Generating Counterexamples for Model Checking by Transformation

G.W. Hamilton
School of Computing and Lero
Dublin City University
Ireland
hamilton@computing.dcu.ie

Counterexamples explain why a desired temporal logic property fails to hold. The generation of counterexamples is considered to be one of the primary advantages of model checking as a verification technique. Furthermore, when model checking does succeed in verifying a property, there is typically no independently checkable witness that can be used as evidence for the verified property. Previously, we have shown how program transformation techniques can be used for the verification of both safety and liveness properties of reactive systems. However, no counterexamples or witnesses were generated using the described techniques. In this paper, we address this issue. In particular, we show how the program transformation technique distillation can be used to facilitate the construction of counterexamples and witnesses for temporal properties of reactive systems. Example systems which are intended to model mutual exclusion are analysed using these techniques with respect to both safety (mutual exclusion) and liveness (non-starvation), with counterexamples being generated for those properties which do not hold.

1 Introduction

Model checking is a well established technique originally developed for the verification of temporal properties of finite state systems [3]. In addition to telling the user whether the desired temporal property holds, it can also generate a counterexample, explaining the reason why this property failed. This is considered to be one of the major advantages of model checking when compared to other verification methods. Fold/unfold program transformation techniques have more recently been proposed as an approach to model checking. Many such techniques have been developed for logic programs (e.g. [11, 15, 4, 1, 8]). However, very few such techniques have been developed for functional programs (with the work of Lisitsa and Nemytykh [12, 2] using supercompilation [17] being a notable exception), and these deal only with safety properties. Unfortunately, none of these techniques generate counterexamples when the temporal property does not hold.

In previous work [6], we have shown how a fold/unfold program transformation technique can be used to facilitate the verification of both safety and liveness properties of reactive systems which have been specified using functional programs. These functional programs produce a trace of states as their output, and the temporal property specifies the constraints that all output traces from the program should satisfy. However, counterexamples and witnesses were not generated using this approach. In this paper, we address this shortcoming to show how our previous work can be extended to generate a counterexample trace when a temporal property does not hold, and a witness when it does.

The program transformation technique which we use is our own distillation [5, 7] which builds on top of positive supercompilation [16], but is much more powerful. Distillation is used to transform the programs defining reactive systems into a simplified form which makes them much easier to analyse. We
then show how temporal properties for this simplified form can be verified, and extend this to generate
counterexamples and witnesses. The described techniques are applied to a number of example systems
which are intended to model mutually exclusive access to a critical resource by two processes. When
a specified temporal property does not hold, we show how our approach can be applied to generate a
Corresponding counterexample and when the property does hold we show our approach can be applied
to generate a corresponding witness.

The remainder of this paper is structured as follows. In Section 2, we introduce the functional
language over which our verification techniques are defined. In Section 3, we show how to specify
reactive systems in our language, and give a number of example systems which are intended to model
mutually exclusive access to a critical resource by two processes. In Section 4, we describe how to
specify temporal properties for reactive systems defined in our language, and specify both safety (mutual
exclusion) and liveness (non-starvation) for the example systems. In Section 5, we describe our technique
for verifying temporal properties of reactive systems and apply this technique to the example systems
to verify the previously specified temporal properties. In Section 6, we describe our technique for the
generation of counterexamples and witnesses, and apply this technique to the example systems. Section
7 concludes and considers related work.

2 Language

In this section, we describe the syntax and semantics of the higher-order functional language which will
be used throughout this paper.

2.1 Syntax

The syntax of our language is given in Figure 1.

\[
e ::= x \quad \text{Variable}
\ |
\ c \ e_1 \ldots e_k \quad \text{Constructor Application}
\ |
\ \lambda x. e \quad \lambda \text{-Abstraction}
\ |
\ f \quad \text{Function Call}
\ |
\ e_0 \ e_1 \quad \text{Application}
\ |
\ \text{case } e_0 \ \text{of } p_1 \rightarrow e_1 \ | \cdots \ | p_k \rightarrow e_k \quad \text{Case Expression}
\ |
\ \text{let } x = e_0 \ \text{in } e_1 \quad \text{Let Expression}
\ |
\ e_0 \ \text{where } f_1 = e_1 \ldots f_n = e_n \quad \text{Local Function Definitions}
\]

\[
p ::= c \ x_1 \ldots x_k \quad \text{Pattern}
\]

Figure 1: Language Grammar

A program is an expression which can be a variable, constructor application, \( \lambda \)-abstraction, function
call, application, \textbf{case}, \textbf{let} or \textbf{where}. Variables introduced by \( \lambda \)-abstractions, \textbf{let} expressions and \textbf{case}
patterns are \textit{bound}; all other variables are \textit{free}. An expression which contains no free variables is said to
be \textit{closed}.

Each constructor has a fixed arity; for example \textit{Nil} has arity 0 and \textit{Cons} has arity 2. In an expression
\( c \ e_1 \ldots e_n \), \( n \) must equal the arity of \( c \). The patterns in \textbf{case} expressions may not be nested. No
variable may appear more than once within a pattern and the same constructor cannot appear within
more than one pattern. We assume that the patterns in a case expression are exhaustive; we also allow a wildcard pattern which always matches if none of the earlier patterns match. Types are defined using algebraic data types, and it is assumed that programs are well-typed. Erroneous terms such as case (λx.e) of p₁ → e₁ | ⋯ | pₖ → eₖ and (c e₁...eₙ) e where c is of arity n cannot therefore occur.

