
http://dx.doi.org/10.1145/1572272.1572279

Available from Middlesex University's Research Repository at http://eprints.mdx.ac.uk/5270/

Copyright:

Middlesex University Research Repository makes the University's research available electronically.

Copyright and moral rights to this thesis/research project are retained by the author and/or other copyright owners. The work is supplied on the understanding that any use for commercial gain is strictly forbidden. A copy may be downloaded for personal, non-commercial, research or study without prior permission and without charge. Any use of the thesis/research project for private study or research must be properly acknowledged with reference to the work’s full bibliographic details.

This thesis/research project may not be reproduced in any format or medium, or extensive quotations taken from it, or its content changed in any way, without first obtaining permission in writing from the copyright holder(s).

If you believe that any material held in the repository infringes copyright law, please contact the Repository Team at Middlesex University via the following email address:

eprints@mdx.ac.uk

The item will be removed from the repository while any claim is being investigated.
A Formal Analysis of Requirements-Based Testing

Charles Pecheur
Université catholique de Louvain
Louvain la Neuve, Belgium
charles.pecheur@uclouvain.be

Franco Raimondi
University College London
London, UK
f.raimondi@cs.ucl.ac.uk

Guillaume Brat
RIACS - NASA Ames
Mountain View (CA), USA
guillaume.p.brat@nasa.gov

ABSTRACT

The aim of requirements-based testing is to generate test cases from a set of requirements for a given system or piece of software. In this paper we propose a formal semantics for the generation of test cases from requirements by revising and extending the results presented in previous works (e.g. [21, 20, 13]). We give a syntactic characterisation of our method, defined inductively over the syntax of LTL formulae, and prove that this characterisation is sound and complete, given some restrictions on the formulae that can be used to encode requirements. We provide various examples to show the applicability of our approach.

Categories and Subject Descriptors

D.2.5 [Software Engineering]: Testing and Debugging;
D.2.4 [Software Engineering]: Software/Program Verification

General Terms

Verification

Keywords

Coverage metrics, Requirements-based testing

1. INTRODUCTION

A number of systems currently deployed present a significant amount of complexity, as in the case of the NASA rovers Spirit and Opportunity [18, 19] exploring the surface of Mars since January 2004. The complexity of these systems make them prone to errors and there is a growing interest in tools and methodologies to perform formal verification of these systems in order to avoid safety issues, economical losses, and mission failures. For instance, in the case of the rovers, a number of conditions are imposed to avoid damage and to minimize the risk of failures; examples of conditions (i.e., requirements) include “all scientific instruments must be appropriately stored when the rover is moving” and “if the rover is at a given rock, then it must send a picture or a chemical analysis of the rock”. These kinds of conditions are called flight rules and affect various stages of system development, from design to deployment.

Typically, a model is available for this kind of applications, in the form of a labelled transition system or some other equivalent formalism (e.g. a Promela model for the model checker SPIN [12], a planning model written in PDDL [10], etc.). The availability of such models makes theoretically possible the direct verification of flight rules in a formal way using model checking and verifying the requirement against the given model. In practice, a number of issues arise:

- the size of the state space may be too large to be analysed exhaustively with a model checker;
- the model of the system could be provided in a language that is not easily encoded in the input language of a model checker (see, for instance, the problem of translating PDDL models into an adequate input for a model checker [15, 14]);
- consider the formula “if the rover is moving, then all instruments are stored”: this formula could be true because the rover never moves, which is something a model checker cannot capture directly. In some cases, we are interested in “stressing” a particular atomic proposition in a formula, and make a formula true because of that particular proposition.

As a consequence, testing comes as a natural choice to enable the verification of domains that cannot be translated into model checking problems for the first two issues mentioned above. Moreover, the third issue can be alleviated by extending the Modified Condition/Decision Coverage (MC/DC) metric: this metric is required by critical avionic software and can be used to stress all the atoms in a formula (see Section 3.1 for further details).

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

1. Define in a formal way what it means for an execution path \( \pi \) to be an adequate test case for a formula \( \varphi \) and an atom \( a \) appearing in the formula. We will use the notation \( \text{FLIP}(\varphi, a) \) to denote the set of execution paths that are adequate tests for \( a \) in \( \varphi \) (the meaning of FLIP will become clear in the following sections).

2. Given a formula \( \varphi \) and an atom \( a \), provide a procedure to derive a new formula \( [\varphi]_a \) (called a trap formula) such that
   \[
   \pi \models [\varphi]_a \iff \pi \in \text{FLIP}(\varphi, a)
   \]
   i.e., the test cases for a formula \( \varphi \) being true in a path \( \pi \) because of atom \( a \) are all (and only) the paths \( \pi \) that satisfy the trap formula \([\varphi]_a\).

Recent works in this direction include [21, 20, 13]: a discussion and comparison is presented in Section 3.2.

The rest of the paper is organised as follows: we introduce our definitions. We provide examples of our metric in Section 3.1, together with a discussion on how results should be interpreted. We conclude in Section 5.

2. PRELIMINARIES AND NOTATION

We assume some familiarity with temporal logic and with LTL in particular. We refer to [6] for more details.

