The ANM Lite Language and Logic for Specifying Planning Problems

Ricky W. Butler
Langley Research Center, Hampton, Virginia

Radu I. Siminiceanu and César A. Muñoz
National Institute of Aerospace, Hampton, Virginia
Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program Office plays a key part in helping NASA maintain this important role.

The NASA STI Program Office is operated by Langley Research Center, the lead center for NASA’s scientific and technical information. The NASA STI Program Office provides access to the NASA STI Database, the largest collection of aeronautical and space science STI in the world. The Program Office is also NASA’s institutional mechanism for disseminating the results of its research and development activities. These results are published by NASA in the NASA STI Report Series, which includes the following report types:

- **TECHNICAL PUBLICATION.** Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers, but having less stringent limitations on manuscript length and extent of graphic presentations.

- **TECHNICAL MEMORANDUM.** Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- **CONTRACTOR REPORT.** Scientific and technical findings by NASA-sponsored contractors and grantees.

- **CONFERENCE PUBLICATION.** Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- **SPECIAL PUBLICATION.** Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- **TECHNICAL TRANSLATION.** English-language translations of foreign scientific and technical material pertinent to NASA’s mission.

Specialized services that complement the STI Program Office’s diverse offerings include creating custom thesauri, building customized databases, organizing and publishing research results ... even providing videos.

For more information about the NASA STI Program Office, see the following:

- E-mail your question via the Internet to help@sti.nasa.gov
- Fax your question to the NASA STI Help Desk at (301) 621-0134
- Phone the NASA STI Help Desk at (301) 621-0390
- Write to:
  NASA STI Help Desk
  NASA Center for AeroSpace Information
  7115 Standard Drive
  Hanover, MD 21076-1320
The ANMLite Language and Logic for Specifying Planning Problems

Ricky W. Butler
Langley Research Center, Hampton, Virginia

Radu I. Siminiceanu and César A. Muñoz
National Institute of Aerospace, Hampton, Virginia
## Contents

1 Overview of Planning Problems 3

2 Timelines 3
   2.1 Transitions .................................................. 4
   2.2 Goal Statements and Initialization .......................... 5
   2.3 Transition Statement Extension .............................. 6

3 Constraints 6
   3.1 Contains Example ............................................. 7
   3.2 Meets Example .................................................. 8
   3.3 Repetitive Actions ............................................ 8
      3.3.1 The \texttt{at} Expression ................................. 10
      3.3.2 Using a Default Time Reference Point .................. 11
   3.4 Timeline Instance Specific Constraints ...................... 13
   3.5 The Interleaving Example .................................... 13
   3.6 Vacuous solutions ............................................ 15
   3.7 Summary of Constraint Semantics ............................ 17
   3.8 Some More Illustrative Examples ......................... 18
      3.8.1 Example: Spread-out Contains ......................... 18
      3.8.2 Example: Stretch It Out ................................. 19
      3.8.3 Example: Forcing a Future Action to Occur Within a Time Interval 20
      3.8.4 Delayed Initiation ...................................... 20
   3.9 Mandatory \texttt{at} Expressions .............................. 21
   3.10 Convenient Macros ............................................ 21

4 Condition and Effects 23

5 Translating ANMLite to SAL 24
   5.1 Simple Example ................................................ 24
   5.2 Multiple variables ............................................ 25
   5.3 Modeling Time .................................................. 26
   5.4 Model Variables ............................................... 28
   5.5 Transitions ..................................................... 29
   5.6 Translating Constraints ...................................... 34
   5.7 Current and next variables .................................. 35

6 The Crew Activity Planning Model in ANMLite 37

7 Conclusion 40
A  The ANMLite Syntax
   A.1  Timeline declarations .................................................. 43
   A.2  Constraints ................................................................. 44
   A.3  Condition and Effect Statements .................................... 45

B  The Dock-Worker Robots Problem in ANMLite 46
1 Overview of Planning Problems

In this report we seek to define a simple language that can be used to describe planning problems. Hopefully, by drastically restricting the constructs in the language, two benefits will accrue: (1) the language will be easy to understand and write, and (2) the language will lend itself to formal verification.

We have named the language ANMLite because it was developed to support the analysis of planning domains described in the Action Notation Modeling Language (ANML) [1] under development at NASA Ames. In ANMLite, a planning problem consists of a finite set of disjoint timelines, a set of valid actions for each timeline, and a set of temporal constraints that govern the correct scheduling of the actions. The constraints can be broadly categorized into two groups. The first group is specified by a transition relation and only involves actions on the same timeline. These constraints express the valid succession of actions along the timeline. The transition relation disallows overlapping actions and gaps on a timeline. The second group consists of general constraints, expressed in some logic of choice, which specify cross-timeline relationships between actions. The temporal logic must be chosen with care. It has to be rich enough to cover all the significant relations that can occur (such as Allen temporal operators [2], a popular logic in planning), but simple enough to avoid inconsistencies and ambiguities. Furthermore, since we seek to develop a framework for formal verification, it must be translatable into a form suitable for model checking or theorem proving. We are currently targeting the SAL model checker [3].

Some planning problems require data structure mechanisms to properly specify them. We have begun to look at some approaches to specifying such problems. This has led to the introduction of simple constraint and effect statements that operate on global variables and data structures. We suspect that it is wise to limit the power of these constructs and avoid them where possible, but we are not prepared at this time to make any firm recommendations about these new constructs. At this time they are significantly weaker than the corresponding ANML constructs.

2 Timelines

Discovering a suitable sequence of actions on a timeline is fundamental to the planning/scheduling problem. The first step is to identify all the actions that can be scheduled on a timeline. We have followed the ANML convention and will specify timelines using the keyword OBJTYPE. All of the allowed actions are then enumerated as in the following example:

OBJTYPE A ACTIONS
A0
A1: [10, _]  
A2: [2, _]  
A3

This specification defines the timeline A and its four actions: A0, A1, A2, and A3. Actions A1 and A2 have time duration constraints: A1 takes at least 10 time units and A2 takes at
least 2 time units. Usually, in a planning problem, there are also constraints on the sequence of actions, so an intuitive, unambiguous specification of these constraints is highly desirable. There are two different approaches to the specification of these constraints:

- Assume that all action sequences are possible unless specifically forbidden and then specify the sequences that are \textit{not} allowed.
- Assume that no sequences are allowed and then systematically add the allowed sequences.

We have currently opted for the second approach. We recognize that this is different from many AI planning systems, but it follows the approach frequently used in the formal methods community. We currently believe that this leads to a clearer specification, though we recognize that we may be biased by the historic conventions of our discipline.

2.1 Transitions

The transition relation on a timeline is similar to state-transition systems. Here, the states are the actions and a directed edge represents a valid transition between states. We have used the same construction deployed in the Abstract Plan Preparation Language (APPL) [4]. Hence, the transition relation is a set of pairs of actions, which can be declared by listing for each action the (complete) set of its successors, as in the following example:

\textbf{TRANSITIONS}

\begin{verbatim}
A0 -> A1 -> A2 -> (A0 | A1 | A3)
A3 -> A2
\end{verbatim}

Action \textit{A0} can only be followed by action \textit{A1}. Action \textit{A1} can only be followed by action \textit{A2}. Action \textit{A2} can be followed by actions \textit{A0}, \textit{A1}, or \textit{A3}. Action \textit{A3} can only be followed by action \textit{A2}.

The flexibility of the language is increased by allowing parametrization of actions. For example, the following

\textit{A1(x,y: animal): [10,\_]}

defines an action \textit{A1} with two parameters of type \textit{animal} that takes at least 10 units of time. The type \textit{animal} is defined as follows:

\textbf{TYPE animal = {cat, dog, fish, horse, eel, chicken, donkey, snake}}

and \textit{A1(cat,snake)} is a valid instance of this action. We allow more restrictive forms of transitions to be defined using a simple parameter matching scheme, with implicitly declared variables. For example,

\textit{A1(cat,yy) -> A2(yy,\_)}
This constraint states that only \( A1 \) actions with a first parameter equal to \texttt{cat} are to be followed by an \( A2 \) action and that the first parameter of \( A2 \), represented by the variable \( yy \), must be equal to the second parameter of \( A1 \). Unless explicitly specified on a different constraint, no other transition from \( A1 \) is allowed. Similarly,

\[
A1(xx,\_) \rightarrow A2(dog,xx)
\]

Here, all \( A1 \) actions must be followed by an \( A2 \) action where the first parameter equals \texttt{dog} and the second parameter, represented by the variable \( xx \), equals the first parameter of \( A1 \). Notice the use of the place holder \( _{\_} \) in the second parameter of \( A1 \), which matches any possible value of the given type.

Timeline instances are defined using the \texttt{VARIABLE} section as follows:

\[
\text{VARIABLES}
\begin{align*}
t1,t2 &: A \\
t3 &: B
\end{align*}
\]

This specification declares two distinct timelines, \( t1 \) and \( t2 \), defined by \texttt{OBJTYPE A}, and one timeline \( t3 \) defined by \texttt{OBJTYPE B}.

