Exact and Approximate Probabilistic Symbolic Execution for Nondeterministic Programs

Kasper S. Luckow  
Aalborg University, Denmark

Corina S. Păsăreanu  
CMU/NASA Ames Research Center, USA

Matthew Dwyer  
University of Nebraska, USA

Antonio Filieri  
University of Stuttgart, Germany

Willem Visser  
University of Stellenbosch, South Africa

ABSTRACT

Probabilistic software analysis seeks to quantify the likelihood of reaching a target event under uncertain environments. Recent approaches compute probabilities of execution paths using symbolic execution, but do not support nondeterminism. Nondeterminism arises naturally when no suitable probabilistic model can capture a program behavior, e.g., for multithreading or distributed systems.

In this work, we propose a technique, based on symbolic execution, to synthesize optimal schedulers that resolve nondeterminism to maximize the probability of reaching a target event. To scale to large systems, we also introduce approximate algorithms to search for near-optimal schedulers, speeding up established random sampling and reinforcement learning results through the quantification of path probabilities based on symbolic execution.

We implemented the techniques in Symbolic PathFinder and evaluated them on nondeterministic Java programs. We show that our algorithms significantly improve upon a state-of-the-art statistical model checking algorithm, originally developed for Markov Decision Processes.

1. INTRODUCTION

Probabilistic software analysis aims to quantify the probability that a software system satisfies a required property, under given probabilistic usage profiles. Recent applications include cyber-physical systems, e.g. check that the probability of an unmanned aerial vehicle turning too fast is less than $10^{-6}$, by analyzing the vehicle’s control software, under suitable profiles built from the telemetry data of previous versions or similar systems. Such critical systems are usually checked through simulation only and probabilistic software analysis can complement that, for increased assurance. Other applications include program understanding and debugging [18], computing software reliability [15, 6], quantitative information flow analysis for security [22], etc.

Traditional formal approaches based on probabilistic model checking [21, 2] require a high-level design or architectural model of the software. However such models are difficult to maintain and may abstract important details that impact the chance of property satisfaction in the system. Our goal is to perform probabilistic analysis directly on implementations, not on high-level models. Recent promising approaches, developed by us and others, have proposed to use bounded symbolic execution [18, 15, 35, 6] to support probabilistic analysis on the source code. The analyses in [18, 15] address programs with integer domains and linear constraints, with [15] also treating complex data structures as inputs, while the analyses in [35, 6] address programs with linear and complex floating-point computations, respectively.

However, none of these approaches (with the exception of [15], discussed below) treat the orthogonal but important issue of nondeterminism. Nondeterminism arises naturally when no suitable probabilistic model can capture a program behavior, e.g., for multithreaded, distributed or component-based systems.

In this paper, we extend probabilistic symbolic execution of programs to deal with nondeterminism. We aim to compute an optimal scheduler that resolves nondeterminism to maximize the probability of property satisfaction, or conversely that maximizes the probability of non-satisfaction. The benefit of our approach is twofold: first, any other possible scheduler will provide the probabilistic guarantees between the reported worst and best cases; second, inspection of the best/worst case could possibly provide insights for the design of the analyzed system, e.g. to debug or improve it. In [15] we proposed to compute probabilities along linear schedules (i.e. thread interleavings) and report the best/worst cases to the user. Although very intuitive, it turns out that linear schedules are insufficient for computing the maximum (or minimum) values for the probability of property satisfaction in a program, and hence have limited use in practice. Instead tree-like schedulers are in general needed and we show in the next section why this is the case.

We describe an (exact) algorithm for computing an optimal tree-like scheduler that resolves the nondeterminism to maximize the probability of property satisfaction (or failure). The algorithm takes a bottom-up approach to propagate computed values, and resembles the value-iteration for...
Markov Decision Processes (MDPs) [38], but it works directly on the code (not on MDP models) and is tailored to efficiently process the symbolic tree generated with a bounded symbolic execution of the program.

