An Operational Semantics for a Fragment of PRS

Lavindra de Silva¹, Felipe Meneguzzi² and Brian Logan³

¹ Institute for Advanced Manufacturing, University of Nottingham, Nottingham, UK
² Pontifical Catholic University of Rio Grande do Sul, Porto Alegre, Brazil
³ School of Computer Science, University of Nottingham, Nottingham, UK
lavindra.desilva@nottingham.ac.uk, felipe.meneguzzi@pucrs.br, brian.logan@nottingham.ac.uk

Abstract

The Procedural Reasoning System (PRS) is arguably the first implementation of the Belief–Desire–Intention (BDI) approach to agent programming. PRS remains extremely influential, directly or indirectly inspiring the development of subsequent BDI agent programming languages. However, perhaps surprisingly given its centrality in the BDI paradigm, PRS lacks a formal operational semantics, making it difficult to determine its expressive power relative to other agent programming languages. This paper takes a first step towards closing this gap, by giving a formal semantics for a significant fragment of PRS. We prove key properties of the semantics relating to PRS-specific programming constructs, and show that even the fragment of PRS we consider is strictly more expressive than the plan constructs found in typical BDI languages.

1 Introduction

The Procedural Reasoning System (PRS) [Georgeff and Ingrand, 1989; Georgeff and Lansky, 1987; 1986] is generally recognised as one of the first implementations of the Belief–Desire–Intention (BDI) [Bratman, 1987] model of agency and practical reasoning. PRS has been extremely influential, and is still widely used [Ghallab et al., 2016], particularly in robotics, e.g., [Ingrand et al., 1996; Alami et al., 1998; Foughali et al., 2016; Niemueller et al., 2017; Lemaignan et al., 2017]. For example, PRS-based systems secured first and second places in recent RoboCup and ICAPS logistics competitions. PRS has also influenced the design of many subsequent BDI-based agent programming languages, e.g., [Rao, 1996; Huber, 1999; Busseta et al., 1999; Winikoff et al., 2002; Morley and Myers, 2004; Sardina et al., 2006; Sardina and Padgham, 2011], though most of these languages implement only a subset of the programming language features supported by PRS. Surprisingly, given its centrality in the BDI paradigm, PRS lacks a formal operational semantics, which makes it difficult to determine its expressive power relative to other BDI agent programming languages, or to verify the correctness of PRS programs. For example, there is a widespread "folk belief" in the agent programming community that the plan graphs used by PRS are more expressive than most if not all other BDI agent formalisations, yet no proof of this intuition exists.

In this paper, we give a formal semantics for a significant fragment of PRS. We focus on language features specific to PRS, and in particular, its graph-based representation for plans and its programming constructs for maintaining a condition (i.e., maintenance goals). We make three main contributions. First, we develop a formalisation for the syntax of PRS as a directed bipartite graph (Section 2). Second, we provide an operational semantics that accounts for graph-based plans and adopting, suspending, resuming, and aborting (nested) maintenance goals (Section 3). Third, we prove key properties of the semantics of these PRS-specific programming constructs, and show that PRS plan-graphs are strictly more expressive than the plan rules found in typical BDI languages (Section 4). In Section 5, we briefly discuss related work and conclude.

2 PRS Syntax

We briefly recall the syntax and deliberation cycle of PRS, as defined in [Ingrand, 1991]. In the interests of brevity, we omit some features of the language, including meta-level reasoning, ‘true concurrency’, semaphores, and features such as ‘if’ and ‘else’ statements expressible in terms of the fragment we define. Plans in PRS consist of graphs. For compactness, and to allow a precise specification of the semantics, we adopt a plan-rule notation similar to that used in other BDI-based agent programming languages to specify the triggering and context conditions of plans, and specify plan bodies using a textual representation of bipartite graphs. We assume a first-order language with a vocabulary consisting of mutually disjoint and infinite sets of variable, constant, predicate, node, event-goal, and action symbols.

A PRS agent is defined by a belief base B, an action-library A, and a plan-library Π. A belief base is a set of ground atoms. An action-library is a set of action-rules specifying the actions available to the agent. An action is of the form act(ℓ), where act is an n-ary action symbol denoting an evaluable function that may change the agent’s environment, and ℓ = t₁, . . . , tᵣ are (possibly ground) terms. Action-rules are similar to STRIPS operators, and are of the form act(ℓ); ψ ← ∆⁺; ∆⁻, where ψ = v₁, . . . , vₙ are variables; ψ is a formula specifying the precondition of the action; and the
add-list \( \Phi^+ \) and delete-list \( \Phi^- \) are sets of atoms that specify the effects of executing the action. A plan-library II consists of a set of plan-rules of the form \( e(t) \colon \varphi ; \psi \leftarrow G \), where \( e \) is an n-ary event-goal symbol, \( t = t_1, \ldots, t_n \) are terms, \( \varphi \) and \( \psi \) are formulas, and \( G \) is a plan-body graph. The rule states that, if the context condition \( \psi \) holds, \( G \) is a 'standard operating procedure' for achieving the event-goal \( e(t) \) or the goal-condition \( \varphi \).

