Software Model Checking Based on Game Semantics and CSP\(^1\)

Aleksandar Dimovski\(^2\) and Ranko Lazić\(^3\)

Department of Computer Science
University of Warwick
Coventry CV4 7AL, UK

Abstract

We present an approach for software model checking based on game semantics and CSP. Open program fragments are compositionally modelled as CSP processes which represent their game semantics. This translation is performed by a prototype compiler. Observational equivalence and verification of properties are checked by traces refinement using the FDR tool. Effectiveness of our approach is evaluated on several examples.

Key words: Software model checking, Game semantics, CSP process algebra, FDR refinement checker

1 Introduction

Model checking [6] is a system verification technique based on semantics: the verifier checks whether the semantics of a given system satisfies some property. It has gained industrial acceptance because, in contrast to the approaches of simulation, testing and theorem proving, model checking offers automatic and exhaustive verification, and it also reports counter-examples.

The success of model checking has been mainly for hardware and communication protocols. Recently, model checking of software has become an active and important area of research and application (e.g. [5]). Unfortunately, applying model checking to software is complicated by several factors, ranging from the difficulty to model programs, due to the complexity of programming languages as compared to hardware description languages, to difficulties in specifying meaningful properties of software using the usual temporal logical

\(^1\) We acknowledge support by the EPSRC (GR/S52759/01). The second author was also supported by the Intel Corporation.
\(^2\) Email: aleks@dcs.warwick.ac.uk
\(^3\) Email: lazic@dcs.warwick.ac.uk

This is a preliminary version. The final version will be published in Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs
formalisms. Another reason is the state explosion problem: industrial programs are large and model checking is computationally demanding.

Many of the problems above are due to difficulties in obtaining sound and complete semantic models of software and expressing such models in an algorithmic fashion suitable for automatic analysis. Game semantics has potential to overcome these problems, since it has produced the first accurate, i.e. fully abstract and fully complete models for a variety of programming languages and logical systems (e.g. [1]). Recently, it was shown that the fully abstract game-based model of second-order finitary Idealised Algol (i.e. with finite data types and without recursion) with iteration can be represented using only regular expressions [10], and that this can be used for efficient program analysis and verification [3].

Game semantics has several very suitable features for software model checking. It produces observationally fully abstract models with a maximum level of abstraction, since internal state changes during computation are abstracted away. It can compositionally model terms-in-context, i.e. open program fragments. This ability is essential in analysing properties of software components which contain undefined (free) variables and procedures.

We present an approach for compositional software modelling and verification, based on game semantics and the CSP process algebra (e.g. [15]). We focus on second-order finitary Idealised Algol with iteration. Game semantics of any term-in-context is represented as a CSP process. Observational equivalence between terms, and verification of regular properties, are decidable by checking traces refinement between CSP processes.

Compared with the regular expressions approach [10], this CSP based approach offers several benefits. Using the wide range of operators available in CSP, program terms are represented as processes in a clear and compositional way. The process which models a term is defined as a parallel composition of processes which model its subterms, with synchronisation events being hidden. Traces refinement between CSP processes can be automatically checked by the FDR tool [9], which is highly optimised for verification of parallel networks of processes. FDR also offers a range of compositional state-space reduction algorithms [14], enabling smaller models to be generated before or during refinement checking.

We have implemented a prototype compiler which, given any term-in-context, outputs a CSP process representing its game semantics. The output can be loaded into the ProBe tool for interactive exploration, or the FDR tool for automatic analysis. FDR also contains an interactive debugger, when the answer to a refinement query is negative.

Effectiveness of our approach is evaluated on several variants of two examples: a sorting algorithm, and an abstract data type implementation. Some of the experimental results show that, for minimal model generation, we outperform the approach based on regular expressions [3].

The paper is organised as follows. Sections 2 and 3 briefly recall the pro-
gramming language, the CSP representation of its game semantics, and verifica-
tion of observational equivalence. Further details can be found in the
companion paper [7] which concentrates on theory, whereas this paper is de-
voted to applications and property verification. Section 4 shows how propo-
ties given in a linear temporal logic on finite traces, or as finite automata, can
be verified. In Sections 5 and 6, we present the compiler and two case studies.

2 The programming language

The input to our compiler is a term-in-context of second-order finitary Ide-
alised Algol with iteration. Idealised Algol [12] is a compact programming
language, similar to Core ML, which combines the fundamental features of
imperative languages with a full higher-order procedure mechanism.

The language has basic data types $\tau$, which are a finite subset of the
integers and the booleans. The phrase types of the language are expressions,
commands and variables, plus first-order function types.

$$
\tau ::= \text{int} \mid \text{bool}
$$

$$
\sigma ::= \text{exp}[\tau] \mid \text{comm} \mid \text{var}[\tau]
$$

$$
\theta ::= \sigma \mid \sigma \times \sigma \times \cdots \sigma \to \sigma
$$

Terms are introduced using type judgements of the form $\Gamma \vdash M : \theta$, where
$\Gamma = \{\iota_1 : \theta_1, \ldots, \iota_k : \theta_k\}$.

Expression-type terms are built from constants and arithmetic/logic opera-
tors ($E_1 \ast E_2$). Command-type terms are built by the standard imperative
operators: assignment ($V := E$), conditional (if $B$ then $M_1$ else $M_2$), while
loop (while $B$ do $C$), sequencing ($C_3 M$, note that commands can be sequenced
not only with commands but also with expressions or variables), no-op ($\text{skip}$),
and a non-terminating command ($\text{diverge}$). There are also term formers for
dereferencing variables ($!V$), application of first-order free identifiers to argu-
ments ($\iota M_1 \cdots M_k$), local variable declaration ($\text{new}[\tau] \ i$ in $C$), and function
definition constructor ($\text{let} \ i (\iota_1 : \sigma_1, \ldots, \iota_k : \sigma_k) = N$ in $M$). Full typing
rules can be found in [7].