In the worst case, the exact algorithm needs to explore the full symbolic execution tree of the program, making it infeasible for large programs. To address this scalability problem, we aim to develop approximate, randomized algorithms for the synthesis of schedulers. We propose an algorithm that uses Monte Carlo sampling over program paths as dictated by the conditional probabilities computed from the conditions in the code (using symbolic execution). One well-known shortcoming of sampling-based techniques [27] is that, unlike an exact probabilistic analysis, they cannot be directly applied to systems featuring nondeterminism, since it is not clear how to take meaningful decisions for nondeterministic choices during the Monte Carlo sampling. To address this problem, our algorithm starts by assuming a uniform distribution over the nondeterministic choices (i.e., assumes all nondeterministic choices are equally likely) and then iteratively uses reinforcement learning to provably improve the resolution of nondeterminism with respect to the target event. A key insight for our randomized algorithm is that the search for an optimal scheduler can be accelerated by exploiting the full probabilistic quantification of sampled symbolic paths. This also enables state pruning to reduce the sampling space and speed-up the technique.

To study the effectiveness of learning, we have also implemented a baseline algorithm that simply uses a uniform distribution for the nondeterministic choices (with no learning), but which can also benefit from the state pruning.

Both our approximate algorithms significantly improve upon a state-of-the-art statistical model checking algorithm, originally developed for MDPs [20]. That algorithm also uses sampling and reinforcement learning, but it needs to sample multiple (possibly many) times along the same path to obtain a good estimate of the quality function used for reinforcement [37]. In our case, it is sufficient to sample a path only once to gather the full count of all the inputs associated with that path. Despite the potentially high cost of computing the full count, the benefit over pure statistical estimation, which works with counts incremented once per sample, leads to a significant improvement in performance for our algorithms. Furthermore, our algorithms enable aggressive state pruning which is not possible with classical statistical approaches.

Our approximate algorithms are true biased (meaning that true results can always be trusted), can be made arbitrarily correct (Theorem 1) and in the limit converge to the results of the exact analysis (Theorem 3 and Proposition 2), making them suitable for the analysis of critical software. In contrast, we show that the statistical approach from [20] does not always converge, as claimed in that paper (see the example in the next section).

Our work yields methods for computing upper and lower bounds on the probability of property satisfaction in programs enriched with nondeterministic choice constructs. We make our presentation in terms of Java bytecode analysis and the Symbolic Pathfinder (SPF) symbolic execution tool [33]. However, our algorithms are applicable in the context of other languages for which symbolic execution tools exist (e.g., Klee [8] for C). The contributions of our work are: (1) an exact algorithm for probabilistic bounded symbolic execution of nondeterministic programs; (2) approximate algorithms that exploit accelerated sampling of symbolic paths, reinforcement learning and state-space pruning, with theoretical guarantees; (3) the extension of SPF to implement probabilistic symbolic execution of nondeterministic programs, and (4) evidence from applying the implementation to a collection of multithreaded Java programs that our algorithms outperform existing methods.

2. EXAMPLES

In this section, we provide examples that illustrate our approach and facilitate comparison with [20, 15].

Example 1 Figure 1 shows an example Java program with nondeterministic code obtained by method Verify.getBoolean(), which nondeterministically returns true or false in SPF. Assume that the input \( x \) ranges over \([1\ldots100]\) – in practice, the input domain can be much larger.

The corresponding symbolic execution tree is also sketched in the figure; it encodes all the paths taken during the symbolic execution of the program. Shaded nodes represent nondeterministic choices; white nodes represent probabilistic choices. We also annotated tree edges with the conditions on the inputs to reach that edge, i.e. the path conditions computed with symbolic execution. The probabilities are computed from the path conditions, using a quantification procedure (as described in Section 4). For example, assuming a uniform usage profile, the probability of taking the then branch through the code corresponding to condition \( x \leq 60 \) is \( 60/100 = 0.6 \), since there are 60 inputs that satisfy the condition, out of 100 possible inputs. Similarly, the probability of taking the else branch corresponding to condition \( x > 60 \) is 0.4 etc.