Plan-body graphs are built from the following set of user programs: actions; belief addition \( +b \) adds the atom \( b \) to \( B \); belief removal \( -b \) removes the atom \( b \) from \( B \); test \( ?\varphi \), where \( \varphi \) is a formula, tests whether \( \varphi \) holds in \( B \); event-goal or goal-condition, or executing a single step in an instantiated plan-body graph to achieve an event-goal \( \varphi \) or goal-condition \( \varphi \). If the goal succeeds and \( \varphi \) does not hold; and active preserve \( PR_a(\varphi) \), which is similar to the former except that if condition \( \varphi \) does not hold, the plan-body graph for \( \varphi \) is suspended and the re-achievement of \( \varphi \) is attempted by posting the goal \( \varphi \).

Figure 1: Plan-body graphs \( G_{walk} \) and \( G_{pw} \). \( G_{pw} \) occurs in a plan-rule for the event-goal program \( !pw \) (prepare to walk) in \( G_{walk} \).

G lead anywhere. Formally, the plan-body graph is initial if \( N = \{s_0\} \), and finished, denoted by \( fin(G) \), if \( N \subseteq S \), and for all \( s \in N \) and \( t \in T \colon (s, t) \notin E_{in} \). All plan-body graphs occurring in a plan-library are initial.

Example 1. Consider an agent that has a goal to travel from its current location to a destination \( d \) [Sardina and Padgham, 2011]. The goal can be achieved in various ways depending on the distance to the destination, represented by the following plan-rules (each omitted goal-condition \( \varphi \) is \( \top \)):

\[
\begin{align*}
\text{travel}(d) & : At(x) \land WalkDist(x, d) \rightarrow G_{walk} \\
\text{travel}(d) & : At(x) \land \exists y (\text{InCity}(x, y) \land \text{InCity}(y, d)) \rightarrow G_{city} \\
\text{travel}(d) & : At(x) \land \neg \exists y (\text{InCity}(x, y) \land \text{InCity}(y, d)) \rightarrow G_{far}.
\end{align*}
\]

The first plan-rule refers to the plan-body graph \( G_{walk} \) shown in Fig. 1.

3 PRS Semantics

Our semantics for PRS follows the approach adopted by the CAN [Winikoff et al., 2002] agent programming language, as defined in [Sardina and Padgham, 2011], where a transition relation on agent configurations is defined in terms of a set of derivation rules [Plotkin, 1981]. An agent configuration is a tuple \( \langle \Pi, \Lambda, B, A, \Gamma \rangle \) where \( \Pi \) is a plan-library, \( \Lambda \) is an action-library, \( B \) is a belief base, \( A \) is a sequence of executed actions, and \( \Gamma \) is a set of intentions (as \( \Pi \) and \( \Lambda \) do not change during execution, we omit them from derivation rules). Agent configurations represent the execution state of a PRS agent, and intentions are the current states of full programs being pursued in order to achieve top-level event-goals. As in CAN, full programs extend the syntax of user programs to represent the current evolution of a user program, and may contain information used to decide the next transition, e.g. the plan-body graphs yet to be tried in achieving an event-goal.

Formally, a full program (or simply program) is a formula in the language defined by the grammar \( P ::= \)

\[
\begin{align*}
\eta & \mid act \mid \varphi \mid +b \mid -b \mid \varphi \mid \psi \mid \text{WT}(\varphi) \mid PR_a(\varphi) \\
\text{ev} : & \langle \psi_1 : G_1, \ldots, \psi_n : G_n \rangle \mid P \rightsquigarrow P' \mid G \triangleright P \mid \eta \triangleright P
\end{align*}
\]

where \( \eta \), (‘nil’) indicates that there is nothing left to execute; \( \text{WT}(\varphi) \) denotes either \( \text{WT}(\varphi) \) or \( \text{WT}(\varphi) \), where \( \text{WT}(\varphi) \) indicates that program \( \text{WT}(\varphi) \) has been adopted (i.e., its execution has started); \( \text{ev} : \langle \psi_1 : G_1, \ldots, \psi_n : G_n \rangle \) represents the set of relevant plan-rules for achieving the event-goal or goal-condition \( \varphi \); \( P \rightsquigarrow P' \) represents a suspended active preserve program \( P' \) whose associated condition is being re-achieved by a recovery program \( P \); \( G \triangleright P \), where \( P = \text{ev} : \langle \psi_1 : G_1, \ldots, \psi_n : G_n \rangle \), represents the default deliberation mechanism for ‘goal commitment’: achieve \( \text{ev} \) using an applicable plan-body graph \( G \), but if that fails, try an
alternative applicable graph from those appearing in $P$; and $\eta \vdash P$ indicates that a plan-body graph for $\psi \theta$ has succeeded. Note that full programs are more general than those yielded by our semantics.

We first give derivation rules for configurations of the form $[\Pi_1, A, B, \bar{A}, \bar{P}]$, where $P$ is a full program, i.e., for a single intention. We give the derivation rules for actions, belief operations, goal and plan adoption, and goal commitment in Section 3.1; for advancing plan-body graphs in Section 3.2; for PRS-specific wait and preserve programs in Section 3.3; and for agents with configurations of the form $[\Pi_1, A, B, \bar{A}, \bar{P}, \Gamma]$, i.e., multiple intentions, in Section 3.4.

### 3.1 Semantics for Actions, Belief Updates, Goal and Plan Adoption, and Goal Commitment

Fig. 2 shows the derivation rules for actions and belief operations. Rules $\text{add}$ and $\text{del}$ simply update $B$, replacing programs $+b$ and $-b$ with $\eta$ ($A$ remains unchanged). The semantics for actions is given by rule $A$. The antecedent checks whether there is a relevant action-rule for $\alpha$ (i.e., one whose ‘head’ $\alpha'$ matches $\alpha$ under substitution $\theta$) and whether the action is applicable (i.e., its precondition holds in $B$); the conclusion of the derivation rule applies the action’s add- and delete-lists to $B$ and appends the action to $A$.