Consider a LTL formula \( \varphi \), interpreted over (finite or infinite) paths \( \pi \), built from a set of states \( S \). By a slight abuse of notation, we equate logic formulae to their semantic validity set and consider that

\[
\varphi(\pi) \equiv \pi \models \varphi \equiv \pi \in \varphi
\]

Given a finite path \( \pi = s_1 \rightarrow s_2 \rightarrow \ldots \rightarrow s_n \in S^* \) and \( 1 \leq i \leq j \leq |\pi| \), we define

\[
\pi(i) = s_i
\]
\[
\pi(i : j) = s_i \rightarrow \ldots \rightarrow s_j
\]
\[
\pi(i:) = s_i \rightarrow \ldots
\]

By extension, for infinite paths \( \pi = s_1 \rightarrow s_2 \rightarrow \ldots \) in \( S^\omega \), \( |\pi| = \omega \) and these notations still apply, with \( \pi(i:) = s_i \rightarrow \ldots \).

2.1 Projections and Variants

Let \( AC(\varphi) \) be the set of atomic conditions in a formula \( \varphi \), and \( a \in AC(\varphi) \) one such condition. We write \( s(a) \) for the truth value of condition \( a \) in state \( s \), and \( \pi(a) \) for the sequence of truth values of \( a \) along states of a path \( \pi \). More generally, given a set of atomic conditions \( X \) we denote by \( s(X) \) the (vector of) values of conditions in \( X \) in state \( s \) and by \( \pi(X) \) the sequence of such values along \( \pi \) (also called the projection of \( \pi \) over \( X \)).

Definition 1. Given \( X \subseteq AC(\varphi) \), a path \( \pi' \) is an \( X \)-variant of a path of \( \pi \), denoted \( \pi \triangleleft X \pi' \), iff

\[
\pi(AC(\varphi) - X) = \pi'(AC(\varphi) - X)
\]

In what follows, we will only consider variants with respect to a single condition \( a \), which we will denote \( \triangleleft a \pi' \).

Obviously, \( \triangleleft a \) is an equivalence relation over paths, so each path \( \pi \) induces an equivalence class \([\pi]_a = \{ \pi' \mid \pi' \triangleleft a \pi \}\). By construction, if \( \pi \triangleleft a \pi' \), then \( |\pi| = |\pi'| \) and for any \( i, j \) we have that \( \pi(i : j) \triangleleft a \pi'(i : j) \).

2.2 Linearity

This section discusses the distinction between atomic conditions \( a_1, \ldots, a_n \) occurring in a (propositional or temporal) formula \( \varphi(a_1, \ldots, a_n) \) and the possibly multiple occurrences of the same condition, and the impact on the functional dependency between the value of those conditions and the value of the formula. This will be used to consider coverage of test cases with respect to single occurrences (or possibly multiple covariant occurrences, see below) of a given condition.

Definition 2. A formula \( \varphi \) is linear in a condition \( a \) if \( a \) occurs only once in \( \varphi \). It is constant in \( a \) if \( a \) does not occur in \( \varphi \).

For instance, \( F(a \land b) \land F(\neg a \land c) \) is linear in \( b \) and \( c \) but it is not linear in \( a \).

Let \( count(a, \varphi) \) be the number of occurrences of \( a \) in \( \varphi \). \( \varphi \) is linear or constant in \( a \) iff \( count(a, \varphi) \) is 1 or 0. The linearization of \( \varphi \), denoted \( \text{lin}(\varphi) \), is obtained by replacing every occurrence of any condition \( a \) in \( \varphi \) by a distinct variant \( a' \), where \( 1 \leq i \leq \text{count}(a, \varphi) \). By construction, \( \text{lin}(\varphi) \) is linear in all its conditions. We define \( \text{unlin}(\text{lin}(\varphi)) = \varphi \); in particular \( \text{unlin}(a') = a \).

In what follows, we will restrict the analysis to formulae that are linear in their conditions, or equivalently, consider multiple occurrences of the same condition in a formula as distinct conditions.

2.3 Monotonicity

We define an ordering relation on paths, based on the value of a condition \( a \). Given two paths \( \pi, \pi' \) such that \( |\pi| = |\pi'| \),

\[
\pi \subseteq_a \pi' \iff \pi \subseteq \pi' \land \forall i \leq |\pi| : \pi(i)(a) \Rightarrow \pi'(i)(a)
\]

where \( \pi(i)(a) \) denotes the value of \( a \) in the \( i \)-th state of \( \pi \). Intuitively, this means that \( a \) is true “more often” over \( \pi' \) than over \( \pi \), all other conditions remaining the same.

It is easily seen that \( \subseteq_a \) is a Boolean lattice over each equivalence class \([\pi]_a \), with Boolean operations \( \land_a, \lor_a, \neg_a \) defined point-wise, e.g. \( \pi' \land_a \pi'' \) is a new path \( \pi \) where \( \pi(i)(a) = \pi'(i)(a) \land \pi''(i)(a) \). Top and bottom elements of this lattice are \( [a := T] \) and \( [a := F] \), where \( [a := v] \) means the \( a \)-variant of \( \pi \) where \( \pi(i)(a) = v \) for all indices \( i \).