The variables of the same \texttt{OBJTYPE} share the transition relation, but might still behave differently, in case specific constraints are declared in the general constraint section. This is beneficial in terms of keeping the model compact, and it is frequently seen in practice. For example, the crew activity model (see Section 6) declares a general timeline for a crew member, which describes the common activities, such as sleeping, eating, etc. Additional constraints referring to non-routine tasks are then expressed by using specific crew member identifiers to enforce, for example, that a given astronaut is disassembling the sleeping unit, while a different one is fixing the power unit.

\section*{2.2 Goal Statements and Initialization}

In ANMLite, goals can be specified by an action name:

\[
\text{GOALS}
\begin{align*}
t1.A3 \\
t2.A2
\end{align*}
\]

This specifies that \( A3 \) is scheduled and completes on timeline \( t1 \), and that \( A2 \) is scheduled and completes on timeline \( t2 \). A generic form is also supported:

\[
\text{GOALS}
\begin{align*}
A.A2
\end{align*}
\]

where \( A \) is declared to be a timeline using an \texttt{OBJTYPE} declaration. This expression means that \( A2 \) is scheduled and completes on \textit{every} timeline of type \( A \). For example, if we have

\[
\text{VARIABLES}
\begin{align*}
t1,t2,t3,t4 &: A
\end{align*}
\]
then the generic goal \( A.A2 \) is equivalent to

\[
\text{GOALS} \\
\quad t1.A2 \\
\quad t2.A2 \\
\quad t3.A2 \\
\quad t4.A2 \\
\]

Initial states can also be specified using an `INITIAL-STATE` declaration though they are not necessary. For example,

\[
\text{INITIAL-STATE} \\
|-> t1.A0 \\
|-> t2.A1 \\
\]

This specifies that \( A0 \) is the first scheduled action on timeline \( t1 \) and that \( A1 \) is the first scheduled action on timeline \( t2 \). A generic form is also allowed

\[
\text{INITIAL-STATE} \\
|-> A.A0 \\
\]

This means that on every timeline of type \( A \), \( A0 \) is the first scheduled action.

### 2.3 Transition Statement Extension

For specifications where there is a large fan-out from many states, we are experimenting with the following extension to the transition statement

\[
A1 \rightarrow * \\
\]

which means that \( A1 \) can transition into any of the actions on the timeline including itself. One can restrict the allowed transitions by adding a list of exceptions as illustrated below

\[
A1 \rightarrow * \setminus (A2 \mid A5) \\
\]

This means that \( A1 \) can transition into any of the actions on the timeline except \( A2 \) and \( A5 \).

### 3 Constraints

The transition statements are adequate to specify the allowed sequences of actions on a timeline, but they cannot be used to specify constraints between actions on different timelines. The constraint section is used to accomplish this. The ANMLite constraints are built upon a simple but powerful foundation: the start and end times of actions. These time points can be referenced as follows
A1.start + 16 < B2.end

This constraint can be visualized on a timeline as follows

```
A1
   ^
   |   d > 16
  |         |
  |         |

B2
```

The constraints can also be chained as follows

\[
A1.\text{start} + 4 < B1.\text{start} < C1.\text{end} - 10
\]

This is equivalent to writing

\[
A1.\text{start} + 4 < B1.\text{start} \text{ AND } B1.\text{start} < C1.\text{end} - 10
\]

Restricting the constraint language to these simple linear relationships enables a very natural translation into the SAL model checking language (see Section 5).

### 3.1 Contains Example

Suppose we want to specify a contains-like constraint between actions, inspired from the Allen Temporal Logic [2]. In the New Domain Description Language (NDDL) [5], we would write

```
B1 \text{ contains A1}
```

and in ANML we might write something like

```java
objtype B {
     ...
     action B1 { ... }
}

objtype A {
     action A1 {
         condition over all : B.state == B1;
     }
}
```
The following diagram illustrates the intended behavior graphically

<table>
<thead>
<tr>
<th></th>
<th>A1</th>
<th>A2</th>
<th>A3</th>
</tr>
</thead>
<tbody>
<tr>
<td>B0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In ANMLite we would express this constraint as follows:

\[
B1.\text{start} < A1.\text{start} < A1.\text{end} < B1.\text{end}
\]

### 3.2 Meets Example

Suppose we want to specify a \texttt{meets}-like constraint. In NDDL we write

\[
A1 \text{ meets } B1
\]

The following diagram illustrates the intended behavior

<table>
<thead>
<tr>
<th></th>
<th>A1</th>
<th>A2</th>
<th>A3</th>
</tr>
</thead>
<tbody>
<tr>
<td>B0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In ANMLite we would express this constraint simply as:

\[
A1.\text{end} = B1.\text{start}
\]

### 3.3 Repetitive Actions

Consider the following fragment of ANML:

```anml
objtype FastingWindow {
    FastingState fs;
    transition fs {
        "fasting" -> "not_fasting";
        "not_fasting" -> "fasting"
    };

    action not_fasting() {
        change over all { fs = "fasting" -> "not_fasting" -> "fasting" };
    }
}
```
objcype CrewMember {
    FastingWindow fw;
    action pre_sleep {
        condition over all : fw.state == fasting();
    }
}

The condition statement asserts that the state of another timeline, called fw, must be fasting throughout the execution of pre_sleep:

<table>
<thead>
<tr>
<th></th>
<th>pre_sleep</th>
<th>sleep</th>
</tr>
</thead>
<tbody>
<tr>
<td>not_fasting</td>
<td>fasting</td>
<td>not_fasting</td>
</tr>
</tbody>
</table>

We can express this as follows in ANMLite:

fasting.start < pre_sleep.start < pre_sleep.end < fasting.end

This states that the start of the fasting action must take place before the start of pre_sleep and the end of the fasting action must take place after the end of pre_sleep. The question is whether this specification rules out the following scenario:

<table>
<thead>
<tr>
<th></th>
<th>pre_sleep</th>
<th>sleep</th>
</tr>
</thead>
<tbody>
<tr>
<td>not_fasting</td>
<td>fasting</td>
<td>not_fasting</td>
</tr>
</tbody>
</table>

It does if fasting.start and fasting.end refer to the first fasting interval and not the second one. So we clearly need to distinguish between these intervals. We could call the first interval fasting and the second interval next fasting. Now suppose we want to specify that pre_sleep must start with fasting active and end with fasting active and that not_fasting executes in between as shown above. This can be expressed as:

fasting.start < pre_sleep.start < pre_sleep.end < next fasting.end AND pre_sleep.start < not_fasting.start < not_fasting.end < pre_sleep.end

Another question is whether not_fasting should be considered as current or not, that is whether to use not_fasting or next not_fasting. To disambiguate, we need a reference point from which the current action and the next action can be determined.

We consider two approaches:

1. Provide a new construct to establish a reference point.
2. Define a default reference point such as the earliest or latest time point in the expression.

\(^1\)We have also explored the use of logic quantifiers (∀, ∃), but we currently believe that the next operator approach is simpler and easier to understand. However, it is not without some difficulties which will be discussed subsequently.
3.3.1 The at Expression

The first approach could be achieved by introducing a new expression, namely an at expression, which specifies a reference timepoint. For example

\[ \text{at } A0.\text{start}: \ B0.\text{end} < \text{next } A0.\text{start} \]

In this case, all actions that are active at the timepoint \( A0.\text{start} \) are the current ones. The next instance after the completion of the current one is the next one. For example

<table>
<thead>
<tr>
<th>A0</th>
<th>A1</th>
<th>A0</th>
<th>A2</th>
</tr>
</thead>
<tbody>
<tr>
<td>B0</td>
<td>B1</td>
<td>B0</td>
<td>B1</td>
</tr>
</tbody>
</table>

\[ \text{B0.start} \quad \text{B0.end} \quad \text{next } A0.\text{start} \quad \text{next } B0.\text{end} \]

If the action is not active at the reference point, then the “current” one is the last one and the next one is the first occurrence after the reference point. For example

<table>
<thead>
<tr>
<th>A0</th>
<th>A1</th>
<th>A0</th>
<th>A2</th>
</tr>
</thead>
<tbody>
<tr>
<td>B1</td>
<td>B0</td>
<td>B1</td>
<td>B0</td>
</tr>
</tbody>
</table>

\[ \text{B1.start} \quad \text{next } B1.\text{start} \]

It should also be noted that there is an implicit universal quantifier in every constraint. If the reference point involves action \( A1 \), e.g., \( A1.\text{start} \), and \( A1 \) can occur multiple times on a timeline, then this constraint applies every time \( A1 \) is scheduled.

Note that the constraint above, namely

\[ \text{at } A0.\text{start}: \ B0.\text{end} < \text{next } A0.\text{start} \]

would rule out the following solution

<table>
<thead>
<tr>
<th>A0</th>
<th>A1</th>
<th>A0</th>
<th>A2</th>
</tr>
</thead>
<tbody>
<tr>
<td>B0</td>
<td>B1</td>
<td>B0</td>
<td>B0</td>
</tr>
</tbody>
</table>

Because of the flexibility in attaching a reference point and the implicit universal quantifier, it becomes apparent that the same constraint could have a different set of solutions, depending on the location of the at expression.

