Knowledge-Based Programs as Plans
– The Complexity of Plan Verification –

Jérôme Lang¹ and Bruno Zanuttini²

1 CNRS and LAMSADE, Université Paris-Dauphine, CNRS UMR 7243, email: lang@lamsade.dauphine.fr
2 GREYC, Université de Caen Basse-Normandie, CNRS UMR 6072, ENSICAEN, email: bruno.zanuttini@unicaen.fr

Abstract. Knowledge-based programs (KBPs) are high-level protocols describing the course of action an agent should perform as a function of its knowledge. The use of KBPs for expressing action policies in AI planning has been surprisingly underlooked. Given that each KBP corresponds an equivalent plan and vice versa, KBPs are typically more succinct than standard plans, but imply more online computation time. Here we compare KBPs and standard plans according to succinctness and to the complexity of plan verification.

1 INTRODUCTION

Knowledge-based programs (KBPs) [4] are high-level protocols which describe the actions an agent should perform as a function of its knowledge, such as, typically, if $K \varphi$ then $\pi$ else $\pi'$, where $K$ is an epistemic modality and $\pi$, $\pi'$ are subprograms.

Thus, in a KBP, branching conditions are epistemically interpretable, and deduction tasks are involved at execution time (online). KBPs can be seen as a powerful language for expressing policies or plans, in the sense that epistemic branching conditions allow for exponentially more compact representations. In contrast, standard policies (as in POMDPs) or plans (as in contingent planning) either are sequential or branch on objective formulas (on environment and internal variables), and hence can be executed efficiently, but they can be exponentially larger (see for instance [1]).

KBPs have surprisingly been underlooked in the perspective of planning. Initially developed for distributed computing, they have been considered in AI for agent design [13] and game theory [7]. For planning, the only works we know of are by Reiter [12], who gives an implementation of KBPs in Golog; Classen and Lakemeyer [3], who implement KBPs in a decidable fragment of the situation calculus; Herzig et al. [6], who discuss KBPs for propositional planning problems, and Laverny and Lang [9, 10], who generalize KBPs to belief-based programs allowing for uncertain action effects and noisy observations.

None of these papers really addresses computational issues. Our aim is to contribute to filling this gap. After some background on epistemic logic (Section 2), we define KBPs (Section 3). Then we address expressivity and succinctness issues (Section 4): we show that, as expected, KBPs can be exponentially more compact than standard policies/plans. Then we give our main contributions, about the complexity of verifying that a KBP is a valid plan for a planning problem: we show $\Pi^2_5$-completeness for while-free KBPs (Section 5) and EXPSPACE-completeness in the general case (Section 6).

2 KNOWLEDGE

A KBP is executed by an agent in an environment. We model what the agent knows about the current state (of the environment and internal variables) in the propositional epistemic logic $S_5$. Let $X = \{x_1, \ldots, x_n\}$ be a set of propositional symbols. A state is a valuation of $X$. For instance, $\pi_{x_1 x_2}$ is the state where $x_1$ is false and $x_2$ is true. A knowledge state $M$ for $S_5$ is a nonempty set of states, representing those which the agent considers as possible: at any point in time, the agent has a knowledge state $M \subseteq 2^X$ and the current state is some $s \in M$. For instance, $M = \{x_1 \bar{x}_2, \bar{x}_1 x_2\}$ means that the agent knows $x_1$ and $x_2$ to have different values in the current state.

Formulas of $S_5$ are built up from $X$, the usual connectives, and the knowledge modality $K$. An $S_5$ formula is objective if it does not contain any occurrence of $K$. Objective formulas are denoted by $\varphi$, $\psi$, etc. whereas general $S_5$ formulas are denoted by $\Phi$, $\Psi$ etc. For an objective formula $\varphi$, we denote by $\text{Mod}(\varphi)$ the set of all states which satisfy $\varphi$ (i.e., $\text{Mod}(\varphi) = \{s \in 2^X, s \models \varphi\}$). The size $|\Phi|$ of an $S_5$ formula $\Phi$ is the total number of occurrences of propositional symbols, connectives and modality $K$ in $\Phi$.

It is well-known (see, e.g., [4]) that any $S_5$ formula is equivalent to a formula without nested $K$ modalities; therefore we disallow them. An $S_5$ formula $\Phi$ is purely subjective if objective formulas occur only in the scope of $K$. In the whole paper we only need purely subjective formulas, because we are only interested in what the agent knows, not on the actual state of the environment. A purely subjective $S_5$ formula is in knowledge negative normal form ($\text{KNNF}$) if the negation symbol $\neg$ occurs only in objective formulas (in the scope of $K$) or directly before a $K$ modality. Any purely subjective $S_5$ formula $\Phi$ can be rewritten into an equivalently $\text{KNNF}$ of polynomial size, by pushing all occurrences of $\neg$ that are out of the scope of $K$ as far as possible with de Morgan’s laws. For instance, $K\neg(p \land q) \lor \neg(Kr \lor \neg K\neg r)$ is not in $\text{KNNF}$, but is equivalent to $K\neg(p \land q) \lor (\neg K\neg r \land \neg K\neg r)$. Summarizing, a subjective $S_5$ formula $\Phi$ in $\text{KNNF}$ (for short, $\Phi \in \text{SKNNF}$) is either a positive (resp. negative) epistemic atom $K\varphi$ (resp. $\neg K\varphi$), where $\varphi$ is objective, or a combination of such atoms using $\land$, $\lor$.

The satisfaction of a purely subjective formulas depends only on a knowledge state $M$, not on the actual current state (see, e.g., [4]):

- $M \models K\varphi$ if for all $s' \in M$, $s' \models \varphi$,
- $M \models \neg K\varphi$ if $M \neq K\varphi$,
- $M \models \Phi \land \Psi$ (resp. $\Phi \lor \Psi$) if $M \models \Phi$ and (resp. or) $M \models \Psi$.

