Active Learning of Abstract System Models from Traces using Model Checking

1st Natasha Yogananda Jeppu  
University of Oxford  
Oxford, UK  
natasha.yogananda.jeppu@cs.ox.ac.uk

2nd Tom Melham  
University of Oxford  
Oxford, UK  
tom.melham@cs.ox.ac.uk

3rd Daniel Kroening  
Amazon, Inc  
London, UK  
daniel.kroening@magd.ox.ac.uk

Abstract—We present a new active model-learning approach to generating abstractions of a system implementation, as finite state automata (FSAs), from execution traces. Given an implementation and a set of observable system variables, the generated automata admit all system behaviours over the given variables and provide useful insight in the form of invariants that hold on the implementation. To achieve this, the proposed approach uses a pluggable model learning component that can generate an FSA from a given set of traces. Conditions that encode a completeness hypothesis are then extracted from the FSA under construction and used to evaluate its degree of completeness by checking their truth value against the system using software model checking. This generates new traces that express any missing behaviours. The new trace data is used to iteratively refine the abstraction, until all system behaviours are admitted by the learned abstraction. To evaluate the approach, we reverse-engineer a set of publicly available Simulink Stateflow models from their C implementations.

Index Terms—active model learning, execution traces, system abstraction, software model checking

I. INTRODUCTION

Automaton inference from trace data is an established method for automated generation of system abstractions. Modern passive learning algorithms also infer guards and operations on system variables from the trace data, yielding symbolic models [1]–[4]. But the behaviours admitted by these models are, of course, limited to only those manifest in the traces. On the other hand, active learning algorithms can, in principle, generate symbolic abstractions from trace data, such as [5], the approach can learn models that are more expressive than the abstractions learned using existing active learning algorithms. Exact details of the procedure are discussed in Section III.

The procedure to evaluate degree of completeness of the learned model yields a set of new traces that exemplify system behaviours identified to be missing from the model. New traces are used to augment the input trace set for model learning and iteratively generate an extended abstraction that covers missing behaviours. Given a model learning algorithm that can infer symbolic abstractions from trace data, such as [6], the approach can learn models that are more expressive than the abstractions learned using existing active learning algorithms.

II. BACKGROUND

The system for which we wish to generate an abstraction is represented as a tuple $S = (X, X', R, \text{Init})$. $X = \{x_1, \ldots, x_m\}$ is a set of observable system variables over some domain $D$. We simplify the presentation by assuming all variables have the same domain. The set $X' = \{x'_1, \ldots, x'_m\}$ contains corresponding primed variables, which represent an update to the unprimed variable after a discrete time step. The transition relation $R(X, X')$ describes the relationship between $x_i$ and $x'_i$ for $1 \leq i \leq m$ and is represented using a characteristic function, i.e., a Boolean-valued expression over $(X \cup X')$. The set of initial system states is represented using its characteristic function $\text{Init}(X)$.

A valuation $v : X \rightarrow D$ maps the variables in $X$ to values in $D$. An observation at time step $t$ is a valuation of the variables at that time, and is denoted by $v_t$. A trace is a sequence of observations over time; we write a trace $\sigma$ with $n$ observations as a sequence of valuations $\sigma = v_1, \ldots, v_n$. We define an execution trace or positive trace for $S$ as a trace $\sigma = v_1, \ldots, v_n$ that corresponds to a system execution path, i.e., $(v_t, v_{t+1}) \in R$ for $1 \leq t < n$ and there exists a valuation $v' \models \text{Init}$ such that $(v', v_1) \models R$. A negative trace is a trace that does not correspond to any system execution path. We represent the set of execution traces by $\text{Traces}_X(S)$.