Consider the following constraint
If the reference point is chosen as \texttt{A1.start}

\texttt{at A1.start: \texttt{B0.start} + 5 < \texttt{next A2.start} < \texttt{next B0.start} + 7}

then the following timeline is a potential solution, when \texttt{next B0.start} + 7 > \texttt{next A2.start}

\begin{tabular}{l|l|l|l}
 & A1 & & A2 \\
\hline
\texttt{B0} & \texttt{B1} & \texttt{B2} & \texttt{B0} \\
\hline
\texttt{B0.start} & & & \texttt{next B0.start} \\
\end{tabular}

If we change the \texttt{at} expression as follows:

\texttt{at A1.end: \texttt{B0.start} + 5 < \texttt{next A2.start} < \texttt{next B0.start} + 7}

the above timeline no longer satisfies the constraint

\begin{tabular}{l|l|l|l|l|l|l}
 & A1 & & & A2 & & \\
\hline
\texttt{B0} & \texttt{B1} & \texttt{B2} & \texttt{B0} & \texttt{B2} & \texttt{B0} & \\
\hline
\texttt{B0.start} & & & & \texttt{next B0.start} & & \\
\end{tabular}

because the location of \texttt{B0.start} has changed. Therefore, one should use much care in the application of the \texttt{at} expression.

3.3.2 Using a Default Time Reference Point

We have also experimented with a default reference point, namely the first or last timepoint that appears in the expression. However, without a restriction on the \texttt{at} expression, some ambiguities can arise. These ambiguities will be demonstrated using the following transition graphs:

\texttt{A0 \rightarrow A1 \rightarrow A2 \rightarrow A1 \rightarrow A3}

\texttt{B0 \rightarrow B1 \rightarrow B2 \rightarrow B1 \rightarrow B3}

Suppose we use the first timepoint that appears in the expression. But how should one interpret the following?

\texttt{next A1.start < B1.end}
Here the first expression is \texttt{next A1.start}. In this case, determining which instance of \texttt{A1} is the reference point is problematic:

\begin{table}[h]
\begin{center}
\begin{tabular}{cccc}
A0 & A1 & A0 & A1 \\
B0 & B1 & B0 & B1 \\
\end{tabular}
\end{center}
\end{table}

The same impasse is reached when trying to determine which instance of \texttt{B1} is referred to by the \texttt{B1.end} term.

Now suppose we make the last timepoint the reference expression. To create an ambiguity, one only needs reverse the constraint

\begin{equation}
\texttt{A1.start < next B1.end}
\end{equation}

Of course we can disallow the use of \texttt{next} in the first position in the first approach (or last position in the second approach), though this is a bit artificial. Nevertheless, this is probably the best approach. We need only decide whether to use the first or last term. If we use the first term as the default, then the first constraint we looked at, namely,

\begin{equation}
\texttt{A1.start + 16 < B2.end}
\end{equation}

would have to be rewritten as

\begin{equation}
\texttt{A1.start + 16 < next B2.end}
\end{equation}

if the following timeline is to be a solution:

\begin{table}[h]
\begin{center}
\begin{tabular}{c}
A1 \\
\hline
B2 \\
\end{tabular}
\end{center}
\end{table}

\begin{center}
\framebox{ule{1cm}{1pt}}
\text{d > 16}
\end{center}

Therefore, we think that the best approach is to make the default the last term. By making the default reference point the last term, all of the previous terms are earlier in time and hence they are current ones (by definition of the reference point). Therefore, this choice provides a nice seamless unification with the non-repetitive cases. If the last term has a \texttt{next} operator, then an explicit \texttt{at} expression must be provided\textsuperscript{2}.

\textsuperscript{2}Another attractive alternative is to require an \texttt{at} expression whenever there is a repetitive action.
3.4 Timeline Instance Specific Constraints

Constraints can be specialized by using a timeline variable in the constraint. Suppose we have

VARIABLES
- t1, t2: A
- t3, t4: B

CONSTRAINTS
- t1.A1.start < t4.B1.end

Now this constraint only affects timelines t1 and t4. But the constraint
- A1.start < B1.end

is equivalent to four constraints:
- t1.A1.start < t4.B1.end

Mixing qualified and unqualified action names may be problematic. For example
- t1.A1.start < B2.end

Even though a default interpretation can be envisioned as treating the unqualified term as “for all” timeline instances tb of B

This is however dangerous when the terms are on the same timeline, because it can easily lead to contradictions, such as in
- t1.A1.end < t2.A2.start < A1.end

3.5 The Interleaving Example

Suppose we need to specify that repetitive actions A0 and B0 are interleaved as illustrated below:

<table>
<thead>
<tr>
<th></th>
<th>A0</th>
<th></th>
<th>A0</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>B0</td>
<td></td>
<td>B0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Let’s try to write some constraints that enforce this behavior
Immediately we encounter a problem. Consider the following timeline:

<table>
<thead>
<tr>
<th>A0</th>
<th>A0</th>
<th>A0</th>
</tr>
</thead>
<tbody>
<tr>
<td>B0</td>
<td>B0</td>
<td></td>
</tr>
</tbody>
</table>

It satisfies the constraints because there are multiple instances of A0 and B0. In this case, it is possible that A0 and B0 overlap but the constraint is still satisfied. If instead we combine the two inequalities in a single chain

\[
\text{at B0.start: } A0.\text{end} < B0.\text{start} < B0.\text{end} < \text{next A0.start}
\]

we rule out the possibility of overlap: A0 has to have ended before B0 starts and cannot occur again until B0 ends. However, this is still not the complete specification. This constraint requires that \textit{at least one} instance of B0 occurs between successive instances of A0. But consider the following timeline:

<table>
<thead>
<tr>
<th>A0</th>
<th>A0</th>
<th>A0</th>
</tr>
</thead>
<tbody>
<tr>
<td>B0</td>
<td>B0</td>
<td>B0</td>
</tr>
</tbody>
</table>

Unfortunately this solution meets the specification, even though there are multiple occurrences of B0 between first and second A0. So we need to write one more constraint that is symmetric with respect to B0:

\[
\text{at A0.start: } A0.\text{end} < \text{next B0.start} < \text{next B0.end} < \text{next A0.start} \\
\text{at B0.start: } B0.\text{end} < \text{next A0.start} < \text{next A0.end} < \text{next B0.start}
\]

The previous undesired scenario is no longer a solution. The care needed to solve this simple problem, illustrates that correctly specifying a constraint can be a subtle matter. In fact there is one additional aspect of this solution that should be mentioned. Namely, we have implicitly assumed that we lift the requirements at the end of the planning horizon. The last occurrence of either A0 or B0 has no successor, hence the constraint is satisfied by default. Suppose || represents the end of the planning horizon on the following timeline.

<table>
<thead>
<tr>
<th>A0</th>
<th>A0</th>
<th>A0</th>
</tr>
</thead>
<tbody>
<tr>
<td>B0</td>
<td>B0</td>
<td>B0</td>
</tr>
</tbody>
</table>

The final A0 has no next A0 action and there is no subsequent B0 so the constraint
at A0.start: A0.end < B0.start < B0.end < next A0.start

is not strictly satisfied. Therefore, an exception must be made at the end of the horizon.

Note: we currently allow only one application of next. In other words, the following is not allowed: next next A2. Allowing multiple instances of next will increase the power of the language (and the difficulty of translation), but we are not convinced that this additional power is needed.

3.6 Vacuous solutions

Consider the Allen operator \( A1 \) contains \( B1 \). A constantly debated issue is whether the constraint can be satisfied by the following timeline

\[
\begin{array}{c|c|c|c}
A0 & A2 & & \\
B0 & B1 & B2 & \\
\end{array}
\]

Because the Allen operator has the implicit quantifiers \( \text{FORALL} A1: \text{EXISTS} B1: A1 \text{ contains } B1 \), this constraint can be vacuously met in case \( A1 \) is never scheduled. Whether this is desirable or not is a recurring theme in the plan specification domain. A non-ambiguous semantics should be chosen for all these situations.

In ANMLite, the existence of vacuous solutions takes another dimension in the presence of flexible at expressions. For example, an equivalent ANMLite specification for the Allen operator \( A1 \text{ contains } B1 \) is the following:

\[
A1.start < B1.start < B1.end < A1.end
\]

There could be three types of vacuous solutions, depending on whether \( A1 \) is never scheduled, \( B1 \) is never scheduled, or both. If the at expression is associated with \( A1 \), then there exists a vacuous solution when \( A1 \) is never scheduled, even if \( B1 \) is. If, on the other hand, the at expression is associated with \( B1 \), then no such vacuous solution exists, because if \( B1 \) is scheduled, then the satisfaction of \( A1.start < B1.start \) immediately requires the existence of a preceding \( A1 \) to \( B1 \).