Rule $E_{\text{v1}}$ adopts the event-goal program $\psi \theta$ by creating the set $\Delta$ of plan-rules relevant for the event, i.e., the rules in $\Pi_1$ with event-goals matching $\psi \theta$. The proof uses a most general unifier $\mu G$.

$$\Delta = \{\psi \theta : G \theta | \eta \in \Pi_1, \theta = \mu G(e, e') \} \neq \emptyset \quad \text{Ev}_1$$

**Example 2.** Processing an event-goal program of the form $\text{travel}(\text{Uni})$ using rule $\text{Ev}_1$ yields the following (full) program, encoding all relevant options for this event:

$$\text{travel}(\text{Uni}) : \{\psi_1 : G_{\text{walk}}, \psi_2 : G_{\text{city}}, \psi_3 : G_{\text{fare}}\}$$

with $\psi_1 = \text{At}(x) \land \text{WalkDist}(x, \text{Uni})$; $\psi_2 = \text{At}(x) \land \exists y (\text{InCity}(x, y) \land \text{InCity}(\text{Uni}, y))$; and $\psi_3 = \text{At}(x) \land \neg \exists y (\text{InCity}(x, y) \land \text{InCity}(\text{Uni}, y))$.

Similarly, rule $\text{Ev}_2$ adopts the goal-condition program $!\phi$ by creating the set $\Delta$ of plan-rules in $\Pi_1$ that can achieve $\phi$.

$$\Delta = \{\psi \theta : G \theta | \eta \in \Pi_1, \theta \models \phi \} \neq \emptyset \quad \text{Ev}_2$$

Rule $\text{Sel}$ selects an applicable plan-rule for event-goal or goal-condition $\psi \theta$ from the set of relevant rules, and schedules the associated plan-body graph for execution.

$$\psi : G \in \Delta \quad B \models \psi \theta \Rightarrow [B, A, \psi \theta \triangleright \psi \theta]$$

Rules for goal commitment are shown in Fig. 2. Rule $\triangleright_{\text{stp}}$ executes a single step in a program $G \triangleright P$ if the plan-body graph $G$ has neither failed nor finished (see Section 3.2). Rule $\triangleright_{\text{end}}$ discards the alternative program $P$ in a program $\eta \triangleright P$ (where $\eta$ here represents a completed graph). Finally, rule $\triangleright_f$ schedules the alternative program $P = \psi \theta : \{\Delta\}$ for execution and executes a single step in it, provided $G$ has failed and $P$ has not, i.e., an applicable plan-rule exists for $\psi \theta$.

### 3.2 Semantics for Plan-Body Graphs

We extend the definition of a plan-body graph in Definition 1 to a full plan-body graph, representing the current ‘state’ in the evolution of an initial plan-body graph. A full plan-body graph is of the form $G = (S, T, E_{\text{in}}, E_{\text{out}}, L_0, L_c, N, s_0)$ where $L_c : T \rightarrow P$ is a function that maps each transition node $t \in T$ to a full program $P \in P$, which represents the current form of the possibly evolved (initial) user program $L_0(t)$. We use the following auxiliary definitions: $\text{bef}(t) = \{s \in S | (s, t) \in E_{\text{in}}\}$ are the input state nodes of $t$; $\text{aft}(t) = \{s \in S | (t, s) \in E_{\text{out}}\}$ are the output state nodes; and the update to function $L_c$ with a (new) program $P$ for $t$ is

$$\text{UPD}(L_c, t, P) = \{L_c \cup \{t, L_c(t)\}\} \cup \{(t, P)\}.$$

The first rule states that a transition node $t$, in the case where it is not initially associated with a test condition, becomes active if it is not already active but all of its input states are. Becoming active includes (re-)initialising $t$ to correspond to its user program. This is done in case $t$ is part of a cycle.

$$\begin{align*}
\text{UPD}(L_c, t, P) & = \{L_c \cup \{t, L_c(t)\}\} \cup \{(t, P)\}.
\end{align*}$$

Once a transition node $t$ is active, it can perform a single execution step in its associated (current) program $L_c(t)$.

$$\begin{align*}
\text{UPD}(L_c, t, P) & = \{L_c \cup \{t, L_c(t)\}\} \cup \{(t, P)\}.
\end{align*}$$

If a transition node’s program has finished execution, the node becomes inactive and its outgoing nodes become active.

$$\begin{align*}
\text{UPD}(L_c, t, P) & = \{L_c \cup \{t, L_c(t)\}\} \cup \{(t, P)\}.
\end{align*}$$

We treat the functions $L_0$ and $L_c$ as relations, i.e., as sets of ordered pairs of the form $(t, P)$.
Example 3. Suppose that the agent believes it is currently at home, which is walking distance to the university. In this case, the Sel rule transforms the set of relevant options represented by the program in Example 2 into the program

\[ G_{walk} \triangleright travel(uni) : \langle \psi_2 : G_{city}, \psi_1 : G_{park} \rangle, \]

i.e., the agent selects the G_{walk} plan-body graph while keeping the other graphs as backup alternatives, represented by the right-hand side of the \( \triangleright \) operator. When the agent starts executing the G_{walk} graph, the rule G^{P}_{start} removes s_0 from N and adds the transition node associated with subgoal \( \psi_{pw} \). This is then executed using rule G^P_{stp}, whose antecedent uses rule Ev_{1} to resolve the subgoal.