The active learning algorithm learns a system model as a finite state automaton (FSA). Our abstractions are represented symbolically and feature predicates on the transition edges, such as the abstraction in Fig. 1 and therefore extend FSAs to operate over infinite alphabets. We represent the learned abstraction as a non-deterministic finite automaton (NFA) $M = (Q, Q', \Sigma, F, \delta)$ over an infinite alphabet $\Sigma$, where $Q$ is a finite set of states, $Q_0 \subseteq Q$ are the initial states, $F \subseteq Q$ is the

This research was funded in part by the Semiconductor Research Corporation, Task 2707.001, and Balliol College, Jason Hu scholarship.
set of accepting states, and \( \delta : Q \times \Sigma \rightarrow \mathcal{P}(Q) \) is the transition function. The alphabet \( \Sigma \) corresponds to the set of valuations for variables in \( X \), i.e., \( \Sigma = (X \rightarrow D) \).

The NFA admits a trace \( \sigma = v_1, \ldots, v_n \) if there exists a sequence of automaton states \( q_1, \ldots, q_n+1 \) such that \( q_1 \in Q^0 \) and \( q_{i+1} \in \delta(q_i, v_i) \) for \( 1 \leq i \leq n \). Any finite prefix of a system execution trace \( \sigma \) is also an execution trace. Thus, if the generated NFA admits \( \sigma \), it must also admit all finite prefixes of \( \sigma \). In other words, the language of the automaton, \( L(M) \), must be prefix-closed. All states of our automaton are accepting, i.e., the NFA rejects traces by running into a ‘dead end’.

### III. Active Learning of Abstract System Models

The approach uses a pluggable model learning component to generate models from traces. Our requirement for this component is simple: given a set of execution traces \( T \), the component returns an NFA \( M \) that accepts (at least) all traces in \( T \).

To evaluate the degree of completeness of the set of traces, we use the structure of the NFA \( M \) to extract conditions that can be checked against the system implementation. The conditions collectively encode the following completeness hypothesis: for any transition available in the system defined by the transition relation \( R \), there is a corresponding transition in \( M \). The hypothesis is formulated based on defining a simulation relation between the system \( S \) and abstraction \( M \).

**Definition 1:** If \( Q \) represents the set of system states for \( S \) and \( q'_i, q_i \in Q \) represent the system state characterised by valuation \( v_i \) of variables in \( X \), then we define a binary relation \( R' \subseteq Q \times Q \) to be a simulation if \( (q'_i, q_i) \in R' \) implies that \( \forall (v_t, v_{t+1}) = R \) i.e., \( q'_i \rightarrow q'_{i+1} \), \( 3q_{i+1} \in Q \) such that \( q_{i+1} \in \delta(q_i, v_{i+1}) \) and \( (q'_{i+1}, q_{i+1}) \in R' \).

**A. Completeness Conditions for a Candidate Abstraction**

Given a candidate abstraction \( M \) for a system \( S \), we extract the following conditions encoding the completeness hypothesis:

\[
v_1 \models \text{Init} \land (v_t, v_{t+1}) = R \implies v_{t+1} \models p_0 \quad (1)
\]

where \( P_{(0, out)} \) is the set of predicates for all outgoing transitions from an automaton state \( q_0 \in Q^0 \), and for all \( p_i \in P_{(j, in)} \)

\[
v_t \models p_i \land (v_t, v_{t+1}) = R \implies v_{t+1} \models p_0 \quad (2)
\]

where \( P_{(j, in)} \) is the set of predicates on the incoming transitions to state \( q_j \in Q \) and \( P_{(j, out)} \) is the set of predicates on outgoing transitions from \( q_j \). Condition (2) is extracted for all states in \( Q \).

We compute the fraction of conditions that hold on the system, denoted by \( \alpha \), as a quantitative measure of the degree of completeness of the learned model. If all extracted conditions hold, i.e., \( \alpha = 1 \), then the generated model admits all system behaviours. A violation indicates missing behaviour in \( M \). A proof is provided in [10].

**B. Verifying Extracted Conditions Against the System**

To enable the application of existing software model checkers, we construct source code for functions that encode conditions (1) and (2) of the form \( v_1 \models R \land (v_t, v_{t+1}) = R \implies v_{t+1} \models s \) as assume/assert pairs, as illustrated in Fig. 2a.

To check if the system satisfies a condition, we run model checking on the constructed code. When all assume/assert pairs are proved valid, this implies that the extracted conditions are always satisfied and therefore can be used as system invariants.