The implementation of a verifier by means of a model checker further adds to the complexity of this discussion, because \( A1.start < B1.start \) could be satisfied not only by the actual scheduling of \( A1 \), but also by the choice of initializing the variable associated to \( A1.start \) in the model. Usually, an action that has not been scheduled yet has a distinctive value which is not in the range of the planning horizon. The natural choices are \(-\infty \) or \( \infty \). If a negative initial value is chosen, \( A1.start < B1.start \) is always satisfied when \( A1 \) is not (yet) scheduled before \( B1.start \). A positive initial value will rule this situation out. But, of course, the situation is reversed when requiring the symmetric case: \( A1.start > B1.start \).

In conclusion, the existence of vacuous solutions is influenced by three factors: the reference point, the implicit quantifiers, and the initialization of variables.
We have added the chained constraint syntax as an alternative to the conjunctive form. For the existence of vacuous solutions the two formats are not equivalent. Consider the following constraint:

\[
B.\text{start} = A.\text{end} < B.\text{end} = C.\text{start}
\]

which is satisfied by the following:

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The semantics for this constraint is

\[
\text{FORALL C: EXISTS A,B: at C.\text{start: } B.\text{start} = A.\text{end} < B.\text{end} = C.\text{start}}
\]

The last term is universally quantified and the other terms are existentially quantified. Therefore if C does not execute, the constraint is satisfied, but if C does execute, then there must also be executions of A and B as well. If one breaks up the above constraint into two separate constraints, i.e.,

\[
B.\text{start} = A.\text{end} \\
B.\text{end} = C.\text{start}
\]

the following defines the meaning:

\[
\text{FORALL A: EXISTS B: at A.\text{end: } B.\text{start} = A.\text{end}} \\
\text{FORALL C: EXISTS B: at C.\text{start: } B.\text{end} = C.\text{start}}
\]

Note that the split version allows the following timeline:

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

whereas the first version does not. It should be noted that an equality within a constraint is not an equivalence relation, except with respect to the timepoints. Because of the default reference points and default quantifier rules, the timelines defined by \( A = B \) can be different than those defined by \( B = A \). For example,

\[
A.\text{end} = B.\text{start} \\
B.\text{end} = C.\text{start}
\]
has the following meaning:

\[
\text{FORALL B: EXISTS A: at B.start: A.end = B.start}
\]
\[
\text{FORALL C: EXISTS B: at C.start: B.end = C.start}
\]

so that the diagram above with two Bs separated by an x action does not satisfy it. The second B does not have an associated A for which the first constraint is satisfied.

In the future, we would like to look at the implications of eliminating all vacuous solutions or restricting them. Many times vacuous solutions are not desirable solutions at all. It is very easy for the writer of a domain specification to add a constraint with the expectation that this constraint will be required to happen. But if the planner finds a solution that avoids the implicit FORALL variable of the constraint, then it can ignore the stated constraint. In a safety-critical application, this could result in some important action being omitted or an important constraint not being satisfied. Of course, the domain specification can be strengthened by explicitly listing every action that must execute. But, it is not always intuitively obvious that this needs to be done. We believe that the clarity of a specification language is very important. It would be interesting to investigate whether the clarity of ANMLite would be increased by eliminating vacuous solutions or at least making it very clear where vacuous solutions are allowed.

### 3.7 Summary of Constraint Semantics

There are two major issues that need to be resolved when interpreting a constraint in ANMLite:

- Determination of the time point from which the current and next instances of an action can be disambiguated.
- Determination of which actions are universally quantified and which ones are existentially quantified.

These issues are orthogonal and hence the most general solution allows an independent specification of them. The first issue is handled by the at expression. If the at expression is omitted, the last term determines the time point. For example, given

\[
A.end < B.end
\]

the reference time point is B.end. All actions that are active at the refererence point are current. If an action is not scheduled at the reference point, the last instance is the current one and the future one is next.

The second issue is handled by a syntactic convention, namely, that the last term in the chain of inequalities determines the universally quantified action. For example, if we have

\[
A.start < B.end < C.start < W.end
\]

then the universally quantified action is W and the actions A, B, and C are existentially quantified:
FORALL W: EXISTS A,B,C: A.start < B.end < C.start < W.end

This choice is justified by the way the constraint checking has to performed (efficiently) in the SAL models (see Section 5). The other alternative, of attaching the universal quantifier to the first term, is equally valid from the theoretical point of view.

Also note that these conventions depend upon the restriction that all of the operators must be either <, <=, or =\(^3\).

If the last term contains a next operator:

\[
\text{at C.start: A.start < B.end < C.start < next B.end}
\]

then the existence of two instances of B (current and next) are assumed. This constraint is interpreted as follows

\[
\text{FORALL B: (EXISTS B': B = next B' => (EXISTS A,C: at C.start: A.start < B'.end < C.start < B.end))}
\]

It should be noted that inconsistent expressions can easily be created:

\[
A.end < A.start
\]

Such expressions are unsolvable and produce plan specifications for which there are no solutions.

### 3.8 Some More Illustrative Examples

#### 3.8.1 Example: Spread-out Contains

Suppose we want a B1 contains A1 that is also time-constrained:

\[
\begin{array}{c|c|c}
 & \text{A1} & \\
\hline
\text{B0} & & \\
\hline
\text{B1} & & \\
\text{B2} & & \\
\end{array}
\]

We want d1 > 10 and d2 > 20. We do this as follows

\(^3\)We could generalize and also allow sequences of >, >=, = operators and then make the first syntactic term be the universally quantified action. We believe the added flexibility is not worth the potential confusion that could arise from trying to remember the quantification rule. Alternatively, we could add an explicit quantifier to the constraint expression, e.g. FORALL W: A.start < B.end < C.start < W.end, but we would then either have to make this mandatory or define a default. At this point we prefer not to add an explicit quantifier to the language.
at B1.start: B0.start + 10 < next A1.start < next A1.end < B1.end - 20

or more concisely as

B0.start + 10 < A1.start < A1.end < B1.end - 20

where the default reference point is at B1.end.

3.8.2 Example: Stretch It Out

Suppose we want each B1 action to contain at least two instances of A1. This can be achieved with one chained constraint as follows:


Here is an example solution:

\[
\begin{array}{c|c|c|c|c}
\hline
& A0 & A1 & A0 & A1 \\
\hline
B0 & & & B1 & \\
\hline
\end{array}
\]

Note that the constraint


has no solution. Consider the following diagram to see this:
3.8.3 Example: Forcing a Future Action to Occur Within a Time Interval

Suppose we wish to constrain action A2 to always be scheduled after action A1 and that this must occur between 10 and 20 time units after the end of A1 as illustrated below

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A0</td>
<td>A1</td>
<td>A2</td>
</tr>
</tbody>
</table>

which can be written in ANMLite syntax as

\[
\text{at } A2.\text{start}: \text{A1.end} + 10 < A2.\text{start} < \text{A1.end} + 20
\]

3.8.4 Delayed Initiation

Suppose that you want to insure that action A1 does not begin until after 15 time units. The following constraint

15 < A1.start

accomplishes this. Note that it is more difficult to specify something like “the final action on the timeline is A3 and it starts after 70 time units”. If A3 is not a repetitive action, then this can be accomplished by

CONSTRANTS

70 < A3.start

GOALS

A.A3

But what if A3 is a repetitive task and we just want the last instance of A3 to start after 70? We could use a parameter and count the instances of A3 as follows:

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A0</td>
<td>A3(1)</td>
<td>A0</td>
<td>A3(2)</td>
<td>A0</td>
<td>A3(3)</td>
</tr>
</tbody>
</table>

We could then extend the constraint language to allow parameters and constrain a specific instance, say 4, to occur after a specified time as follows

70 < A3(4).start
But this still does not solve the stated problem. Perhaps we could extend the at expression so that it could refer to the horizon beginning or end. Then we could write

\[ \text{at end: } 70 < A3.\text{start} \]

This will work if A3 is the goal state.

<table>
<thead>
<tr>
<th>A0</th>
<th>A3</th>
<th>A0</th>
<th>A3</th>
<th>A0</th>
<th>A3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[ A3.\text{start} \]

\[ \text{reference point} \]

3.9 Mandatory at Expressions

We have explored the possibility of not having a default at reference time point. If there are no cycles in the transition graph then each action can only occur once. In this case, the next syntax is not needed and hence there is no need to specify a reference time point. But suppose the user makes a mistake and specifies a constraint without a reference time point and there is a cycle in the graph. The translator would need to detect this situation and report an error. This will require a traversal of the graph to see if a cycle is present. This is relatively straight-forward in the absence of parameters. But with parameters, it is possible for there to be cycles for only certain parameter combinations. So what might appear to be a cycle situation, may really be unreachable. If at expressions are made optional and there is no default, it seems prudent to make the cycle check in the absence of parameters. This is clearly conservative and will rule out some cases where the at expression can be omitted, but the implementation code is much simpler. But, due to the difficulties associated with this approach, we have chosen to define a default reference point whenever an at expression is not present.