If a transition node is initially associated with a test condition, then the node becomes active only if the condition holds in the current belief base. The chosen transition node also becomes inactive at the same execution step, as once the condition is tested there is nothing left to execute. Under this semantics, PRS allows choices in execution within the graph: either a non-deterministic choice when multiple transition nodes, with non-\textit{mutex} test programs, exit the same state node, or deterministic choices induced by such tests.

\[
t \in T \text{ bef}(t) \subseteq N \quad L_0(t) = \emptyset \quad B = \emptyset \quad G \overset{!}{\rightarrow} \quad G^\phi_{stp}
\]

\[ G' = (S, G^\prime) = (S, T, E_{in}, E_{out}, L_0', L_c', N', s_0); \quad L'_c = \text{upd}(L_c, t, \eta); \quad N = (N \setminus \text{bef}(t)) \cup \text{afh}(t). \]

The case where \( B \not\models \phi \) holds represents failure, i.e., the inability to execute a step in \( t \).

Finally, if a plan-body graph has finished (Section 2), rule G^{P}_{end} replaces it with program \( \eta \).

\[
\text{fin}(G) \quad \text{if} \quad B \not\models \phi \quad G \overset{P}_{end} \rightarrow [\exists, A, \eta].
\]

Example 4. Consider the evolution G^{P}_{pw} \triangleright pw : \langle \Delta_{pw} \rangle of subgoal \( \psi_{pw} \). Achieving the former using the graph in Figure 1 involves the parallel execution of the programs \( P^1_{pw} \) and \( P^2_{pw} \). This ‘split’ is represented by the outgoing edges from the transition node associated with the ‘?’ user program, and results in state nodes \( s_4 \) and \( s_5 \) being added to \( N \), using rule G^{P}_{stp}. Note that for the transition node associated with \( \psi_{pw} \) to become active, both \( P^1_{pw} \) and \( P^2_{pw} \) must complete execution, and transition to \( s_6 \) and \( s_7 \), respectively.

3.3 Semantics for Wait and Preserve Programs

We now give a semantics for wait and preserve programs of the form WT(\( \phi \)), PR(P, \( \phi \)), and suspended active preserve programs of the form \( P_1 \triangleright PR(P_2, \phi) \), where \( P_1 \) is the recovery program. In all cases, assume that condition \( \phi \) is ground when the program is adopted.

Rule W^{P}_{adopt} adopts a wait program, i.e., changes its form to indicate that condition \( \phi \) is now being monitored. Rule W specifies that the wait for \( \phi \) should continue if \( \phi \) does not hold in the belief base. Finally, rule W^{P}_{end} specifies that the wait should end if \( \phi \) does hold. In all cases, \( C = [B, A, WT(\phi)] \).

\[
\begin{align*}
[B, A, WT(\phi)] & \rightarrow C \quad W^{P}_{adopt} \quad B \not\models \phi \\
C & \rightarrow C \quad W \\
C & \rightarrow [B, A, \eta] \quad W^{P}_{end}
\end{align*}
\]

The first set of derivation rules for preserve programs apply to both passive and active preserves. Rule PR^{P}_{adopt} specifies the adoption of a preserve program, i.e., the adoption of its event-goal or event-condition program \( \psi \). Rule PR^{P}_{stp} executes a single step in a preserve program if \( \phi \) is not violated, and PR^{P}_{succe} removes a completed preserve program.

\[
\begin{align*}
[B, A, \psi] & \rightarrow [B, A, \psi : (\Delta)] \\
[B, A, PR(P, \phi)] & \rightarrow [B, A, PR(P, \psi : (\Delta), \phi)] \\
\quad P \not\triangleright \psi \quad B \not\models \phi \\
[B, A, PR(P, \phi)] & \rightarrow [B, A, PR(P, \psi : (\Delta), \phi)] \\
\quad P \not\triangleright \psi \quad B \not\models \phi \\
[B, A, PR(P, \phi)] & \rightarrow [B, A, \psi] \\
\quad P \not\triangleright \psi \quad B \not\models \phi
\end{align*}
\]

Rule PR^{P}_{end} specifies that the passive preserve fails if \( \phi \) is violated or \( P \) is blocked.

\[
\begin{align*}
P \not\in \{ \psi, \eta \} \\
\quad \{ \phi \} \quad \vee \quad [B, A, \psi] \not\models \phi \quad PR^{P}_{end} \\
\quad \{ \phi \} \quad \vee \quad [B, A, \psi] \not\models \phi
\end{align*}
\]

Rules AP\{PR^P, PR^P\} operationalise adopted active and suspended preserve programs. We define three special multisets:\(^2\) Given an expression \( \mathcal{E} \) that is either a program or plan-body graph \( G = (S, T, E_{in}, E_{out}, L_0, N, s_0) \), we define a ‘path’ of ‘nested’ (adopted) preserve and wait programs as any element in the multiset \( T(\mathcal{E}) \), defined as \( T(\mathcal{E}) = \{ \mathcal{E} \cdot \tau \mid \tau \in T(\mathcal{E}) \} \).