Our goal is to identify an optimal scheduler that decides for each nondeterministic choice the best alternative to select to maximize the probability of success. The execution tree can be seen as an MDP and analyzed by probabilistic model checking [38, 17]. The result can also be computed with our Exact algorithm, yielding the scheduler that selects \( 0 \rightarrow 1 \rightarrow 3 \) in the tree, with the maximum success probability 0.6.

We have also analyzed the example using our approximate algorithms where we fixed the number of samples to 100 (de-
public static void testMethod2(int x) {
    if(x > 50)
        x++;
    if(Verify.getBoolean()) {
        //T1
        if(x > 61)
            println("success");
    } else {
        assert false;
    }
    if(x <= 81)
        else {
            if(Verify.getBoolean()) {
                println("success");
            } else {
                println("Fail");
            }
        }
        else {
            println("Fail");
        }
    }
}

(a) Source snippet.  (b) Tree.
Figure 2: Example 2

3. PRELIMINARIES

In this section, we give background information for symbolic execution and probabilistic analysis in the context of sequential programs. We will extend these notions to programs with nondeterminism in Section 4.

Symbolic Execution Symbolic Execution [22] [11] is a program analysis technique that executes programs on unspecified inputs, by using symbolic inputs instead of concrete data. The state of a symbolically executed program is defined by the (symbolic) values of the program variables, a path condition (pc), and a program counter. The path condition is a (quantifier-free) boolean formula over the symbolic inputs; it accumulates constraints that concrete on the inputs to follow that path. The program counter defines the next statement to be executed.

A symbolic execution tree characterizes the execution paths followed during symbolic execution. The tree nodes represent program states and the arcs the transitions between states due to the execution of program instructions. We built our approach upon the symbolic execution tool Symbolic Java PathFinder (SPF) [33], which has built-in support for preconditions (used for encoding usage profiles).

Probabilistic Analysis The goal of the analysis is: (1) to identify the symbolic constraints characterizing the inputs that make the execution satisfy a given property, and then (2) to quantify the probability of satisfying the constraints. For simplicity, we assume the satisfaction of the target property to be characterized by the occurrence of a target event (e.g. successful termination or failure), but our work generalizes to bounded LTL properties [40].

To deal with programs with loops, we perform a bounded symbolic execution of the program. The result is a finite set of symbolic paths, each with a path condition. Some of these paths lead to failure, some of them to success (termination without failure) and some of them lead neither to success nor failure (they were interrupted because of the bounded exploration) – the latter are called grey paths. The path conditions are therefore classified in three sets: $PC^*$ contains the path conditions where the scheduler chooses $T_1$, $PC^G = \{p_{c1}, p_{c2}, \ldots, p_{cn}\}$, and $PC^G = \{p_{c1}, p_{c2}, \ldots, p_{cn}\}$. The path conditions define disjoint input sets and they cover the whole input domain.

If we take the approach from [15], we compute the probability of success along each linear schedule and then report the maximum. For our simple example, we only have two linear schedules, corresponding to choosing to perform either task $T_1$ or task $T_2$. If the scheduler chooses $T_1$, then the probability of success is 0.4 (for path $0 \rightarrow 1 \rightarrow 3$) while if the scheduler chooses $T_2$, the probability of success is the sum of probabilities along paths $0 \rightarrow 1 \rightarrow 4$ and $0 \rightarrow 2 \rightarrow 6$, respectively, yielding 0.3 plus 0.5 for a total of 0.8, which can be deemed as the maximum value. However consider now a tree-like scheduler that in state 1 decides to take $T_1$ while in state 2 decides to take $T_2$. This yields probability of success 0.4 (path $0 \rightarrow 1 \rightarrow 3$) plus 0.5 (path $0 \rightarrow 2 \rightarrow 6$), yielding 0.9 which is larger than the probabilities computed along linear schedules. Using established results for MDPs [58] [17], it can be shown that this is indeed the maximum possible value for the success probability of the example program. In the rest of the paper, we will describe exact and approximate algorithms for computing tree-like schedulers.
Probability techniques, i.e. LattE [14], to estimate (algorithmically) the generated constraints. In [18, 15] we used model counting of path conditions, we use a quantification procedure for the Quantification Procedure to compute the probabilities under current exploration bound [15].