3 The CSP model

Here we recall the main properties of the CSP representation of game seman-
tics of program terms. The details of this representation and some examples
can be found in [7]. An introduction to game semantics is available in [2]. A
comprehensive text on CSP is [15].
3.1 Interpretations of types and terms

With each type \( \theta \), we associate a set of possible events, the alphabet \( A_\theta \). The alphabet of a type contains events \( q \in Q_\theta \) called questions, which are appended to channel with name \( Q \), and for each question \( q \), there is a set of events \( a \in \mathbb{A}_\theta^q \) called answers, which are appended to channel with name \( A \).

\[
\begin{align*}
A_{\text{int}} &= \{0, \ldots, N_{\text{max}} - 1\}, \\
A_{\text{bool}} &= \{\text{true}, \text{false}\} \\
Q_{\text{exp}[r]} &= \{q\}, \\
A_{\text{exp}[r]} &= A_r \\\nQ_{\text{comm}} &= \{\text{run}\}, \\
A_{\text{comm}} &= \{\text{done}\} \\
Q_{\text{var}[r]} &= \{\text{read}, \text{write}.x \mid x \in A_r\}, \\
A_{\text{var}[r]} &= A_r, \\
A_{\text{write}.x} &= \{\text{ok}\} \\
Q_{\sigma_1 \times \cdots \times \sigma_k \rightarrow \sigma_0} &= \{j.q \mid q \in \mathbb{Q}_{\sigma_j}, 0 \leq j \leq k\}, \\
A_{\sigma_1 \times \cdots \times \sigma_k \rightarrow \sigma_0} &= \{j.a \mid a \in \mathbb{A}_{\sigma_j}^q\}, \text{for } 0 \leq j \leq k \\\nA_\theta &= Q_{\theta} \cup A. \bigcup_{q \in Q_{\theta}} A_{\theta}^q
\end{align*}
\]

We interpret any typed term-in-context \( \Gamma \vdash M : \sigma \) by a CSP process \( \llbracket \Gamma \vdash M : \sigma \rrbracket_{\text{CSP}} \) whose set of terminated traces

\[
\mathcal{L}_{\text{CSP}}(\Gamma \vdash M : \sigma) = \{ t \mid t^\wedge(\check{\cdot}) \in \text{traces}(\llbracket \Gamma \vdash M : \sigma \rrbracket_{\text{CSP}}) \}
\]

is the set of all complete plays of the game strategy for the term. Events of this process are from the alphabet \( A_{\Gamma+\sigma} \), defined as:

\[
\begin{align*}
A_{\sigma_\theta} &= \{\text{l.} a \mid a \in A_\theta\} \\
A_\Gamma &= \bigcup_{\sigma \in \Gamma} A_{\sigma_\theta} \\
A_{\Gamma+\sigma} &= A_\Gamma \cup A_\sigma
\end{align*}
\]

The compositional definition of the processes \( \llbracket \Gamma \vdash M : \sigma \rrbracket_{\text{CSP}} \) is given in Appendix A.

3.2 Observational equivalence

Two terms \( M \) and \( N \) are observationally equivalent, written \( M \equiv_{\sigma} N \), if and only if for any context \( C[-] \) such that both \( C[M] \) and \( C[N] \) are closed terms of type \( \text{comm} \), \( C[M] \) converges if and only if \( C[N] \) converges. It was proved in [1] that this coincides to equality of sets of complete plays of strategies for \( M \) and \( N \), i.e. that the games model is fully abstract.

For the programming language fragment treated in this paper, it was shown in [7] that observational equivalence is captured by two traces refinements:

**Theorem 3.1 (Observational equivalence)**

\[
\begin{align*}
\Gamma \vdash M \equiv_{\sigma} N & \iff \llbracket \Gamma \vdash M : \sigma \rrbracket_{\text{CSP}} \not\sqsubseteq T \llbracket \Gamma \vdash N : \sigma \rrbracket_{\text{CSP}} \quad \land \\
\llbracket \Gamma \vdash N : \sigma \rrbracket_{\text{CSP}} \not\sqsubseteq T \llbracket \Gamma \vdash M : \sigma \rrbracket_{\text{CSP}} \quad (1)
\end{align*}
\]

where \( \text{RUN}_A = \exists x : A \rightarrow \text{RUN}_A \).

It is also proved in [7] that the process representing any term is finite state, and so observational equivalence is decidable using FDR.
4 Property verification

In addition to checking observational equivalence of two program terms, it is desirable to be able to check properties of terms. Recall that for any term $\Gamma \vdash M : \sigma$, the CSP process $[\Gamma \vdash M : \sigma]^{CSP}$ has the property that its set of terminated traces

$$\mathcal{L}_{CSP}(\Gamma \vdash M : \sigma) = \{ t \mid t^\wedge(\checkmark) \in traces([\Gamma \vdash M : \sigma]^{CSP}) \}$$

is the set of all complete plays of the strategy for $\Gamma \vdash M : \sigma$. We therefore focus on properties of finite traces, and take the view that $\Gamma \vdash M : \sigma$ satisfies such a property if and only if all traces in $\mathcal{L}_{CSP}(\Gamma \vdash M : \sigma)$ satisfy it.

4.1 Linear temporal logic

A standard way of writing properties of linear behaviours is by linear temporal logic. Given a finite set $\Sigma$, we consider the following formulas. In addition to propositional connectives, they contain the temporal operators 'next-time' and 'until'.

$$\phi ::= \text{true} \mid \text{false} \mid a \in \Sigma \mid \neg \phi \mid \phi_1 \lor \phi_2 \mid \bigcirc \phi \mid \phi_1 U \phi_2$$

We call this logic $\text{LTL}_I^\Sigma$, because we give it semantics over finite traces (i.e. sequences) of elements of $\Sigma$. In particular, formulas $a$, $\bigcirc \phi$ and $\phi_1 U \phi_2$ require the trace to be non-empty. For any trace $t$ of length $k$, we write its elements as $t_1, \ldots, t_k$, and we write $t^i$ for its $i^{th}$ suffix $\langle t_i, \ldots, t_k \rangle$.