\[
\begin{align*}
\{ \mathcal{E} \cdot \tau \mid \tau \in T(\mathcal{E}) \} & = (\{ \mathcal{E} \cdot \tau \mid \tau \in T(\mathcal{E}) \} \cup \{ \mathcal{E} \} \cup T(G) \cup T(L_c(t_1)) \cup T(L_c(t_n)) \cup \emptyset) \\
\quad \vee \quad T(L_c(t_1)) & = G \not\models \mathcal{E} \text{ and } N \cap T \{ t_1, \ldots, t_n \}; \quad \text{otherwise.}
\end{align*}
\]

When \( G = G \) we take the multisets of the branches corresponding to transition nodes in \( G \) that are executed in parallel. The first element in such a sequence is a ‘most abstract’ preserve or wait program occurring in \( \mathcal{E} \), and the last element is a ‘most deeply’ nested preserve or wait program occurring in \( \mathcal{E} \). We use \( \mathcal{S}_r(\mathcal{E}) \) and \( \mathcal{P}_r(\mathcal{E}) \) to denote the multisets of all the elements in all the sequences in \( T(\mathcal{E}) \) that are, and are not, of the form \( P \not\triangleright P' \), respectively; i.e., any element in \( \mathcal{S}_r(\mathcal{E}) \) is a suspended (adopted) active preserve program, and any element in \( \mathcal{P}_r(\mathcal{E}) \) is an adopted wait, passive preserve, or active preserve program that is not suspended. We use \( T(\mathcal{E}) \) to check whether a wait/preserve program in some ‘path’ in \( \mathcal{E} \) may be ‘pruned’ by a more abstract preserve program in the path, and we use \( \mathcal{S}_r(\mathcal{E}) \) and \( \mathcal{P}_r(\mathcal{E}) \) to count the number of suspended and unsuspended programs occurring in \( \mathcal{E} \).

Example 5. Suppose \( P^1_{pw} \) and \( P^2_{pw} \) have evolved to, respectively, adopted programs \( WT(\phi) \) and \( PR(P, \psi) \), with \( P = e : (\Delta) \) (i.e., one parallel branch waits for a condition \( \phi \) while the other tries to achieve an event-goal program \( e \) while preserving \( \phi \)). Then, \( T(G_{walk}) = \{ WT(\phi), PR(P, \psi) \} \). Moreover, if \( P \) evolves to \( P' = G_c \triangleright e : (\Delta) \), then \( G_c \) mentions an adopted program, e.g., \( WT(\phi'), PR(P', \phi') \cdot WT(\phi'') \), then \( T(G_{walk}) = \{ WT(\phi), PR(P', \phi'), WT(\phi'') \} \).

\(^2\)Adapted from Sardina and Padgham, 2011.
Rule $APr_{\mathit{fail}}$ specifies that the adopted active preserve program $pr_a(P, \phi)$ fails if $P$ fails and the monitored condition $\phi$ is not violated. If $\phi$ is false, $APr_{\mathit{sus}}$ suspends the preserve program and attempts to re-establish $\phi$ using the recovery (goal-condition) program $!\phi$. Rules $APr_{\mathit{fail}}$ and $APr_{\mathit{unsus}}$ specify, respectively, that a suspended preserve program fails if the recovery program fails, and is resumed if the recovery program completes.

$$\begin{array}{c}
P \notin \{\eta, \mathit{lev}\} \quad \text{B} = \phi \quad [B, A, P] \not\rightarrow \quad APr_{\mathit{fail}} \\
P \notin \{\eta, \mathit{lev}\} \quad \text{B} \neq \phi \quad [B, A, pr_a(P, \phi)] \rightarrow [B, A, !\phi \mathrel{\leftarrow} pr_a(P, \phi)] \\
P \neq \eta \quad [B, A, P_1 \mathrel{\leftarrow} P_2] \rightarrow [B, A, \mathit{false}] \\
[B, A, \eta \mathrel{\leftarrow} pr_a(P, \phi)] \rightarrow [B, A, pr_a(P, \phi)] \\
\end{array}$$

Finally, rules $APr_{\mathit{sus}}^{\star 1}$ and $APr_{\mathit{sus}}^{\star 2}$ define the execution of recovery programs and suspended (active preserve) programs. Rule $APr_{\mathit{sus}}^{\star 1}$ executes a single ‘cleanup’ or ‘notification’ step in the suspended program. Such an execution step amounts to a program $P_1$ evolving to a program $P_2$ that has fewer suspended programs, or fewer unsuspended preserve or wait programs, e.g. due to a failed passive preserve that had a ‘nursed’ wait program. The relation $P \prec P'$ is defined for programs $P$ and $P'$ as: $P \prec P' \iff |P_s(P)| < |P_s(P')| \lor |S_e(P)| < |S_e(P')|.

$$\begin{array}{c}
[B, A, P_1] \rightarrow [B', A', P'_1] \\
[B, A, P_1 \mathrel{\leftarrow} P_2] \rightarrow [B', A', P'_1 \mathrel{\leftarrow} P_2] \\
[B, A, P_2] \rightarrow [B, A, P'_2] \\
[B, A, P_1 \mathrel{\leftarrow} pr_a(P, \phi)] \rightarrow [B, A, P_2 \mathrel{\leftarrow} pr_a(P, \phi)] \\
\end{array}$$

Note that rule $APr_{\mathit{sus}}^{\star 2}$ implies that if an active preserve is suspended, all of the (possibly adopted) ‘nursed’ programs occurring in $P_2$ are ‘implicitly suspended’, i.e., they can only perform ‘cleanup’ or ‘notification’ steps, so we are guaranteed to terminate.