An $S_5$ formula is valid (resp. satisfiable) if it is satisfied by all (resp. at least one) knowledge states $M \subseteq 2^X$. Given two $S_5$ formulas $\Phi$ and $\Psi$, $\Phi$ entails $\Psi$, written $\Phi \models \Psi$, if every knowledge state $M \subseteq 2^X$ which satisfies $\Phi$ also satisfies $\Psi$, and $\Phi$ is equivalent to $\Psi$ if $\Phi$ and $\Psi$ entail each other. Note that $K\varphi \land K\psi$ is equivalent to
Mod $\Phi$ refer either to some $M$. Deciding that can be solved using exponential space. NP oracles, actions is partitioned into Following [6], we assume without loss of generality that the set of $O$. Formally, $O$ is an epistemic modality whose semantics is given in the logic of all I know [11] by

- $M \models O \varphi$ if $M = Mod(\varphi)$.

Hence any atom $\Phi$ of the form $O \varphi$ has exactly one model, written $M(\Phi) = Mod(\varphi) \subseteq 2^X$. We use the term “knowledge state” to refer either to some $M \subseteq 2^X$ or to some atom $O \varphi$. For instance, $M = \{x_1, x_2, x_3, x_4\}$ will also be written $O = O(\neg x_1 \lor x_2)$.

Satisfiability in the logic of all I know is $\Sigma^P_2$-complete [14]. However, we only need restricted entailment tests, which we show to be easier. We recall that $\Delta^P_2 = P^{NP}$ is the class of all decision problems that can be solved in deterministic polynomial time using NP-oracles, $\Pi^P_2 = coNP^{NP}$ the class of all decision problems whose complement can be solved in nondeterministic polynomial time using NP-oracles, and EXPSPACE the class of all decision problems that can be solved using exponential space.

**Proposition 1** Deciding $O \varphi \models \Phi$, where $\varphi$ is objective and $\Phi$ is purely subjective, is in $\Delta^P_2$.

**Proof** Let $\varphi$ and $\Phi$ be as in the claim. Hence $\Phi$ is a Boolean combination of atoms $K \psi$. We give a polynomial time algorithm for deciding $O \varphi \models \Phi$ with a linear number of calls to an oracle for propositional satisfiability, reasoning by induction on the structure of $\Phi$.

First let $\Phi = K \psi$. Then $O \varphi \models \Phi$ reads $\forall M \subseteq 2^X, (M \models O \varphi \Rightarrow \exists s \in M, s \models \psi)$. Since $O \varphi$ has exactly one model $M = Mod(\varphi)$, this is equivalent to $\varphi \models \psi$, i.e., $\varphi \land \neg \psi$ is not satisfiable.

Now let $\Phi = \Phi_1 \lor \Phi_2$ ($\land, \neg$ are similar). Then $O \varphi$ entails $\Phi$ iff it entails $\Phi_1$ or it entails $\Phi_2$. Indeed, $O \varphi$ has only one model $M(O \varphi)$, hence $O \varphi$ entails $\Phi$ iff $M(O \varphi)$ satisfies $\Phi_1$ or $\Phi_2$, that is, iff $O \varphi \models \Phi_1$ or $O \varphi \models \Phi_2$ holds. Hence, deciding $O \varphi \models \Phi$ involves a linear number of calls to the oracle by the induction hypothesis. \hfill $\square$

### 3 KBPS AS PLANS

Our definitions specialize those in [4] to our propositional framework and to a single-agent version. Given a set $A$ of primitive actions, a knowledge-based program (KBP) is defined inductively as follows:

- the empty plan is a KBP,
- any action $\alpha \in A$ is a KBP,
- if $\pi$ and $\pi'$ are KBPs, then $\pi; \pi'$ is a KBP;
- for KBPs $\pi$, $\pi'$ and $\Phi \in SKNNF$, if $\Phi$ then $\pi$ else $\pi'$ is a KBP;
- for a KBP $\pi$ and $\Phi \in SKNNF$, while $\Phi$ do $\pi$ is a KBP.

The class of while-free KBPs is obtained by omitting the while construct. The size $|\pi|$ of a KBP $\pi$ is defined to be the number of occurrences of actions, plus the size of branching conditions, in $\pi$.

#### 3.1 Representation of Actions

Following [6], we assume without loss of generality that the set of actions is partitioned into purely ontic and purely epistemic actions.

An ontic action $\alpha$ modifies the current state of the environment but gives no feedback. Ontic actions may be nondeterministic. For the sake of simplicity we assume them to be fully executable.

Each ontic action is represented by a propositional theory expressing constraints on the transitions between the states of the environment before and after $\alpha$ is taken. Let $X' = \{x' \mid x \in X\}$, denoting the values of variables after the action was taken. The theory of $\alpha$ is a propositional formula $\Sigma_\alpha$ over $X \cup X'$ such that for all states $s \in 2^X$, the set $\{s' \in 2^X \mid ss' \models \Sigma_\alpha\}$ is nonempty, and is exactly the set of possible states after $\alpha$ is performed in $s$. For instance, with $X = \{x_1, x_2\}$, the action $\alpha$ which nondeterministically reinitializes the value of $x_1$ has the theory $\Sigma_\alpha = (\alpha x_1 \leftrightarrow x_2)$.

In the paper we will use the following actions:

- $\text{reinit}(\alpha)$ (for some $Y \subseteq X$) with theory $\bigwedge_{x \in Y} x' \leftrightarrow x$,
- $x_i := \varphi$ (for $\varphi$ objective) with theory $x_i' \leftrightarrow \varphi \land \bigwedge_{j \neq i} x'_j \leftrightarrow x_j$,
- $\text{switch}(x_i)$ with theory $x_i' \leftrightarrow \neg x_i \land \bigwedge_{j \neq i} x'_j \leftrightarrow x_j$,
- the void action $\Lambda$ with theory $\bigwedge_{x \in X} x' \leftrightarrow x$.

