From Operational to Declarative Specifications using a Genetic Algorithm

Facundo Molina
Dept. of Computer Science, University of Rio Cuarto, Argentina

Renzo Degiovanni
Dept. of Computer Science, University of Rio Cuarto, Argentina

Germán Regis
Dept. of Computer Science, University of Rio Cuarto, Argentina

Pablo Castro
Dept. of Computer Science, University of Rio Cuarto, Argentina

Nazareno Aguirre
Dept. of Computer Science, University of Rio Cuarto, Argentina

Marcelo Frias
Dept. of Software Engineering, Buenos Aires Institute of Technology, Argentina

ABSTRACT

In specification-based test generation, sometimes having a formal specification is not sufficient, since the specification may be in a different formalism from that required by the generation approach being used. In this paper, we deal with this problem specifically in the context in which, while having a formal specification in the form of an operational invariant written in a sequential programming language, one needs, for test generation, a declarative invariant in a logical formalism. We propose a genetic algorithm that given a catalog of common properties of invariants, such as acyclicity, sortedness and balance, attempts to evolve a conjunction of these that most accurately approximates an original operational specification. We present some details of the algorithm, and an experimental evaluation based on a benchmark of data structures, for which we evolve declarative logical invariants from operational ones.

1 INTRODUCTION

Various approaches to automated test generation require a specification in order to automatically generate tests or test inputs. Examples of these are test generation tools based on symbolic or concolic execution [10, 17], tools that generate inputs from program invariants [2, 9], and tools that combinatorially generate inputs and use specifications for filtering [7]. However, not all tools use the same specification formalism; some tools require specifications to be given as operational predicates, i.e., as program routines in a programming language [2, 10] (e.g., so called repOK routines are class invariants captured operationally through a program); others support constraints in a logical formalism [5, 9]; and a few are able to combine different formalisms [4, 7, 15].

An issue that arises with the availability of multiple specification formalisms is that many times one does count with a specification, but this specification is not provided in the right language for the use of a given test generation approach. For instance, one may have a class invariant for a given Java class, written as a repOK routine, but in order to use, say a SAT-solving based generation mechanism, such invariant has to be somehow translated to an appropriate logical formalism. This is particularly relevant with the increasing growth of tools and techniques for program analysis, and the potential combined use of these tools, which may be inhibited by the “mismatch” in the specification styles required by the tools involved. A concrete example of this situation can be observed, for instance, in bounded lazy initialization with SAT support [16], where a combination of symbolic execution and SAT solving requires the user to provide two equivalent program invariants, one given as a repOK routine (used for lazy initialization), and the other as a logical specification (used for computing bounds and pruning symbolic execution).

This is exactly the problem we are interested in, in this paper. The problem is relevant because even in the case in which a translation from one formalism to the other is available, the “target” specifications resulting from the translations may be unsuitable for analysis reasons. For example, one can indeed translate a Java repOK routine into Alloy’s relational logic [8], through the use of translations that capture programming language constructs in the logic, as those embedded in some program analysis tools [3, 5]. But the obtained logical formulas (that capture program executions) lead to unacceptable performances if these are used for test generation.

To deal with the above situation, we propose a genetic algorithm, that given a catalog of properties commonly used as part of invariants, such as acyclicity, sortedness and balance, appropriately specified in relational logic, attempts to evolve the conjunction of these that most accurately approximates an original operational specification, given as a repOK routine. We present some details of the algorithm, and an experimental evaluation based on a benchmark of data structures, for which we evolve declarative logical invariants from operational ones. The experiments show that declarative invariants that very precisely approximate provided operational ones can be efficiently produced.
2 MOTIVATION

To motivate our approach, let us consider an implementation of lists given as heap allocated doubly linked lists, as shown in Figure 1. Suppose that we are interested in testing that a routine that manipulates such data structure, for example the insertion routine, works as expected, or in particular, that it preserves the representation invariant of doubly linked lists. To perform automated testing in this context, we would need a specification establishing when a given list is valid, both to be used for assertions in tests, as for automatically producing test inputs satisfying such specification. As put forward in [10], one can specify the representation invariant as a boolean routine, the repOK(), that returns true iff the structure it is applied to satisfies the corresponding representation invariant. In the case of doubly linked lists, this routine, shown in Figure 2, must state two points: first, header holds a cyclic linked list, and second, the number of nodes in the list coincides with the value in field size.

Some test generation tools, notably those based on constraint-solving [5, 9], can profit from specifications written in a logical formalism, in contrast with the previously mentioned operational repOK routines. Indeed, some constraint-solving based approaches can more efficiently generate test inputs if invariants are given in a declarative formalism like JML or Alloy [8]. These languages offer a different specification “paradigm”, and properties such as reachability, (acyclic)ity and the like, are typically captured through some transitive closure expressions. As an example, Figure 3 shows a declarative predicate, in Alloy’s relational logic, that expresses an invariant equivalent to property repOK() of Figure 2.