**Proposition 1.** Any sequence of configurations $[B_1, A_1, P_1], \ldots, [B_n, A_n, P_n]$ is finite if for all $i \in [1, n - 1]$, we have that $P_{i+1} \prec P_i$ and $[B_i, A_i, P_i] \rightarrow [B_{i+1}, A_{i+1}, P_{i+1}]$.

**Proof.** Since each such execution step from $P_i$ to $P_{i+1}$ must yield fewer wait programs, preserve programs, and/or programs of the form $P \mathrel{\leftarrow} pr_a(P, \phi)$, it is sufficient to consider whether a ‘switch’ of the latter to resume $pr_a(P', \phi)$ can lead to it (possibly with an ‘evolved’ $P'$) being suspended again, and whether this can continue indefinitely.

For $pr_a(P, \phi)$ to resume, we must have $P = \eta$, and then if $\phi$ still does not hold, the program will indeed evolve to $!\phi \mathrel{\leftarrow} pr_a(P', \phi)$. Moreover, recovery program $!\phi$ does have at least one relevant plan-rule, as it was once able to evolve to $\eta$ (recall that $\phi$ has been ground from the moment its associated active preserve program was adopted). However, the only possible execution step on $!\phi$ cannot reduce the number of aforementioned programs.

We use the notation $C \rightarrow C'$ to denote that there exists a non-empty sequence of configurations from $C$ to $C'$.

### 3.4 Agent-Level (‘Top-Level’) Semantics

We now give the derivation rules for the top-level execution of an agent program. Transitions between agent configurations are defined by the derivation rules in Fig. 3; an expression $C \rightarrow C'$ denotes a transition of type $t \in \{\mathit{INT}, \mathit{EVENT}, \mathit{COND}, \mathit{INT}\}$.

Rule $A_{\mathit{prs}}$ is the top-level rule, and represents the PRS deliberation cycle. A single PRS type execution step comprises three things: progressing an intention by one step, or removing a completed intention (i.e., $P = \eta$) or a failed one (using rules $A_{\mathit{int}}$ or $A_{\mathit{rem}}$, respectively); processing newly observed event-goals (using rule $A_{\mathit{ev}}$), i.e., creating an intention for each new event-goal that is observed from the (external) environment; and finally, performing all the necessary ‘notification’ and ‘cleanup’ steps on wait, preserve, suspended, and recovery programs (using rule $A_{\mathit{cond}}$) to leave the agent in a ‘sound’ or ‘stable’ configuration. More specifically, $A_{\mathit{cond}}$ takes a single step in an intention if the step will yield an intention with fewer suspended programs, or fewer unsuspended (adopted) preserve or wait programs.

### 4 Properties of the Semantics

We now prove key properties of the semantics and show the greater expressivity of our PRS fragment compared to CAN. In what follows, we use $[B, A, P] \rightarrow$ as an abbreviation for $\exists B', A', P' : [B, A, P] \rightarrow [B', A', P']$, and $C_1, C_2$ are agent configurations of the form $[B_1, A_1, P_1]$ such that $C_1$ is sound and $C_1 \mathrel{\leftarrow} C_2$. A configuration $C = [A, \Pi, B, A, \Gamma]$ is sound iff (i) for all $\Pi \in \mathit{prs}(\phi)$, $B \neq \phi$; (ii) for all $P \mathrel{\leftarrow} P' \in S_e(\Gamma)$, $[B, A, P] \rightarrow$; and (iii) for all $pr_a(P, \phi) \in S_e(\Gamma)$, $B = \phi$ and $[B, A, P] \rightarrow$.

**Theorem 1.** Let $C_1$ and $C_2$ be as above. Then, $C_2$ is sound.

**Proof sketch.** Observe from the antecedent of derivation rule $A_{\mathit{prs}}$ that only one step of type $\mathit{INT}$ is performed on $C_1$,
followed by one of type EVENT, and zero or more of type COND. Assume the theorem does not hold because there is a passive preserve $\text{Pr}_P(P, \phi) \in \mathcal{P}_\tau(\Gamma_2)$, for some $P$, such that $B_2 \not\equiv \phi$ or $[B_2, A_2, P'] \not\models$. Then, since $\text{Pr}_P(P, \phi)$ is an adopted program appearing in some intention $P_I \in \Gamma_2$, either rule $\text{Pr}_f$ or $\text{Pr}_s$ can be applied to configuration $[B_2, A_2, \phi, \text{Pr}_P(P, \phi)]$ to yield an intention $P_I'$. Since $P_I' \not\models P_I$, rule $\text{Pr}_s$ will be applied (possibly multiple times) to $P_I$ until $\text{Pr}_P(P', \phi) \not\in \mathcal{P}_\tau(\Gamma_2)$ for all $P'$, which contradicts our assumption. Assume instead that the theorem does not hold because there is a program $P \leadsto P' \in \mathcal{S}_\tau(\Gamma_2)$ such that $[B_2, A_2, P'] \not\models$. Then, either rule $\text{AP}_s$ or $\text{AP}_u$ will be applied to configuration $[B_2, A_2, P']$ or its ‘evolution’, again resulting in a contradiction. The remaining cases are proved similarly.