$$t \models \text{true}$$
$$t \nvdash \text{false}$$
$$t \models a \iff t \neq \langle \rangle \text{ and } t_1 = a$$
$$t \models \neg \phi \iff t \nvdash \phi$$
$$t \models \phi_1 \lor \phi_2 \iff t \models \phi_1 \text{ or } t \models \phi_2$$
$$t \models \bigcirc \phi \iff t \nvdash \langle \rangle \text{ and } t^2 \models \phi$$
$$t \models \phi_1 U \phi_2 \iff \text{there exists } i \in \{1, \ldots, |t|\} \text{ such that } t^i \models \phi_2$$

and for all $j \in \{1, \ldots, i - 1\}$, $t^j \models \phi_1$

The 'eventually' and 'always' operators can be defined as abbreviations in the usual way:

$$\bigcirc \phi = \text{true} U \phi \quad \Box \phi = \neg \bigcirc \neg \phi$$

Duals of the 'next-time' and 'until' operators are also useful:

$$\bigcirc \phi = \neg \bigcirc \neg \phi \quad \phi_1 V \phi_2 = \neg (\neg \phi_1 U \neg \phi_2)$$
Their semantics is as follows:

\[ t \models \bigcirc \phi \quad \text{iff} \quad t = \emptyset \text{ or } t^2 \models \phi \]
\[ t \models \phi_1 \lor \phi_2 \quad \text{iff} \quad \text{either for all } i \in \{1, \ldots, |t|\}, \ t^i \models \phi_1 \]
\[ \quad \text{or there exists } i \in \{1, \ldots, |t|\} \text{ such that } t^i \models \phi_1 \]
\[ \quad \text{and for all } j \in \{1, \ldots, i\}, \ t^j \models \phi_2 \]

A term \( \Gamma \vdash M : \sigma \) satisfies a formula \( \phi \) of \( \text{LTL}^{A_{\Gamma}} \) if and only if for every trace \( t \in \mathcal{L}_{\text{CSP}}(\Gamma \vdash M : \sigma) \), \( t = \phi \).

Example 4.1 Consider the following term:

\[ b : \text{bool}, \ C : \text{comm} \vdash \text{while } b \text{ do } C : \text{comm} \]

The transition system of the CSP process for this term is shown in Figure 1. Since both \( b \) and \( C \) are free identifiers, the successfully terminated traces of this process are all those corresponding to executing \( C \) zero or more times while the value of \( b \) is true, and finishing when the value of \( b \) is false.

Therefore, this term satisfies \( \diamond b.\text{false} \), but does not satisfy \( \diamond C.\text{Q.run} \). It also satisfies \( \square (b.\text{true} \rightarrow \diamond C.\text{Q.run}) \), but does not satisfy \( \square (b.\text{Q.q} \rightarrow \diamond C.\text{Q.run}) \). □

There is an algorithm which, given any formula \( \phi \) of \( \text{LTL}^{A_{\Gamma}} \), constructs:

- a CSP process \( P^\Sigma_\phi \) such that \( t \models \phi \) if and only if \( t^\prec \sqrt{\checkmark} \in \text{traces}(P^\Sigma_\phi) \);
- a finite transition system which has the same finite traces as \( P^\Sigma_\phi \).

This is similar to constructing a finite automaton which accepts a finite trace \( t \) if and only if \( t \models \phi \). The details can be found in Appendix B.

We therefore have a decision procedure which, given a program term \( \Gamma \vdash M : \sigma \) and a formula \( \phi \) of \( \text{LTL}^{A_{\Gamma}} \), checks satisfaction. It works by constructing the CSP processes \( \llbracket \Gamma \vdash M : \sigma \rrbracket_{\text{CSP}} \) and \( P^\Sigma_\phi \), and checking the
traces refinement \(^4\)

\[
P^\mathcal{A}_{\Gamma} \mathcal{R} \quad \square \text{RUN}_\mathcal{A}_{\Gamma} \quad \subseteq \quad \Gamma \vdash M : \sigma]^\text{CSP}
\]

(2)

4.2 Finite automata

More generally, any property such that the set of all finite traces which satisfy it is regular, can be represented in CSP. Suppose \(A\) is an automaton with finite alphabet \(\Sigma\), finite set of states \(Q\), transition relation \(T \subseteq Q \times \Sigma \times Q\), initial states \(Q^0 \subseteq Q\), and accepting states \(F \subseteq Q\). For any \(q \in Q \setminus F\), we define

\[
P_q = \bigwedge_{(q', a, q') \in T} a \rightarrow P_{q'}
\]

For any \(q \in F\), we define

\[
P_q = (\bigwedge_{(q', a, q') \in T} a \rightarrow P_{q'}) \quad \square \text{SKIP}
\]

This is a valid system of recursive CSP process definitions, so we can let

\[
P_A = \bigwedge_{q \in Q^0} P_q
\]

We then have that \(P_A\) has finitely many states and

\[
t \text{ is accepted by } A \text{ iff } t \prec \checkmark \in \text{traces}(P_A)
\]

Example 4.2 Consider the automaton \(A\) in Figure 2, whose alphabet is \(\{a, b, c\}\). It accepts a finite trace \(t\) if and only if \(t = \diamond b\).

The CSP process \(P_A\) is defined as:

\[
P_A = P_1
\]

\[
P_1 = (a \rightarrow P_1) \quad \square (b \rightarrow P_2) \quad \square (c \rightarrow P_1)
\]

\[
P_2 = (a \rightarrow P_2) \quad \square (b \rightarrow P_2) \quad \square (c \rightarrow P_2) \quad \square \text{SKIP}
\]

\[
\square
\]

Therefore, given a program term \(\Gamma \vdash M : \sigma\) and a finite automaton \(A\) with alphabet \(\mathcal{A}_{\Gamma} \mathcal{R}\), we can decide whether \(A\) accepts each complete play of the strategy for \(\Gamma \vdash M : \sigma\) by checking (e.g. using FDR) the traces refinement

\[
P_A \mathcal{R} \quad \text{RUN}_\mathcal{A}_{\Gamma} \quad \subseteq \quad \Gamma \vdash M : \sigma]^\text{CSP}
\]

(3)

\(^4\) If \(\phi\) contains the \(U\) operator, the standard FDR procedure for constructing a transition system for \(P^\mathcal{A}_{\Gamma} \mathcal{R}\) may not terminate. In this case, the traces refinement above can be checked by FDR either by representing as a CSP process the finite transition system for \(P^\mathcal{A}_{\Gamma} \mathcal{R}\) which the algorithm in Appendix B produces, or by the approach in Section 4.2.
This also provides another way of deciding satisfaction of a formula $\phi$ of $\text{LTL}^A_{\tau^*}$: construct a finite automaton $A$ which accepts a finite trace $t$ if and only if $t \models \phi$, and then check the traces refinement above.