2.2 Semantics

The call-by-name operational semantics of our language is standard: we define an evaluation relation ↓ between closed expressions and values, where values are expressions in weak head normal form (i.e. constructor applications or λ-abstractions). We define a one-step reduction relation ~ inductively as shown in Figure 2, where the reduction r can be f (unfolding of function f), c (elimination of constructor c) or β (β-substitution).

\[
\begin{align*}
(λx.e₀)₁ & \xrightarrow{β} (e₀₁)₁ & (\text{let } x = e₀ \text{ in } e₁) & \xrightarrow{β} (e₁₁)₁ \\
\frac{f = e}{f \xrightarrow{r} e} & \quad \frac{e₀ \xrightarrow{r} e₀₁}{(e₀₁)₁ \xrightarrow{r} (e₀₁₁)₁} \\
\frac{p₁ = c x₁...xₙ}{(\text{case } c e₁...eₙ \text{ of } p₁ : e₁₁ | ⋯ | pₖ : eₖ₃) \xrightarrow{r} (e₁₁₁)₁} & \quad \frac{(\text{case } e₀ \text{ of } p₁ : e₁₁ | ⋯ | pₖ : eₖ₃) \xrightarrow{r} (\text{case } e₀₁ \text{ of } p₁ : e₁₁ | ⋯ | pₖ : eₖ₃)}
\end{align*}
\]

Figure 2: One-Step Reduction Relation

We use the notation e ~ if the expression e reduces, e ↑ if e diverges, e ↓ if e converges and e ↓ v if e evaluates to the value v. These are defined as follows, where ~ is denotes the reflexive transitive closure of ~:

\[
\begin{align*}
e & \xrightarrow{r} \text{ iff } \exists e'.e \xrightarrow{r} e' \\
e \downarrow v & \text{ iff } \exists e'.e \xrightarrow{r} e' \\
e \downarrow v & \text{ iff } \exists e'.e \xrightarrow{r} e' \\
e \downarrow v & \text{ iff } \exists e'.e \xrightarrow{r} e' \Rightarrow e' \xrightarrow{r}
\end{align*}
\]

3 Specifying Reactive Systems

In this section, we show how to specify reactive systems in our programming language. While reactive systems are usually specified using labelled transitions systems (LTSs), our specifications can be trivially derived from these. Reactive systems have to react to a series of external events by updating their states. In order to facilitate this, we make use of a list datatype, which is defined as follows for the element type a:

\[
\text{List } a ::= \text{Nil} | \text{Cons } a (\text{List } a)
\]

We use [] as a shorthand for Nil, and [s₁,...,sₙ] as a shorthand for a list containing the elements s₁...sₙ. We also use ++ to represent list concatenation. Our programs will map a (potentially infinite) input list of external events and an initial state to a (potentially infinite) output list of observable states (a trace), which gives the values of a subset of state variables whose properties can be verified.
In this paper, we wish to analyse a number of systems which are intended to implement mutually exclusive access to a critical resource for two processes. In all of these systems, the external events belong to the following datatype:

\[
\text{Event ::= Request}_1 \mid \text{Request}_2 \mid \text{Take}_1 \mid \text{Take}_2 \mid \text{Release}_1 \mid \text{Release}_2
\]

Each of the two processes can therefore request access to the critical resource, and take and release this resource. Observable states in all of our example systems belong to the following datatype:

\[
\text{State ::= ObsState ProcState ProcState}
\]

\[
\text{ProcState ::= T \mid W \mid U}
\]

Each process can therefore be thinking (T), waiting for the critical resource (W) or using the critical resource (U).

Each of our example systems is transformed into a simplified form as previously shown in [6] using distillation [5, 7], a powerful program transformation technique which builds on top of the supercompilation transformation [17, 16]. Due to the nature of the programs modelling reactive systems, in which the input is an external event list, and the output is a list of observable states, the programs resulting from this transformation take the form \( e^\rho \), where \( e^\rho \) is defined as shown in Figure 3 where the let variables are added to the set \( \rho \), and will not be used as case selectors.

\[
e^\rho ::= \text{Cons } e_0^\rho e_1^\rho \\
\quad | \quad f x_1 \ldots x_n \\
\quad | \quad \text{case } x \text{ of } p_1 \rightarrow e_1^\rho | \cdots | p_k \rightarrow e_n^\rho, \text{ where } x \notin \rho \\
\quad | \quad x e_1^\rho \ldots e_n^\rho, \text{ where } x \in \rho \\
\quad | \quad \text{let } x = \lambda x_1 \ldots x_n. e_0^\rho \text{ in } e_1^{(\rho \cup \{x\})} \\
\quad | \quad e_0^\rho \text{ where } f_1 = \lambda x_{i_1} \ldots x_{i_k}. e_1^\rho \ldots f_n = \lambda x_{n_1} \ldots x_{n_k}. e_n^\rho
\]

Figure 3: Simplified Form Resulting From Distillation

The crucial syntactic property of this simplified form is that all functions must be tail recursive; this is what allows the resulting programs to be verified more easily. In all of the following examples, the variable \( es \) represents the external event list.

**Example 1** In the first example shown in Figure 4 each process can request access to the critical resource if it is thinking and the other process is not using it, take the critical resource if it is waiting for it, and release the critical resource if it is using it. The LTS representation of this program is shown in Figure 5 (for ease of presentation of this and subsequent LTSs, transitions back into the same state have been omitted).

**Example 2** In the second example shown in Figure 6 each process can request access to the critical resource if it is thinking and the other process is not using it, take the critical resource if it is waiting for it and the other process is thinking, and release the critical resource if it is using it. The LTS representation of this program is shown in Figure 7.
\( \text{Cons (ObsState } T \ T) (f_1 \ es) \)

where

\( f_1 = \lambda es. \text{case } es \text{ of} \)

\( \text{Cons } e \ es \rightarrow \text{ case } e \text{ of} \)

\( \text{Request}_1 \rightarrow \text{Cons (ObsState } W \ T) (f_2 \ es) \)
\( \text{| Request}_2 \rightarrow \text{Cons (ObsState } T \ W) (f_3 \ es) \)
\( \text{| } \rightarrow \text{Cons (ObsState } T \ T) (f_1 \ es) \)

\( f_2 = \lambda es. \text{case } es \text{ of} \)

\( \text{Cons } e \ es \rightarrow \text{ case } e \text{ of} \)

\( \text{Take}_1 \rightarrow \text{Cons (ObsState } U \ T) (f_4 \ es) \)
\( \text{| Request}_2 \rightarrow \text{Cons (ObsState } W \ W) (f_5 \ es) \)
\( \text{| } \rightarrow \text{Cons (ObsState } W \ T) (f_2 \ es) \)

\( f_3 = \lambda es. \text{case } es \text{ of} \)

\( \text{Cons } e \ es \rightarrow \text{ case } e \text{ of} \)