In case of a failure, the checker returns a sequence of valuations \( \sigma'' = v_t, v_{t+1} \) as the counterexample, such that \( v_t \models R \land (v_t, v_{t+1}) \models R \land v_{t+1} \not\models s \). This can be used to construct a set of new traces as follows. For each trace \( \sigma \in T \) we find the smallest prefix \( \sigma' = v_1, v_2, \ldots, v_j \) such that \( v_j \models R \). We then construct a new trace \( \sigma'' = v_1, \ldots, v_j, v_{j+1}, v_{j+2} \) for each prefix \( \sigma' \). Note that since \( v_j \models R \), the new trace \( \sigma'' \) does not change the system behaviour represented by \( \sigma' \) but merely augments it to include the missing behaviour. The set of new traces \( T_{CE} \) thus generated is used as an additional input to the model learning component, which in turn generates a new abstraction that admits the missing behaviour.

For a violation of condition (1), the checker returns a counterexample \( \sigma'' = v_0, v_1 \) such that \( v_0 \models \text{Init} \) and \( (v_0, v_1) \models R \). \( \sigma'' \) is therefore a valid counterexample. However, the counterexample for a violation of condition (2) could be spurious. Let \( \sigma'' = v_t, v_{t+1} \) be the corresponding counterexample generated by the model checker. Here, it is not guaranteed that the system state characterised by \( v_t \) is reachable from an initial system state. Therefore, the counterexample may not actually correspond to missing system behaviour.

**C. Identifying Spurious Violations**

To check if a counterexample \( \sigma'' = v_t, v_{t+1} \) is spurious, the valuation \( v_t \) is encoded as the following Boolean formula:

\[
s' := \bigwedge_{x \in X} (x_t = v_t(x_i))
\]

and the negation, \( \neg s' \), is used to assert that \( s' \) never holds at any point in the execution of \( S \) starting from an initial state, as shown in Fig. 2b. The system \( S \) is modelled as multiple

![Fig. 2: Constructed source code for (a) Condition check (b) Counterexample validity check.](image-url)
TABLE I: Results of experimental evaluation of the active learning algorithm.

