This is the accepted version of a paper presented at 30th Int. Conf. on Automated Software Engineering (ASE 2015).

Citation for the original published paper:


N.B. When citing this work, cite the original published paper.

Permanent link to this version:
http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-199102
import modbat.dsl._

class SimpleListModel extends Model {
  val SUT = new java.util.ArrayList[Integer]()
  var n = 0
  def add {
    val ret = SUT.add(new Integer(choose(0, 10)))
    assert {ret}
    n += 1
  }
  def remove {
    require(n > 0)
    SUT.remove(choose(0, n))
    n -= 1
  }
  def bounds {
    choose{
      [ ] => SUT.remove(-1) ,
      [ ] => SUT.remove(n) 
    }
    "main" => "main" := add weight 10
    "main" => "main" := remove
    "main" => "main" := { assert {SUT.size == n} }
    "main" => "main" := { SUT.clear; n = 0 }
    "main" => "main" := bounds throws("IndexOutOfBoundsException")
  }
}

Figure 2. Simple list model.

include a reference to the SUT and model variables to track
the model’s view of the SUT to verify its results. In this case
the model only keeps track of the expected size of the list.
The model code can also define a number of functions (in the
middle) that can be referenced from the declared transitions
(at the bottom). This example uses only one model state,
main, because most actions are available in any state.1 To use
random data, the model calls Modbat’s choose functions,
which return a random number and a random element in a list
of functions, respectively.

The example shows that test code can be kept in a separate
function or be directly written as an anonymous function. We
can also modify the weight of a transition function; by default
its value is 1. In this example, we emphasize adding elements
by giving more weight to add so calls to clear do not
repeatedly empty the list before several elements can be added.
Finally, we can easily declare that an exception must occur in
a given transition. In this case, calls to remove with index
−1 or n access an entry outside the valid range, so the SUT
is expected to throw a corresponding exception.

B. Key Features of Modbat

Modbat’s light-weight DSL has been inspired by a prepro-
cessor to ModelJUnit [8]. Compared to similar tools, it is more
concise and expressive for models that are based on transition
systems [2], especially for non-deterministic actions like non-
blocking network input/output, where the result of an operation
depends not only on inputs but also on the physical state of
the network [3]. As models are Scala classes, they inherit all
variables, functions, and transitions in a natural way, which
makes Modbat ideal for testing libraries implementing several
related data structures or protocols. Furthermore, the current
version of Modbat introduces observer state machines, similar
to abstract state machines in Spec Explorer [9].

1It is also possible to use multiple states in the model, such as empty and
non-empty, and to define transitions with pre- and postconditions.

In this demonstration, we take advantage of being able
to use multiple models in parallel. Unlike in other tools [9],
the number of parallel models does not have to be fixed a
priori. Instead, models are instantiated dynamically with func-
tion launch, which initializes a new (possibly parametrized)
model. Newly launched models become active at the end of
the current transition.

III. SCENARIO 1: JAVA ITERATORS

The Java library contains collections, data structures for
data types such as lists, sets, and maps [10]. Iterators provide
a way to access elements of a collection one by one.

A. Semantics of the Iterator API

Iterators can be instantiated on an underlying collection
through the methods iterator and listIterator. The
former provides a simple forward iterator (see Table I), while
the latter provides a bidirectional iterator (see Table II) [10].

Java iterators do not allow a concurrent modification of the
underlying collection while iterating on it. Any modification
of the underlying collection invalidates all previously created
iterators on it. Invalid iterators produce an undefined result
for calls to hasNext and similar methods,2 and throw a
ConcurrentModificationException if attempts are
made to access or modify data through them. Through
experiments we confirmed that this exception is usually only
thrown upon a successful modification of the underlying collection.

While directly modifying the collection invalidates all of
its iterators, it is possible to modify data, if the iterator
itself provides a set of optional methods (add, set, and
remove). Such modifications are intricately linked with it-
eration: remove and set both require a preceding call to
either next or previous. Furthermore, calls to remove or
add require another iterator step before remove or set can
be called again. We discuss this property in more depth below.