Definition 3. Given a condition \( a \), a temporal formula \( \varphi \) is covariant (resp. contravariant) in \( a \) iff for all \( \pi \), \( \pi' \subseteq_a \pi' \) (resp. \( \pi' \subseteq_a \pi \)) we have that if \( \pi \models \varphi \) then \( \pi' \models \varphi \). \( \varphi \) is monotonic in \( a \) iff it is either covariant or contravariant in \( a \).

All usual logic operators preserve monotonicity, in the following sense:

\footnote{The notation \([\varphi]_a \) over paths is not to be confused with forthcoming notation \([\varphi]_a \) for trap formulae.}
Definition 4. Given a condition \( a \), a temporal logic operator \( \theta \) is covariant (resp. contravariant) in \( a \) iff for any \( \varphi \) that is covariant in \( a \), \( \theta(\varphi) \) is covariant (resp. contravariant) in \( a \), and vice-versa, for \( \varphi \) contravariant in \( a \). \( \theta \) is monotonic in \( a \) iff it is either covariant or contravariant in \( a \).

A composition \( \theta' \circ \theta \) is monotonic if \( \theta \) and \( \theta' \) are both monotonic, where the usual sign rules apply for variance. As base cases, \( a \) and \( \neg a \) are obviously covariant and contravariant in \( a \). If \( a \) does not occur in \( \varphi', \) then \( \bullet \land \varphi' \) and \( \bullet \lor \varphi' \) are covariant and \( \neg \) is contravariant in \( a \). Note however that \( \odot \) and \( \equiv \) are not monotonic. All LTL operators \((X, U, R, F, G)\) are covariant in \( a \) with respect to each of their arguments, if the other argument is constant in \( a \). This is because (i) these operators are covariant in their arguments in the logical sense (if \( \varphi \Rightarrow \varphi' \) then \( \theta(\varphi) \Rightarrow \theta(\varphi') \)) and (ii) if \( \pi \models \varphi_a \lor \varphi' \) (or any other temporal operator) depends only on \( \pi(i : j) \models \varphi_a \) and \( \pi(j : j) \models \varphi' \) on suffixes of \( \pi \), and \( \pi \models_a \varphi' \) implies \( \pi(i : j) \models_a \varphi'(i : j) \). As a result, if a formula \( \varphi \) (built from these operators) is linear in \( a \) then it is monotonic in \( a \).

3. COVERAGE OF REQUIREMENTS

In this section we present our approach to automatically generate test cases from a requirement expressed in LTL. We begin by briefly reviewing MC/DC coverage (Section 3.1) and previous approaches (Section 3.2), and we introduce our approach in Section 3.3.

3.1 Overview of MC/DC coverage

MC/DC coverage is required for the most critical categories of avionic software [17] and it is defined in terms of the approach in Section 3.3. We begin by briefly reviewing MC/DC coverage (Section 3.1) and it is defined in terms of the approach in Section 3.3.

We begin by briefly reviewing MC/DC coverage (Section 3.1) and it is defined in terms of the approach in Section 3.3.

1. Every basic condition in any decision has taken on all possible outcomes at least once.

2. Each basic condition has been shown to independently affect the decision’s outcome.

As an example, the program fragment if \( (a \lor b) \{ \ldots \} \) contains the decision \( c \equiv (a \lor b) \) with conditions \( a \) and \( b \). MC/DC is achieved if this decision is exercised with the following three valuations:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>( a \lor b )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Indeed, evaluations 1 and 3 only differ in \( a \), showing cases where \( a \) independently affects the outcome of \( c \), respectively in a positive and negative way. The same argument applies to evaluations 2 and 3 for \( b \). In particular, if \( a = T \), then \( a \) affect \( \varphi \) positively, and if \( a = \bot \), then \( a \) affect \( \varphi \) negatively.

3.2 Related work

Coverage metrics for temporal logic have been presented in the past. In [13], a metric is provided to measure the degree of coverage of a model. This is fundamentally different from what we do in this paper, as our aim is to cover requirements expressed in LTL.

A metric for specifications is provided in [20] using mutations: intuitively, a “good” test case is a path that can “detect” all mutations of a formula. The authors also define the notion of vacuous sub-formula, which present an interesting similarity with our notion of \( \alpha \)-variants presented above. In this approach tests are generated using a model checker, and thus differ from our work in that we provide a constructive method starting from formulae directly.

The work presented in [21] shares most of our aims. The notion of unique first cause is defined in [21] as “a condition \( a \) is the unique first cause (UFC) for \( \varphi \) along a path if in the first state along a path in which \( \varphi \) is satisfied, it is satisfied because of \( a \).” This definition is a generalization of the notion of MC/DC presented above.