The next theorem states that an adopted wait program is only removed in a PRS step if either its condition becomes satisfied, or the program is *pruned*, i.e., it is deactivated by a program that is pruned away or a suspended preserve that is discarded. Given a program $P$ and ‘path’ $\tau \in T(P)$, we denote the program at index $n > 0$ as $\tau[n]$ (where $\tau[1]$ is $\tau$’s most abstract program). A program $P$ is *pruned* between $C_1$ and $C_2$ iff for any $\tau \in T(\Gamma_1)$ with $T(\Gamma) = \bigcup_{\tau \in T(\Gamma')} T(\Gamma')$ and $\tau[k] = P$ for some $k > 0$, there exists a $0 < j < k$ such that:

1. $\tau[j] = \text{Pr}_P(P_j, \phi_j)$ and $B_2 \not\equiv \phi_j$;
2. $\tau[j] = \text{Pr}_A(P_j, \phi_j)$, $B_2 \not\equiv \phi_j$, and $[B_2, A_2, \phi_2] \not\models$; or
3. $\tau[j] = \text{Pr}_S(P_j, \phi_j)$, $B_2 \not\equiv \phi_j$, and $[B_2, A_2, P_j] \not\models$.

**Theorem 2.** Let $C_1$ and $C_2$ be as before. For each $\mathcal{W}(\phi) \in \mathcal{P}_\tau(\Gamma_1)$ such that $\mathcal{W}(\phi) \not\in \mathcal{P}_\tau(\Gamma_2)$, we have that $B_2 \not\models \phi$ or $\mathcal{W}(\phi)$ is pruned between $C_1$ and $C_2$.

**Proof Sketch.** Let $\mathcal{W}(\phi) \in \mathcal{P}_\tau(\Gamma_1)$ be a program such that $\mathcal{W}(\phi) \not\in \mathcal{P}_\tau(\Gamma_2)$. Let $t$ be a transition node currently labelled with $\mathcal{W}(\phi)$, where $T = \{t, \ldots\}$ and $N = \{t, \ldots\}$ are the transition nodes and current nodes in a (‘partially executed’) plan-body graph $G$. We consider the case where if $B_2 \not\models \phi$, then $\mathcal{W}(\phi)$ must have been pruned between $C_1$ and $C_2$, because no other derivation rules can ‘remove’ $\mathcal{W}(\phi)$. First, rule $G_{end}$ (which, if applicable, ‘removes’ $G$) requires $\text{fin}(G)$ to hold, which cannot be the case as $t \in N$; for the same reason, rule $G_{start}$ cannot ‘reset’ $\mathcal{W}(\phi)$. Second, the antecedent of rule $\rightarrow$ requires that $[B, A, G] \not\models$ for some $A$ and $B \in \{B_1, B_2\}$, which cannot hold as we can take a step on $\mathcal{W}(\phi)$ via rule $W$. Similarly, if $P$ is an intention in which $G$ occurs, the antecedent of agent-level rule $\text{Arem}$ cannot hold (i.e., $[B_1, A, P] \not\models$ cannot hold for any $A$). Then, it follows that $\mathcal{W}(\phi)$ is pruned between $C_1$ and $C_2$. 

Theorem 3 states that an adopted preserve program is only ‘removed’ if: its condition becomes violated; its associated program becomes blocked; or the preserve program is pruned.

---

3The definitions of $\mathcal{P}_\tau(\mathcal{E})$ and $\mathcal{S}_\tau(\mathcal{E})$, for some expression $\mathcal{E}$, can be generalised similarly.
\[ i \in [1, n-1]; \text{the solution in } C_1, \ldots, C_n \text{ is the sequence } A \text{ of actions such that } A_n = A_1 \cdot A \]

With \( \Lambda, \Pi, B, \text{ and } \Gamma \) as above, \( \text{SOL}(\Lambda, \Pi, B, \Gamma) \) denotes the set of solutions, i.e., the set of sequences of actions performed in the execution traces of configuration \([\Lambda, \Pi, B, \epsilon, \Gamma]\), where \( \epsilon \) denotes the empty string. Theorem 5 states that a CAN plan-library \( \Pi^- \) not mentioning Goal\( (\phi_s, P, \phi_p) \) programs (as there is no corresponding program in PRS) can be translated into an equivalent PRS plan-library.

**Theorem 5.** If \( \Pi^- \) is a CAN library and \( \Lambda \) an action-library, there exists a PRS library \( \Pi_1 \) s.t. for any event-goal \( \epsilon \) and beliefs \( B : \text{SOL}(\Lambda, \Pi_1, B, \{ \epsilon \}) \neq \text{SOL}(\Lambda, \Pi, B, \{ \epsilon \}) \).

**Proof Sketch.** Given a CAN plan-rule \( e : \psi \leftarrow P \in \Pi_1 \), the first step is to obtain the corresponding PRS plan-rule \( e : \top \psi \leftarrow G \). We define three functions: \( g(P, n)_{in} \), \( g(P, n)_{out} \), and \( g(P, n)_{L} \), where \( n \in \mathbb{N} \). When \( n = 1 \), these functions represent respectively the elements \( E_{in}, E_{out} \), and \( L_0 \) in \( G \). If \( P = \text{act} \), we define \( g(P, n)_{in} = \{ (n \cdot s, n \cdot t) \} \); \( g(P, n)_{out} = \{ (n \cdot t, n \cdot s') \} \); and \( g(P, n)_{L} = \{ (n \cdot t, P) \} \), where \( s, s' \) and \( t \) are unique symbols (and thus, for example, is a string). We also define \( g(P, n)_{\text{start}} = n \cdot s \) and \( g(P, n)_{\text{end}} = n \cdot s' \). Intuitively, \( n \) uniquely identifies the PRS plan-body ‘subgraph’ corresponding to \( P \). If \( P = P_1 \cup P_2 \) is the sequential composition of CAN programs \( P_1 \) and \( P_2 \),