3.10 Convenient Macros

The ANMLite language can be extended with some macros which emulate some of the Allen operators. For example, the Allen operator \( A \) contains \( B \) can be emulated by

\[ A.\text{start} < B.\text{start} < B.\text{end} < A.\text{end} \]

We can introduce the notation

\[ \text{CONSTRAINTS} \]

\[ A \text{ contains } B \]

which is then automatically expanded into

\[ A.\text{start} < B.\text{start} < B.\text{end} < A.\text{end} \]
Similarly

A meets B
can automatically be translated into

B.start = A.end

and

A met_by B
can automatically be translated into

B.end = A.start

Some of the Allen operators cause some difficulty. Consider B contained_by A. At first we might suppose that the same constraint

A.start < B.start < B.end < A.end

will suffice. But, the semantics of the Allen operator mandates that if B executes, then it must be contained by an A. In other words, there is an implicit universal quantification for B and an implicit existential quantification for A, i.e. FORALL B: EXISTS A: B contained_by A. However, the semantics of the constraint: A.start < B.start < B.end < A.end is

FORALL A: at A.end: A.start < B.start < B.end < A.end

which is satisfied by

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>x</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>y</td>
<td>B</td>
</tr>
</tbody>
</table>

It appears that there is no convenient way to create a contained_by macro that exactly matches the semantics of the corresponding Allen Operation using the constructs that we have defined. To obtain exactly the same solutions would require something new like

FORALL B: at A.end: A.start < B.start < B.end < A.end

Another possibility would be to attach the default FORALL to the at or to create a special at! where this is done:

at! B.end: A.start < B.start < B.end < A.end

But, we are not sure whether this is a wise extension of the language. Perhaps we should not seek to duplicate the Allen Operation Semantics? Often vacuous solutions are not desirable solutions. It is very easy for the writer of a domain specification to write a constraint expecting that this would insure that the described situation will actually happen. But the constraint can be avoided altogether by the planner by finding a solution where the FORALL variable is not scheduled at all. It would be interesting to study the implications of eliminating all or some of the vacuous solutions in ANMLite. See section 3.6 for more information about this issue.
4 Condition and Effects

We are currently experimenting with condition and effects clauses within the definition of an action. This is motivated by similar clauses in the ANML language. However, we have introduced these constructs with some reluctance because they operate through use of global variables. Global variables are usually an attribute of programming languages rather than specification languages. Although this makes it possible to express things in the style that programmers are familiar with, it ultimately leads to a less abstract specification, and hence a more difficult one to formally verify. Nevertheless, one of the main purposes of this work is to develop verification methods suitable for verifying properties of the ANML language under development at NASA Ames.

We augment the body of an action definition, with a condition clause and an effects clause as illustrated below:

\[
A1: [7\_\_] \{ \\
\quad \text{condition: start} > \text{vf} + 10; \\
\quad \text{effect: vf} := \text{end}; \\
\}
\]

where \( \text{vf} \) is a variable defined in a preceding VARIABLES section:

\[
\text{VARIABLES} \\
\quad \text{vf: TM\_rng} = 0;
\]

The keyword start refers to the time that the action started execution and the keyword end refers to the time that the action finishes execution. The condition statement represents a constraint that must hold before the action is allowed to execute. The effect statement results in the update of the value of variables when the task terminates. The ANML language is more general in that it allows an arbitrary predicate and the specification of a time interval over which this predicate must hold. This time interval can be in the future, so very complex behaviors can be specified with that construct. However, we have restricted our effects section to be just a sequence of variable updates. The condition statement in A1 above prevents the initiation of A1 until the time is \( \text{vf} + 10 \). Initially \( \text{vf} \) is 0, so the first execution of A1 is delayed until after time 10. At the termination of A1, the effect statement updates the value of the variable \( \text{vf} \) to the termination time of A1. The net effect on subsequent executions of A1 is to make sure that they are 10 time units apart.

The use of condition and effect statements is to introduce an algorithmic flavor to the language. If the updates to the variables are in a very restricted and controlled manner, then the intended meaning can be easy to discern. But if variables are updated in multiple places in different actions, then we have all of the subtleties of concurrent programming to deal with. It seems to us that these condition/effect statements can easily lead to complex specifications that are difficult to understand and even more difficult to verify. The more general ANML constructs are even more dangerous.

Note that the above specification can be accomplished more naturally using the following constraints
The advantage of this latter approach is that the specification is abstract and not algorithmic.

5 Translating ANMLite to SAL

Although using a model checker might not be the most efficient means of finding a solution to a planning problem, building a translator has provided a sanity check on the meaning of the language constructs.

5.1 Simple Example

We will begin our look at the technique for translating ANMLite to SAL with a very simple two timeline example:

PLAN ex1

TIMELINE A
ACTIONS
    A0: [2,_
    A1
    A2

TRANSITIONS
    A0 -> A1 -> A2

END A

TIMELINE B
ACTIONS
    B0: [2,_
    B1: [1,10]

TRANSITIONS
    B0 -> B1

END B
INITIAL-STATE

|-> A.A0
|-> B.B0

GOALS

A.A2
B.B1

END ex1

Timeline A has three actions A0, A1, and A2 with only one possible sequence. The duration of action A0 is at least 2 time units, while the other two actions have no restrictions on their duration. Similarly, timeline B has two actions B0 and B1, with only one possible sequence. B0 has a duration of at least 2 time units, while B1 takes between 1 and 10 units.

Corresponding to these actions, the following types are generated

A_actions: TYPE = {A0, A1, A2, A_null};

B_actions: TYPE = {B0, B1, B_null};

In addition to the declared actions, a null state is created for each of the timelines. There are two purposes for these extra states:

- They provide a means for the completion of an action when the action has no successor.
- They provide a convenient mechanism for recording when a goal state has been reached on each timeline. As shown below, a transition from a timeline’s goal state to the null state is generated by the translator.

The generated SAL model will consist of three modules:

- Module A_m which corresponds to timeline A.
- Module B_m which corresponds to timeline B.
- Module Clock which advances time.

5.2 Multiple variables

If there are multiple variables of a timeline, say

VARIABLES

  t1,t2: A
then a variable id type is generated,

\[
A_{\text{ids}}: \text{TYPE} = \{t1, t2\};
\]

and the module \( A_m \) is parametrized with the variable id

\[
A_m[i: A_{\text{ids}}] : \text{MODULE} =
\]

Furthermore, since each instance of the timeline is a separate module, all the local and global variables in the parametrized module have to be arrays. For example, a non-parametrized module \( A_m \) might include a variable for \( A0_{\text{start}} \)

\[
\text{GLOBAL}
\]

\[
A0_{\text{start}}: \text{TM\_rng};
\]

The parametrized version has to be

\[
\text{GLOBAL}
\]

\[
A0_{\text{start}}: \text{ARRAY A_{ids} OF TM\_rng};
\]

This way, the start of \( A0 \) for instance \( t1 \) is referred to as \( A0_{\text{start}}[t1] \).

### 5.3 Modeling Time

Time is governed by the generic clock module. We have experimented with various implementations of this module. The most straightforward approach is to have the clock module increment the current time by one time unit at each step. This approach is very simple but is not scalable, because the system would traverse a very large number of states that are identical with the exception of the clock value. This state explosion problem is exacerbated by problems with large planning horizons. A possible alleviation of problem is to allow the clock to advance by larger amounts. However, this still does not rule out the traversal of multiple states in an interval of time when nothing interesting happens (from the point of view of action change). The best solution in this case is to use the concept of timeouts [6] that model the event driven clocks. In this approach, each timeline maintains a future clock value where an event is scheduled to occur, and time jumps directly to the next interesting event. The timeouts are stored in an array of timepoints and the clock module determines the next (minimum value in the future) timeout.

The structure of the module generated for a timeline \( A \) is:

\[
A_m : \text{MODULE} =
\]

\[
\text{BEGIN}
\]

\[
\text{INPUT}
\]

\[
\text{OUTPUT}
\]

\[
\text{GLOBAL}
\]
LOCAL

INITIALIZATION

TRANSITION
[
  A0_to_A1: % % A0 -> A1
]
[
  A1_to_A2: % % A1 -> A2
]
[
  A2_to_A_null: % % A2 -> A_null
]
]
END; % % A

Each of these sections is used in the translation:

- **INPUT** is used to select values for parameters of actions.
- **OUTPUT** is used to store timeout values for the clocking mechanism
- **GLOBAL** is used to hold state values and their current parameter values.
- **LOCAL** is used to hold the start time of the currently scheduled action.
- **INITIALIZATION** is used to set initial values.
- **TRANSITION** specifies rules for transitioning from one action to another.

The three modules will be asynchronously composed. In SAL this is specified as follows:

```
System: MODULE = A_m [] B_m [] Clock;
```

The SAL tool links the variables named in the **GLOBAL** and **INPUT** sections together. In other words, variables with the same name are equated even though they are specified in different modules.

The SAL model checker will be used to search through all possible sequences of actions on the timelines to find sequences which satisfy all of the constraints specified in the ANMLite model. These constraints fall into three broad categories:

- Timing constraints that impact durations and start/stop times of actions.

---

4 It is actually slightly more complicated than this because of the need to coordinate the timeout variables of the modules. This will be discussed later.
• Simple relationships between start and end variables
• Constraints defined through condition and effect statements.