Now, an epistemic action has no effect on the current state, but gives some feedback about it, that is, it modifies only the knowledge state of the agent (typically, a sensing action). We represent such an action by the list of possible feedbacks. Formally, the feedback theory of $\alpha$ is a list of positive epistemic atoms, of the form $\Omega_\alpha = (K\varphi_1, \ldots, K\varphi_n)$. For instance, the epistemic action which senses the value of an objective formula $\varphi$ is

- $\text{test}(\varphi)$ with feedback theory $\Omega_{\text{test}(\varphi)} = (K\varphi, K \neg \varphi)$.

Finally, for an objective formula $\varphi$ over $X$, we write $\varphi'$ for the formula obtained from $\varphi$ by replacing each occurrence of $x \in X$ with $x'$. We also write $\Sigma^{\varphi'}_{\alpha \leftarrow i}$ for the formula obtained from $\Sigma_\alpha$ by replacing each unprimed variable $x \in X$ with $x'$, and each primed variable $x'$ with $x^{i+1}$. For instance, for $\varphi_2 = (x_1 \lor x_2)$, $\varphi_5' = (x_1' \lor x_2')$, and for $\Sigma_\alpha = (\alpha x_1 \leftrightarrow x_2)$, $\Sigma_\alpha'$ is $(\alpha x_2 \leftrightarrow x_2')$.

#### 3.2 Semantics

The agent executing a KBP starts in some knowledge state $M_0$, and at any timestep $t$, it has a current knowledge state $M'_t$. When execution comes to a branching condition $\Phi$, $\Phi$ is evaluated in the current knowledge state (the agent decides $M'_t \models \Phi$).

The knowledge state $M'_t$ is defined inductively as the progression of $M_{t-1}$ by the action executed between $t-1$ and $t$. Formally, given a knowledge state $M \subseteq 2^X$ and an ontic action $\alpha$, the progression of $M$ by $\alpha$ is defined to be the knowledge state $\text{Prog}(M, \alpha) = M' \subseteq 2^X$ defined by $M' = \{s' \in 2^X \mid ss' \models \Sigma_\alpha\}$, Intuitively, after taking $\alpha$ in a state which it knows to be one in $M$, the agent knows that the resulting state is one of those $s'$ which are reachable from any $s \in M$ through $\alpha$. Note that the agent knows that some outcome of the action has occurred (it knows $\Sigma_\alpha$), but not which one.

Now given an epistemic action $\alpha$, a knowledge state $M$, and a feedback $K\varphi \in \Omega_\alpha$ with $M \not\models K \neg \varphi$, the progression of $M$ by $K\varphi$ is defined to be $\text{Prog}(M, K\varphi) = M_\varphi = \{s \in M \mid s \models \varphi\}$. The progression is undefined when $M \models K \neg \varphi$. Intuitively, a state is considered to be possible after obtaining feedback $\varphi$, if and only if it was considered to be possible before taking the epistemic action, and it is consistent with the feedback obtained. Here, observe that though an epistemic action can yield different feedbacks, at execution time the agent knows which one it gets.

---

3 This induces a loss of generality, but in practice, if $\alpha$ is not executable in $s$, this can be expressed by letting $\alpha$ lead to a sink (nongoal) state.
Example 1 (from [6]). Consider the following KBP $\pi$:

$$
test(x_1 \leftrightarrow x_2);
$$

If $K(x_1 \leftrightarrow x_2)$ then $test(x_1 \land x_2)$ else $switch(x_1); test(x_1 \land x_2)$

With $M^0 = O(\text{nothing known})$, $Prog(M^0, K(\neg(x_1 \leftrightarrow x_2)))$ is $M^1 = O(x_1 \leftrightarrow \neg x_2)$. $Prog(M^1, switch(x_1))$ is $M^2 = O(x_1 \leftrightarrow x_2)$, and $Prog(M^2, K(\neg(x_1 \land x_2)))$ is $M^3 = O(\neg x_1 \land \neg x_2)$.

We are now ready to give an operational semantics for KBPs. Given a knowledge state $M$ involving only primed variables of the form $x^i$ ($x \in X$), we write plain($M$) for the knowledge state obtained by replacing $x^i$ with $x$ for all $x \in X$.

An execution trace (or trace) $\tau$ of a KBP $\pi$ in $M^0$ is a sequence of knowledge states, either infinite, i.e., $\tau = (M^i)_{i \geq 0}$, or finite, i.e. $\tau = (M^0, M^1, \ldots, M^T)$, and satisfying:

- if $\pi$ is the empty plan, then $\tau = (M^0)$;
- if $\pi$ is an ontic action $\alpha$, then $\tau = (M^0, \text{plain}(Prog(M^0, \alpha)))$;
- if $\pi$ is an epistemic action $\alpha$, then $\tau = (M^0, Prog(M^0, K(\varphi_\alpha)))$ for some $K \varphi_\alpha \in \Omega_\alpha$ with $M^0 \not\models K \varphi_\alpha$;
- for $\pi = \pi_1 \cup \pi_2$, either $\tau_1$ with $\tau_1$ an infinite trace of $\pi_1$, or $\tau = \tau_1 \tau_2$ with $\tau_1$ a finite trace of $\pi_1$ and $\tau_2$ a trace of $\pi_2$;
- if $\pi$ is if $\Phi$ then $\pi_1$ else $\pi_2$, then either $M^0 \not\models \Phi$ and $\tau$ is a trace of $\pi_1$, or $M^0 \models \Phi$ and $\tau$ is a trace of $\pi_2$;
- if $\pi$ is while $\Phi$ do $\pi_1$, then either $M^0 \models \Phi$ and $\tau$ is a trace of $\pi_1$, or $M^0 \not\models \Phi$ and $\tau = (M^0)$.