To compute the probabilities of failure, \( \Pr(\text{failure}) \), any of the successful path conditions: \( \Pr(p) \) is then defined as \( \frac{\sharp(c)}{\sharp(D)} \) (where \( \sharp(D) \) is the size of \( D \)).

The success probability (or failure or grey probability) can then be computed as \( \Pr^*(P) = \sum_i \Pr(p_i) = \frac{\sum_i \sharp(c_i)}{\sharp(D)} \).

4. PROBABILISTIC ANALYSIS FOR NON-DETERMINISTIC PROGRAMS

We consider now the problem of probabilistic analysis for nondeterministic programs. Without making any assumption on the way the nondeterministic choices are resolved (i.e. without assuming a-priori a next-choice distribution nor a specific scheduling policy) we want to identify the best possible choices from each state, i.e., the choices that lead to the highest probability of success; conversely, we may want to identify the worst possible choices which lead to the lowest probability of success.

Symbolic Execution First, we extend the definition of symbolic execution provided in Section 9 to account for nondeterministic choices. We extend the symbolic execution tree with a new kind of node corresponding to nondeterministic choices in the program. Thus, the symbolic execution tree of a nondeterministic program has three kinds of nodes (or states): i) PC: path condition choice; ii) NC: nondeterministic choice; iii) other: all the other nodes (i.e. assignments, method invocations, returns, etc.)

A PC choice is introduced whenever a conditional statement is executed in the program. The evaluation of the statement (on condition \( c \)) introduces two new transitions. The first one leads to the execution of the \( \text{then} \) block in the code and the path condition is updated as \( \text{pc}_{\text{then}} = c \land \text{pc} \). The second leads to the execution of the \( \text{else} \) block and the path condition is updated with \( \text{pc}_{\text{else}} = \neg c \land \text{pc} \). If the path condition for a branch is not satisfiable, symbolic execution will not follow the branch.

A NC choice is introduced whenever nondeterminism is present in the analyzed application; this may be due to handling of multithreading or to explicit nondeterministic instructions in the code (e.g. Verify.getBoolean()).

A symbolic execution tree is then denoted as \( T = (S, s_0, \rightarrow, S_{NC}, S_{PC}) \), where \( S \) is the set of nodes, \( s_0 \) is the initial state, \( \rightarrow \subseteq S \times S \) is the transition relation, \( S_{NC} \subseteq S \) is the set of NC nodes and \( S_{PC} \subseteq S \) is the set of PC nodes (\( S_{NC} \) and \( S_{PC} \) are disjoint by construction). Let \( \text{child}(s) \) denote the children nodes of \( s \) and let \( \text{parent}(s) \) denote the parent of \( s \). Note that both NC and PC nodes can have more than one child, while all the other nodes can have at most one.

Branch probabilities for PC nodes For a PC node, we define branch probabilities as the probability of taking the \( \text{then} \) or the \( \text{else} \) branch from the given PC node. These branch probabilities can be computed using model counting as was done in [15]. Let \( \text{pc}_c \) be the path condition at the current PC node \( s_c \), and let \( c \) be the branching condition at
that state. We can then compute the branch probabilities as follows.

\[
\begin{align*}
pr_{\text{then}} &= Pr(c|pc_e) = \frac{\sharp(c \land pc_e)}{\sharp(pc_e)} \\
pr_{\text{else}} &= Pr(\neg c|pc_e) = \frac{\sharp(\neg c \land pc_e)}{\sharp(pc_e)}
\end{align*}
\]

Note that \(\sharp(pc_{\text{then}}) + \sharp(pc_{\text{else}}) = \sharp(pc_e)\), thus \(pr_{\text{then}} + pr_{\text{else}} = 1\).

**Probabilistic Analysis** In our setting, the symbolic execution trees computed with the probabilistic symbolic execution described above can be seen as a tree-shaped MDP [17]. MDPs are a popular choice to model discrete state transition systems that are both probabilistic and nondeterministic. Schedulers are functions used to resolve the nondeterminism in MDPs. An MDP in which nondeterminism has been resolved becomes a fully probabilistic system known as a Markov Chain. In our case, the NC nodes in the symbolic execution tree have only outgoing nondeterministic transitions, while the PC nodes only have probabilistic transitions.