The search is started at time 0 and proceeds forward in time until the planning horizon is reached. The stop time is specified via a constant as follows:

\[
\begin{align*}
\text{MAX_TM: int } &= 30; \\
\text{TM_rng: TYPE } &= [0 .. \text{MAX_TM}+1];
\end{align*}
\]

The progress of the “clock” is controlled by the clock module:

\[
\begin{align*}
\text{Clock: MODULE } &= \\
\text{BEGIN} &\\
\text{INPUT timeout: TIMEOUT_ARRAY} &\\
\text{OUTPUT time: TM_rng} &\\
\text{INITIALIZATION} &\\
time &= 0; \\
\text{TRANSITION} &\\
\text{[} &\\
\text{time_elapses:} &\\
\text{(EXISTS (i: timeline): time < timeout[i])} &\\
&\text{AND (FORALL (i: timeline): time /= timeout[i])} &\\
&\text{-->} &\\
&time' \text{ IN } \{ t: TM_rng \mid \text{is_min(timeout, t)} \} &
\end{align*}
\]

END;

5.4 Model Variables

The GLOBAL sections of all of the timeline modules contain variables which record the action that is scheduled during the current time:

\[
\begin{align*}
\text{GLOBAL} &\\
\text{A0\_start: TM\_rng,} &\\
\text{B0\_start: TM\_rng,} &\\
\text{B1\_start: TM\_rng,} &\\
\text{B\_state: B\_actions,} &\\
\text{A\_state: A\_actions,}
\end{align*}
\]

The _state variables contain the current action and the _start and _end variables contain the start and end times of the actions.

The durations of the actions are controlled by the use of the _start variables. Whenever an action is initiated, the initiation time is stored in this variable. The durations of an action will be controlled through this variable. This will be explained more carefully when we discuss the transitions section.

The initial actions on a timeline can be specified as follows:
INITIAL-STATE
|-> A.A0
|-> B.B0

If a timeline’s initial state is not specified, then the model checker will explore all possible start states. The above initialization results in

INITIALIZATION
A_state = A0;
A0_start = 0;
in the A_m module and

INITIALIZATION
B_state = B0;
B0_start = 0;
B1_start = MAX_TM+1;
in the B_m module.

5.5 Transitions

The ANMLite TRANSITIONS section is the major focus of the translation process. The SAL TRANSITIONS section is constructed from this part of the ANMLite model. For example, the following

TRANSITIONS

A0 -> A1 -> A2

is translated into

TRANSITION
[
  A_starts:
    A_state = A0
  -->
    timeout’ IN {t:TM_rng | t > time}
[]
A0_to_A1: % % A0 -> A1
  A_state = A0
  AND time >= A0_start + 2
  -->
    A_state’ = A1;
    timeout’ IN {t:TM_rng | t > time}
 When a transition occurs, an action is completed and another transition is initiated. No empty time slots are allowed. The TRANSITIONS section defines three transitions which are labeled as follows:

\[
\begin{align*}
A0_to_A1: & \quad \text{A0} \to \text{A1} \\
A1_to_A2: & \quad \text{A1} \to \text{A2} \\
A2_to_A_null: & \quad \text{A2} \to \text{A_null}
\end{align*}
\]

The first transition is guarded by the following expression:

\[
\text{A_state} = \text{A0} \land \text{time} \geq \text{A0_start} + 2
\]

The first conjunct insures that this transition only applies when the current action on the timeline is \text{A0} and the second conjunct insures that the duration of the action is at least 2 time units. This corresponds to the fact that \text{A0} was declared as \text{A0: [2, _]} . The expressions after the \to specify that the new state is \text{A1}. Note that start times are not maintained for \text{A1} and \text{A2} because no constraints use them.

The ANMLite GOALS statement

\[
\text{GOALS} \\
\text{A.A2} \\
\text{B.B1}
\]

lists two actions that need to be reached (where the default meaning of the expression is the logical conjunction of the terms). This statement is translated into the following SAL specification:

\[
\text{sched_sys: THEOREM} \\
\text{System |- AG(NOT(A_state = A_null AND B_state = B_null))} \\
\]

30
Since the “null” states can only be reached from the goal states (i.e., A2 and B1), these efficiently record the fact that the appropriate goal has been reached on each timeline. Note that the ANMLite goal statement has been negated. Therefore when the model checker is instructed to establish the property, any counterexample provided by SAL will serve as a feasible realization of the plan.

The complete generated SAL model is

```
ex1: CONTEXT =
BEGIN

MAX_TM: int = 30;
TM_rng: TYPE = [0 .. MAX_TM+1];

A_actions: TYPE = {A0, A1, A2, A_null};

B_actions: TYPE = {B0, B1, B_null};

timeline: TYPE = {A, B};

TIMEOUT_ARRAY: TYPE = ARRAY timeline OF TM_rng;

is_min(x: TIMEOUT_ARRAY, t: TM_rng): bool =
  t >= 0
  AND (FORALL (i: timeline): t <= x[i])
  AND (EXISTS (i: timeline): t = x[i]);

A_m : MODULE =
BEGIN
  INPUT
    time: TM_rng
  OUTPUT
    timeout: TM_rng
  GLOBAL
    A0_start: TM_rng,
    B0_start: TM_rng,
    B1_start: TM_rng,
    B_state: B_actions,
    A_state: A_actions

```
INITIALIZATION
  A_state = A0;
  A0_start = 0;
TRANSITION
[ 
  A_starts:
    A_state = A0
    -->
    timeout' IN {t:TM_rng | t > time}
[ ]
  A0_to_A1:  \% A0 -> A1
    A_state = A0
    AND time >= A0_start + 2
    -->
    A_state' = A1;
    timeout' IN {t:TM_rng | t > time}
[ ]
  A1_to_A2:  \% A1 -> A2
    A_state = A1
    -->
    A_state' = A2;
    timeout' IN {t:TM_rng | t > time}
[ ]
  A2_to_A_null:  \% A2 -> A_null
    A_state = A2
    -->
    A_state' = A_null;
    timeout' = MAX_TM+1;
]
END; \% A

B_m  : MODULE =
BEGIN
  INPUT
    time: TM_rng
  OUTPUT
    timeout: TM_rng
  GLOBAL
    A0_start: TM_rng,
    B0_start: TM_rng,
    B1_start: TM_rng,
A_state: A_actions,
B_state: B_actions

INITIALIZATION
B_state = B0;
B0_start = 0;
B1_start = MAX_TM+1;

TRANSITION
[
  B0_to_B1:  \%
  B0 -> B1
  B_state = B0
  AND time >= B0_start + 2
  -->
  B_state' = B1;
  B1_start' = time;
  \timeout' IN \{t:TM_rng | t > time\}
]

[
  B1_to_B_null:  \%
  B1 -> B_null
  B_state = B1
  AND time >= B1_start + 1
  AND time <= B1_start + 10
  -->
  B_state' = B_null;
  \timeout' = MAX_TM+1;
]

END;  \%

Clock: MODULE =
BEGIN
  INPUT timeout: TIMEOUT_ARRAY
  OUTPUT time: TM_rng

  INITIALIZATION
  time = 0;

  TRANSITION
  [
    time_elapses:
      (EXISTS (i: timeline): time < timeout[i])
      AND (FORALL (i: timeline): time /= timeout[i])
      -->
      time' IN \{t: TM_rng | is_min(timeout, t)\}
  ]

END;
5.6 Translating Constraints

There are major conceptual differences between specifying constraints and checking constraints that need to be reconciled. In principle, the specification is declarative by nature and the modeler usually looks “forward” in time in expressing what needs to happen in order for the plan to complete. The checking of the plan is operational by nature, because start and end variables are assigned values as they occur, hence testing that a constraint is valid cannot be performed until the last timepoint has occurred. Therefore, in the checking of the constraints the modeler has to look “backwards” in time.

For example, the constraint \( A.\text{start} < B.\text{end} < C.\text{start} \) cannot be established when \( A \) starts. Even if \( B \) has not ended yet, its relationship to the start of \( C \) cannot be established.

The mechanism of checking constraints with a model checker is based on assigning and updating the values of timeline state and each action start and end variables. This is performed at the timepoints when a timeline transitions from one action to another, according to the TRANSITIONS section.

Repetitive actions require special care, as multiple occurrences of the same actions will overwrite the values of the corresponding start and end variables, so only the most recent one is actually available (and possibly the previous occurrence, given that we allow the next qualifier).

For example, if there is a transition \( A_1 \rightarrow A_2 \) on timeline \( A \), the following updates are necessary:

- \( A_\text{state}' = A_2 \)
- \( A_1.\text{end}' = \text{time} \)
- \( A_2.\text{start}' = \text{time} \)

A constraint is, in principle, applicable to all the transitions that affect the variables present in the constraint expression. That is, a start variable is relevant to entering an
action, while the end variable is relevant to exiting an action. Transition guards are generated for the events that are involved.