A syntactic characterization of UFC is proposed in [21]: for a formula \( \varphi \) and condition \( a \) in \( \varphi \), a trap formula ufc(\( \varphi, a \)) can be derived such that ufc(\( \varphi, a \)) holds in all suitable execution paths in which \( a \) is the first cause for \( \varphi \). We report here only a few derivation rules that will be used below and refer to [21] for further details (\( \varphi_a \) denotes a formula in which \( a \) occurs):

\[
\begin{align*}
\text{ufc}(\varphi, a) &= F & \text{where } a \text{ does not occur in } \varphi \\
\text{ufc}(a, a) &= a \\
\text{ufc}(\varphi_a \lor \psi) &= \text{ufc}(\varphi_a, a) \land \neg \psi \\
\text{ufc}(F \varphi_a, a) &= \neg \varphi_a U \text{ufc}(\varphi_a, a)
\end{align*}
\]

These definitions are further refined in a number of ways in [21] to deal with finite/truncated execution paths, but no formal proof is provided that the definition of ufc(\( \varphi, a \)) corresponds indeed to the fact that “\( \varphi \) is true because of \( a \)” and, moreover, the causality link in the definition is not formally defined and may be subject to ambiguous interpretations.

As a running example, consider the formula \( \varphi = F (a \lor b) \). The derivation rules presented above give

\[
\text{ufc}(\varphi_a, a) = (-a \land F) U (a \land \neg b)
\]

The trace \( \pi = \{1\} \rightarrow \{a\} \rightarrow \{b\} \) does satisfy ufc(\( \varphi, a \)). However, this trace does not guarantee that \( a \) is the unique cause for \( a \). Indeed, it is not possible to flip the value of \( a \) in any way to make \( F (a \lor b) \) false along this trace (cf. the criteria
appearing in MC/DC). In essence, using the definition of $\alpha$-variant defined above, there is no $\alpha$-variant of $\pi$ such that $\nu$ does not hold along this variant.

Other examples can be found for the remaining operators: the essence is that $\text{ufc}(\nu, \alpha)$ is satisfied along all valid test cases, but it is also satisfied on execution paths that are not adequate test cases, i.e., $\text{ufc}(\nu, \alpha)$ is “too generous”. Equivalently, as it will be described below, $\text{ufc}(\nu, \alpha)$ is not sound with respect to the definition of adequate test cases.

### 3.3 FLIP

In this section we introduce our definition of “adequate” test cases and we present a syntactic derivation of trap formulae for adequate test cases. We also prove the soundness and correctness of our approach.

**Definition 5.** An execution path $\pi$ is an adequate test case for an atom $\alpha$ occurring in a formula $\nu$ if $\pi \models \nu$ and there exists an $\alpha$-variant $\nu'$ of $\pi$ such that $\nu' \not\models \nu$. We denote with $\text{FLIP}(\nu, \alpha)$ the set of all such paths.

We denote with $[\nu]_{\alpha}$ the trap formula characterising adequate test cases (i.e., test cases as defined in Definition 5). We define $[\nu]_{\alpha}$ by structural induction on LTL formulae in negation normal form as follows:

**Definition 6.** Syntactic characterisation of trap formulae

\[

[\nu']_{\alpha} = F \quad \text{where } \alpha \text{ does not occur in } \nu' \\
[a]_{\alpha} = a \\
[-a]_{\alpha} = \neg a \\
[\nu \land \nu']_{\alpha} = [\nu]_{\alpha} \land [\nu']_{\alpha} \\
[\nu \lor \nu']_{\alpha} = [\nu]_{\alpha} \lor [\nu']_{\alpha} \\
[X \nu]_{\alpha} = X [\nu]_{\alpha} \\
[\nu' \ U \nu]_{\alpha} = (\nu' \ U \nu) \land (\neg \nu' \ R (\nu \Rightarrow [\nu]_{\alpha})) \\
[\nu' \ U \nu']_{\alpha} = (\nu' \ U \nu') \land (\neg \nu' \ U ([\nu]_{\alpha} \land \neg \nu')) \\
[\nu' \ R \nu']_{\alpha} = (\nu' \ R \nu') \land (\nu \Rightarrow [\nu]_{\alpha}) \\
[\nu' \ R \nu]_{\alpha} = (\nu' \ R \nu) \land (\neg \nu' \ U [\nu]_{\alpha}) \\

\]

(where $R$ is the standard release operator).

Other cases are obtained by syntactic derivation:

\[

[F \nu]_{\alpha} = F \nu \land G (\nu \Rightarrow [\nu]_{\alpha}) \\
[G \nu]_{\alpha} = G \nu \land F [\nu]_{\alpha} \\
[\nu' \ W \nu]_{\alpha} = (\nu' \ W \nu) \land ((\nu \Rightarrow [\nu]_{\alpha}) \lor (\neg \nu \ U (\neg \nu' \ U [\nu]_{\alpha}))) \\
[\nu' \ W \nu']_{\alpha} = (\nu' \ W \nu') \land (\neg \nu' \ U (\neg \nu' \ U [\nu]_{\alpha})) \\

\]