We say that $\pi$ terminates in $M^0$ if every trace of $\pi$ in $M^0$ is finite.

Example 2 Let $\pi, M^0, \ldots, M^3$ as in Ex. 1, and $M^4 = O(x_1 \land x_2)$. The traces of $\pi$ in $M^0$ (with the corresponding feedbacks) are:

- $(M^4, M^3, M^2, M^1)$, $K(\neg(x_1 \leftrightarrow x_2)), K(\neg(x_1 \land x_2))$
- $(M^4, M^3, M^2, M^1)$, $K(\neg(x_1 \leftrightarrow x_2)), K(x_1 \land x_2)$
- $(M^4, M^3, M^2, M^1)$, $K(x_1 \leftrightarrow x_2), K(\neg(x_1 \land x_2))$
- $(M^4, M^3, M^2, M^1)$, $K(x_1 \leftrightarrow x_2), K(x_1 \land x_2)$

4 KBPS VS. STANDARD POLICIES

We now briefly compare KBPs with standard policies (or plans) with respect to succinctness and expressiveness. As opposed to a KBP, a standard policy is a program with objective branching conditions. This encompasses plans for classical planning, which are sequences of feedbacks for the epistemic actions executed, and other types of policies, such as controllers with finite memory.

Clearly, every KBP $\pi$ can be translated into an equivalent standard policy (a “protocol” in [4]), by simulating all possible executions of $\pi$ and, for all possible executions of the program, evaluating all (epistemic) branching conditions. Vice versa, it is clear that any standard policy can be translated to an equivalent KBP.

Such translations are of course not guaranteed to be polynomial. In particular, a standard policy $\pi$ described in space $O(n)$ can manipulate at most $n$ variables (through actions or branching conditions). It follows that it can be in at most $|\pi|^{2^n}$ different configurations (value of each variable plus control point in the policy), hence if it terminates, its traces can have length at most $|\pi|^{2^n}$ (being twice in the same configuration would imply a potential infinite loop). In contrast, we will give in Section 6 a KBP described in space polynomial in $n$ but with a finite trace of length $2^{2^n}$.

However, what is gained on succinctness is lost on the complexity of execution. When executing a KBP, the problem of evaluating a branching condition is in $\Delta^P_2$, but is both NP- and coNP-hard. Indeed, it is coNP-hard because $O(T) \models K\varphi$ corresponds to $\varphi$ being valid, and NP-hard because $O(T) \models \neg K\varphi$ corresponds to $\varphi$ being satisfiable. On the other hand, when executing a standard policy, evaluating an (objective) condition can be done in linear time by reading the values of the (internal and environment) variables involved.

Interestingly, even the restriction to while-free KBPs does not imply a loss of expressivity. Indeed, if a loop terminates, then it is guaranteed to be executed less than $2^{2^n}$ times (see Section 6), and hence it can be unrolled, yielding an equivalent while-free KBP. However, this obviously comes also with a loss of succinctness.

When KBPs are seen as plans which achieve goals, as we consider in this article, the translations outlined above preserve the property that the KBP/policy indeed achieves the goal. Therefore, from the point of view of plan existence, considering KBPs or standard plans makes no difference: there is a plan for a given problem if and only if there is a KBP for it (provided the size of plans is not restricted).

Moreover, since the input is the same in both cases, the complexity of plan existence is independent of whether we look for policies or KBPs. Things are different for the problem of verifying that a KBP/policy is a plan for some goal, because the KBP or policy is part of the input. For example, we will see in Section 6 that verifying while-free KBPs is $\Pi^P_2$-complete. In contrast, it can easily be shown that verifying a while-free policy is in coNP (with essentially the same proof as Proposition 2).

5 VERIFYING WHILE-FREE KBPS

We now investigate the computational problem of verifying that a KBP $\pi$ is valid for a planning problem. Precisely, we define a knowledge-based planning problem $P$ to be a tuple $(\Phi^0, A_0, A_E, G)$, where $\Phi^0 = O\varphi^0$ is the initial knowledge state, $G$ is a SKNNF S5 formula called the goal, and $A_0$ (resp. $A_E$) is a set of ontic (resp. epistemic) actions together with their theories. Then a KBP $\pi$ (using actions in $A_0 \cup A_E$) is said to be a (valid) plan for $P$ if its execution in $\Phi^0$ terminates, and for all traces $(M^0, \ldots, M^T)$ of $\pi$ with $M^0 = M(\Phi^0), M^T \models G$ holds. Intuitively, this means that executing $\pi$ always leads to a knowledge state where the agent is sure that $G$ holds. For instance, in Example 1, $\pi$ is a plan for $\Phi^0 = O(T)$ and the goal $G = (Kx_1 \lor K\neg x_1) \land (Kx_2 \lor K\neg x_2)$.

Definition 1 (verification) The plan verification problem takes as input a knowledge-based planning problem $P = (\Phi^0, A_0, A_E, G)$ and a KBP $\pi$, and asks whether $\pi$ is a plan for $P$.

In this section we show that verification is $\Pi^P_2$-complete for while-free KBPs, even under several further restrictions. Observe first that a while-free KBP always terminates.

We start with membership in $\Pi^P_2$. In the broad lines, the argument is that $\pi$ is not a plan for $P$ if there exists a trace $\tau$ of $\pi$ (or, equivalently, a sequence of feedbacks for the epistemic actions executed) in which the last knowledge state does not satisfy $G$. Hence $\pi$ can be verified not to be a plan for $P$ by guessing such a sequence of feedbacks and simulating the corresponding execution.