\( \text{Request}_1 \rightarrow \text{Cons (ObsState } W \ W) (f_5 \ es) \)
\( \text{| Take}_2 \rightarrow \text{Cons (ObsState } T \ U) (f_6 \ es) \)
\( \text{| } \rightarrow \text{Cons (ObsState } T \ W) (f_3 \ es) \)

\( f_4 = \lambda es. \text{case } es \text{ of} \)

\( \text{Cons } e \ es \rightarrow \text{ case } e \text{ of} \)

\( \text{Release}_1 \rightarrow \text{Cons (ObsState } T \ T) (f_1 \ es) \)
\( \text{| } \rightarrow \text{Cons (ObsState } U \ T) (f_4 \ es) \)

\( f_5 = \lambda es. \text{case } es \text{ of} \)

\( \text{Cons } e \ es \rightarrow \text{ case } e \text{ of} \)

\( \text{Take}_1 \rightarrow \text{Cons (ObsState } U \ W) (f_7 \ es) \)
\( \text{| Take}_2 \rightarrow \text{Cons (ObsState } W \ U) (f_8 \ es) \)
\( \text{| } \rightarrow \text{Cons (ObsState } W \ W) (f_5 \ es) \)

\( f_6 = \lambda es. \text{case } es \text{ of} \)

\( \text{Cons } e \ es \rightarrow \text{ case } e \text{ of} \)

\( \text{Release}_2 \rightarrow \text{Cons (ObsState } T \ T) (f_1 \ es) \)
\( \text{| } \rightarrow \text{Cons (ObsState } U \ U) (f_6 \ es) \)

\( f_7 = \lambda es. \text{case } es \text{ of} \)

\( \text{Cons } e \ es \rightarrow \text{ case } e \text{ of} \)

\( \text{Release}_1 \rightarrow \text{Cons (ObsState } T \ W) (f_3 \ es) \)
\( \text{| Take}_2 \rightarrow \text{Cons (ObsState } U \ U) (f_9 \ es) \)
\( \text{| } \rightarrow \text{Cons (ObsState } U \ T) (f_4 \ es) \)

\( f_8 = \lambda es. \text{case } es \text{ of} \)

\( \text{Cons } e \ es \rightarrow \text{ case } e \text{ of} \)

\( \text{Release}_2 \rightarrow \text{Cons (ObsState } W \ T) (f_2 \ es) \)
\( \text{| Take}_1 \rightarrow \text{Cons (ObsState } U \ U) (f_9 \ es) \)
\( \text{| } \rightarrow \text{Cons (ObsState } U \ W) (f_9 \ es) \)

\( f_9 = \lambda es. \text{case } es \text{ of} \)

\( \text{Cons } e \ es \rightarrow \text{ case } e \text{ of} \)

\( \text{Release}_1 \rightarrow \text{Cons (ObsState } U \ U) (f_6 \ es) \)
\( \text{| Release}_2 \rightarrow \text{Cons (ObsState } U \ T) (f_4 \ es) \)
\( \text{| } \rightarrow \text{Cons (ObsState } U \ U) (f_9 \ es) \)

Figure 4: Example 1
Example 3 In the final example shown in Figure 8, each process can request access to the critical resource if it is thinking, take the critical resource if it is waiting for it and requested access before the other process, and release the critical resource if it is using it. Note that this program is the result of transforming an implementation of Lamport’s bakery algorithm [9] for two processes as shown in [6]. Although the original program makes use of numbered tickets and is therefore an infinite state system, the use of tickets is completely transformed away and the resulting program has a finite number of states. The LTS representation of this program is shown in Figure 9.

4 Specification of Temporal Properties

In this section, we describe how temporal properties of reactive systems are specified. We use Linear-time Temporal Logic (LTL), in which the set of well-founded formulae (WFF) are defined inductively as follows. All atomic propositions $p$ are in WFF; if $\varphi$ and $\psi$ are in WFF, then so are:

- $\neg \varphi$
- $\varphi \lor \psi$
- $\varphi \land \psi$
- $\varphi \Rightarrow \psi$
- $\Box \varphi$
- $\Diamond \varphi$
- $\Diamond \Diamond \varphi$

Figure 5: LTS Representation of Example 1
\[ \text{where} \]
\[ f_1 = \lambda e. \text{case } e \text{ of} \]
\[ \quad \text{Cons } e \text{ es } \rightarrow \text{ case } e \text{ of} \]
\[ \qquad \text{Request}_1 \rightarrow \text{Cons } (\text{ObsState } W \ T) (f_2 \ es) \]
\[ \qquad \text{Request}_2 \rightarrow \text{Cons } (\text{ObsState } T \ W) (f_3 \ es) \]
\[ \quad \quad \quad \rightarrow \text{Cons } (\text{ObsState } T \ T) (f_1 \ es) \]
\[ f_2 = \lambda e. \text{case } e \text{ of} \]
\[ \quad \text{Cons } e \text{ es } \rightarrow \text{ case } e \text{ of} \]
\[ \qquad \text{Take}_1 \rightarrow \text{Cons } (\text{ObsState } U \ T) (f_4 \ es) \]
\[ \qquad \text{Request}_2 \rightarrow \text{Cons } (\text{ObsState } W \ W) (f_5 \ es) \]
\[ \quad \quad \quad \rightarrow \text{Cons } (\text{ObsState } W \ T) (f_2 \ es) \]
\[ f_3 = \lambda e. \text{case } e \text{ of} \]
\[ \quad \text{Cons } e \text{ es } \rightarrow \text{ case } e \text{ of} \]
\[ \qquad \text{Request}_1 \rightarrow \text{Cons } (\text{ObsState } W \ W) (f_5 \ es) \]
\[ \qquad \text{Take}_2 \rightarrow \text{Cons } (\text{ObsState } T \ U) (f_6 \ es) \]
\[ \quad \quad \quad \rightarrow \text{Cons } (\text{ObsState } T \ W) (f_3 \ es) \]
\[ f_4 = \lambda e. \text{case } e \text{ of} \]
\[ \quad \text{Cons } e \text{ es } \rightarrow \text{ case } e \text{ of} \]
\[ \qquad \text{Release}_1 \rightarrow \text{Cons } (\text{ObsState } T \ T) (f_1 \ es) \]
\[ \quad \quad \quad \rightarrow \text{Cons } (\text{ObsState } U \ T) (f_4 \ es) \]
\[ f_5 = \lambda e. \text{case } e \text{ of} \]
\[ \quad \text{Cons } e \text{ es } \rightarrow \text{ case } e \text{ of} \]
\[ \quad \quad \quad \rightarrow \text{Cons } (\text{ObsState } W \ W) (f_5 \ es) \]
\[ f_6 = \lambda e. \text{case } e \text{ of} \]
\[ \quad \text{Cons } e \text{ es } \rightarrow \text{ case } e \text{ of} \]
\[ \qquad \text{Release}_2 \rightarrow \text{Cons } (\text{ObsState } T \ T) (f_1 \ es) \]
\[ \quad \quad \quad \rightarrow \text{Cons } (\text{ObsState } T \ U) (f_6 \ es) \]