Without going into much detail about MDPs, we can borrow from the literature on MDPs and define a (memoryless) scheduler \(\sigma\) for a symbolic execution tree which resolves the nondeterminism in each NC node. We first define a probabilistic scheduler, which provides a distribution over the set of children of that NC node [20] (we will use this later in our approximate algorithms).

Let \(S_{\text{NCchildren}}\) denote all the children of NC nodes, i.e., \(S_{\text{NCchildren}} = \{s \in S \mid \text{parent}(s) \in S_{\text{NC}}\}\).

**Definition 1.** A memoryless scheduler \(\sigma\) for a symbolic execution tree \(T\) is a function \(\sigma : S_{\text{NCchildren}} \to [0,1]\) s.t. \(\forall s \in S_{\text{NC}}: \Sigma_{\sigma' \in \text{child}(s)}(\sigma(s')) = 1\).

A scheduler for which either \(\sigma(s)\) is 0 or 1 for all \(s \in S_{\text{NCchildren}}\) is called deterministic. Similar to [20], we consider here only memoryless schedulers.

The goal is to identify the best possible deterministic scheduler, that is the one that leads to the highest probability of success. Let us first note that a (nondeterministic) program \(P\) and a deterministic scheduler \(\sigma\), induce what amounts to a sequential program \(P_\sigma\), with all the nondeterminism resolved according to \(\sigma\). The symbolic execution tree of this program is the same as \(P\)'s but with transition relation \(\rightarrow \leftarrow \{(n,c) \mid n \in S_{\text{NC}} \land \sigma(c) = 0\}\) (i.e., we remove from \(\rightarrow\) all transitions \((n,c)\) for which \(\sigma(c) = 0\)). For \(P_\sigma\), one can then compute \(Pr^*(P_\sigma)\) as described in Section [13]. For a nondeterministic program one can then define the maximum probability of success as:

\[
Pr^*(P) = \max Pr^*(P_\sigma)
\]

where \(\sigma\) is deterministic. Similar definitions apply for \(Pr^f(P)\) and \(Pr^r(P)\). Below we describe a procedure for computing \(Pr^r(P)\), where \(r \in \{s,f,g\}\); the procedure forms the basis of the approximate algorithms described in the next section.

**Exact Analysis** The procedure is depicted in Algorithm [1]. It takes as input a nondeterministic program \(P\) and a target event \(t\). The procedure performs a bounded symbolic execution of the program (in depth-first search order). For each explored path \(\pi\), it checks whether it reaches the target event, in which case it computes the count associated with the path condition (\(\sharp(pc_e)\)). This count is then propagated up along the path, to record how many inputs reach the target event. For this purpose, the procedure maintains a count \(s^+\) for each state \(s\). For NC nodes, \(s^+\) is updated with the maximum value among the children, while for all the other nodes \(s^+\) is the sum of the counters for their children.

**Algorithm 1** Exact analysis.

1. **function** \(\text{EXACT}(\text{Program } P; \text{ target event } t)\)
2. Perform bounded SE of \(P\)
3. For each \(\pi = s_0s_1...s_k\) do
4. If \(\pi\) yielded event \(t\) then
5. \(s_k^+ \leftarrow \sharp(pc_e)\)
6. For \(i = k, k-1, ..., 0\) do
7. If \(s_i \in S_{\text{NC}}\) then
8. \(s_i^+ \leftarrow \max_{s \in \text{child}(s_i)}(s^+)\)
9. Else
10. \(s_i^+ \leftarrow \sum_{s \in \text{child}(s_i)}(s^+)\)
11. End if
12. If \(s_k^+\) unchanged then
13. Break
14. End if
15. End for
16. End if
17. End for
18. Return \(Pr^r(P) = s_0^+ / \sharp(D)\)
19. **end function**