![Java classes defining doubly linked lists](image)

Having the operational invariant specified through routine repOK() enables the use of various tools for test generation that expect this kind of property (e.g., Korat [2], where the doubly linked list example was taken from, in one such tool). But if we need to use a tool that expects the specification to be given declaratively (e.g., those in [1, 9]), our repOK is of little use. Even though one may employ a translation from operational specifications into declarative specifications (in bounded contexts), like those provided in tools like TACO [5, 6] and CBMC [11], the obtained specifications are in general unsuitable for analysis. In particular, the excessive use of quantifiers to capture program executions lead to specifications that are very costly to compile, that many times do not pass, in the context of SAT-based test generation, the CNF generation phase.

The following section will describe our proposal to tackle this problem, which in essence consists of taking a catalog of properties that are commonly part of invariant specifications, appropriately characterized in the target formalism (in our case, Alloy’s relational logic), and using a genetic algorithm to evolve an expression (a conjunction in our case) involving properties from the catalog, that more closely approximate a given operational invariant.

3 THE GENETIC ALGORITHM

As we mentioned in previous sections, our objective is to generate a declarative specification $\Phi$ that most accurately approximates an operational specification $\Phi_{op}$, by combining common invariant properties taken from a catalog. Below we describe the main components of the genetic algorithm designed for this purpose.

3.1 Genes and Chromosomes for Candidate Specifications

In order to capture candidate specifications, we simply define chromosomes as vectors of integer genes. Each chromosome has as many genes as there are properties in the catalog, and the value of each gene can be 0, 1 or 2. If the $i$-th gene has value 0, then the $i$-th formula of the catalog is negated; if the gene has value 1, then

```
public boolean repOK() {
    Set visited = new java.util.HashSet();
    visited.add(header);
    Entry current = header;
    while (true) {
        Entry next = current.next;
        if (next == null) return false;
        if (next.previous != current) return false;
        current = next;
        if (!visited.add(next)) break;
        if (current != header) return false;
        if (visited.size() != size) return false;
        return true;
    }
    Figure 2: Operational version of the representation invariant for doubly linked lists.

    one sig Null { }
    sig List { }
    sig Node { }
        (all n: thiz.header.*(next+prev) | n.prev.next) and 
        #(thiz.header.*(next+prev)-Null) = thiz.size
    }
    Figure 3: Declarative version of the representation invariant for doubly linked lists, in Alloy’s relational logic.
```
the i-th formula is considered positively; finally, if the gene has
value 2, then the i-th formula is disabled (not part of the candidate
specification). Thus, the candidate specification represented by a
given chromosome is the conjunction of the formulas obtained from
the interpretation of the genes, depending on their respective values.
For instance, if the catalog is composed by the (ordered) set of
formulas \{f_0, f_1, f_2, f_3, f_4\}, then chromosome [0, 1, 2, 0, 2] will
represent the specification \(\neg f_0 \land f_1 \land \neg f_2\).

In our experiments, the initial population is produced by generat- ing
all individuals with exactly one positive gene (value 1), and all
the others disabled (value 2). That is, we initially have as many
individuals as specifications in the catalog. The maximum size for
the population is set to 100.

3.2 Genetic Operators

Genetic operators are used to produce the search space, by generat- ing new individuals from existing ones in a population. The main
mechanism to achieve this is by combining parts of existing
chromosomes through \textit{crossover}. We use one-point crossover to
build new chromosomes, by randomly selecting a point to “split”
two chromosomes, and combining the initial (resp., final) part of
one of them with the final (resp., initial) part of the other. In our
experiments, we use a crossover rate of 35%.

The second mechanism to generate new chromosomes is \textit{muta}-
tion, i.e., the generation of a new individual by randomly changing
characteristics of an existing one. Since in our case genes only have
three possible values (0, 1 or 2), our mutation operator simply ran-
domly sets a value in the range [0, 2] of each gene to be mutated.

3.3 Fitness of Candidate Specifications

Our fitness function is meant to assess how close are the corre-
sponding candidates to the desired specification, and is the most
important part of our algorithm. We exploit the operational specifi-
cation \(\Phi_{op}\), to (indirectly) compare candidate specifications against
this one. In order to do so, we automatically generate from \(\Phi_{op}\)
a set of \textit{positive and negative} examples. These are instances that
satisfy and do not satisfy \(\Phi_{op}\), respectively. These instances can be
generated using any test input generation mechanism that requires
an operational specification, e.g., [2]. We use an ad hoc variant of
Korat, that generates inputs using that “cover” different values for
object fields. The number of generated positive and negative cases
is limited to a provided bound \(k\).

Fitness \(f(c)\) for a chromosome \(c\) is computed as follows. First, we
build the specification \(\Phi_c\) corresponding to \(c\), and evaluate whether
the positive and negative cases satisfy \(\Phi_c\). If any positive case fails
with \(\Phi_c\), meaning that there are cases that should be accepted
but our specification rejects them, then \(f(c) = 0\). Instead, if the
candidate has only negative cases (cases that should not pass the
specification but do so), fitness is defined as follows:

\[
f(c) = (\text{MAX} - \text{neg}(c)) + \left(\frac{1}{\text{len}(\text{spec}(c)) + 1}\right)
\]

where \(\text{MAX}\) is a constant larger than \(k\), the total number of negative
cases; \(\text{neg}(c)\) is the number of negative cases that satisfy \(\Phi_c\); and
\(\text{len}(\text{spec}(c))\) is the length of \(c\), i.e., the number of formulas from
the catalog present in the conjunction.