5 Compiler

We have implemented a compiler in Java [4], which automatically converts a term-in-context (i.e. an open program fragment) into a CSP process which represents its game semantics. The input is code, with simple type annotations to indicate sizes of finite integer data types. The resulting CSP process is defined by a script in machine-readable CSP [15] which the compiler outputs.

The scripts output by the compiler can be loaded into the tools ProBE for interactive exploration of transition systems, and FDR for automatic analysis and interactive debugging [9]. One of the functions of FDR is to check traces refinement between two finite-state processes. As we saw above, this can be used to decide observational equivalence between two terms (1), satisfaction of a linear temporal logic formula (2), and containment in a regular language (3).

FDR offers a number of hierarchical compression algorithms, which can be applied during either model generation or refinement checking. The scripts which our compiler produces normally contain instructions to apply diamond elimination and strong bisimulation quotienting to subprocesses which model local variable declaration subterms. This exploits the fact that game semantics hides interactions between a local variable and the subterm which is its scope. They become silent (i.e. $\tau$) transitions, enabling the model to be reduced.

Instead of the infinite data type of all integers, the programming language fragment considered in this paper has finite data types. We work with sets of integers modulo $k$. Each integer variable is declared to be of type $\text{int}\%k$ for some $k$, and different values of $k$ can be used for different variables. Operations between variables with distinct integer types $\text{int} \%k_1$ and $\text{int} \%k_2$ are interpreted as modulo the minimum of $k_1$ and $k_2$.

6 Applications

We now consider application of the approach proposed above and discuss experimental results for two kinds of example: a sorting algorithm, and an abstract data type implementation.

6.1 A sorting algorithm

In this section we analyse the bubble-sort algorithm, whose implementation is given in Figure 3. The code includes a meta variable $n$, representing array size, which will be replaced by several different values. The integers stored in the array are of type $\text{int}\%3$, which consists of values 0, 1 and 2. The type of
\[ x[n] : \text{var int\%3} \vdash \]
\[ \text{new int\%3 \(a[n]\)} \text{ in} \]
\[ \text{new int\%n+1 \(i\)} \text{ in} \]
\[ \text{while} \ (i < n) \ \{ \quad a[i] := x[i]; \quad i := i + 1; \quad \} \]
\[ \text{new bool \(flag\)} := \text{true in} \]
\[ \text{while} \ (flag) \{ \]
\[ \quad flag := \text{false}; \]
\[ \quad \text{while} \ (i < n - 1) \ \{ \]
\[ \quad \quad \text{if} \ (a[i] > a[i+1]) \ \{ \]
\[ \quad \quad \quad \quad \text{flag} := \text{true}; \]
\[ \quad \quad \quad \text{new int\%3 \(temp\)} \text{ in} \]
\[ \quad \quad \quad \quad temp := a[i]; \]
\[ \quad \quad \quad \quad a[i] := a[i+1]; \]
\[ \quad \quad \quad \quad a[i+1] := temp; \quad \} \]
\[ \quad \quad \quad i := i + 1; \quad \} \}
\[ i := 0; \]
\[ \text{while} \ (i < n) \ \{ \quad x[i] := a[i]; \quad i := i + 1; \quad \} \]
\[ : \text{comm} \]

Fig. 3. Implementation of bubble sort

Fig. 4. Transition system of the model for \(n = 2\)

index \(i\) is \(\text{int\%}n+1\), i.e. one more than the size of the array.

The implementation of bubble-sort is standard. The program first copies
the input array \(x[]\) into a local array \(a[]\), which is then sorted and copied back
into \(x[]\). The array being effectively sorted, \(a[]\), is not visible from the outside
of the program because it is locally defined, and only reads and writes of the
non-local array \(x[]\) are seen in the model. A transition system of the model
CSP process for \(n = 2\) is shown in Figure 4. The left-hand half represents
reads of all possible combinations of values from \(x[]\), while the right-hand half
represents writes of the same values in sorted order.

Table 1 contains the experimental results for minimal model generation.
This consisted of running the compiler on the bubble-sort implementation,
and then letting FDR generate a transition system for the resulting process.
Table 1
Experimental results for bubble-sort minimal model generation

<table>
<thead>
<tr>
<th>n</th>
<th>CSP</th>
<th>Regular expressions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Time (m)</td>
<td>Max. st.</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>1 775</td>
</tr>
<tr>
<td>10</td>
<td>20</td>
<td>18 752</td>
</tr>
<tr>
<td>15</td>
<td>50</td>
<td>115 125</td>
</tr>
<tr>
<td>20</td>
<td>110</td>
<td>378 099</td>
</tr>
<tr>
<td>30</td>
<td>750</td>
<td>5 204 232</td>
</tr>
</tbody>
</table>

![Graph](image.png)

Fig. 5. Effects of compression for bubble sort with \( n = 20 \)

The latter stage involved a number of hierarchical compressions, as outlined in Section 5. We list the execution time in minutes, the size of the largest generated transition system, and the size of the final transition system. We ran FDR on a Research Machines 2.5 GHz Xeon with 2GB RAM. The results from the tool based on regular expressions were obtained on a SunBlade 100 with 2GB RAM [3]. The results confirm that the two approaches give isomorphic models, where the CSP models have an extra state due to representing termination by a ✓ event.