Nevertheless, we must perform such simulation in polynomial space. Unfortunately, in general the progression of a knowledge state $M$ represented as $O\varphi$ cannot be performed in polynomial space.

Example 3 The progression of $O\varphi$, for $\varphi = \bigwedge_{i=1}^n (x_i \land y_i \rightarrow z_i) \land (\bigwedge_{i=1}^n z_i \rightarrow z)$, by reinit($\{z_1, \ldots, z_n\}$), is equivalent to
progression that using an oracle for propositional satisfiability. Intuitively, it simulates \( \Phi \mod{\Sigma} \Phi \), Plan verification is in Proposition 2

\[
O(2^n) \equiv \sum_{k \in \{2^n_1, \ldots, 2^n_r\}} (f_1 \land \ldots \land f_n \rightarrow z), \text{ which has no polynomial representation, while } |\varphi| \text{ is linear.}
\]

Hence we introduce another form of progression, called memoryful progression, which explicitly keeps track of successive knowledge states instead of projecting to the current instant. Namely, we define a memoryful knowledge state for a timestep \( t \) to be a formula of the form \( O^{t+1}_\varphi \), where \( \varphi \) is an objective formula over the set of variables \( \{x^1, \ldots, x^n\}, \) \( X \in \mathbb{X} \). Intuitively, \( O^{t+1}_\varphi \) represents the past and present knowledge of the agent at timestep \( t \). Formally:

- for an ontic \( \alpha \), \( \text{MemProg}(O^{t+1}_\varphi, \alpha) = O(\varphi \land \Sigma_{t+1}^{\varphi}) \)
- for a feedback \( K_{\varphi_1} \), \( \text{MemProg}(O^{t+1}_\varphi, K_{\varphi_1}) = O(\varphi \land \varphi_1) \)

Observe that ontic actions increment the current timestep, while epistemic actions do not (they do not modify the current state).

**Example 4 (Example 1, continued) The memoryful progression of \( O^t \) by \( K(\bar{x}_1 \leftrightarrow \bar{x}_2) \), then switch(\( x_1 \)), then \( K(\bar{x}_1 \land \bar{x}_2) \) is \( O(\top \land (x_1 \land \neg x_2) \land (x_1 \land \neg x_2) \land (x_1 \land \neg x_2) \land \neg(x_1 \land x_2)). \)

Clearly, the memoryful progression of \( O^{t+1}_\varphi \) by \( \alpha \) (resp. \( K_{\varphi_1} \)) has a size linear in \( |\varphi| \) and \( |\Sigma_a| \) (resp. \( |K_{\varphi_1}| \)). Hence iterating the memoryful progression of \( \Phi \) a polynomial number of times \( \text{poly}(|\varphi|) \) yields a (memoryful) knowledge state of polynomial size.

**Lemma 1 Let \( O^{t}_\varphi \) be a knowledge state, and \( L = (\ell_1, \ldots, \ell_k) \) be a sequence of \( U \) ontic actions and \( \top \land \neg U \) feedbacks. Then the iterated progression \( M \circ M' \) by \( L \) satisfies an epistemic formula \( \Phi \) iff the iterated memoryful progression \( O^{tU}_\varphi \) of \( O^{tU}_\varphi \) by \( L \) entails \( \Phi^t \).

**Proof Sketch** Renaming variables, \( M \models \Phi \) is equivalent to \( M^{t} \models \Phi^{t} \). On the other hand, it is easily seen from the definitions that \( M^{t} \) is exactly \( \text{Mod}(\exists X^1, \ldots, \exists X^n \land \neg \Phi^{tU}) \). Because \( \Phi^{tU} \) contains only variables in \( X^{tU} \), it follows that \( M^{t} \models \Phi^{t} \) is equivalent to \( \text{Mod}(\Phi^{tU}) = \Phi^{tU} \text{ [8, Corollary 7], i.e., to } O^{tU}_\varphi \models \Phi^{tU} \).

Recall that a problem is in \( \Pi^0_2 \) if its complement can be solved by a polytime nondeterministic algorithm which uses an NP-oracle.

**Proposition 3 Plan verification is in \( \Pi^0_2 \) for while-free KBPs.

**Proof** We use Algorithm 1, which decides whether \( \pi \) is not valid using an oracle for propositional satisfiability. Intuitively, it simulates an execution of \( \pi \), and guesses a sequence of feedbacks witnessing that \( \pi \) is not valid. Clearly, it runs in nondeterministic polynomial time, and it uses a polynomial number of calls to the oracle: one per check that \( \varphi \land \varphi_1 \) is satisfiable, a linear number per check \( O^{tU}_\varphi \models \Phi^t \) (Proposition 1), and a linear number for the final check.

**6 VERIFYING KBPS WITH LOOPS**

For general KBPs, we now show verification to be \( \text{EXPSPACE-complete} \) (\( \text{EXPSPACE} \) is the class of decision problems with an exponential space algorithm). On the way, we build a polythesize KB with a doubly exponentially long trace, which we use as a clock. Since the construction is of independent interest, we present it first.

**6.1 A Very Slow KBP**

We write \( > \) for the lexicographic order on states. For instance, \( 2^k \) is ordered by \( x_1 x_2 x_3 \rightarrow x_1 x_2 x_3 \rightarrow x_1 x_2 x_3 \rightarrow \cdots \rightarrow x_1 x_2 x_3 \) for \( n = 3 \) variables. Given \( X \) and a knowledge state \( M \) over a superset of \( X \), we write \( M_X \) for \( \{x \mid s \in M\} \), where \( s_X \) denotes the restriction of \( s \) to the variables in \( X \). This allows us to use auxiliary variables and still talk about the knowledge state about \( X \).