B. Model of the Iterator API

Our list model closely mirrors Java’s collections but uses
simpler data structures to ensure correctness. We use random
data as items to be added and also add a function to validate
internal model invariants. Modbat’s support for inheritance is
very useful here because ArrayList implements a strict
subset of all operations in LinkedList.\textsuperscript{3} Our generic list model uses the following data structures: testData (the SUT); data, a fixed-size array that models the list contents; n, which counts the number of elements; and version, which counts the number of changes to the collection. We use preconditions to distinguish between cases where a method can be used successfully, and cases where we expect an exception to be thrown. Modbat’s direct support for exceptions in transitions allows us to express these features succinctly [2].

Iterators and list iterator models are instantiated by transitions in the list model that launch a new child model instance, and link it to the resulting iterator that is obtained from the SUT. Each model may affect the collection and/or an iterator (see Figure 3). The iterator models remember the version of the list so the occurrence or absence of a ConcurrentModificationException can be modeled based on whether the version counts of the collection and of the iterator match. Furthermore, we use a state “modifiable” to model whether calls to set and remove are permitted; these calls require a previous call to next or previous, without any other modification in between (see Figure 4).

Other requirements are captured using preconditions and postconditions. We choose to model valid and invalid usage contexts using mutually exclusive preconditions, and verify the correct result using exception declarations and postconditions (see Figure 5; details can be found online [11]).

\textbf{C. Defect Found in Java 1.8}

When running the test model against Java’s list implementation, some tests fail on ArrayList: After a failed remove(-1), the Java library marks the list as modified; subsequent calls to next throw a ConcurrentModificationException (see Figure 6). Other types of failed modifications (such as remove with n > 0) do not mark the list as modified. All other data structures behave consistently in all cases. Modbat finds the problem quickly; Oracle has confirmed the issue as a defect.\textsuperscript{4}

\textsuperscript{3}Some operations are not provided by ArrayList because they cannot be implemented efficiently on arrays.
\textsuperscript{4}https://bugs.openjdk.java.net/browse/JDK-8114832
B. Model-based Testing of SAT Solvers

In previous work, we have presented model-based testing for SAT solvers [13]. To this end, we considered a data model describing expressive random formulas as input as well as a model describing the usage of the API. We presented specific solutions for the SAT solver Lingeling [14], which has always ranked highly in the SAT solver competition because of its sophisticated pruning techniques. In various experiments we showed the power of model-based testing for the SAT solver Lingeling [13]. Those models are very specific to Lingeling, which provides an extensive API and many options, and hence cannot be used for other SAT solvers directly. At that time no standards for incremental SAT solver APIs existed.

This year the SAT competition offers a special track for incremental solving, acknowledging its practical relevance. In this track, submissions include incremental solvers as well as applications which use incremental SAT solvers. To this end, a standardized interface called IPASIR has been specified which the participating SAT solvers have to implement and which can be used by the applications [15]. We contribute to the incremental track of the SAT solver competition by providing a model-based tester for incremental SAT solvers.

We implemented this model-based tester with Modbat by specifying the model shown in Figure 7. The transitions between the states trigger the call of various solver API functions specified by the IPASIR interface. First, the solver is initialized, and then the input formula is generated (left hand side). The input formula consists of unit clauses (clauses of size one), binary clauses, ternary clauses and clauses of arbitrary size. It is important to ensure that the formula contains clauses of size smaller than four because these clauses are often handled in a different manner. The literals and their polarity (negated/not negated) are randomly selected and given to the solver under test. After enough clauses have been generated, the solving function is called. As formulas are generated at random, the outcome of the SAT solver cannot be predicted by the model. The dashed transitions from state `solve` indicate alternative outcomes (un satisfiable formulas or a time-out) overriding the default successor state `sat`, with `unsat` and `inc`, respectively, using `nextIf` statements [2] that specify pairs of predicates and successor states. If we use option `--dotify-coverage`, Modbat indicates that the first five tests generate only unsatisfiable formulas (see Figure 7).