| Benchmark | $|X|$ | $k$ | Our Algorithm | Random Sampling |
|-----------|-----|-----|---------------|----------------|
|           |     |     | $s$ | $d$ | $N$ | $\alpha$ | $T(s)$ | $\% T_{sm}$ | $N$ | $\alpha$ | $T(s)$ |
| Automatic Transmission UsingDurationOperator | 4   | 125 | 6   | 1   | 1   | 3678.3 | 2.7 | 4 | 0.2 | 38.2 |
| BangBangControl UsingTemporalLogic | 4   | 562 | 4   | 1   | 4   | 11843.5 | 0.1 | 3 | 0.6 | 64 |
| CountEvents | 3   | 20  | 5   | 1   | 4   | 17078 | 0.2 | 5 | 0.7 | 89.5 |
| FrameSyncController | 3   | 530 | 1   | 0   | 1   | timeout | 2 | 0.7 | 31 |
| HomeControlUsingTheTruthTableBlock | 7   | 10  | 1   | 1   | 2   | 18.2 | 2 | 1 | 47.2 |
| KarplusStrongAlgorithm UsingStateflow | 5   | 100 | 2   | 1   | 4   | 430.9 | 0.8 | 3 | 1 | 33.9 |
| LadderLogicScheduler | 3   | 10  | 9   | 4   | 1   | 151.6 | 3.0 | 3 | 0 | 52.9 |
| MealyVendingMachine | 2   | 10  | 1   | 4   | 1   | 8.9 | 49.1 | 4 | 1 | 67 |
| ModelingACdPlayer UsingEnumeratedDataType | 13  | 205 | 4   | 0.1 | 4   | 0.2 | timeout | 12 | 0.2 | 95.7 |
| ModelingALaunchAbortSystem UsingAtomicStateflow | 6   | 22  | 4   | 0.8 | 6   | 0.6 | timeout | 7 | 0.6 | 282.8 |
| ModelingAnIntersectionOf Two1wayStreetsUsingStateflow | 11  | 60  | 1   | 4   | 1   | 10.9 | 22.2 | 4 | 1 | 416.1 |
| ModelingAREdundantSensorPartUsingAtomicSubchart | 6   | 29  | 4   | 0.8 | 4   | 0.4 | timeout | 8 | 0.4 | 105.6 |
| ModelingASecuritySystem | 16  | 100 | 16  | 4   | 1   | 1599 | 18.5 | seg fault |
| MonitorTestPointInStateflowChart | 2   | 20  | 1   | 1   | 9   | 39.2 | 2 | 1 | 29.6 |
| MooreTrafficLight | 3   | 40  | 3   | 1   | 7   | 89.3 | 38.4 | 9 | 0.1 | 24 |
| ReuseStatesByUsingAtomicSubcharts | 2   | 10  | 1   | 3   | 5   | 5.8 | 27.3 | 5 | 1 | 52.8 |
| SchedulingSimulinkAlgorithmsUsingStateflow | 3   | 127 | 5   | 1   | 3   | 54.7 | 17.7 | 4 | 0.8 | 35.9 |
| SequenceRecognitionUsingMealyAndMooreChart | 2   | 30  | 1   | 5   | 1   | 9.8 | 54.4 | 5 | 1 | 88.2 |
| ServerQueuingSystem | 4   | 40  | 2   | 1   | 3   | 13.8 | 31 | 4 | 0.6 | 99.3 |
| StatesWhenEnabling | 2   | 30  | 1   | 4   | 1   | 4.3 | 35.8 | 4 | 1 | 32.1 |
| StateTransitionMatrixViewForStateTransitionTable | 3   | 25  | 4   | 1   | 5   | 51.9 | 32.8 | 8 | 0.3 | 89.1 |
| Superstep | 1   | 10  | 1   | 1   | 1   | 139.7 | 0.4 | 1 | 21.8 |
| TemporalLogicScheduler | 2   | 202 | 6   | 1   | 4   | 270.8 | 4.4 | 4 | 1 | 36 |
| UsingSimulinkFunctionsToDesignSwitchingControllers | 3   | 10  | 1   | 4   | 1   | 7.2 | 27.1 | 4 | 1 | 41.5 |
| VarSize | 4   | 35  | 2   | 3   | 3   | 115.6 | 3.4 | 4 | 0.6 | 38.9 |
| ViewDifferencesBetweenMessagesEventsAndData | 2   | 40  | 2   | 1   | 4   | 9.4 | 46.9 | 4 | 1 | 34.8 |
| YoYoControlOfSatellite | 8   | 10  | 1   | 3   | 5   | 19.5 | 46.7 | 4 | 1 | 71.9 |

unwindings of the transition relation $R$ (lines 2-5 in Fig. 25). We verify this using model checking with $k$-induction [12], [13]. If both the base case and step case for $k$-induction hold, it is guaranteed that the counterexample is spurious, in which case we strengthen the assumption in Fig. 2a to $(r \land \neg s' \land R)$ and repeat the condition check. In case of a violation only in the step case, there is no conclusive evidence for validity. Since we are not interested in generating an exact system model but rather an over-approximation that provides useful insight into the system, we treat such a counterexample as valid.

For the bound $k$, a value greater than or equal to the diameter of the system guarantees completeness [12]. We discuss ways to approximate this value in [10]. Note that a poor choice for the bound $k$ results in more spurious behaviours being added to the model, resulting in low accuracy. But, the learned models are guaranteed to admit all system traces defined over $X$, irrespective of the value for $k$.

IV. EVALUATION AND RESULTS

A. Evaluation Setup

For our experiments we use Trace2Model (T2M) [10] as the model learning component. To evaluate the degree of completeness we use the C Bounded Model Checker (CBMC v5.35) [15]. We implement Python modules for the following: constructing the source code to check each condition, processing the CBMC output, and translating CBMC counterexamples into a set of trace inputs for model learning. Note that any model checker can be used in place of CBMC.