Further information about minimal model generation for \( n = 20 \) is shown in Figure 5. FDR first produces a transition system for the subprogram which is the scope of the declaration of the local array \( a[] \). Each component of \( a[] \), which are indexed from 0 to 19, is represented by a process which keeps its value, and performs reads and writes to that component. FDR obtains the final model by taking the transition system for the scope of \( a[] \) and composing it (by parallel composition and hiding) with transition systems for the components of \( a[] \) in turn. At each step, compression algorithms are applied. In the figure, we show numbers of states before and after compression, after every two steps.

We expect FDR to perform even better in property verification. For check-
Experimental results for queue minimal model generation with $m = 3$

<table>
<thead>
<tr>
<th>$n$</th>
<th>Time</th>
<th>Model states</th>
<th>Max. states</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>5 sec</td>
<td>70</td>
<td>237</td>
</tr>
<tr>
<td>5</td>
<td>18 sec</td>
<td>1 825</td>
<td>12 351</td>
</tr>
<tr>
<td>10</td>
<td>80 min</td>
<td>442 870</td>
<td>5 225 757</td>
</tr>
</tbody>
</table>

6.2 An abstract data type implementation

Figure 6 contains an implementation of a queue of maximum size $n$ as a circular array. There are four free identifiers: commands `empty()` and `overflow()`, expression $p$ of integers type modulo $m$, and command `ANALYSE` which takes two arguments. After implementing the queue by a sequence of local declarations, we export the functions `add` and `next` by calling `ANALYSE` with arguments `add(p)` and `next()`. Game semantics will therefore give us a model which contains all interleavings of calls to `add(p)` and `next()`, corresponding to all possible behaviours of the non-local function `ANALYSE`. Since the expression $p$ is also non-local, the value of $p$ can be different each time `add` is called. The queue implementation uses the non-local commands `empty()` and `overflow()` for handling calls to `next` on the empty queue, respectively `add` on a full queue.

A transition system of the model CSP process for a data set of size $m = 1$ and maximum queue size $n = 2$ is shown in Figure 7. For clarity, labels `ADD` and `NEXT` are used instead of `ANALYSE.1` and `ANALYSE.2`.

Table 2 contains results for minimal model generation for a data set of size $m = 3$ and several maximum queue sizes. For maximum size $n = 10$, further information is displayed in Figure 8. Similar to the corresponding figure for the bubble-sort example, we show numbers of states before and after compression, when transition systems for components of the local array `buffer[]` are composed in turn with the transition system for the rest of the program.

Using the techniques in Section 4, we can check a range of properties of the queue implementation. For example, linear temporal logic formulas $\neg \Diamond \text{overflow}$ and $\neg \Diamond \text{empty}$ assert that the non-local commands handling writes to full queues and reads from empty queues are never called. As expected, checking them returns that they are not satisfied. Counter-example traces which the FDR debugger gives correspond to $n + 1$ consecutive calls of `ADD` after which `overflow` is called, and a single `NEXT` call after which `empty` is called.
empty() : comm,
overflow() : comm,
p : exp int\textsubscript{m},
\textsc{analyse}(comm, exp int\textsubscript{m}) : comm +
new int\textsubscript{m} buffer\{n\} in
new int\textsubscript{n} front in
new int\textsubscript{n} tail in
new int\textsubscript{n+1} queue\_size in
let exp bool isempty() \{ return queue\_size == 0; \} in
let exp bool isfull() \{ return queue\_size == n; \} in
let comm add(exp int\textsubscript{m} x) \{
  if (isfull()) overflow();
  else {
    buffer[tail] := x;
    tail := tail + 1;
    queue\_size := queue\_size + 1;
  }
\} in
let exp int\textsubscript{m} next() \{
  if (isempty()) {
    empty();
    return 0;
  } else {
    front := front + 1;
    queue\_size := queue\_size - 1;
    return buffer[front - 1];
  }
\} in
\textsc{analyse}(add(p), next())
: comm

Fig. 6. A queue implementation

Fig. 7. Transition system of the model for \(n = 2\) and \(m = 1\)

Specifically, the CSP process \(P_{\Sigma, empty}^\Sigma\), where \(\Sigma\) is the alphabet of events for the queue implementation term, is equivalent to

\[
\mu p \cdot (?w : \Sigma \setminus \{\text{empty}\} \rightarrow p) \parallel \text{SKIP}
\]
Checking the traces refinement (2) on FDR produces the following counterexample trace:

1. Q.run
2. ANALYSE.0.Q.run
3. NEXT.Q.q
4. empty.0.run
5. empty.0.done

6. NEXT.A.0
7. ANALYSE.0.A.done
8. A.done
9. ✓

Table 3 shows some experimental results for checking the two formulas. We compared refinement checking without first generating a minimal model against refinement checking preceded by minimal model generation. In the former case, compressions are not applied when components of the array buffer are composed with the rest of the program. Instead, a composite model is generated on-the-fly during refinement checking. This enabled us to check the two properties up to maximum queue size \( n = 13 \), whereas minimal model generation did not succeed for \( n > 10 \). The times shown are sums of times which FDR took to process the specification, to process the implementation, and to perform the refinement check.

In addition to checking properties of external behaviours of given terms, we can check assertions which refer to internal data. Assertions can be added to a term using a local function assert whose argument is a boolean expression. If the argument is true, the assert function does nothing, but otherwise it calls
a non-local function \textit{error}. In the game semantics of the augmented term, any occurrence of events \textit{error.0.run} and \textit{error.0.done} represents an assertion violation.

For example, we can check that whenever a value \( y \) is added to the queue, and then all items except one are removed from the queue, the remaining item has value \( y \). We do this by replacing the call of the \textit{ANALYSE} function in Figure 6 by the following code:

\begin{verbatim}
let comm assert(exp bool b) { 
  if b then skip;
  else error();
} in
let exp bool validate() { 
  new int%n y in 
  y = p;
  add(y);
  while (queue_size > 1) 
    next();
  return (next() == y);
} in
ANALYSE(add(p), next(), assert(validate()))

\end{verbatim}

where \textit{error()} and \textit{ANALYSE(comm, int%n, comm)} are non-local commands.