We build a compact KB (of size polynomial in \( n \)) with exactly one trace, of size \( 2^{2^n} - 1 \). As discussed in Section 4, this is impossible with standard policies, but possible for KBPs because their configurations include a knowledge state, and there are \( 2^{2^n} - 1 \) of them (every nonempty subset of \( 2^n \)). Hence there can be a program \( \pi \), which passes through \( 2^{2^n} - 1 \) different configurations while being specified with only \( O(n) \) variables and in space \( |\pi| \) polynomial in \( n \).

**Routines and Actions** We build our KBP so that its execution passes through each possible knowledge state exactly once. To do so, we need some specific actions and routines which allow to go from a knowledge state to the next one.

The first routine determines the state \( s \) in \( M \) with the greatest restriction \( M_X \) (wrt \( > \)), and stores it over some auxiliary variables \( g_1, \ldots, g_n \). For instance, if the current knowledge state satisfies \( M_X = \{x_1 x_2 x_3, x_1 x_2 x_3, x_1 x_2 x_3\} \), then after executing the routine, the agent knows \( g_1 \land \neg g_2 \land \neg g_3 \) (and \( M_X \) is unchanged).

We define \( \pi^+_n \) to perform a dichotomic search in \( M \). For instance, if \( K(\bar{x}_1 \leftrightarrow g_1) \rightarrow \neg \bar{x}_2 \) is true, then no assignment in \( M \) which satisfies \( x_1 \leftrightarrow g_1 \) (i.e., by construction, none of the assignments with greatest \( x_1 \)) satisfies \( x_2 \), hence the greatest one satisfies \( \neg \bar{x}_2 \). Precisely, \( \pi^+_n \) is the following KBP:

**Algorithm 1: Deciding whether a while-free \( \pi \) is not valid**

\[
t := 0, O^{tU}_\varphi = \Phi^t; \]

\[\text{while } \pi \text{ is not the empty KBP do}
\]

\[\text{if } \pi = \alpha; \pi' \text{ and } \alpha \text{ is ontic then}
\]

\[O^{tU+1}_\varphi := \text{MemProg}(O^{tU}_\varphi, \alpha);
\]

\[\pi := \pi', t := t + 1;
\]

\[\text{else if } \pi = \alpha; \pi' \text{ and } \alpha \text{ is epistemic then}
\]

\[\text{guess a feedback } K_{\varphi_1} \in \Omega_{\alpha} ;
\]

\[\text{check that } \varphi^\prime \land \varphi_1 \text{ is satisfiable;}
\]

\[O^{tU}_\varphi := \text{MemProg}(O^{tU}_\varphi, K_{\varphi_1});
\]

\[\text{else ( } \pi \text{ is of the form if } \varphi \text{ then } \pi_1 ; \text{ else } \pi_2 ; \text{ else } \pi_3 ; \text{ else } \pi_4 ; \text{ else } \pi_5 )
\]

\[\text{check } O^{tU}_\varphi \models \Phi^t; \]

\[\text{then return } \pi_1 ; \text{ else return } \pi_2 ; \text{ else return } \pi_3 ; \text{ else return } \pi_4 ; \text{ else return } \pi_5 .\]

If \( K(\neg x_1) \) then \( g_1 := 0 \text{ else } g_1 := 1; \)

If \( K((x_1 \leftrightarrow g_1) \rightarrow \neg \bar{x}_2) \) then \( g_2 := 0 \text{ else } g_2 := 1; \)
... 

If \( K(\wedge_{i=1}^{n-1} x_i \leftrightarrow g_i) \rightarrow \neg x_n \) then \( g_n := 0 \) else \( g_n := 1 \);

We now introduce an ontic action which adds a given state \( s_a \in 2^X \) to \( M \). We assume \( s_a \) is encoded over some auxiliary variables \( a_1, \ldots, a_n \). The action \( a_{add} \) is a simple nondeterministic one, which either does nothing or sets \( x_1, \ldots, x_n \) to the values of \( a_1, \ldots, a_n \). Formally, its action theory is \( (\wedge_{i=1}^{n-1} x_i \leftrightarrow g_i) \lor (\wedge_{i=1}^{n-1} x_i \leftrightarrow a_i) \) (and no effect on auxiliary variables). Hence after taking this action, the agent exactly knows that either the environment is in the same state as before, or it is in the state \( a_1 \ldots a_n \).

We finally introduce a routine \( \pi_i^n \), which removes a given state \( s_r \in 2^X \) (encoded over auxiliary variables \( r_1, \ldots, r_n \)) from \( M \). We assume that the agent knows the state to be removed, that is, \( M \) satisfies \( K r_i \lor K \neg r_i \) for all \( i = 1, \ldots, n \).

Recall that by definition, knowledge states are nonempty. Hence we allow removal of \( s_r \) only if there is another state \( s_g \in M \), ensuring \( M \setminus \{ s_r \} \neq \emptyset \). Then \( \pi_i^n \) removes \( s_r \) from \( M \) by identifying a distinguished state \( s_g \neq s_r \) in \( M \), then executing an action \( a_i^n \) which maps any state to itself except for \( s_r \), which it maps to \( s_g \).

We identify \( s_g \) by running \( \pi_i^n \). If it turns out that \( s_g \) is precisely \( s_r \), as can be decided since the agent knows (i) the value of \( s_r \) by assumption, and (ii) that of \( s_g \) by construction of \( \pi_i^n \), then \( \pi_i^n \) replaces \( s_g \) with the least assignment in \( M \), using the dual of \( \pi_i^n \).

Finally, \( a_i^n \) is defined to be the deterministic ontic action with theory \( \bigwedge_{i=1}^n x_i \leftrightarrow (x_i \oplus (\wedge_{i=1}^{n-1} x_i \leftrightarrow r_i) \land (x_i \oplus g_i)) \) (and no effect on auxiliary variables). A case analysis shows that \( a_i^n \) maps \( s \) to itself except for \( s_r \), which it maps to \( s_g \), as desired.