The new model can be used for any solver implementing the IPASIR interface. Therefore, it can be easily integrated in the solver development process. For the competition we suggest to measure the time a solver takes to finish a given number of tests generated from a fixed random seed.

In the provided demo, we test SAT solver PicoSAT [16]. We demonstrate the tests on the original version 961 and a modified version, where we introduced a small bug in a pruning technique called `failed literal probing` (in the faulty version, a literal is not negated). The bug causes the program to crash sporadically. With Modbat this bug can be found quickly. Note that Picosat can be easily exchanged against any incremental SAT solver implementing the IPASIR interface.

V. RELATED WORK

A variety of model-based testing tools with different features and characteristics have been proposed up to now. In a systematic review, Shafique and Labiche [17] identified a total of 46 tools and 2 APIs providing support for model-based testing. Micskei maintains an online overview of model-based testing tools [18]; currently (according to the information last modified in July 2014) the list contains 20 academic, commercial and open source tools plus 13 tools that are not developed anymore. Several tools have features and characteristics that are similar to those of Modbat. To highlight and explain the differences between Modbat and related tools, we selected three widely-known tools for comparison: ModelJUnit [1], ScalaCheck [19] and Spec Explorer [9]. We consider these tools to be representative examples as we have practical experience from applying them in previous projects and since some of their features were a source of inspiration when implementing Modbat. References to further tools are included in the discussion of Modbat’s specific features below.

The underlying modeling approach has a big impact on the implementation and features of the tools. Like in ModelJUnit [1], Modbat’s models are based on extended finite-state machines (EFSMs). Yet there is a wide range of different modeling approaches used by different tools, for example, RT-Tester [20] and MoMuT::UML [21]. Currently, RT-Tester [20] and MoMuT::UML [21] use UML, T-VEC [22] uses models from Simulink, LOTOS, timed automata, etc. Furthermore, TTCN-3 is a popular testing language to model communication systems and protocols, and it is supported by various tools [23].

Compared to other notations, EFSMs are simple but expressive, and can be readily integrated with existing test code...
Table III. CHARACTERISTICS OF RELATED TOOLS.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>input + output</td>
<td>input + output</td>
<td>input + output</td>
<td>input + output</td>
</tr>
<tr>
<td>Characteristic</td>
<td>untimed</td>
<td>untimed</td>
<td>untimed</td>
<td>untimed</td>
</tr>
<tr>
<td>Model specification</td>
<td>non-deterministic</td>
<td>deterministic</td>
<td>deterministic</td>
<td>non-deterministic</td>
</tr>
<tr>
<td>Paradigm</td>
<td>transition-based</td>
<td>transition-based</td>
<td>generator-based</td>
<td>state-based + history-based</td>
</tr>
<tr>
<td>Interface</td>
<td>internal DSL</td>
<td>API</td>
<td>API</td>
<td>external DSL</td>
</tr>
<tr>
<td>Test generation</td>
<td>Test selection criteria</td>
<td>random + stochastic</td>
<td>random + stochastic</td>
<td>structural model coverage + data coverage</td>
</tr>
<tr>
<td>Technology</td>
<td>random + search-based</td>
<td>random + search-based</td>
<td>random + search-based</td>
<td>model checking</td>
</tr>
<tr>
<td>Test execution</td>
<td>Online/offline</td>
<td>online</td>
<td>online</td>
<td>both</td>
</tr>
<tr>
<td>License</td>
<td>base version open source, extended version proprietary</td>
<td>open source</td>
<td>open source</td>
<td>proprietary</td>
</tr>
</tbody>
</table>

Because the DSL or API is hosted by a widely used execution platform (in many cases, the Java VM) [7]. This advantage makes such tools ideally suited to test software directly, without any external test harness. Other tools like OSMO and NModel also use state machines and take a similar approach as ModelJUnit; the structure of the model is defined via annotated methods [24], [25]. In general, these tools are related to Modbat as they model both inputs and outputs, and have a notation of discrete transitions without timing constraints. However, models differ in whether the SUT (and its output) is considered to be strictly deterministic, and whether the model is centered on actions, random choices (specified by generators), or states and transition histories. A key feature distinguishing Modbat from other tools is its ability to deal with non-determinism.