We then check whether this modified queue implementation satisfies \( \neg \Diamond \text{error} \). We performed this on FDR for a data set of size \( m = 2 \) and for maximum queue size \( n = 2 \). As expected, a counter-example trace was produced, showing that this particular assertion is violated after \( n \) calls of \textit{ADD}, i.e. when the queue is full. When the assertion is corrected so that it applies only to non-full queues, the check succeeds.

7 Conclusion

In this paper, we extended the approach to software model checking proposed in [7] to checking properties given as formulas of linear temporal logic or as finite automata, and we evaluated it on two kinds of example: a sorting algorithm, and an abstract data type implementation.

The experimental results show that open program fragments with large internal state spaces can be verified, partly due to efficiency of the FDR tool for on-the-fly checking of parallel networks of processes. They also show that this approach can outperform the approach based on regular expressions [3].

As future work, we intend to extend the compiler so that parameterised program terms (such as parametrically polymorphic programs) are translated to single parameterised CSP processes. Such processes could then be analysed by techniques which combine CSP and data specification formalisms (e.g. [8,13]) or by algorithms based on data independence [11].
References


A Processes for terms

Expression constructs

\[ [\Gamma \vdash v : \text{exp}[\tau]]^{CSP} = Q.q \rightarrow A.v \rightarrow \text{SKIP}, \ v \in A \tau \text{ is a constant} \]

\[ [\Gamma \vdash \text{not } B : \text{exp[bool]}]^{CSP} = \]
\[ [\Gamma \vdash B : \text{exp[bool]}]^{CSP} \ || \]
\[ [\Gamma \vdash B : \text{exp[bool]}]^{CSP} \ || \]
\[ [Q_1/Q, A_1/A] \ ]
\[ \{Q_1, A_1\} \]
\[ (Q.q \rightarrow Q_1.q \rightarrow A_1?v : A \rightarrow A.(\text{not } v) \rightarrow \text{SKIP}) \ \{Q_1, A_1\} \]

\[ [\Gamma \vdash E_1 \cdot E_2 : \text{exp[\tau]}]^{CSP} = \]
\[ [\Gamma \vdash E_1 : \text{exp[\tau]}]^{CSP} \ || \]
\[ [\Gamma \vdash E_2 : \text{exp[\tau]}]^{CSP} \ || \]
\[ [Q_1/Q, A_1/A] \ ]
\[ \{Q_1, A_1\} \]
\[ (Q.q \rightarrow Q_1.q \rightarrow A_1?v_1 : A \rightarrow Q_2.q \rightarrow A_2?v_2 : A \rightarrow A.(v_1 \cdot v_2) \rightarrow \text{SKIP}) \ \{Q_2, A_2\} \]
\[ \{Q_1, A_1\} \]

\[ [\Gamma \vdash t : \text{exp[\tau]}]^{CSP} = Q.q \rightarrow t.Q.q \rightarrow t.A?v : A \rightarrow A.v \rightarrow \text{SKIP} \]

Command constructs

\[ [\Gamma \vdash \text{skip : comm}]^{CSP} = Q.\text{run} \rightarrow A.\text{done} \rightarrow \text{SKIP} \]

\[ [\Gamma \vdash \text{diverge : comm}]^{CSP} = \text{STOP} \]

\[ [\Gamma \vdash C \parallel M : \sigma]^{CSP} = \]
\[ [\Gamma \vdash C : \text{comm}]^{CSP} \ || \]
\[ [\Gamma \vdash M : \sigma]^{CSP} \ || \]
\[ [Q_1/Q, A_1/A] \ ]
\[ \{Q_1, A_1\} \]
\[ [Q_2/Q, A_2/A] \ ]
\[ \{Q_2, A_2\} \]
\[ (Q.q : Q.q \rightarrow Q_1.\text{run} \rightarrow A_1.\text{done} \rightarrow Q_2.q \rightarrow A_2?a : A_a \rightarrow A.a \rightarrow \text{SKIP}) \]
\[ \{Q_2, A_2\} \ \{Q_1, A_1\} \]

16
$$\llbracket \Gamma \vdash \text{if } B \text{ then } M_1 \text{ else } M_2 : \sigma \rrbracket_{\text{CSP}} =$$

$$\llbracket \Gamma \vdash B : \text{exp[bool]} \rrbracket_{\text{CSP}} [Q_0 / Q, A_0 / A]_{\{Q_0, A_0\}} \parallel$$

$$\left( \left( \llbracket \Gamma \vdash M_1 : \sigma \rrbracket_{\text{CSP}} [Q_1 / Q, A_1 / A] \square \text{SKIP} \right)_{\{Q_1, A_1\}} \right) \parallel$$

$$\left( \left( \llbracket \Gamma \vdash M_2 : \sigma \rrbracket_{\text{CSP}} [Q_2 / Q, A_2 / A] \square \text{SKIP} \right)_{\{Q_2, A_2\}} \right) \parallel$$

$$(Q?q : Q_0.q \rightarrow A_0?v : A_\text{bool} \rightarrow (Q_1.q \rightarrow A_1?a : A_\sigma \rightarrow A.a \rightarrow \text{SKIP}) <$ v $\rightarrow Q_2.q \rightarrow A_2?a : A_\sigma \rightarrow A.a \rightarrow \text{SKIP}))$$

$$\backslash \{Q_2, A_2\} \backslash \{Q_1, A_1\} \backslash \{Q_0, A_0\}$$

$$\llbracket \Gamma \vdash \text{while } B \text{ do } C : \text{comm} \rrbracket_{\text{CSP}} =$$

$$\left( \left( \mu p'.(\llbracket B : \text{comm} \rrbracket_{\text{CSP}} [Q_1 / Q, A_1 / A] \triangleright p') \square (A.\text{done} \rightarrow \text{SKIP}) \right)_{\{Q_1, A_1, A\}} \right) \parallel$$

$$\left( \left( \mu p''.(\llbracket C : \text{comm} \rrbracket_{\text{CSP}} [Q_2 / Q, A_2 / A] \triangleright p'') \square (A.\text{done} \rightarrow \text{SKIP}) \right)_{\{Q_2, A_2, A\}} \right) \parallel$$

$$(Q.\text{run} \rightarrow \mu p.Q_1.q \rightarrow A_1?v : A_\text{bool} \rightarrow (Q_2.\text{run} \rightarrow A_2.\text{done} \rightarrow p \ll v \gg A.\text{done} \rightarrow \text{SKIP}) \backslash \{Q_2, A_2\} \backslash \{Q_1, A_1\}$$

$$\llbracket \Gamma \vdash \iota : \text{comm} \rrbracket_{\text{CSP}} = Q.\text{run} \rightarrow \iota.Q.\text{run} \rightarrow \iota.A.\text{done} \rightarrow A.\text{done} \rightarrow \text{SKIP}$$