To evaluate our algorithm, we reverse-engineer a set of FSAs from their respective C implementations. We use a dataset of Simulink Stateflow models [10] as our benchmark set. For each benchmark, we use Embedded Coder [17] to automatically generate a C implementation. The generated C implementation is used as the system $S$. Further details are provided in [10].
The implementation and benchmarks are available online [18].

B. Experiments and Results

For each benchmark, we generate an initial set of 50 traces, each of length 50, by executing the system with randomly sampled inputs. Some of the Stateflow models are implemented as multiple parallel and hierarchical FSAs. For a given implementation \( S \) and a set of observables \( X \), we attempt to reproduce each state machine separately using traces defined over all variables in \( X \). We therefore generate an abstraction with state transitions at a system level for each FSA in \( S \).

The results are summarised in Table I. We quantitatively assess the quality of the final generated model for each FSA by assigning a score \( d \), computed as the fraction of state transitions in the Stateflow model that match corresponding transitions in the abstraction. For hierarchical Stateflow models, we flatten the FSAs and compare the learned abstraction with the flattened FSA. We record the number of model learning iterations \( i \), the number of states \( N \) and degree of completeness \( \alpha \) for the final model, the total runtime \( T \) and the percentage of total runtime attributed to model learning, denoted by \( \%T_m \). We set a timeout of 10h for our experiments. For benchmarks that time out, we present the results for the model generated right before timeout.

1) Runtime: The active learning algorithm is able to generate abstractions in under 1h for the majority of the benchmarks. For the benchmarks that time out, the model checker tends to go through a large number of invalid counterexamples before arriving at a valid counterexample for a condition violation. This is because, depending on the size of the domain \( D \), there can be a large number of possible valuations that violate an extracted condition, of which very few may correspond to a valid system state. In such cases, runtime can be improved by strengthening the assumption \( r \wedge R \) in Fig. 2a with domain knowledge to guide the model checker towards valid counterexamples. For FrameSyncController, CBMC takes a long time to check each condition. This is because the implementation features several operations, such as memory access and array operations, that condition. This is because the implementation features several operations, such as memory access and array operations, that condition.

2) Generated Model Accuracy: The algorithm is guaranteed to generate an abstraction that admits all system behaviours, as is confirmed by \( \alpha \) in Table I. We also see that \( d = 1 \) for these benchmarks. For two benchmarks, although the Simulink model matched the generated abstraction \( (d = 1) \), the algorithm timed out before it could eliminate all spurious violations \( (\alpha < 1) \).

3) Number of Learning Iterations: In each learning iteration \( j \), \( |L(M_j)| > |L(M_{j-1})| \) as \( L(M_j) \supseteq L(M_{j-1}) \cup T_{CE,j} \) and \( T_{CE} \cap L(M_{j-1}) = \emptyset \). Here, \( M_i \) and \( T_{CE} \) are the generated abstraction and the set of new traces collected in iteration \( j \) respectively. The algorithm terminates when \( L(M_j) \supseteq Traces_X(S) \). The number of learning iterations therefore depends on \( |Traces_X(S) \cap L(M_0)| \), where \( M_0 \) is the abstraction generated from the initial trace set.

C. Comparison with Random Sampling

We performed a set of experiments to check if random sampling is sufficient to learn abstractions that admit all behaviours. A million randomly sampled inputs are used to execute each benchmark. Generated traces are fed to T2M to passively learn a model. T2M fails to generate a model for 7 benchmarks, as its predicate synthesis procedure returns ‘segmentation fault’. For 50% of the remaining benchmarks, random sampling fails to produce a model admitting all system behaviours \( (\alpha < 1) \).

D. Threats to Validity

The key threat to the validity of our experimental claim is benchmark bias. We have attempted to limit this bias by using a set of benchmarks that was curated by others. Further, we use C implementations of Simulink Stateflow models that are auto-generated using a specific code generator. Although there is diversity among these benchmarks, our algorithm may not generalise to software that is not generated from Simulink models, or software generated using a different code generator.

REFERENCES