Figure 6: Example 2

Figure 7: LTS Representation of Example 2
Generating Counterexamples by Transformation

Cons (ObsState T T) (f₁ es)
where

\[ f₁ = \lambda es. \text{case } es \text{ of} \]
\[ \quad \text{Cons } es \rightarrow \text{ case } e \text{ of} \]
\[ \quad \quad \text{Request₁ } \rightarrow \text{ Cons } (\text{ObsState W T}) (f₂ es) \]
\[ \quad \quad \text{Request₂ } \rightarrow \text{ Cons } (\text{ObsState T W}) (f₃ es) \]
\[ \quad \quad \_ \quad \rightarrow \text{ Cons } (\text{ObsState T T}) (f₁ es) \]

\[ f₂ = \lambda es. \text{case } es \text{ of} \]
\[ \quad \text{Cons } es \rightarrow \text{ case } e \text{ of} \]
\[ \quad \quad \text{Take₁ } \rightarrow \text{ Cons } (\text{ObsState U T}) (f₄ es) \]
\[ \quad \quad \text{Request₁ } \rightarrow \text{ Cons } (\text{ObsState W W}) (f₆ es) \]
\[ \quad \quad \_ \quad \rightarrow \text{ Cons } (\text{ObsState W T}) (f₂ es) \]

\[ f₃ = \lambda es. \text{case } es \text{ of} \]
\[ \quad \text{Cons } es \rightarrow \text{ case } e \text{ of} \]
\[ \quad \quad \text{Take₂ } \rightarrow \text{ Cons } (\text{ObsState T U}) (f₅ es) \]
\[ \quad \quad \text{Request₂ } \rightarrow \text{ Cons } (\text{ObsState W W}) (f₇ es) \]
\[ \quad \quad \_ \quad \rightarrow \text{ Cons } (\text{ObsState T W}) (f₃ es) \]

\[ f₄ = \lambda es. \text{case } es \text{ of} \]
\[ \quad \text{Cons } es \rightarrow \text{ case } e \text{ of} \]
\[ \quad \quad \text{Release₁ } \rightarrow \text{ Cons } (\text{ObsState T T}) (f₁ es) \]
\[ \quad \quad \text{Request₂ } \rightarrow \text{ Cons } (\text{ObsState U W}) (f₉ es) \]
\[ \quad \quad \_ \quad \rightarrow \text{ Cons } (\text{ObsState T W}) (f₃ es) \]

\[ f₅ = \lambda es. \text{case } es \text{ of} \]
\[ \quad \text{Cons } es \rightarrow \text{ case } e \text{ of} \]
\[ \quad \quad \text{Release₂ } \rightarrow \text{ Cons } (\text{ObsState T T}) (f₁ es) \]
\[ \quad \quad \text{Request₁ } \rightarrow \text{ Cons } (\text{ObsState W U}) (f₈ es) \]
\[ \quad \quad \_ \quad \rightarrow \text{ Cons } (\text{ObsState W T}) (f₂ es) \]

\[ f₆ = \lambda es. \text{case } es \text{ of} \]
\[ \quad \text{Cons } es \rightarrow \text{ case } e \text{ of} \]
\[ \quad \quad \text{Take₁ } \rightarrow \text{ Cons } (\text{ObsState W W}) (f₈ es) \]
\[ \quad \quad \_ \quad \rightarrow \text{ Cons } (\text{ObsState W W}) (f₆ es) \]

\[ f₇ = \lambda es. \text{case } es \text{ of} \]
\[ \quad \text{Cons } es \rightarrow \text{ case } e \text{ of} \]
\[ \quad \quad \text{Take₂ } \rightarrow \text{ Cons } (\text{ObsState W U}) (f₉ es) \]
\[ \quad \quad \_ \quad \rightarrow \text{ Cons } (\text{ObsState W W}) (f₇ es) \]

\[ f₈ = \lambda es. \text{case } es \text{ of} \]
\[ \quad \text{Cons } es \rightarrow \text{ case } e \text{ of} \]
\[ \quad \quad \text{Release₁ } \rightarrow \text{ Cons } (\text{ObsState T W}) (f₃ es) \]
\[ \quad \quad \_ \quad \rightarrow \text{ Cons } (\text{ObsState U W}) (f₈ es) \]

\[ f₉ = \lambda es. \text{case } es \text{ of} \]
\[ \quad \text{Cons } es \rightarrow \text{ case } e \text{ of} \]
\[ \quad \quad \text{Release₂ } \rightarrow \text{ Cons } (\text{ObsState W T}) (f₂ es) \]
\[ \quad \quad \_ \quad \rightarrow \text{ Cons } (\text{ObsState W U}) (f₉ es) \]

Figure 8: Example 3
The temporal operator $\Box\varphi$ means that $\varphi$ is always true; this is used to express safety properties. The temporal operator $\Diamond\varphi$ means that $\varphi$ will eventually be true; this is used to express liveness properties. The temporal operator $\circ\varphi$ means that $\varphi$ is true in the next state. These modalities can be combined to obtain new modalities; for example, $\Box\Diamond\varphi$ means that $\varphi$ is true infinitely often, and $\Diamond\Box\varphi$ means that $\varphi$ is eventually true forever. Fairness constraints can also be specified for some external events (those belonging to the set $F$) which require that they occur infinitely often. For the examples given in this paper, it is assumed that all external events belong to $F$.

