, 18] is a data structure that compactly represents a Boolean function \( \{0, 1\}^n \mapsto \mathbb{R} \) using a directed acyclic graph. Nevertheless, the propositional nature prevents us from using ADDs directly since case statements contain general FOL formulas (potentially with modality \([a]\) and \(B\)) and program expressions. Our solution is to maintain a mapping that maps each first-order sentence to a corresponding proposition (hence the name FOADD). In the same spirit, the mapping also maps each reachable sub-program \( \delta_i \in \text{Sub}(\delta) \) to a proposition \( p_{\delta_i} \) (mutually exclusive). Below is an illustration of the FOADD for Case60 in Eq. (2).

With the FOADD, the operators \( \oplus \) and \( \otimes \) defined over case statements can be implemented by direct use of standard Apply operations such as addition and multiplication for ADDs. A notable exception is the \( Pre \) function which requires a program graph \( G_\delta \) and a ground action \( t_a \) as inputs. In practice, we process as follows:

1. updating the FOL-Propositions mapping by adding \( [t_a] \) in front of all formulas (excluding \( [t_a] \) in front of the given FOADD;
2. collecting edges \( E := \{ \delta_i, j \xrightarrow{\alpha/\gamma} \delta_i \in \text{Sub}(\delta) \} \) whose label \( \gamma \) can instantiate the ground action \( t_a \). Let \( \Delta = \bigcup \{ \delta_i \} \) be the set of relevant program expressions (whose predecessors need to be computed);
3. setting propositions \( \text{Sub}(\delta) = \Delta \) to be \text{FALSE};
4. replacing propositions \( \delta_i \in \Delta \) with \( \bigvee_j p_{\delta_{i,j}} \land p_{\delta_{i,j}} \).

We comment our notion of FOADD goes beyond the one by Santer [35] as our mapping includes sentences that might contain modalities, even nested modalities.

**Reducing space** Several tricks can be used to reduce the number of introduced propositions.

1. For the basis, formulas, one could use regression to eliminate modality \([a]\) and identify potential equivalent formulas. E.g. under the BAT of coffee domain \( D_{\text{dop}} \), the formula \( h = 1 \) is logically equivalent to \( [\text{east}(1)]h = 2 \);
2. Besides, one can rewrite terms [22] to identify potential equivalent formulas. E.g. we can rewrite \( h + 1 + 1 \) to \( h + 2 \);
3. For subjective formulas, since the agent has no knowledge about the actual outcome of stochastic actions, we could ignore their uncontrollable parameters. E.g. since \( [\text{east}(1)]B(\alpha: r) \) is equivalent to \( [\text{east}(2)]B(\alpha: r) \), we simply ignore arguments \( \{1, 2\} \).

Although the contribution of the paper is mainly theoretical and conceptual as the primary focus is on converting SDP [36] for verification, we implemented the algorithm (with the above tricks) in a prototype system and evaluate it for the coffee robot domain. We conceive an extended evaluation for variants of domains, programs, and program properties in the future [12]. We exploit PREGO [7] for regression and the Z3 theorem prover [17] for satisfiability checking. Besides, Z3 provides built-in rules for term rewriting. The experiment is conducted on an Intel@ Core™ i5-1135G7 @2.4GHz with 8GB RAM. The table below demonstrates time and space consumption under different horizon \( H \) settings. “PRM” stands for the primitive version while “RDC” stands for the version of SDP that applies tricks to reduce space. The result suggests that while the tricks can significantly reduce the number of \( \alpha \text{Case} \) in the value function \( \#V \) and the number of propositions in ADDs \( \#\text{Prop} \), especially when \( H \) grows large, it requires significantly more time to process. Unfortunately, both versions run out of memory for \( H = 5 \). This is not surprising since the set of \( \alpha \)-vectors grows exponentially with every iteration [38]. After all, the exact value iteration could not solve the well-known Tiger domain for \( H = 2 \) with more than 1 door [36].

<table>
<thead>
<tr>
<th>( H )</th>
<th>#V</th>
<th>#Prop</th>
<th>Time(in ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>6</td>
<td>15</td>
</tr>
<tr>
<td>3</td>
<td>22</td>
<td>42</td>
<td>34</td>
</tr>
<tr>
<td>4</td>
<td>132</td>
<td>1806</td>
<td>78</td>
</tr>
</tbody>
</table>

### 5 Related Work & Conclusion

We review related works from the perspective of GOLOG program verification and symbolic model-checking.

Our notion of belief programs stems from [31, 28]. A primitive form of belief programs (propositional beliefs) can be found in [25]. The first work on verifying GOLOG program is [15, 16]. Later, verifying variants of GOLOG programs and program properties are studied. E.g. [14] investigated the verification of DT-GOLOG program, a variant with decision theoretical feature, against PCTL-like properties, [43] studied the verification of ALCCK-GOLOG programs, a variant with features of knowledge and sensing, against LTL-like properties [43]. Similarly, [13, 43, 44] resp. studied the verification of CTL*, LTL, and CTL properties of GOLOG programs. On verifying algorithms, a common step of many works above is to abstract the infinite ground transition systems (or MDP, POMDP) induced by program execution to abstract (symbolic) ones, and thereafter perform symbolic model-checking. If the abstractions are finite [43, 44, 14], tools such as PRISM [23] and Storm [21] can be used. Otherwise, one has to devise GOLOG-specific algorithms that, e.g. do similar fixpoint computations as (symbolic) model-checking techniques [13].

On the other hand, symbolic methods are common in model-checking to tackle the state space explosion problem [5]. In this regard, the most relevant work to us is [36] where an SDP algorithm is proposed for value iteration in FO-POMDP, nevertheless, states of FO-POMDP there only contain FOL formulas while ours include modality and program expressions as well, leading to special treatments in computing preimage and evaluating for case statements. Prior to [36], symbolic model-checking can be applied to transition systems [5], Markov chains [4], MDP [3], first-order MDP [35], or relational POMDP [41], stochastic game [24].

Future work includes exploring the possibility of integrating point-based value iteration [38] in verification. Besides, it would be desirable to provide also a lower bound on reachability probability [10].
Acknowledgements

This research was supported partly by a Royal Society University Research Fellowship, UK, partly by a grant from the UKRI Strategic Priorities Fund, UK to the UKRI Research Node on Trustworthy Autonomous Systems Governance and Regulation (EP/V026607/1, 2020–2024), partly by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) RTG 2236/2 ‘UnRAVeL’, and partly by the EU ICT-48 2020 project TAILOR (No. 952215).

References