These derivations for fixed point modalities are all of the form $[\nu]_{\alpha} = \nu \land \nu'$, where the recursive step occurs only in $\nu'$. They can be rewritten into equivalent forms $[\nu]_{\alpha} = \nu \lor (\nu' \ U [\nu]_{\alpha} \land \nu)$:

\[

[\nu' \ U \nu]_{\alpha} = (\nu' \land \nu) U (\nu \land (\neg \nu' \ R (\nu \Rightarrow [\nu]_{\alpha}))) \\
[\nu' \ U \nu']_{\alpha} = (\nu' \land \neg \nu') U (\nu \land (\neg \nu \ U (\neg \nu' \ U [\nu]_{\alpha}))) \\
[\nu' \ R \nu']_{\alpha} = (\nu \land \neg \nu' \ U (\nu' \ U [\nu]_{\alpha} \land \nu' \land (\nu \Rightarrow [\nu]_{\alpha} U \neg \nu'))) \\
[\nu' \ R \nu]_{\alpha} = (\nu' \land \neg \nu' \ U (\nu' \ U [\nu]_{\alpha} \land (\neg \nu' \ R \nu))) \\
[F \nu]_{\alpha} = \neg \nu \lor (\nu \land G \nu \Rightarrow [\nu]_{\alpha}) \\
[G \nu]_{\alpha} = \nu \lor (\nu \land G \nu) \\

\]

**Proof of correctness.** We now show that $\pi \models [\nu]_{\alpha}$ if and only if $\pi \in \text{FLIP}(\nu, \alpha)$. We prove completeness (only if) and soundness (if) separately.

We first need the following simple lemma:

**Theorem 1 (Extremal $\alpha$-variants).** If $\nu$ is covariant (resp. contravariant) in $\alpha$ and $\pi \models [\nu]_{\alpha}$ then $\pi|\alpha := F \not\models \nu$ (resp. $\pi|\alpha := T \not\models \nu$).

Proof. We prove the covariant case; the contravariant case follows by duality. Since $\pi \in [\nu]_{\alpha}$, there is a $\pi' \not\models \nu'$ such that $\pi' \not\models \nu$. By contrapositive of covariance, if $\pi'' \subseteq \pi'$ and $\pi' \not\models \nu$ then $\pi'' \not\models \nu$. But $\pi|\alpha := F$ is minimal in $[\pi]_{\alpha}$, therefore $\pi|\alpha := F \subseteq \pi'$ and $\pi|\alpha := F \not\models \nu$. □

**Theorem 2 (Soundness of $[\nu]_{\alpha}$).** Let $\nu$ be a formula in negation-normal form, linear and monotonic in $\alpha$. If $\pi \models [\nu]_{\alpha}$, then $\pi \models \nu$ and there exists $\pi' \subseteq \pi$ such that $\pi' \not\models \nu$ (i.e., $\pi \in \text{FLIP}(\nu, \alpha)$).

Proof. Let $\pi \models [\nu]_{\alpha}$. We have to show that $\pi \models \nu$ and build $\pi'$ such that $\pi' \subseteq \pi$ and $\pi' \not\models \nu$. By induction, we can assume that for any sub-formula $\nu_1$ of $\nu$, if $\pi_1 \models [\nu_1]_{\alpha}$, then $\pi_1 \models \nu_1$ and there is $\pi_1' \subseteq \pi_1$ such that $\pi_1' \not\models \nu_1$.

The proof goes by structural induction on $\nu$, where $\nu_2$ is the sub-formula where we consider. We consider the case where $\nu_2$ is covariant in $\alpha$; the contravariant case follows by duality.

- $[\nu]_{\alpha} = F$, where $\alpha$ does not occur in $\nu$:
  
  Trivially, there is no such $\pi$.

- $[a]_{\alpha} = a$:
  
  Obviously, $\pi \models \nu$, which means $\pi(1)(a) = T$ and $\pi' = \pi[a := F] \not\models \nu$.

- $[-a]_{\alpha} = -a$:
  
  Dual of the previous case: $\pi(1)(a) = F$ and $\pi' = \pi[a := T] \not\models \nu$.

- $[\nu \land \nu']_{\alpha} = [\nu]_{\alpha} \land [\nu']_{\alpha}$:
  
  Since $\pi \models [\nu]_{\alpha}$, $\pi \models \nu_2$ and there is $\pi' \subseteq \pi$ such that $\pi' \not\models \nu_2$ (and $\alpha$ does not occur in $\nu'$). Hence $\pi \models \nu \land \nu'$ and $\pi' \not\models \nu \land \nu'$.

- $[\nu \lor \nu']_{\alpha} = [\nu]_{\alpha} \lor [\nu']_{\alpha}$:
  
  Similar to $\nu \land \nu'$, but in this case $\pi \not\models \nu'$ so $\pi' \not\models \nu'$.

- $[X \nu]_{\alpha} = X [\nu]_{\alpha}$:
  
  We have $\pi(2 \cdot) \models [\nu]_{\alpha}$ so (i) $\pi(2) \models \nu_2$ and thus $\pi \models \nu$ and (ii) there is $\pi_1' \subseteq \pi(2)$ such that $\pi_1' \not\models \nu_2$. Build $\pi'(1) = \pi(1)$ and $\pi'(2) = \pi_2'$, thus $\pi' \not\models \nu$.