Here, propositional models for linear-time temporal formulas consist of a list of observable states $\pi = [s_0,s_1,\ldots]$. The satisfaction relation is extended to formulas in LTL for a model $\pi$ and position $i$ as follows:

\[
\begin{align*}
\pi,i & \models p \quad \text{iff} \quad p \in s_i \\
\pi,i & \models \neg\varphi \quad \text{iff} \quad \pi,i \not\models \varphi \\
\pi,i & \models \varphi \lor \psi \quad \text{iff} \quad \pi,i \models \varphi \text{ or } \pi,i \models \psi \\
\pi,i & \models \varphi \land \psi \quad \text{iff} \quad \pi,i \models \varphi \text{ and } \pi,i \models \psi \\
\pi,i & \models \varphi \Rightarrow \psi \quad \text{iff} \quad \pi,i \not\models \varphi \text{ or } \pi,i \models \psi \\
\pi,i & \models \Box\varphi \quad \text{iff} \quad \forall j \geq i. \pi,j \models \varphi \\
\pi,i & \models \Diamond\varphi \quad \text{iff} \quad \exists j \geq i. \pi,j \models \varphi \\
\pi,i & \models \circ\varphi \quad \text{iff} \quad \pi,i+1 \models \varphi
\end{align*}
\]

A formula $\varphi$ holds in model $\pi$ if it holds at position 0 i.e. $\pi,0 \models \varphi$.

The atomic propositions of these temporal formulae can be trivially translated into our functional language. For our verification rules, we define the following datatype for truth values:

\[\text{TruthVal ::= True | False | Undefined}\]
We use a Kleene three-valued logic because our verification rules must always return an answer, but some of the properties to be verified may give an undefined outcome. For our example programs which attempt to implement mutual exclusion, the following two properties are defined. Within these temporal properties, we use the variable $s$ to denote the current observable state whose properties are being specified.

**Property 1 (Mutual Exclusion)** This is a safety property which specifies that both processes cannot be using the critical resource at the same time. This can be specified as follows:

\[
\square (\text{case } s \text{ of } \\
\text{ObsState } s_1 s_2 \rightarrow \text{case } s_1 \text{ of } \\
U \rightarrow \text{case } s_2 \text{ of } \\
U \rightarrow \text{False} \\
| \_ \rightarrow \text{True} \\
| \_ \rightarrow \text{True})
\]

**Property 2 (Non-Starvation)** This is a liveness property which specifies that each process must eventually get to use the critical resource if they are waiting for it. This can be specified for process 1 as follows (the specification of this property for process 2 is similar):

\[
\square ((\text{case } s \text{ of } \\
\text{ObsState } s_1 s_2 \rightarrow \text{case } s_1 \text{ of } \\
W \rightarrow \text{True} \\
| \_ \rightarrow \text{False}) \Rightarrow \Diamond (\text{case } s \text{ of } \\
\text{ObsState } s_1 s_2 \rightarrow \text{case } s_1 \text{ of } \\
U \rightarrow \text{True} \\
| \_ \rightarrow \text{False}))
\]

5 Verification of Temporal Properties

In this section, we show how temporal properties of reactive systems defined in our functional language can be verified. We define our verification rules on the restricted form of program defined in Figure 3 as shown in Figure 10. The parameter $\phi$ denotes the property to be verified and $\Phi$ denotes the function variable environment. $\rho$ denotes the set of function calls previously encountered; this is used for the detection of loops to ensure termination. $\rho$ is also used in the verification of the $\square$ operator (which evaluates to True on encountering a loop), and the verification of the $\Diamond$ operator (which evaluates to False on encountering a loop); $\rho$ is reset to empty when the verification moves inside these temporal operators. For all other temporal formulae, the value Undefined is returned on encountering a loop.

The verification rules can be explained as follows. Rules (1-4) deal with the logical connectives $\land$, $\lor$, $\Rightarrow$ and $\neg$. These are implemented in our language in the usual way for a Kleene three-valued logic using the corresponding operators $\land_3$, $\lor_3$, $\Rightarrow_3$ and $\neg_3$. Rules (5a-d) deal with a constructed stream of states. In rule (5a), if we are trying to verify that a property is always true, then we verify that it is true for the first state (with $\rho$ reset to empty) and is always true in all remaining states. In rule (5b), if we are trying to verify that a property is eventually true, then we verify that it is either true for the first state (with $\rho$ reset to empty) or is eventually true in all remaining states. In rule (5c), if we are trying to verify that a property is true in the next state then we verify that the property is true in the next state then we verify that the property is true for the next state. In rule (5d), if we are trying to verify that a property is true in the current state then we verify that the property is true in the current state by evaluating the property using the value of the current state for the state variable $s$. Rules (6a-c) deal with function calls. In rule (6a), if we are trying to verify that a property is
always true, then if the function call has been encountered before while trying to verify the same property we can return the value True; this corresponds to the standard greatest fixed point calculation normally used for the □ operator in which the property is initially assumed to be True for all states. Otherwise, the function is unfolded and added to the set of previously encountered function calls for this property. In rule (6b), if we are trying to verify that a property is eventually true, then if the function call has been encountered before while trying to verify the same property we can return the value False; this corresponds to the standard least fixed point calculation normally used for the ◁ property in which the property is initially assumed to be False for all states. Otherwise, the function is unfolded and added to the set of previously encountered function calls for this property. In rule (6c), if we are trying to verify that any other property is true, then if the function call has been encountered before we can return the value Undefined since a loop has been detected. Otherwise, the function is unfolded and added to the set of previously encountered function calls for this property. Rules (7a-b) deal with case expressions. In rule (7a), if we are trying to verify that a property is eventually true, then we verify that it is either eventually true for at least one of the branches for which there is a fairness assumption (since these branches must be selected eventually), or that it is eventually true for all branches. In Rule (7b), if we are trying to verify that any
other property is true, then we verify that it is true for all branches. In rule (8), if we encounter a free variable, then we return the value Undefined since we cannot determine the value of the variable; this must be a let variable which has been abstracted, so no information can be determined for it. In rule (9), in order to verify that a property is true for a let expression, we verify that it is true for the let body; this is where we perform abstraction of the extracted sub-expression. In rule (10), for a where expression, the function definitions are added to the environment φ.