**Proposition 4** The progression \( M' \) of a knowledge state \( M \) by \( \pi_i^n \) satisfies \( \bigwedge_{i=1}^n K g_i^n \), where \( g_i^n \) is \( g_i \) (resp. \( \neg g_i \)) if the greatest state in \( M \cdot x_i \) (resp. \( \neg x_i \)). The progression by \( a_{add} \) (resp. \( \pi_i^n \)) satisfies \( M_X = M \cup \{ s_a \} \) (resp. \( M_X = M \setminus \{ s_g \} \)).

Importantly, \( g_i^n, a_{add}^n, \pi_i^n \) all have a description of size at most quadratic in \( n \). Finally, we use a routine, written \( \pi_d \) ("decrement"), which replaces the state encoded by \( g_i \), \( a_{add} \), \( \pi_i^n \) by its predecessor \( w > (\text{its definition is straightforward, and omitted for space reasons}).

**A Slow KBP** We see a knowledge state \( M \) as a vector \( \vec{m} = m_1 m_2 \ldots m_{n-1} m_{2^n+1} \), with \( m_i \) if and only if the \( i \)th state \( s_{i-1} \) (wrt \( > \)) is in \( M \). Then our KBP starts with \( m_0 = 00 \ldots 01 \) (i.e., \( M_0 = \{ 11 \ldots 1 \} \equiv K x_1 \land \ldots \land x_n \)), and loops until \( m_i = 10 \ldots 00 \) \((M^i = \{ 00 \ldots 0 \} \equiv K \neg x_1 \land \ldots \land \neg x_n \)) specialization. The loop changes the current \( m_i \) to \( m_{i+1} \) using the Gray code, which is a way to enumerate all Boolean vectors by changing exactly one bit at a time.

**Definition 2** (Gray Code) The successor of \( \vec{m} \) according to the Gray Code is obtained from \( \vec{m} \) as follows:

1. if \( \vec{m} \) has an even number of 1’s, flip \( m_{2^n} \),
2. otherwise, let \( g = \max \{ i \mid m_i = 1 \} \) and flip \( m_{g-1} \).

For instance, the enumeration is 0001, 0011, 0010, 0110 ... 1000 for \( n = 2 \) (we do not use 0000). In terms of knowledge states, this is \( \{ x_1 x_2 \}, \{ x_1 x_2, x_1 x_2 \}, \{ x_1 x_2, x_1 x_2 \}, \ldots, \{ x_1 x_2 \} \), which indeed passes through all knowledge states.

By definition of \( m_i \), the greatest \( i \) with \( m_i = 1 \) identifies the greatest state in \( M \), and flipping \( m_i \) amounts to add/remove \( s_i \) from \( M \).

With this in hand, our KBP clock\(^n\) (Algorithm 2) uses a set of \( n \) variables \( X \) and auxiliary variables \( g_1, \ldots, g_n, a_1, \ldots, a_n, r_1, \ldots, r_n \).

**Proposition 5** The unique trace for clock\(^n\) in \( M \bar{a} \) has size \( 2^{2^n} - 1 \).

---

### 6.2 EXSPACE-hardness

We now show that verifying general KBPs is EXSPACE-complete. We prove hardness with a reduction from nondeterministic unobservable planning (NUP) [5]. An instance of NUP is a triple \((\varphi^0, A_H, \varphi_C)\) where \( \varphi^0, \varphi_C \) are propositional formulas and \( A_H \) is a set of ontic, nondeterministic actions (see below). The question is whether there is a plan, i.e., a sequence of actions, which reaches a state satisfying \( \varphi_C \) from any state satisfying \( \varphi^0 \) (in our terms, whose traces in \( O \varphi^0 \) all end in a knowledge state satisfying \( K \varphi_C \)).

The algorithms considered by Haslum and Jonsson (HJ-actions for short) [5] are different from ours. They are defined inductively as follows (we adapt their notation for consistency):

- \( x_1 := 0 \) and \( x_1 := 1 \) are HJ-actions for any \( x_1 \in X \),
- if \( a_1, a_2 \) are HJ-actions, then \( a_1; a_2 \) is an HJ-action,
- if \( \varphi \) is a propositional formula and \( a_1, a_2 \) are HJ-actions, then if \( \varphi \) then \( a_1 \) else \( a_2 \) is an HJ-action,
- if \( a_1, a_2 \) are HJ-actions, then \( a_1; a_2 \) is an HJ-action.

The semantics of executing such an action is the same as ours for the three first constructs, given that \( \varphi_0 \) defines the initial knowledge state \( O \varphi^0 \). As for nondeterminism, the progression of \( M^i \) by \( a_1; a_2 \) is simply defined to be \( \text{Prog}(M^i, a_1) \cup \text{Prog}(M^i, a_2) \) (at execution time exactly one of \( a_1, a_2 \) occurs, but we do not know which one).

The idea of our reduction is to build a KBP, written simulate, which explores all possible plans (up to size \( 2^{2^n} \)), see below) for an NUP problem, and which is valid if and only if none achieves the goal. For this, we first associate a routine (KBP) \( \pi(a) \) to any HJ-action \( a \), so as to be able to use \( a \) in simulate. Indeed, conditional HJ-actions are not allowed in KBPs because they branch on objective formulas, and nondeterministic HJ-actions are not directly allowed.