The general approach of translating constraints into transition guards consists of determining the last timepoint in the chain and substituting that term with the value of the system variable time. For example, in the constraint

\[ A1\text{.start} + 4 < B1\text{.start} < C1\text{.end} \]

the last timepoint is \( C1\text{.end} \). The transitions of relevance to this timepoint are from a predecessor of \( C1 \) to \( C1 \), i.e., entering \( C1 \). For simplicity, in the following, assume there is only one successor/predecessor of an action, according to its index (\( X_n \) precedes \( X_{n+1} \), for any action \( X \) and any index \( n \)). Then, the above constraint will results in a transition guard for \( C0\_to\_C1 \):

**TRANSITION**

\[
\begin{align*}
C0\_to\_C1: & \quad C\_state = C0 \\
& \quad \text{AND } \text{time} >= \text{C0\_start} + d \ %\ %\ \text{any duration constraint here} \\
& \quad \text{AND } (A1\_start + 4 < B1\_start) \ \text{AND } (B1\_start < \text{time}) \\
& \quad \text{-->} \\
& \quad C\_state' = C1; \\
& \quad C1\_start' = \text{time}; \\
& \quad \text{timeout' IN } \{t: \text{TM\_rng} \mid t > \text{time}\}
\end{align*}
\]

A chained constraint can be broken down into all of its pairs, e.g., treat \( A1\text{.start} + 4 < B1\text{.start} \) and \( B1\text{.start} < C1\text{.end} \) separately. However, this simple decomposition does not work in the presence of a repetitive action, where both the current and the next instance are involved simultaneously. For example,

\begin{align*}
\text{at } B1\text{.end: } & \quad A1\text{.end} < B1\text{.start} < B1\text{.end} < \text{next } A1\text{.start} \\
\text{at } A1\text{.end: } & \quad B1\text{.end} < A1\text{.start} < A1\text{.end} < \text{next } B1\text{.start}
\end{align*}

enforcing that \( A1\text{.end} < B1\text{.start} \) separately from \( B1\text{.end} < \text{next } A1\text{.start} \) results in an unwanted scenario: each \( B1 \) is now required to end before the next instance of \( A1 \) which practically delays the scheduling of \( A1 \) indefinitely.

### 5.7 Current and next variables

When both the current and next instances are involved in a constraint, special care is required. Since we check constraints “backwards”, the two variables needed have to be labeled \( A1\_start \) and \( \text{prev}_A1\_start \). The current instance is the last in time, so it corresponds to next \( A1 \), while the start of earlier \( A1 \) is now denoted by \( \text{prev}_A1\_start \), which could be
a little counter-intuitive. When no repetitive instances are involved, no such variable name transformations are necessary.

The generated guard for the first constraint in the above example is

TRANSLITION
[
    A0_to_A1:
    A_state = A0
    AND time >= A0_start + d  %% any duration constraint here
    AND (prev_A1_end < B1_start)
    AND (B1_start < B2_end)
    AND (B1_end < time)
    -->
    A_state' = A1;
    A1_start' = time;
    prev_A1_start' = A1_start;
    timeout' IN {t:TM_rng | t > time}
]

Note that the value of the prev_ variables are also maintained. A special case is the first occurrence of a repetitive action, which has no predecessor. Hence, the complete guard is actually:

TRANSLITION
[
    A0_to_A1:
    A_state = A0
    AND time >= A0_start + d  %% any duration constraint here
    (prev_A1_end == MAX_TM+1) OR  %% first occurrence is a special case
    ((prev_A1_end < B1_start) AND (B1_start < B2_end) AND (B1_end < time))
    -->
    A_state' = A1;
    A1_start' = time;
    prev_A1_start' = A1_start;
    timeout' IN {t:TM_rng | t > time}
]

Further processing is required in case the constraint refers to a particular timeline instance. For example, the constraint


generates the following transition guard:
The Crew Activity Planning Model in ANMLite

The Crew Activity Planning Model is an example problem taken from the ANML distribution. The task is to plan the basic daily routines for several crew members over a period of four days. The activities include, besides physiologic states (sleeping, meals), routine activities, such as regular filter changes, medical conferences, and some payload operations. The ANML specification of this problem is described below.

The definition of an action

```
action pre_sleep {
    condition over all : fw.state == not_fasting();
}
```

is captured in the following ANMLite as follows:

```
not_fasting.start < pre_sleep.start 
< pre_sleep.end < not_fasting.end
```

The three condition statements in the definition of meal

```
action meal {
    condition over all : fw.state == not_fasting();

    // keep separation between meals >= 4 hrs
    condition over [start-240 start] : fw.state == fasting();
    condition over [end end+240] : fw.state == fasting();
}
```
can be condensed into

\[
\text{not\_fasting.start + 240 < meal.start < meal.end < not\_fasting.end - 240}
\]

The following ANML specification uses an effect statement to specify that the next filter change happens within the next 24 to 48 hours

```plaintext
action change_filter(FilterState fs) {
    change over all : fs -> {changed, changing, changed};

    // make sure next filter change happens
    // within the next 24 to 48 hours
    effect in [end+1440 end+2880] : fs == changing;
}
```

This specification relies on the use of an auxiliary variable fs, which has no other role than to provide a way of saying that something must occur in the future. Compare the opaqueness of the ANML specification with the elegance of the ANMLite equivalent:

```plaintext
at change_filter.end:
    change_filter.end + 1440 < next change_filter.start
    < change_filter.end + 2880
```

Notice that there is no need for an auxiliary variable and it is far easier to understand. In fact, it would be very difficult to discern the intended meaning of the ANML specification without the presence of the comment.

The crew planning problem is centered around the idea that there is a set of jobs that need to be done by the crew but the allocation of crew to the jobs is left to the planner. The set of jobs is specified using the predicate

```plaintext
predicate payload_act_completed(
    int id,
    string desc,
    int length,
    int priority,
    int dueDate,
    int usesComms,
    int isPhysicallyRestraining);
```

The only parameter that is referenced in the current model is dueDate. So at this point in the development of the model, the other parameters are just stubs. We need to augment the ANMLite language to conveniently handle this aspect of the problem. In particular, we need variables which are declared to be arrays. For example:
VARIABLES

payload_act: ARRAY [1..numacts] OF RECORD
  completed: boolean,
  dueTime: TM_rng
END

= (false,1440; false,1440; false,1440; false,60; false,60)

The first variable records when a payload activity is completed and the second holds the
deadline for a particular activity (note that it is a constant). The payload_activity action
is then defined as follows

pact(id: 1..numacts; desc:StringData;
  length, priority, dueDate, usesComms, isPhysicallyRestraining: myint)
{
  effect: payload_act[id].completed = true;
}

The following constraint is added to the constraints section

  at pact.start: pact(id, ...).end < payload_act[id].dueTime;

and the following goals are added to the goals section:

  FORALL myid: payload_act[myid].completed = true;

The Crew Planning problem raises another issue with its use of a decomposition construct.
This construct represents a hierarchy. There is a high-level action (e.g., daily_routine)
which “contains” a series of low-level actions, e.g., post_sleep, dpc, meal, etc., which have
a partial ordering on them. To accomplish this in NDDL a separate timeline was created with
a single action “perform” which contains all of the required crew actions. Since perform is
a goal action, the FORALL-EXISTS semantics forces all of the actions which it contains to
also occur.

But, if we use the ANMLite version of contains, e.g.,

A contains B

namely

A.start < B.start < B.end < A.end

we have to worry about the possibility of vacuous solutions. In other words, whether this
constraint can be satisfied vacuously with B never executing. The current operational se-
manitics provided by our translator can be summarized as follows: If A terminates, then B will
have to have executed and terminated as well. This is true because the translator initializes
the start/end variables to a virtually infinite value. Therefore the guard on the termination
of A cannot be satisfied unless B has executed once and acceptable values are loaded into
B.start and B.end.

So the semantics of the statement
A.start < B.start < B.end < A.end

can be thought of

\[
\text{FORALL } A: \text{ EXISTS } B: A.\text{start} < B.\text{start} < B.\text{end} < A.\text{end}
\]

So if the last action is required to execute, e.g., because it is in a goal statement, the execution of the other actions in a chain is also required. So we add a boolean variable

\[
\text{RPCM\_done: boolean = false;}
\]

which is initialized to false and add a statement to the final rec_t_loop action:

\[
\text{rec_t_loop(loopCnt: myint): [ 6,6 ] { }
\]

\[
\text{if loopCnt == 2 then RPCM\_done = true; }
\]

and finally add the goal

\[
\text{GOAL}
\]

\[
\text{RPCM\_done;}
\]

Then the following constraints should constrain the appropriate sequence of actions:

\[
\text{Crew.\text{rem\_sleep\_stat}\.end} < \text{Crew.\text{rem\_pow\_src}\.start} < \text{Crew.\text{rem\_pow\_src}\.end} < \text{Crew.\text{replace\_rpcm}\.start} < \text{Crew.\text{replace\_rpcm}\.end} < \text{Crew.\text{place\_power\_source}\.start} \text{Crew.\text{place\_power\_source}\.end} < \text{Crew.\text{ass\_sl\_stat}\.start}
\]

\[
\text{Crew.\text{rec\_t\_loop}\.end} < \text{Crew.\text{replace\_rpcm}\.start}
\]

\[
\text{Crew.\text{replace\_rpcm}\.end} < \text{Crew.\text{rec\_t\_loop}(2)\.start}
\]