**Theorem 5.1 (Soundness)** ∀e ∈ Prog, P ∈ List Event, π ∈ List State, φ ∈ WFF:
\[ (e es \leadsto^* \pi) \land (P[e] \neg \bot \emptyset = True \Rightarrow \pi, 0 \models \phi) \land (P[e] \neg \bot \emptyset = False \Rightarrow \pi, 0 \not\models \phi) \]

*Proof.* The proof of this is by structural induction on the program e.

**Theorem 5.2 (Termination)** ∀e ∈ Prog, φ ∈ WFF: \( P[e] \neg \bot \emptyset \) always terminates.

*Proof.* Proof of termination is quite straightforward since there will be a finite number of functions and uses of the temporal operators □ and ◇, and verification of each of these temporal operators will terminate when a function is re-encountered.

Using these rules, we try to verify the two properties (mutual exclusion and non-starvation) for the example programs for mutual exclusion given in Section 3. Firstly, distillation is applied to each of the programs.

**Example 1** For the program shown in Figure 3, Property 2 (non-starvation) holds. The verification of Property 1 (mutual exclusion) is shown below where we represent Property 1 by □ φ and the function environment by φ.

\[
\begin{align*}
& P[\text{Cons} (\text{ObsState} T T) (f_1 es)] (\Box \phi) \emptyset \\
& = \{5a\} \\
& \quad (P[\text{Cons} (\text{ObsState} T T) (f_1 es)] (\Box \phi) \emptyset \land_3 (P[f_1 es] (\Box \phi) \emptyset) \\
& = \{5d\} \\
& \quad (\phi(\text{ObsState} T T) / s) \land_3 (P[f_1 es] (\Box \phi) \emptyset) \\
& = \{\text{calculation, 6a, 7b, 5a, 5d}\} \\
& \quad (P[f_1 es] (\Box \phi) \phi \{f_1\}) \land_3 (P[f_2 es] (\Box \phi) \phi \{f_1\}) \land_3 (P[f_3 es] (\Box \phi) \phi \{f_1\}) \\
& = \{6a\} \\
& \quad (P[f_2 es] (\Box \phi) \phi \{f_1\}) \land_3 (P[f_3 es] (\Box \phi) \phi \{f_1\}) \\
& = \{\text{calculation, 6a, 7b, 5a, 5d}\} \\
& \quad (P[f_2 es] (\Box \phi) \phi \{f_1, f_2\}) \land_3 (P[f_4 es] (\Box \phi) \phi \{f_1, f_2\}) \land_3 (P[f_5 es] (\Box \phi) \phi \{f_1, f_2\}) \\
& \land_3 (P[f_3 es] (\Box \phi) \phi \{f_1\}) \\
& = \{6a\} \\
& \quad (P[f_4 es] (\Box \phi) \phi \{f_1, f_2\}) \land_3 (P[f_5 es] (\Box \phi) \phi \{f_1, f_2\}) \land_3 (P[f_3 es] (\Box \phi) \phi \{f_1\}) \\
& = \{\text{calculation, 6a, 7b, 5a, 5d}\} \\
& \quad (P[f_1 es] (\Box \phi) \phi \{f_1, f_2, f_4\}) \land_3 (P[f_4 es] (\Box \phi) \phi \{f_1, f_2, f_4\}) \land_3 (P[f_5 es] (\Box \phi) \phi \{f_1, f_2\}) \\
& \land_3 (P[f_3 es] (\Box \phi) \phi \{f_1\}) \\
& = \{6a\} \\
& \quad (P[f_5 es] (\Box \phi) \phi \{f_1, f_2, f_5\}) \land_3 (P[f_7 es] (\Box \phi) \phi \{f_1, f_2, f_5\}) \land_3 (P[f_8 es] (\Box \phi) \phi \{f_1, f_2, f_5\}) \\
& \land_3 (P[f_3 es] (\Box \phi) \phi \{f_1\}) \\
& = \{\text{calculation, 6a, 7b, 5a, 5d}\} \\
& \quad (P[f_5 es] (\Box \phi) \phi \{f_1, f_2, f_5\}) \land_3 (P[f_7 es] (\Box \phi) \phi \{f_1, f_2, f_5\}) \land_3 (P[f_8 es] (\Box \phi) \phi \{f_1, f_2, f_5\}) \\
& \land_3 (P[f_3 es] (\Box \phi) \phi \{f_1\})
\end{align*}
\]
True value and belongs to the following datatype:

In this section, we show how counterexamples and witnesses for temporal properties of reactive systems defined in our functional language can be constructed. We augment the verification rules from the previous section to generate a verdict which consists of a trace (a list of observable states) along with a truth value and belongs to the following datatype:

\[ \text{Verdict} ::= \text{TruthVal} \times \text{List State} \]

The trace will give a counterexample if the associated truth value is False, and a witness if the corresponding truth value is True. The logical connectives \(\land_v, \lor_v, \Rightarrow_v\) and \(\neg_v\) are extended to this datatype as \(\land_v, \lor_v, \Rightarrow_v\) and \(\neg_v\), which are defined as follows.
\[(b_1, t_1) \wedge v (b_2, t_2) = (b, t)\]
where
\[b = b_1 \wedge_3 b_2\]
\[t = \min\{t_1, t_2\} \wedge b_i = b\]

\[(b_1, t_1) \vee v (b_2, t_2) = (b, t)\]
where
\[b = b_1 \vee_3 b_2\]
\[t = \min\{t_1, t_2\} \wedge b_i = b\]

\[(b_1, t_1) \Rightarrow v (b_2, t_2) = (\neg v (b_1, t_1)) \vee v (b_2, t_2)\]
\[\neg v (b, t) = (\neg_3 b, t)\]

If there is more than one counterexample or witness, the function \(\text{min}\) is used to ensure that the \text{shortest} one is always returned. The rules for the construction of counterexamples and witnesses for the simplified form of program defined in Figure 3 are as shown in Figure 11.