**Algorithm 2** Optimal scheduler.

1. **function** \(\text{OPTSCHEDULER}(\text{State } s)\)
2. If \(s\) has no children then
3. Return
4. End if
5. If \(s\) is PC then
6. For \(\forall s_c \in \text{child}(s)\) do
7. \(\text{OPTSCHEDULER}(s_c)\)
8. End for
9. Else if \(s\) is NC then
10. \(s_i^+ \leftarrow \max_{s \in \text{child}(s)}(s^+)\)
11. \(\text{mark}(s)\)
12. \(\text{OPTSCHEDULER}(s^+_{\text{root}})\)
13. End if
14. **end function**

After exploring all paths, the maximum probability for the target event (\(Pr^r(P)\), shorthand for \(Pr^r(s_0)\)) is given by \(s_0^+ / \sharp(D)\), where \(s_0^+\) is the root of the symbolic tree and \(D\) is the input domain. The optimal scheduler is simply defined by selecting for each NC node the child with the maximum value of \(s^+\). See Algorithm [2] which recursively visits the children of a state, \(s\), and marks the nodes belonging to the optimal scheduler. In case of a tie for maximum value, we pick the first choice.

The intuition for the exact analysis is captured by the following proposition; let \(Pr^r(s)\) be the maximum probability that a path crossing state \(s\) leads to the target event.

**Proposition 1.** For every state \(s\), the maximum probability of reaching the target event is \(Pr^r(s) = s^+ / \sharp(pc_e)\).

**Proof.** By induction on the structure of the symbolic tree. For leaves and NC nodes it is straightforward. For PC nodes
s: \( Pr^t(s) = p_{then} \cdot Pr^t(s_{then}) + p_{else} \cdot Pr^t(s_{else}) \). From induction hypothesis this is equal to \( \frac{1}{2}(c \land pc) / (pc) \cdot s_{then} + \frac{1}{2}(\neg c \land pc) / (pc) \cdot s_{else} / (pc) = (s_{then} + s_{else}) / (pc) = s^+ / (pc) \).

It follows that the value returned at Line 18 of Algorithm 3 \( s^+_t(D) = s^+_t(pc_a) \) is indeed the probability of reaching the target event in the program. The procedure terminates in \( k \cdot n \) steps, where \( k \) is the bound of symbolic execution and \( n \) is the number of symbolic paths.

**Discussion** In practice, we work with an abstraction of the symbolic execution tree, that only keeps the NC and PC nodes, and merges together all the other nodes. A node in the tree is uniquely characterized by the sequence of choices that lead to that node. We use this sequence as an efficient encoding of a state.

Note also that the grey case can also be interpreted pessimistically or optimistically, meaning that grey will be regarded as failure or success, respectively.

Finally, we mention that in practice we perform an optimized computation for the Exact procedure. Instead of recomputing the maximum count for the target event, \( s^+ \), for state \( s \) by performing the max operation of the counts of the children i.e. \( s^+ = \max_{s_c \in \text{child}(s)} (s_c^+) \), we perform an efficient algorithm that based on the current count for the target event, \( c^+ \), and a count update, \( \Delta c^+ \), updates the count for state \( s \) incrementally. We presented the un-optimized version here for clarity.

### 5. APPROXIMATE ANALYSIS

We describe here two approximate algorithms, Max and Random, which use randomized sampling of symbolic paths to compute approximate solutions to the scheduler synthesis problem. Random uses a uniform distribution for the nondeterministic choices while Max uses Reinforcement Learning to iteratively improve resolutions of nondeterminism. We start with a statement of the verification queries that can be answered with our algorithms. We build upon and use the terminology from [20].

**Verification Query** Instead of computing the maximum probability of reaching \( t \) \((t \in \{s, f, g\})\), as in Exact, we pose the following query: given \( t \) and a hypothesis \( \theta \in \{0, 1\} \), we try to decide whether \( \exists \sigma : Pr^t(P) >_\theta \), where \( op \in \{\geq, \geq\} \). Such queries can be used both for verification and scheduler synthesis. For example, for verification, assume we want to check that \( \forall \sigma : Pr^t(P) \geq 90\% \). This can be decided by the query \( \exists \sigma : Pr^t(P) > 10\% \). On the other hand, for scheduler synthesis, we check directly the existential query: \( \exists \sigma : Pr^t(P) \geq 90\% \). In both cases, if the existential formulation of the query is true, a scheduler is produced. Throughout this section, we assume for simplicity that grey paths are treated pessimistically.