Model-based testing tools can be classified according to whether they provide an API based on a well-known programming language (e.g., Java, C#) or a DSL (which further can be classified into an external or internal DSL) for describing SUT models. An advantage of API-based approach is that practitioners can use their familiar languages. Yet a DSL provides an easy to understand, user-friendly interface for testers writing and maintaining models as they are making models potentially less complex [26]. Describing SUT models with Modbat’s DSL on top of Scala combines the advantages of both approaches. Test selection criteria and search techniques for space exploration of the tools differ as well; furthermore, some tools generate off-line test code, which can be run without executing the state space exploration again.

Table III shows Modbat in comparison with the three selected tool examples. The comparison mainly follows the lines of Utting et al.’s taxonomy of model-based testing approaches [27], additionally considering the model specification interface and the license. ModelJUnit [1] inspired the initial version of Modbat [8] and takes a similar approach but is API-based. With several new versions of Modbat, many more features (test case generation for offline testing, debugging support, support for non-determinism, etc.) have been added. We consider ModelJUnit as a representative example for similar tools such as OSMO and NModel [25], [24]; the latter has been superseded by Spec Explorer. ScalaCheck [19] is a tool for property-based testing [28], primarily designed to generate complex data with constraints, but it can also be used to model transition systems and supports stateful testing. Like Modbat, it is based on Scala and shares some of its features [19]. Spec Explorer [9] is another model-based testing tool that provides a DSL to model state machines, although it also enables mainstream programming languages (e.g., C#) as input notation [29]. Spec Explorer is a commercial tool developed by Microsoft. It is based on the Windows/.NET platform, whereas Modbat runs on Java VMs available for many of the major platforms. Other differences to Spec Explorer are Modbat’s dynamic instantiation and the support for exception handling on the model level.

VI. DISCUSSION AND CONCLUSION

ModelJUnit [1] helped to bring model-based testing to early adopters of test case generation technology. Modbat has been inspired by ModelJUnit [8] and has been created to simplify some of the modeling tasks, such as specifying transitions with their preconditions and checking the occurrence of exceptions in actions [2]. It has been successfully used to model complex systems like SAT solvers [2], where it replaced a custom test generator written in C [13], and the Java network library, including non-deterministic actions like non-blocking input/output [3]. This demonstration shows Modbat on Java’s iterators, where we found a new previously unknown defect, and on a new API for incremental SAT solving. Modbat’s flexible DSL makes it possible to express both models succinctly and clearly. This facilitates focusing on the semantics of a system, which reduces the model development time and the risk of introducing defects in the model. We think that Modbat contributes to making model-based testing more applicable to complex software, and we hope that with an open source release of Modbat, model-based testing will become more widespread.

Even with an elegant and expressive modeling platform, writing a model that includes an output oracle requires an in-depth understanding of the system. Good model design is not always straightforward. In our experience, cognitive bias has sometimes prevented us from modeling the full state space in an initial version of the model [30]. We plan to add graphical tool support, and more ways to visualize model traces and their code coverage in the future, to mitigate this problem.

Modbat is available for download [11]. The material for this demonstration can be found online [31].

ACKNOWLEDGEMENTS

Part of the work was supported by the Japanese Society for the Promotion of Science (kaken-hi grants 23240003 and 26280019), by the Austrian Science Fund (FWF) through the national research network RiSE (S11408-N23), by the Austrian Ministry for Transport, Innovation and Technology, the Federal Ministry of Science, Research and Economy, and the Province of Upper Austria in the frame of the COMET center SCCH.
REFERENCES