1. \(\mathcal{C}[e] (\phi \land \psi) \phi \rho \pi = (\mathcal{C}[e] \phi \phi \rho \pi) \land_v (\mathcal{C}[e] \psi \phi \rho \pi)\)
2. \(\mathcal{C}[e] (\phi \lor \psi) \phi \rho \pi = (\mathcal{C}[e] \phi \phi \rho \pi) \lor_v (\mathcal{C}[e] \psi \phi \rho \pi)\)
3. \(\mathcal{C}[e] (\phi \Rightarrow \psi) \phi \rho \pi = (\mathcal{C}[e] \phi \phi \rho \pi) \Rightarrow_v (\mathcal{C}[e] \psi \phi \rho \pi)\)
4. \(\mathcal{C}[e] (\neg \phi) \phi \rho \pi = \neg_v (\mathcal{C}[e] \phi \phi \rho \pi)\)
5a. \(\mathcal{C}[\text{Cons} e_0 e_1] (\Box \phi) \phi \rho \pi = (\mathcal{C}[\text{Cons} e_0 e_1] \phi \phi \rho \pi) \land_v (\mathcal{C}[e] (\Box \phi) \phi \rho (\pi++[e_0])\)
5b. \(\mathcal{C}[\text{Cons} e_0 e_1] (\Diamond \phi) \phi \rho \pi = (\mathcal{C}[\text{Cons} e_0 e_1] \phi \phi \rho \pi) \lor_v (\mathcal{C}[e] (\Diamond \phi) \phi \rho (\pi++[e_0])\)
5c. \(\mathcal{C}[\text{Cons} e_0 e_1] (\odot \phi) \phi \rho \pi = (\mathcal{C}[e] \phi \phi \rho (\pi++[e_0])\)
5d. \(\mathcal{C}[\text{Cons} e_0 e_1] \phi \phi \rho \pi = (v, \pi ++ [e_0]), \text{where } \phi[e_0/s] \downarrow v\)
6a. \(\mathcal{C}[f x_1 \ldots x_n] (\Box \phi) \phi \rho \pi = \left\{\begin{array}{l} (\text{False}, \pi), \text{if } f \notin \rho \\
\mathcal{C}[e[x_1/x'_1, \ldots, x_n/x'_n]] (\Box \phi) \phi (\rho \cup \{f\}) \pi, \text{otherwise}
\end{array}\right\}
\text{where } \phi(f) = \lambda x'_1 \ldots x'_n e
\)
6b. \(\mathcal{C}[f x_1 \ldots x_n] (\Diamond \phi) \phi \rho \pi = \left\{\begin{array}{l} (\text{False}, \pi), \text{if } f \notin \rho \\
\mathcal{C}[e[x_1/x'_1, \ldots, x_n/x'_n]] (\Diamond \phi) \phi (\rho \cup \{f\}) \pi, \text{otherwise}
\end{array}\right\}
\text{where } \phi(f) = \lambda x'_1 \ldots x'_n e
\)
6c. \(\mathcal{C}[f x_1 \ldots x_n] \phi \phi \rho \pi = \left\{\begin{array}{l} (\text{Undefined}, \pi), \text{if } f \in \rho \\
\mathcal{C}[e[x_1/x'_1, \ldots, x_n/x'_n]] \phi \phi (\rho \cup \{f\}) \pi, \text{otherwise}
\end{array}\right\}
\text{where } \phi(f) = \lambda x'_1 \ldots x'_n e
\)
7a. \(\mathcal{C}[\text{case } x \text{ of } p_1 \rightarrow e_1 | \cdots | p_n \rightarrow e_n] (\Diamond \phi) \phi \rho \pi = (\bigvee_{p_i \in F} \mathcal{C}[e_i] (\Diamond \phi) \phi \rho \pi) \vee v (\bigwedge_{i=1}^n \mathcal{C}[e_i] (\Diamond \phi) \phi \rho \pi)\)
7b. \(\mathcal{C}[\text{case } x \text{ of } p_1 \rightarrow e_1 | \cdots | p_n \rightarrow e_n] \phi \phi \rho \pi = \bigwedge_{i=1}^n \mathcal{C}[e_i] \phi \phi \rho \pi\)
8. \(\mathcal{C}[x e_1 \ldots e_n] \phi \phi \rho \pi = (\text{Undefined}, \pi)\)
9. \(\mathcal{C}[\text{let } x = e_0 \text{ in } e_1] \phi \phi \rho \pi = \mathcal{C}[e_1] \phi \phi \rho \pi\)
10. \(\mathcal{C}[e_0 \text{ where } f_1 = e_1 \ldots f_n = e_n] \phi \phi \rho \pi = \mathcal{C}[e_0] \phi (\phi \cup \{f_1 \mapsto e_1, \ldots, f_n \mapsto e_n\}) \rho \pi\)

Figure 11: Counterexample and Witness Construction Rules
These rules are very similar to the verification rules given in Figure 10, with the addition of the parameter π, which gives the value of the current trace thus far. As each observable state in the program trace is processed in rules (5a-d), it is appended to the end of π and when a final truth value is obtained it is returned along with the value of π. Counterexamples and witnesses can of course be infinite in the form of a lasso consisting of a finite prefix and a loop, while only a finite trace will be returned using these rules. However, loops can be detected in the generated trace as the repetition of observable states.

To prove that the constructed counterexample or witness is valid, we need to prove that it satisfies the original temporal property which was verified.

**Theorem 6.1 (Validity)** \( \forall e \in \text{Prog}, \phi \in \text{WF}: \)
\[
(\mathcal{C}[e] \phi \emptyset \emptyset [] = (\text{True}, \pi) \Rightarrow \pi, 0 \not\vdash \phi) \land (\mathcal{C}[e] \phi \emptyset \emptyset [] = (\text{False}, \pi) \Rightarrow \pi, 0 \not\vdash \phi)
\]

**Proof.** The proof of this is by structural induction on the program e. \( \square \)

Using these rules, we try to construct counterexamples for the two properties (mutual exclusion and non-starvation) for the example programs given in Section 3.