**Approximate Algorithms** Both Max and Random follow the overall algorithm depicted in Algorithm 3 with the difference that Random does not perform scheduler improvement (Line 10). At a high level, the goal of each run of the algorithm (Lines 3-11) is to compute information about the best choices with respect to the target event. The algorithm maintains a probabilistic scheduler \( \sigma \), initialized with a uniform candidate (Line 4). Each run iterates over two procedures (for-loop at Line 5 with parameter \( L \)): scheduler evaluation (Line 6), which uses sampling to compute the counts \( s^+ \) and scheduler improvement (Line 10), which uses the computed information to improve on \( \sigma \).

**Algorithm 3 Approximate analysis.**

```plaintext
1: function APPROXIMATE(T restarts, L optimizations, N samples, History parameter 0 < h < 1, Greediness parameter 0 < c < 1, operator op, hypothesis \( \theta \), target event \( t \))
2: for \( i = 1, ..., T \) do
3: \( \forall \sigma, s^+ \leftarrow 0 \)
4: \( \forall_{\text{NC}} \forall_{\text{child}(s)} \sigma(s) \leftarrow 1 / |\text{child}(s)| \)
5: for \( i = 1, ..., L \) do
6: \( Q \leftarrow \text{SchEvaluation}(\sigma, h, t) \)
7: if \( s^+_i /[i(D) \ op \ \theta \ \text{then} \)
8: return True
9: end if
10: \( \sigma \leftarrow \text{SchImprovement}(\sigma, h, i, Q) \)
11: end for
12: end for
13: return Probably False
14: end function
```

**Algorithm 4 Scheduler evaluation.**

```plaintext
1: function SCHENVALUATION(Scheduler \( \sigma \), N samples, target event \( t \))
2: for \( s \in S_{NC\text{Children}} : Q(s) \leftarrow \sigma(s) \)
3: for \( i = 1, ..., N \) do
4: Sample \( \pi = s_0 s_1 ... s_k \)
5: if \( \pi \) yielded event \( t \) then
6: \( s^+_i \leftarrow \pi(pc_e) \)
7: for \( i = k - 1, ..., 0 \) do
8: if \( s_\pi \in S_{NC} \) then
9: \( s^+_i \leftarrow \max_{s_c \in \text{child}(s_\pi)} (s_c^+) \)
10: else
11: \( s^+_i \leftarrow \Sigma_{s_c \in \text{child}(s_\pi)} (s_c^+) \)
12: end if
13: if \( s^+_i \) unchanged then
14: Break
15: end if
16: end for
17: end if
18: end for
19: for \( s \in S_{NC\text{Children}}, \text{s.t.} \ s^+ \) was updated above do
20: \( Q(s) \leftarrow s^+ / |s(pc_e)| \)
21: end for
22: return Q
23: end function
```

After each scheduler evaluation, we check if the verification query is true (Line 7). Note that the scheduler evaluation has the side effect that the values for each count \( s^+ \) are updated. Note also that while the probabilistic scheduler \( \sigma \) is used to guide the sampling (in scheduler evaluation), it does not participate in the query checking. If the query is true, the answer is returned to the user; the deterministic scheduler that confirms it is built similarly to the exact analysis. Our algorithm is a true-biased Monte Carlo algorithm [7] meaning that it is guaranteed to be correct when it confirms the hypothesis. If it can not, we restart the search
(for-loop at Line 2 with parameter $T$); if it fails again, then the confidence about the unsatisfiability of the hypothesis becomes higher.