\[
\begin{align*}
\text{g}(P, n)_{out} &= g(P_1, n \cdot 1)_{out} \cup g(P_2, n \cdot 2)_{out} \cup \{ (n \cdot t', n \cdot s''),
\langle n \cdot t, g(P_1, n \cdot 1)_{start} \rangle, \langle n \cdot t', g(P_2, n \cdot 2)_{start} \rangle \},
\text{g}(P, n)_{in} &= g(P_1, n \cdot 1)_{in} \cup g(P_2, n \cdot 2)_{in} \cup \{ (n \cdot s, n \cdot t),
\langle g(P_1, n \cdot 1)_{end}, n \cdot t' \rangle, \langle g(P_2, n \cdot 2)_{end}, n \cdot t'' \rangle \},
\text{g}(P, n)_{L} &= g(P_1, n \cdot 1)_{L} \cup g(P_2, n \cdot 2)_{L} \cup 
\{ (n \cdot t, ?T), (n \cdot t', ?T), (n \cdot t'', ?T) \},
\end{align*}
\]

where transition node \( n \cdot t' \) ‘connects’ the subgraphs corresponding to \( P_1 \) and \( P_2 \). As before, we define \( g(P, n)_{\text{start}} = n \cdot s \) and \( g(P, n)_{\text{end}} = n \cdot s' \), and \( s, s', t, t' \) and \( t'' \) are unique symbols. We similarly define the subgraph corresponding to a CAN parallel composition \( P_1 \parallel P_2 \), test program, etc.

We then show by induction on the structures of \( P \) and \( G \) above that their traces yield the same solutions. For example, the derivation rules for CAN’s sequential composition can be simulated by repeatedly applying the \( G_{start}, G_{\text{step}} \) and \( G_{\text{out}} \) rules of PRS, and vice versa.

Theorem 6 states that the converse does not hold: even if we ignore programs that have no counterparts in CAN, PRS plan-libraries cannot be ‘directly mapped’ to CAN libraries. This result follows from a similar one in [de Silva, 2017] which showed that the ‘plan-body’ representation used in HTN planning allows a more fine-grained interleaving of steps than do CAN plan-bodies: a CAN plan-body must specify steps in a ‘series-parallel’ manner, whereas HTN ‘plan-bodies’ (and PRS plan-body graphs) do not.

In what follows, \( \Pi^- \) denotes PRS plan-libraries that do not mention goal-condition, wait, nor preserve programs, and \( \Pi_1 \in \text{CAN}(\Pi^-) \) denotes a directly mapped CAN library, i.e., one obtained from \( \Pi^- \) by ignoring the goal-condition \( \varphi \) in each plan-rule, and replacing each graph \( G \) appearing in \( \Pi^- \) with a CAN plan-body \( P \) such that the multisets of (user) programs occurring in \( G \) and \( P \) are the same.

**Theorem 6.** There exists a PRS library \( \Pi^- \), an action-library \( \Lambda \), and event-goal \( \epsilon \), s.t. for any CAN library \( \Pi_1 \in \text{CAN}(\Pi^-) \) and beliefs \( B : \text{SOL}(\Lambda, \Pi_1, B, \{ \epsilon \}) \neq \text{SOL}(\Lambda, \Pi, B, \{ \epsilon \}) \).

**Proof Sketch.** We translate an example HTN ‘plan-body’ provided in [de Silva, 2017] into a PRS plan-body graph. First, we create the PRS plan-rule \( \epsilon_{\text{top}} : \top \psi \leftarrow G \), in particular by taking the following input and output edges for \( G \):

\[
\begin{align*}
E_{in} &= \{ (s_1, t_1), (s_2, t_1), (s_3, t_3), (s_4, t_4), 
(s_5, t_2), (s_6, t_2), (s_7, t_6), (s_8, t_5) \}; \text{ and}
E_{out} &= \{ (t_1, s_2), (t_2, s_1), (t_3, s_3), 
(t_3, s_6), (t_4, t_7), (t_5, s_8), (t_6, s_9) \}.
\end{align*}
\]

Second, we set the initial program \( L_0(t_i) \) for each \( t_i \in \{ t_1, \ldots, t_9 \} \) to a different event-goal \( e_{t_i} \), each of which is associated with a single plan-body graph representing the sequence of unique actions \( a_{t_1} \cdot a_{t_2} \cdot a_{t_3} \). Finally, we show that the following sequence of actions:

\[
a_{t_1} \cdot a_{t_2} \cdot a_{t_3} \cdot a_{t_4} \cdot a_{t_5} \cdot a_{t_6} \cdot a_{t_7} \cdot a_{t_8} \cdot a_{t_9}
\]

cannot be produced by any CAN trace of program \( \epsilon_{\text{top}} \), relative to any CAN plan-library that is directly mapped from the above set of PRS plan-rules: e.g., the CAN body \( e_{t_1} : (e_{t_2} \parallel (e_{t_3} : e_{t_4} : e_{t_5}) ; e_{t_6}) \) does not allow \( a_{t_7} \) to follow \( a_{t_8} \) to follow \( a_{t_9} \).
Acknowledgements

Lavindra is grateful to Félix Ingrand for useful discussions about OpenPRS while Lavindra was a researcher on the GOAC/MARAE projects (2009-2011) at LAAS-CNRS. Felipe thanks CNPq for partial financial support under its PQ fellowship, grant number 305969/2016-1.

References