**Example 1** For the program shown in Figure 4, the application of these rules for Property 1 (mutual exclusion) is shown below where we represent Property 1 by \( \square \phi \) and the function environment by \( \phi \). We also use the shorthand notation \( (X, Y) \) to denote the state ObsState \( X, Y \).

\[
\mathcal{C}[\text{Cons} (T, T) (f_1 es)] (\square \phi) \emptyset \emptyset [] = \{5a\} \\
(\mathcal{C}[\text{Cons} (T, T) (f_1 es)] \phi \emptyset \emptyset []) \land_\nu (\mathcal{C}[f_1 es] (\square \phi) \emptyset \emptyset [(T, T)]) = \{5d\} \\
(\phi[(T, T)/s]) \land_\nu (\mathcal{C}[f_1 es] (\square \phi) \emptyset \emptyset [(T, T)]) = \{\text{calculation, } 6a, 7b, 5a, 5d\} \\
(\mathcal{C}[f_1 es] (\square \phi) \{f_1\} [(T, T), (T, W)]) \land_\nu (\mathcal{C}[f_2 es] (\square \phi) \{f_1\} [(T, T), (W, W)]) = \{6a\} \\
(\mathcal{C}[f_2 es] (\square \phi) \{f_1\} [(T, T), (W, T)]) \land_\nu (\mathcal{C}[f_3 es] (\square \phi) \{f_1\} [(T, T), (T, W)]) = \{\text{calculation, } 6a, 7b, 5a, 5d\} \\
(\mathcal{C}[f_3 es] (\square \phi) \{f_1, f_2\} [(T, T), (W, T)]) \land_\nu (\mathcal{C}[f_4 es] (\square \phi) \{f_1, f_2\} [(T, T), (W, W)]) = \{6a\} \\
(\mathcal{C}[f_4 es] (\square \phi) \{f_1, f_2, f_3\} [(T, T), (W, U)]) \land_\nu (\mathcal{C}[f_5 es] (\square \phi) \{f_1, f_2, f_3\} [(T, T), (W, W)]) = \{\text{calculation, } 6a, 7b, 5a, 5d\} \\
(\mathcal{C}[f_5 es] (\square \phi) \{f_1, f_2, f_3\} [(T, T), (T, W)])
= \{\text{calculation, 6a, 7b, 5a, 5d}\}
\begin{align*}
&= \{\text{calculation, 6a, 7b, 5a, 5d}\} \\
&= \{\text{calculation, 6a, 7b, 5a, 5d}\} \\
&= \{\text{calculation, 6a, 7b, 5a, 5d}\}
\end{align*}

We can see that the rules that are applied closely mirror those applied in the verification of this property, and that the following counterexample is generated:

**Example 2** For the program shown in Figure 6, the application of these rules for Property 2 (non-starvation) is shown below where we represent Property 2 by \(\Box(\varphi \Rightarrow \Diamond \psi)\) and the function environment by \(\varphi\). We again use the shorthand notation \((X, Y)\) to denote the state \(\text{ObsState } X Y\).

\[
\begin{align*}
\mathcal{E}[\text{Cons } (T,T) \langle f_1 \rangle] (\Box(\varphi \Rightarrow \Diamond \psi)) & \emptyset \emptyset \\
= \{5a\} \\
&= \{5d\}
\end{align*}
\]
= \{6a\}
(\forall [f_3 \in ES] (\Box (\varphi \Rightarrow \Diamond \psi)) \varphi \{f_1, f_2\} [(T, T), (W, T), (W, W)])
\land (\forall [f_3 \in ES] (\Box (\varphi \Rightarrow \Diamond \psi)) \varphi \{f_1\} [(T, T), (T, W)])

= \{calculation, 6a, 7b, 5a, 3, 5b, 6b\}
(\{\text{calculation, } 6a, 7b, 5a, 3, 5b, 6b\})

The following counterexample with a loop at the end is therefore generated:

\text{Cons}\ (\text{ObsState } T\ T) \ (\text{Cons}\ (\text{ObsState } W\ T) \ (\text{Cons}\ (\text{ObsState } W\ W) \ (\text{Cons}\ (\text{ObsState } W\ W) \ \text{Nil})))

7 Conclusion and Related Work

In previous work [6], we have shown how a fold/unfold program transformation technique can be used to verify both safety and liveness properties of reactive systems which have been specified using a functional language. However, counterexamples and witnesses were not constructed using this approach. In this paper, we have therefore extended these previous techniques to address this shortcoming to construct a counterexample trace when a temporal property does not hold, and a witness when it does.

Fold/unfold transformation techniques have also been developed for verifying temporal properties for logic programs [11, 15, 4, 1, 8]). Some of these techniques have been developed only for safety properties, while others can be used to verify both safety and liveness properties. Due to the use of a different programming paradigm, it is difficult to compare the relative power of these techniques to our own. However, none of these techniques construct counterexamples when the temporal property does not hold.

Very few techniques have been developed for verifying temporal properties for functional programs other than the work of Lisitsa and Nemytykh [12, 2]. Their approach uses supercompilation [17, 16] as the fold/unfold transformation methodology, where our own approach uses distillation [5, 7]. Their approach can verify only safety properties, and does not construct counterexamples when the safety property does not hold.

One other area of work related to our own is the work on using Higher Order Recursion Schemes (HORS) to verify temporal properties of functional programs. HORS are a kind of higher order tree grammar for generating a (potentially infinite) tree and are well-suited to the purpose of verification since they have a decidable mu-calculus model checking problem, as proved by Ong [14]. Kobayashi [13] first showed how this approach can be used to verify safety properties of higher order functional programs and for the construction of counterexamples when the safety property does not hold. This approach was then extended to also verify liveness properties by Lester et al. [10], but counterexamples are not constructed when the liveness property does not hold. These approaches have a very bad worst-case time complexity, but techniques have been developed to ameliorate this to a certain extent. It does however appear likely that this approach will be able to verify more properties than our own approach but much less efficiently.

Acknowledgements

This work was supported, in part, by Science Foundation Ireland grant 10/CE/I1855 to Lero - the Irish Software Engineering Research Centre (www.lero.ie), and by the School of Computing, Dublin City University.
References