The rationale for this definition of the fitness function has to do
with the fact that we attempt to over approximate the sought-for
specification. Thus, when a positive case is not accepted by a can-
didate, we will simply consider it unfit. Fitness for other candidates
has two parts. First, the fewer the “counterexamples”, the better;
second, the smaller the specification, the better. This last part can
be thought of as a penalty related to formula length, that will make
the genetic algorithm tend towards producing smaller formulas.

3.4 Selection

The selection operation determines which individuals are to be kept
in the next generation. Our selection operation is very simple. It
maintains a predefined amount of the fittest individuals by sorting
all the chromosomes by decreasing order according to their fitness
values, and then selecting the top individuals. This simple selection
mechanism results useful in our problem since the algorithm will
tend to keep the chromosomes representing specifications contain-
ing formulas with less negative cases that do not satisfy \(\Phi_{op}\) (recall
that the higher the fitness value, the fewer counterexamples the
formula has).

4 EVALUATION

Our evaluation is based on invariants of the following data struc-
tures taken from Korat’s case studies: singly linked lists; sorted
singly linked lists; circular linked lists; doubly linked lists; binary
trees; binary search trees; heaps; (binary) directed acyclic graphs;
and red-black trees. The genetic algorithm has been implemented
using JGAP, and the experiments were run on a workstation with
Intel Core i7 2600, 3.40 Ghz, and 16Gb of RAM. The catalog for our
genetic algorithm is composed of properties commonly found in
invariants, with distinguishing cases for linear structures (struc-
tures with a single reference field per node) and n-ary (tree-like)
structures (e.g., binary trees). More precisely, for linear structures
we considered 23 properties, including (acyclicity, circularity, etc.,
the relationship between number of reachable nodes and integer-
typed fields, and ordering constraints. For n-ary structures, on the
other hand, we considered 28 properties, including all of the linear
cases, and other properties such as disjointness across different
fields, balance, etc.

For each case study, we ran the algorithm 10 times, with a limit
of 20 generations (i.e., evolutions of the genetic algorithm popula-
tion). Table 1 reports the minimum, maximum and average runs,
indicating the number of generations (\(g\)) and the time (\(t\)) in seconds,
that were necessary to obtain declarative invariants. We distinguish
between the cost of computing the first suitable invariant, and the
cost of computing the "best" invariant (the algorithm continues
running, trying to make it more concise). In all these cases the
obtained invariants were indeed \textit{equivalent} to their corresponding
operational ones. Some results were surprising, e.g., an acyclic
property indirectly captured via cardinality constraints:

\[
\text{(thiz.size = # thiz.head.*next - Null)}\quad \text{and} \quad \text{(thiz.size = # thiz.head.*next)}
\]

5 RELATED WORK AND CONCLUSION

The problem of automatically producing specifications has been
extensively studied. In the context of Alloy, the approach in [13]
Table 1: Experimental Results corresponding to learning declarative invariants from operational ones, using our evolutionary algorithm.

<table>
<thead>
<tr>
<th>Data Structure</th>
<th>First Invariant Found</th>
<th>Best Invariant Found</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Min Gen</td>
<td>Sec.</td>
</tr>
<tr>
<td>s. linked lists</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>s. linked sort. lists</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>s. circular lists</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>doubly linked lists</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>binary trees</td>
<td>3</td>
<td>35</td>
</tr>
<tr>
<td>binary search trees</td>
<td>3</td>
<td>14</td>
</tr>
<tr>
<td>heaps</td>
<td>6</td>
<td>39</td>
</tr>
<tr>
<td>binary DAGs</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>red-black trees</td>
<td>7</td>
<td>95</td>
</tr>
</tbody>
</table>

is based solely on positive examples, as opposed to our case. The work in [14] also uses genetic algorithms, but attempts to evolve navigational expressions, as opposed to our (simpler) case based on a specification catalog. Our approach is easier to extend to support new properties, a limitation of [14].

In summary, we have presented an approach to compute a declarative specification in Alloy’s relational logic from an operational one in Java, based on a genetic algorithm. The approach considers a catalog of common invariant properties and tries to achieve a conjunction of these that approximates the original invariant. It produces valid and invalid cases from the operational specification, which are then used as part of the fitness function driving the algorithm, to “grade” specification candidates. Our preliminary experimental evaluation shows promising results.

We plan to further develop our approach, and in particular to search for more general specification patterns to consider in specification catalogs. We also plan to incorporate our operational-to-declarative translation mechanism in the context of BLISS [16], to simplify the requirements for users of the technique to only providing an operational invariant.

REFERENCES