For a of the form if \( \varphi \) then \( a_1 \) else \( a_2 \), we define \( \pi(\varphi) \) by "pushing in" the objective test to the assignments. Precisely, we define \( \pi(\varphi) \) to be the \( c := \varphi; \pi_c(a_1); \pi_{\neg \varphi}(a_2) \) with \( \pi_c \) defined inductively by:

- \( \pi_c(x := \psi) = (x := (x \oplus (c \land (x \oplus \psi)))) \),
- \( \pi_c(a_1; a_2) = (\pi_c(a_1); \pi_c(a_2)) \),
- \( \pi_c(\varphi \land a_1; a_2) = (c \land \varphi; \pi_c(a_1); \pi_{\neg \varphi}(a_2)) \),
- \( \pi_c(\varphi \land a_1; a_2) = (\pi_c(a_1); \pi_c(a_2)) \).

Intuitively, executing \( a_1 \) or \( a_2 \) in \( M \bar{a} \) leads to the same knowledge state \( M^{i+1} \bar{a} \), while \( \pi_0(a) \) leaves \( M \bar{a} \) unchanged (the construction of

---

5 In [5] this operator is \( n \)-ary, but as the conditions are mutually inconsistent, their \( \varphi^0 \in \{ \vdots \varphi_k \in \{ \vdots \varphi_k \} \} \) can be rewritten as if \( \varphi_1 \) then \( a_1 \) else (if \( \varphi_2 \) then \( a_2 \) else (\ldots)).
\(\pi_\psi(x := \psi)\) is the same as for the action \(a_2^\psi\) in Section 6.1. Interestingly, this construction shows that the restriction to purely subjective branching conditions in KBPs is without loss of generality.

Finally, for nondeterminism we use the action \(\text{reinit}(h)\), where \(h\) is an auxiliary variable, for simulating a coin flip (\(h\) stands for “heads”), and we define \(\pi(a_1, a_2)\) to be \((\text{reinit}(h); \pi_\psi(a_1); \pi_\psi(a_2))\).

**Lemma 2** For any HJ-action \(a\), the KBP \(\pi(a)\) can be built efficiently, and for any \(M\), the progressions \(M^*\) and \(M'\) of \(M\) by a (resp. \(\pi(a)\)) satisfy \((M^*_{M'})_X = M'_X\) (ignoring auxiliary variables).

**Proposition 6** The verification problem for KBPs is EXPSPACE-hard. Hardness holds even if only one while-loop is allowed and the KBPs to be verified are known to terminate.

**Proof** We use both results that deciding whether an NUP instance has a plan is EXPSPACE-complete, and that an instance has a plan if and only if it has one of size at most \(2^n\) [5].

Given an NUP instance \((\varphi^0, \Theta, \varphi, G)\), we build the knowledge-based planning problem \((\varphi^0, \Theta, A_E, \varphi, G)\) and the KBP simulate. This KBP uses the set of \(n\) variables \(X\) of the NUP instance, together with auxiliary sets of variables of size \(n\) for use by \(\text{clock}^n\) (using disjoint sets of variables makes \(\text{clock}^n\) run in parallel of the simulation itself). Then it loops over a guess of an action in \(\Theta \equiv \{a_1, \ldots, a_k\}\): this is achieved by flipping \(k\) coins (using \(\text{reinit}(h_1, \ldots, h_k)\)) and executing the first action whose coin turned heads (determined by taking the epistemic actions test\((h_i)\)).

The KBP simulate is depicted as Algorithm 3. We let \(\text{clock}^n\) be a KBP which counts up to \(2^n\) (obtained, say, by adding a dummy action to \(\text{clock}^n\)). Clearly, simulate can be built in polynomial time.

**Algorithm 3:** The KBP simulate

\[
\text{initialize} \quad \text{clock}^n + \\
\{\text{Loop until NUP goal reached for sure or clock beeps}\}; \\
\text{while } \neg \varphi_G \land \neg \varphi_G \land \cdots \land \neg \varphi_G \text{ do} \\
\quad \text{run one step of } \text{clock}^n; \\
\quad \text{reinit}\((h_1, \ldots, h_k)\); \text{test}\((h_1)\); \cdots \text{test}\((h_k)\); \\
\quad \text{if } \text{K}h_1 \text{ then } \pi(a_1); \\
\quad \text{else if } \text{K}h_2 \text{ then } \pi(a_2); \\
\quad \cdots; \\
\quad \text{else if } \text{K}h_k \text{ then } \pi(a_k); \\
\}
\]

Let \(p\) be a plan of length at most \(2^n\) for the NUP instance. Then by definition, the trace of simulate in which precisely the actions in \(p\) are chosen by \(\text{reinit}(h_1, \ldots, h_k)\) ends up with \(\varphi_G\) being true, i.e., the goal \(\neg \varphi_G\) being false. Hence simulate is not valid. Conversely only a choice of actions which achieve \(\varphi_G\) can witness that simulate is not valid, but if simulate is not valid then there is a plan for the NUP instance. Hence NUP reduces to the complement of KBP verification, hence the latter is \(\text{coEXPSPACE}\)-hard, that is, \(\text{EXPSPACE}\)-hard. \(\square\)

**Proposition 7** The verification problem for KBPs is in EXPSPACE.

**Proof** The proof mimicks Proposition 2 and Algorithm 1. Because a while loop being executed more than \(2^n\) times would necessarily start at least twice in the same knowledge state and hence run forever, such loops are unrolled \(2^n\) times. These can be counted over \(2^n\) bits, hence in exponential space. As for the current knowledge state, instead of using memoryful progression (which would grow as the number of steps unrolled), we maintain \(M^*\) in extension (as its explicit list of states), again in exponential space. Hence the problem is in \(\text{coEXPSPACE}\), hence in \(\text{coEXPSPACE} = \text{EXPSPACE}\) by Savitch’s theorem.

**ACKNOWLEDGEMENTS**

Supported by the French National Research Agency under grant ANR-10-BLAN-0215.

**REFERENCES**