- $[\nu' \ U \nu]_{\alpha} = (\nu' \ U \nu) \land (\neg \nu' \ R (\nu \Rightarrow [\nu]_{\alpha}))$:
  
  Obviously $\pi \models \nu$. Let $n$ be the first index such that $\pi(n) \models \nu$. Consider all $j \leq n$ such that $\pi(j) \not\models \nu$. Because $\pi \models (\neg \nu' \ R (\nu \Rightarrow [\nu]_{\alpha}))$, we have $\pi(j) = [\nu]_{\alpha}$. Let $\pi' = \pi[a := F]$. By monotonicity of $\nu_2$ (theorem 1), $\pi'(j \cdot) \not\models \nu_2$ for all $j \leq n$. Therefore there is no $j \leq n$ such that $\pi'(j \cdot) \models \nu_2$, so $\pi' \not\models \nu$.\[\square\]
Figure 1: Execution paths for \( \varphi' \lor \varphi_a \).

- \([\varphi_a \land \varphi']_a = (\varphi' \lor (\varphi' \land \varphi_a)) \land ((\varphi_a \Rightarrow [\varphi_a]_a) \lor \neg \varphi')\):
  Obviously \( \pi \models \varphi \). Since \( \pi \models ((\varphi_a \Rightarrow [\varphi_a]_a) \lor \neg \varphi') \), there is a minimal finite \( n \) such that \( \pi(n) = \neg \varphi' \). The proof follows similarly as for \( \varphi' \lor \varphi_a \), with the difference that the finite \( n \) guarantees that \( \varphi_a \land \varphi' \) is indeed eventually falsified along \( \pi[a := F] \).

- \([\varphi_a \land \varphi']_a = (\varphi_a \land \varphi') \land (\neg \varphi' \lor ([\varphi_a]_a \land \neg \varphi'))\):
  Obviously \( \pi \models \varphi \). Let \( n \) be the first index such that \( \pi(n) = \varphi' \). If \( \pi \models \varphi_a \land \neg \varphi' \lor \varphi_a \land \neg \varphi' \), then there is \( k < n \) such that \( \pi(k) = \varphi_a \). Let \( \pi = \pi[a := F] \). By monotonicity of \( \varphi_a \), we have \( \varphi'(k) \not\models \varphi_a \) hence \( \pi \not\models \varphi_a \lor \varphi' \).

- \([\varphi_a \land \varphi']_a = (\varphi_a \land \varphi') \land (\neg \varphi' \lor ([\varphi_a]_a \land \neg \varphi'))\):
  The proof is similar to that for \( \varphi_a \land \varphi' \), except that \( n \) may be infinite and \( k \) may be equal to \( n \).

Theorem 3 (Completeness of \([\varphi_a]_a \). Let \( \varphi \) be a formula in negation-normal form, linear and monotonic in \( a \).

If \( \pi \models \varphi \) and there exists \( \pi' \models \pi \) such that \( \pi \not\models \varphi \) (i.e., if \( \pi \in \text{FLIP}(\varphi, a) \)), then \( \pi \models [\varphi_a]_a \).

Proof. Let \( \pi \models [\varphi_a]_a \). By induction, we can assume that for any sub-formula \( \varphi_1 \) of \( \varphi \), if there is \( \pi_1 \models \varphi_1 \) such that \( \pi_1 \models [\varphi_a]_a \) and \( \pi_1 \not\models \varphi_1 \), then \( \pi_1 \models [\varphi_a]_a \).

- \([\varphi']_a = F \) where \( a \) does not occur in \( \varphi' \):
  If \( a \) does not occur in \( \varphi' \) and \( \pi \models \varphi' \), then for all \( \pi' \models \pi \) we also have \( \pi' \models [\varphi']_a \).

- \([a]_a = a \):
  Obviously, \( \pi \models a \).

- \([\neg a]_a = \neg a \):
  Obviously, \( \pi \models \neg a \).

- \([\varphi_a \land \varphi']_a = [\varphi_a]_a \land \varphi' \):
  We have \( \pi \models \varphi_a \) and \( \pi \models \varphi' \) so \( \pi \models [\varphi_a \land \varphi']_a \). Hence \( \pi \models [\varphi_a]_a \land \varphi' \).

- \([\varphi_a \lor \varphi']_a = [\varphi_a]_a \land \neg \varphi' \):
  Similar to \( \varphi_a \land \varphi' \), except \( \pi \models \varphi' \) so \( \pi \not\models \varphi_1 \).

- \([X \varphi_a]_a = X [\varphi_a]_a \):
  We have \( \pi \not\models X \varphi_a \). In general, \( \neg X \varphi_a = X \neg \varphi_a \lor X T \).
  However, \( \pi \models \varphi_a \), so \( \pi \) and \( \varphi_a \) must have the same length: since \( \pi \models X T \), we also have \( \pi \models X \lor \neg \varphi_a \). Hence \( \pi(2 : ) \models \varphi_a \) and \( \varphi_a \).