**Variable constructs**

$$\llbracket \Gamma \vdash \iota : \text{var[\tau]} \rrbracket_{\text{CSP}} =$$

$$(Q.\text{read} \rightarrow \iota.Q.\text{read} \rightarrow \iota.A?v : A_\tau \rightarrow A.v \rightarrow \text{SKIP}) \square$$

$$(Q.\text{write}?v : A_\tau \rightarrow \iota.Q.\text{write}.v \rightarrow \iota.A.ok \rightarrow A.ok \rightarrow \text{SKIP})$$

$$\llbracket \Gamma \vdash V := M : \text{comm} \rrbracket_{\text{CSP}} =$$

$$(\llbracket \Gamma \vdash M : \text{exp[\tau]} \rrbracket_{\text{CSP}} [Q_1 / Q, A_1 / A]_{\{Q_1, A_1\}} \parallel$$

$$(\llbracket \Gamma \vdash V : \text{var[\tau]} \rrbracket_{\text{CSP}} [Q_2 / Q, A_2 / A]_{\{Q_2, A_2\}} \parallel$$

$$(Q.\text{run} \rightarrow Q_1.q \rightarrow A_1?v : A_\tau \rightarrow Q_2.\text{write}.v \rightarrow A_2.ok \rightarrow A.\text{done} \rightarrow \text{SKIP}) \backslash \{Q_2, A_2\} \backslash \{Q_1, A_1\}$$

$$\llbracket \Gamma \vdash V : \text{exp[\tau]} \rrbracket_{\text{CSP}} =$$

$$(\llbracket \Gamma \vdash V : \text{var[\tau]} \rrbracket_{\text{CSP}} [Q_1 / Q, A_1 / A]_{\{Q_1, A_1\}} \parallel$$

$$(Q.q \rightarrow Q_1.\text{read} \rightarrow A_1?v : A_\tau \rightarrow A.v \rightarrow \text{SKIP}) \backslash \{Q_1, A_1\}$$
\[ [\Gamma \vdash \text{new}_{\tau} \ i \ in \ M : \text{comm}]^{\text{CSP}} = \\
(\forall_{\{l, r\}}^{\text{CSP}} \ 	ext{U}_{\text{var}[\tau], v} \ 	ext{\{l\}}) \text{\{r\}} \]

where \( a_{\text{int}} = 0 \), \( a_{\text{bool}} = \text{false} \), and:
\[ U_{\text{var}[\tau], v} = (\ i. Q.\text{read} \rightarrow i. A!v \rightarrow U_{\text{var}[\tau], v} ) \square \]
\[ (i. Q.\text{write?} v' : A_r \rightarrow i. A. ok \rightarrow U_{\text{var}[\tau], v'} ) \square \]
\[ (A.\text{done} \rightarrow \text{SKIP} ) \]

**Application and functions**

\[ [\Gamma \vdash \tau(M_1 \ldots M_k) : \sigma]^{\text{CSP}} = \tau?q : Q_r \rightarrow \tau.0.Q.q \rightarrow \\
(\forall_{\{Q, A\}}^{\text{CSP}} \ 	ext{L}_{i,j}^{\text{CSP}} \ 	ext{\{Q, A\}} \{L\} \square \text{SKIP} ) \{L\} \tau.0.A.a : A_\sigma^0 \rightarrow A.a \rightarrow \text{SKIP} \]

\[ [\Gamma \vdash \text{let} \ i(t_1 : \sigma_1, \ldots, t_k : \sigma_k) \in M : \sigma]^{\text{CSP}} = \\
(\forall_{\{l, r\}}^{\text{CSP}} \ 	ext{N}_{i.0.Q/t_1, \ldots, t.k/t_k, A/A} \{l\} \square \text{SKIP} ) \{r\} \]

\[ \text{\{l\}} \text{\{r\}} \]

**B Processes for formulas**

We show how, given any formula \( \phi \) of LTL\( _f^\Sigma \), to construct:

- a CSP process \( P_\phi^\Sigma \) such that \( t \models \phi \) if and only if \( t^\land V \) \( \in \text{traces}(P_\phi^\Sigma) \);
- a finite transition system which has the same finite traces as \( P_\phi^\Sigma \).

Consider the following variant of LTL\( _f^\Sigma \), where only atoms can be negated, and operators \( \land, \lor \) and \( V \) are basic rather than derived. We call it LTL\( _f^+\Sigma \).

\[ \phi ::= \text{true} | \text{false} | a | \neg a | \phi_1 \lor \phi_2 | \phi_1 \land \phi_2 | \bigcirc \phi | \bigcirc \phi | \phi_1 U \phi_2 | \phi_1 V \phi_2 \]

Any formula \( \phi \) of LTL\( _f^\Sigma \) can be transformed into an equivalent formula \( \phi' \) of LTL\( _f^+\Sigma \), since \( \land, \lor \) and \( V \) are duals of \( \lor, \land \) and \( U \). The size of \( \phi' \) is linear in the size of \( \phi \).