7 Conclusion

This paper discusses several design issues of a simple language for specifying planning problems. We call that language ANMLite and it is aimed to be compact, expressive, and suitable for formal analysis. We illustrate with several examples that these objectives are not necessarily compatible and that trade-offs between expressiveness, simplicity, and clarity are often necessary. ANMLite is by no means a replacement for more expressive planning languages such as PDDL [7], NDDL, or ANML. However, the semantic issues that arise in this simple language strongly suggest that subtle semantic issues are probably present in these more complex languages as well. We would argue that a clear semantics for the planning languages is essential if planning systems are to be trusted for safety-critical applications.
We are not completely satisfied that we have arrived at the best choice for the definition of the at reference point or whether it would be better to define repetitive actions using a prev concept instead of a next concept. We are not sure whether we have selected the best defaults. Every option that we have explored so far results in some non-intuitive cases or ugliness. We also are concerned about language constructs which allow vacuous solutions. Because we were attempting to emulate the behavior of EUROPA 2, we have allowed these. But we would like to explore whether the elimination of some or all of the vacuous solutions will improve the clarity of the ANMLite specification language. We have sought to elaborate on these issues in this paper. This work suggests that the semantics of a planning language, even a simple one such as ANMLite, is not a simple effort. We strongly believe that a formal semantics is a prerequisite for the use of these languages in critical aerospace applications. The work presented in this paper is a first step in that direction.

Our efforts at using a model checker to solve planning problems have convinced us that this is not an efficient approach that scales well. But, building the translator has forced us to sharpen our thinking about the meaning of the language constructs. An alternative solution approach that we would like to pursue is to apply a constraint satisfaction solver such as Yices [8]. We believe that the translation of the ANMLite constraints into formulas that can be processed by a constraint solver would be fairly straightforward for the non-repetitive cases. However, the repetitive cases result in an indeterminate number of instances of an action. Constraint solvers need a fixed set. This problem can be addressed in a manner analogous to bounded model checking. First, the satisfaction solver is given formulas that involve only one instance of an action. If the solver fails to find a solution, then second instances of repetitive actions can be introduced, and then three, and so on. This can be continued until a solution is found or a pre-specified quitting point is reached. A nice consequence of this approach is that a plan with minimal repetitions of an action will be discovered.

References


A  The ANMLite Syntax

A.1  Timeline declarations

\[ \text{anml_def} ::= \text{PLAN} \ <\text{identifier}> \]
\[ \ <\text{type_decl}> | \ <\text{timeline_decl}> | \ <\text{constraints_decl}> | \]
\[ \ <\text{vars_decl}> \] *
\[ \ [ \ <\text{inits_decl}> ] \]
\[ \ [ \ <\text{goals_decl}> ] \]
\[ \text{END} \ <\text{identifier}> \]

\[ \text{type_decl} ::= \text{TYPE} \ ( \ <\text{simple_type_decl}> | \ <\text{compound_type_decl}> ) \]

\[ \text{simple_type_decl} ::= \ <\text{identifier}> = \ <\text{type}> \]

\[ \text{compound_type_decl} ::= \ <\text{identifier}> \ <\text{parameters}> [ = \ <\text{type}> ] \]

\[ \text{type} ::= \ <\text{basic_type}> | \ <\text{enumeration}> | \ <\text{interval}> | \ <\text{defined_type}> \]

\[ \text{basic_type} ::= \text{INT} | \text{FLOAT} | \text{BOOL} | \text{STRING} | \]

\[ \text{enumeration} ::= [ \ <\text{identifiers}> ] \]

\[ \text{identifiers} ::= \ <\text{identifier}> \ ( , \ <\text{identifier}> )* \]

\[ \text{identifier} ::= \ <\text{ID}> \]

\[ \text{interval} ::= [ \ <\text{add_expression_or_nil}> , \ <\text{add_expression_or_nil}> ] \]

\[ \text{add_expression_or_nil} ::= \ <\text{additive_expression}> | \ <\text{nil}> \]

\[ \text{defined_type} ::= \ <\text{identifier}> \ <\text{arguments}> \]

\[ \text{arguments} ::= [ \ <\text{strict_arguments}> ] \]

\[ \text{strict_arguments} ::= "(" \ <\text{expression_or_nil}> \ ( , \ <\text{expression_or_nil}> )* ")" \]

\[ \text{expression_or_nil} ::= \ <\text{expression}> | \ <\text{nil}> \]

\[ \text{nil} ::= \ "_" \]

\[ \text{parameters} ::= [ \ <\text{strict_parameters}> ] \]
A.2 Constraints

The proposed BNF for the constraints syntax includes (in)equations involving start/end of actions timepoints, over constraints, and quantifiers (a long awaited new feature!).

```plaintext
<constraints_decl> ::= CONSTRAINTS ( <constraint_decl> )+
```
A.3 Condition and Effect Statements

<action_body> ::= "{" [ condition() ] [ effect() ] "}"

<condition> ::= "condition:" <expression>
<effect> ::= "effect:" <identifier> ":=" <expression>
The Dock-Worker Robots Problem in ANMLite

The book “Automated Planning” by Ghallab, Nau and Traverso presents a planning problem that is used throughout the book. The Dock-Worker Robots problem is centered around a set of robots, cranes, and piles. Robots move containers from one location to another, while cranes move containers between piles and robots. The initial state is defined by allocating containers to piles. The final state is another distribution of containers on the piles. In the general case, there can be multiple piles at a location. Here we assume only one pile per location. The following is an ANMLite version of this problem:

```plaintext
PLAN dwr

TYPE location = [1,3]

TYPE robot_ix = [1..2]

TYPE container = {c1,c2,c3,c4,c5,c6,null}

TYPE pile_ix = [1,3]

VARIABLES

pile: ARRAY [pile_ix, 1..6] OF container = (4*6*null);
top: ARRAY[pile_ix] OF [0..6] = (4*0);

push(p,c) {
    top[p] = top[p] + 1;
    pile[p,top] = c;
}

pop(p): container {
    popv: container;
    if top[p] = 0 then popv = null;
    else
        popv = pile[p,top];
        top[p] = top[p] - 1;
    endif
    return popv;
}

TIMELINE Nav ACTIONS
```

46
At(x: location)

Move(x,y: location) WITH
  y = x + 1 || y = x - 1
  **%** can only move to adjacent position in 1 step

TRANSITIONS

At(x) -> Move(x,y) -> At(y)

END Nav

TIMELINE Robot ACTIONS

Unloaded

Loading(c: container)

Loaded(c: container)

Unloading(c: container)

TRANSITIONS

Unloaded -> Loading(c) -> Loaded(c) -> Unloading(c) -> Unloaded

END Robot

TIMELINE Crane ACTIONS

// need to reference the pile associated with me, e.g. Cr[2] or Cr[3]
// need a way of referencing "my_location" or "my_pile"
// or we can define a local stack variable here
//
// pile: ARRAY [1..6] OF container = (6*null);
// top: [0..6] = 0;
//
// rather than as a two-dimensional global variable.
// If I do it here, it is looking more like an object.

Empty
Take(c:container) {
    condition: top(my_pile) > 0
    effect: c = pop(my_pile);
}

Put(c:container) {
    condition: top(my_pile) <= 6;
    effect: push(my_pile,c);
}

Load_robot(c:container; r: robot_ix)

Unload_robot(c:container; r: robot_ix)

Holding(c: container)

TRANSITIONS

Empty -> (Take(c) | Unload_robot(c,r)) -> Holding(c)

Holding(c) ->( Put(c) | Load_robot(c,r) ) -> Empty

END Crane

VARIABLES

Nv: ARRAY robot_ix OF Nav
Rb: ARRAY robot_ix OF Robot
Cr: ARRAY location OF Crane

CONSTRAINTS

Cr[xx].Load_robot(c,rr) <contained_by> Nv(rr).At(xx)
Cr[xx].Load_robot(c,rr) <meets> Rb[rr].Loaded(c)
Cr[xx].Unload_robot(c,rr) <contained_by> Nv(rr).At(xx)
Cr[xx].Unload_robot(c) <ends> Robot.Loaded(c)

INITIAL-STATE

|-> Nv[1].At(1)
|-> Nv[2].At(2)
|= Rb.Unloaded
|= "some distribution of containers on the piles"

GOAL

"another distribution of containers on the piles"

END dwr
We present the basic concepts of the ANMLite planning language. We discuss various aspects of specifying a plan in terms of constraints and checking the existence of a solution with the help of a model checker. The constructs of the ANMLite language have been kept as simple as possible in order to reduce complexity and simplify the verification problem. We illustrate the language with a specification of the space shuttle crew activity model that was constructed under the Spacecraft Autonomy for Vehicles and Habitats (SAVH) project. The main purpose of this study was to explore the implications of choosing a robust logic behind the specification of constraints, rather than simply proposing a new planning language.