Theorems 2 and 3 prove that our syntactic derivation of trap formulae is sound and complete with respect to our definition of adequate test cases (Definition 5). As a simple example, consider once again the formula \( \varphi = F (a \lor b) \) introduced in Section 3.2 to illustrate the issues with the notion of unique first case of [21]. Following our derivation rules, the trap formula for atom \( a \) is given by:

\[ [F (a \lor b)]_a = F (a \lor b) \lor \neg ((a \lor b) \Rightarrow [a \lor b]_a) \]

Given that \( [a \lor b]_a = (a \land \neg b) \) and that \( (a \lor b) \Rightarrow (a \land \neg b) \) is equivalent to \( \neg b \), we have that

\[ [F (a \lor b)]_a = F (a) \lor \neg(b) \]

Intuitively, this formula says that an adequate test case for \( F (a \lor b) \) because of atom \( a \) is a path where eventually \((a \lor b)\) holds, but nowhere \( b \) holds. Indeed, if \( b \) were true anywhere in the path, then it would not be possible to flip the value of the original formula because of \( a \). Notice how
vars C C' C'' : Atom .
vars X Y Z : Formula .
eq [C]C = C .
eq (C)?C = False [otherwise] .
eq (C)\neg C = False [otherwise] .

cq (X \land Y)C = (X)C \land (Y)C .
if C in X .
cq (X \lor Y)C = (X)C \lor (Y)C .
if C in Z .

eq [X U Y]C = X U Y /
\neg (X U (Y -> (Y)C)) .
if C in Y .

eq [X R Y]C = X R Y /
\neg (X R (Y -> (X)C)) .
if C in Z .

eq [X \lor Y]C = [X]C \lor Y .
if C in Y .
eq [X \land Y]C = [X]C \land Y .
if C in Y .
eq [\neg C]C = \neg C .
eq [C']C = False [otherwise] .
vars X Y Z : Formula .

Figure 2: Maude definition of FLIP.

our characterisation does not allow for the problematic path
\pi = \{a\} -> \{a\} -> \{b\} presented in Section 3.2.

We present further examples in the next section to illustrate the applicability of our approach.

4. EXAMPLES

We have implemented the rules of Definition 6 in a Maude module (Maude is an automated reasoning engine based on rewriting logic [7]). The module extends the temporal model checking module available in the standard Maude distribution. Our extension defines a new operation “square brackets”:

op [_]_ : Formula Atom -> Formula

which takes a formula \phi and an atom, and returns a new formula \psi representing the trap formula for the atom in the original formula \phi. An extract from the module definition is reported in Figure 2. The module, together with all the examples reported below, is available from http://www.cs.ucl.ac.uk/staff/f.raimondi/flip/.

As an example, consider the following requirement from [8]:

**REQUIREMENT:** All messages incoming from the POP server should be marked as unread.

**REFINEMENT:** MarkasUnread will occur after PlacedinMailboxes.

This is encoded by the following LTL formula:

\[
G(\text{PlacedinMailboxes} \Rightarrow F(\text{MarkasUnread}))
\]

Suppose we want to derive a test in which the formula is true because of MarkasUnread. The output of Maude is reported in Figure 3 (where PM corresponds to PlacedinMailboxes and MU to MarkasUnread).

The resulting formula inf Figure 3 can be simplified to

\[
F(\neg \text{PlacedinMailboxes} \land G(\neg \text{MarkasUnread})) \land G(\text{PlacedinMailboxes} \Rightarrow F(\text{MarkasUnread}))
\]

Figure 3: Maude screen shot

This formula characterises all the paths in which \neg MarkasUnread occurs at least once: this is guaranteed by the first part of the formula, in which it is required that PlacedinMailboxes must be false at some point in the future, followed by globally \neg MarkasUnread. Thus, this formula rules out the possibility that MarkasUnread is always true: indeed, in this case it would be impossible to flip the value of the original formula because of MarkasUnread.

The Maude module can be used to produce the trap formula for the other atom PlacedinMailboxes as well. Each of these two trap formulae encode a set of execution paths. The coverage of the original requirement is achieved by verifying that the system allows for execution paths that belong into each of these sets. The actual verification of these inclusions is performed in different ways, depending on the kind of model under investigation. In the following section we present an application to a NuSMV model.

4.1 An example with a model and interpretation of the results

Consider the standard NuSMV [5] example of mutual exclusion of two asynchronous processes by means of a semaphore (see the code in Figure 4).

A property of this protocol is the following:

\[
\varphi_{ME} = G((p1c \lor p2c) \Rightarrow F(p1c \lor p2c))
\]

where \text{p1c} is a short-hand for \text{procl.state=entering}, and similarly for the remaining atoms.

This property encodes the fact that if both processes are trying to enter the critical section, at least one of them will eventually enter it, and NuSMV can be used to show that \varphi_{ME} holds. We can use our Maude module to derive the trap formula encoding an adequate test case for \text{p1c} (i.e., for process 1 in the critical state, see Figure 5). The trap formula can be simplified to:

\[
F(F(p1c \lor p2c) \land G(\neg p2c) \land (p1e \lor p2e)) \land G((p1e \lor p2e) \Rightarrow F(p1c \lor p2c))
\]

This formula is satisfied along a path that (1) satisfies the original requirement and (2) has a state where both processes are trying to enter the critical section, and (3) nowhere along the path does the second process enter the critical section (in this way it is possible to flip the truth value of the formula because of the first process entering the critical section).