For formulas \( \phi \) of LTL\( _f^+\Sigma \), we define CSP processes \( P_\phi^\Sigma \) as follows, by structural recursion on \( \phi \):
\[ P_{true}^\Sigma = RUN_\Sigma^\phi \]
\[ P_{false}^\Sigma = STOP \]
\[ P_a^\Sigma = a \rightarrow RUN_\Sigma^\phi \]
\[ P_{\neg a}^\Sigma = \neg w : \Sigma \rightarrow RUN_\Sigma^\phi \]
\[ P_{\phi_1 \lor \phi_2}^\Sigma = P_{\phi_1}^\Sigma \boxdot P_{\phi_2}^\Sigma \]
\[ P_{\phi_1 \land \phi_2}^\Sigma = P_{\phi_1}^\Sigma \boxor P_{\phi_2}^\Sigma \]
\[ P_{\bigcirc \phi}^\Sigma = \neg w : \Sigma \rightarrow P_{\phi}^\Sigma \]
\[ P_{\bigcirc \phi}^\Sigma = (\neg w : \Sigma \rightarrow P_{\phi}^\Sigma) \Box SKIP \]
\[ P_{\phi_1 V \phi_2}^\Sigma = \mu p \cdot (P_{\phi_2}^\Sigma \Box (\neg w : \Sigma \rightarrow RUN_\Sigma^\phi)) \Box (P_{\phi_1}^\Sigma \Box (\neg w : \Sigma \rightarrow p)) \]
\[ P_{\phi_1 V \phi_2}^\Sigma = \mu p \cdot (P_{\phi_2}^\Sigma \Box (\neg w : \Sigma \rightarrow RUN_\Sigma^\phi)) \Box (P_{\phi_2}^\Sigma \Box (\neg w : \Sigma \rightarrow p)) \Box SKIP \]

where \( RUN_\Sigma^\phi = (\neg w : \Sigma \rightarrow RUN_\Sigma^\phi) \Box SKIP \).

Now, for any formula \( \phi \) of \( \text{LTL}_j^\Sigma \), we define \( P_{\phi}^\Sigma = P_{\phi'}^\Sigma \), where \( \phi' \) is the equivalent formula of \( \text{LTL}_j^\Sigma \).

**Proposition B.1**  For any formula \( \phi \) of \( \text{LTL}_j^\Sigma \), we have that \( t \models \phi \) if and only if \( t \uparrow (\square \phi) \in \text{traces}(P_{\phi}^\Sigma) \), and a finite transition system which has the same finite traces as \( P_{\phi}^\Sigma \) can be constructed.

**Proof.** It suffices to prove the proposition for formulas \( \phi \) of \( \text{LTL}_j^\Sigma \). The proof is by structural induction on \( \phi \).

We show only the most involved case, where \( \phi = \phi_1 V \phi_2 \). Since
\[ P_{\phi_1 V \phi_2}^\Sigma = \mu p \cdot (P_{\phi_2}^\Sigma \Box (\neg w : \Sigma \rightarrow RUN_\Sigma^\phi)) \Box (P_{\phi_2}^\Sigma \Box (\neg w : \Sigma \rightarrow p)) \Box SKIP \]

we have:

\[ t \uparrow (\square \phi) \in \text{traces}(P_{\phi_1 V \phi_2}^\Sigma) \]

iff \( (\forall i \in \{1, \ldots, |t| \} \cdot t_i \uparrow (\square \phi) \in \text{traces}(P_{\phi_2}^\Sigma)) \lor \)
\[ \big( \exists i \in \{1, \ldots, |t| \} \cdot t_i \uparrow (\square \phi) \in \text{traces}(P_{\phi_2}^\Sigma) \cap \text{traces}(P_{\phi_1}^\Sigma) \land \forall j \in \{1, \ldots, i - 1 \} \cdot t_j \uparrow (\Diamond \phi_1) \in \text{traces}(P_{\phi_1}^\Sigma) \big) \]

iff \( (\forall i \in \{1, \ldots, |t| \} \cdot t_i \models \phi_2) \lor \)
\[ \big( \exists i \in \{1, \ldots, |t| \} \cdot t_i \models \phi_1 \land \forall j \in \{1, \ldots, i \} \cdot t_j \models \phi_2 \big) \]

iff \( t \models \phi_1 V \phi_2 \)

Let \( S_1 \) and \( S_2 \) be finite transition systems which have the same finite traces as \( P_{\phi_1}^\Sigma \) and \( P_{\phi_2}^\Sigma \), respectively. From \( S_1 \) and \( S_2 \), operational semantics of CSP
[15] gives us a transition system $S'$ with the same finite traces as $P^{\Sigma}_{\phi_1 V \phi_2}$.

Any node of $S'$ is of one of the following forms:

$$Q_1^1 \parallel \cdots \parallel Q_k^1 \parallel P^\Sigma_{\phi_1 V \phi_2},$$

$$Q_1^2 \parallel \cdots \parallel Q_k^2 \parallel Q_1^1 \parallel P^\Sigma_{\phi_1 V \phi_2},$$

$$\left( (Q_1^{k+1} \parallel Q_1^1 \parallel (?w : \Sigma \rightarrow RUN_\Sigma^*) \diamond \Box \right),$$

$$\left( (Q_1^{k+2} \parallel (?w : \Sigma \rightarrow P^\Sigma_{\phi_1 V \phi_2}) \diamond \Box SKIP \right),$$

$$Q_1^2 \parallel \cdots \parallel Q_k^2 \parallel Q_1^1 \parallel RUN_\Sigma^*,$$

$$Q_1^2 \parallel \cdots \parallel Q_k^2 \parallel Q_1 \parallel \Omega,$$

$$Q_1^2 \parallel \cdots \parallel Q_k^2 \parallel \Omega,$$

where $k \geq 0$, $Q_1$ is a node of $S_1$, $Q_2^i$ are nodes of $S_2$, and $\Omega$ is the state after termination.

Let $S$ be the transition system constructed in the same way as $S'$, except whenever a node as above is to be generated, if there already is a node which is the same subject to permuting $Q_2^1, \ldots, Q_2^k$ and removing duplicates, then that node is used instead. Since the set of all nodes of $S_2$ has finitely many subsets, this procedure terminates, and produces a finite transition system. As $\parallel$ is an associative, commutative and idempotent operator on sets of finite traces, $S$ has the same finite traces as $S'$. \qed