By taking the negation of the formula above we can use NuSMV to check whether an execution of the system (i.e., the model of Figure 4) exists such that the atom \text{p1c} can flip the value of the formula. Indeed, if such an execution exists,
describe sets of execution paths encoded by a trap formula. The formula \( \phi \) can be rewritten to express the notion of MC/DC to temporal formulas in a formal setting. However, care must be taken when comparing the two metrics. Although a strong similarity can be drawn between MC/DC coverage for decisions in programs and FLIP coverage for requirements in temporal logic, the context of application, and hence the interpretation of the results, are quite different. In MC/DC coverage for a condition \( F \), both

\[ \text{module user(semaphore)} \]
\[ \text{VAR} \]
\[ \text{state} : \{ \text{idle, entering, critical, exiting} \}; \]
\[ \text{ASSIGN} \]
\[ \text{init(state)} := \text{idle}; \]
\[ \text{next(state)} := \]
\[ \text{case} \]
\[ \text{state} = \text{idle} \]
\[ (\text{idle, entering}); \]
\[ \text{state} = \text{entering} \& \! \text{semaphore} \]
\[ \text{critical}; \]
\[ \text{state} = \text{critical} \]
\[ (\text{critical, exiting}); \]
\[ \text{state} = \text{exit} \]
\[ \text{idle}; \]
\[ 1 \]
\[ \text{esac}; \]
\[ \text{next(semaphore)} := \]
\[ \text{case} \]
\[ \text{state} = \text{entering} \]
\[ 1; \]
\[ \text{state} = \text{exit} \]
\[ 0; \]
\[ 1 \]
\[ \text{semaphore}; \]
\[ \text{esac}; \]
\[ \text{module main} \]
\[ \text{VAR} \]
\[ \text{semaphore} : \text{boolean}; \]
\[ \text{proc1} : \text{process user(semaphore)}; \]
\[ \text{proc2} : \text{process user(semaphore)}; \]
\[ \text{ASSIGN} \]
\[ \text{init(semaphore)} := 0; \]
\[ \text{FAIRNESS} \]
\[ \text{running} \]

Figure 4: NuSMV code for mutual exclusion

then the negation of the trap formula should be false, and a counterexample should be produced describing the required path. This is the case with the trap formula reported above; a screen-shot from NuSMV is reported in Figure 6 describing the first state of the required execution path.

Full coverage of \( \varphi_{ME} \) is achieved by computing the remaining three trap formulae (one for each of the Boolean atoms) and by repeating their verification with NuSMV.

Notice that there are four possible outcomes for the verification using a model checker of (the negation of) a trap formula \( [\varphi]_a \) encoding a adequate test cases for an atom \( a \) in a formula \( \varphi \). Consider Figure 7, where \( M \) denotes the set of paths enabled by the original model, and the sets (a) to (d) describe sets of execution paths encoded by a trap formula. The four cases are as follows:

- The formula \( \varphi \) is a desired (“positive”) property, and \( \neg[\varphi]_a \) is true in the model; this is case (a), where the negation of the trap formula is false in the intersection of \( M \) and (a), and it is possible to guarantee that \( \varphi \) has been covered with respect to \( a \) by using one of the paths in this intersection. This is the case for the example formula presented above for the mutual exclusion protocol and NuSMV produces one of the paths as a counter-example.
- The formula \( \varphi \) is a desired (“positive”) property, and \( \neg[\varphi]_a \) is false in the model (and a counterexample is produced by NuSMV): this is case (a), where the negation of the trap formula is false in the intersection of \( M \) and (a), and it is possible to guarantee that \( \varphi \) has been covered with respect to \( a \) by using one of the paths in this intersection. This is the case for the example formula presented above for the mutual exclusion protocol and NuSMV produces one of the paths as a counter-example. Notice that there are four possible outcomes for the verification using a model checker of (the negation of) a trap formula \( [\varphi]_a \) encoding a adequate test cases for an atom \( a \) in a formula \( \varphi \). Consider Figure 7, where \( M \) denotes the set of paths enabled by the original model, and the sets (a) to (d) describe sets of execution paths encoded by a trap formula.

5. DISCUSSION AND CONCLUSION

In this section we have presented an example using a NuSMV model and thus the original requirement could have been verified directly. However, this would have not guaranteed the coverage of all the atoms in the requirement. A similar methodology can be applied to other kinds of models that cannot be verified in full. For instance, in the case of a planning model in PDDL [10], trap formulae generated with Maude can be translated into new planning goals and added to the original model as additional constraints, therefore forcing the generation of plans that satisfy the trap formulae. This kind of application is presented in more details in [2].
matically from flight rules for PDDL domains. Preliminary results are reported in [2] and our aim for the future is to deliver a testing platform that integrates our formal approach with the design and development environments currently in use.

Acknowledgments

We are grateful to Dimitra Giannakopoulou and Corina Păsăreanu for their comments on a previous version of this work and to the anonymous reviewers for their valuable input.

6. REFERENCES