**Scheduler Evaluation** Scheduler evaluation (Algorithm 4) performs $N$ Monte Carlo samplings of symbolic paths, according to the branch probabilities for PC nodes and the probabilistic scheduler $\sigma$ for the NC nodes. From each sample, it collects information $s^{+}$ for each state $s$, in a manner similar to the exact algorithm (Lines 5–17 are identical to Exact). In addition, $s^{+}$ is used to compute the quality $Q$ for each choice (child of an NC node) that occurs due to nondeterminism (Line 20). The quality is used for reinforcement, i.e. scheduler improvement, and is ignored by Random. The quality is defined as $Q(s) = s^{+}/\sum_{\text{child}}(s')$, and is an estimate for the maximum probability of reaching $t$ from state $s$, $Pr^t(s)$ (see Proposition 4).

In the absence of new information from sampling (i.e. if it happens to re-sample the same paths), the counts $s^{+}$ remain unchanged and consequently also the values for $Q$. Note also that we do not reset the counts $s^{+}$ at the beginning of each scheduler evaluation. This explains why even Random (with no learning) can be very effective in finding an optimal scheduler, because it keeps accumulating information about the counts the more it samples.

**Scheduler Improvement** Scheduler improvement (Algorithm 5) uses quality $Q$ to compute how likely it is for each choice to lead to success (Line 4); it also updates $\sigma$ by reinforcing the actions that are more promising (Lines 5–6). The procedure is identical to the scheduler improvement in [20] (we show it here for completeness). As in [20], we use a greediness parameter $(1 - \epsilon)$ that controls the probability we assign to the most promising choice. Combining the new greedy choices with the previous scheduler, according to history parameter $h$, ensures that no choice is ever blocked as long as the initial scheduler does not block any actions.

**Algorithm 5** Scheduler Improvement [20]

1: function SCH impro vement($\sigma$) History parameter $0 < h < 1$, Greediness parameter $0 < \epsilon < 1$, Quality function $Q$

2: $\sigma' = \sigma$

3: for $s$ of type NC do

4: $s^{+} = \arg\max_{s' \in \text{child}(s)} \{Q(s')\}$

5: $\forall s' \in \text{child}(s), p(s') = \begin{cases} I(s') = s^{+} & (1 - \epsilon) + \\
Q(s')/\sum_{s' \in \text{child}(s)}(s')] & \epsilon(Q(s')/\sum_{s' \in \text{child}(s)}(s'))\end{cases}$

6: $\forall s' \in \text{child}(s), \sigma(s') = h\sigma(s') + (1 - h)p(s')$

7: end for

8: return $\sigma'$

9: end function

**Correctness and Convergence** As mentioned, our approximate algorithms are true-biased algorithms, for which the following result holds (See [7], p. 266). This general result refers to true-biased $p$-correct algorithms (i.e. algorithms for which the probability that it outputs a correct solution is at least $p$) and it is only of theoretical importance, as in practice it is difficult to quantify $p$.

**Theorem 1** (Bounding Theorem). For a true-biased $p$-correct Monte Carlo algorithm (with $0 < p < 1$) to achieve a correctness level of $(1 - \eta)$ it is sufficient to run the algorithm a number of times: $T = \log_{2}\eta/\log_{2}(1 - p)$. Random and Max are true-biased and $p$-correct.

We also state here the correctness of our approximate algorithms, meaning that the probabilities computed with our approximate algorithms converge to the maximum one, and the deterministic schedulers converge to the optimal one, with respect to the target event.

**Theorem 2** (Scheduler Improvement). Let $c$ and $c'$ be the counters computed in $s^{+}$ for a state $s$ in consecutive Scheduler Evaluation phases, then $c/\sum_{s'}(pc_s) \leq c'/\sum_{s'}(pc_s) \leq Pr^t(s)$.

**Proof**. $s^{+}$ for leaves is constant and $\geq 0$. For a newly sampled path $\pi$, the counters $s^{+}$ are updated with values $\geq 0$. Since both $\max$ and $\sum$ are used in computing $s^{+}$, it can only increase when considering additional positive elements, and since $\sum_{s'}(pc_s) > 0$ for each state, $c/\sum_{s'}(pc_s) \leq c'/\sum_{s'}(pc_s)$ follows. When all the execution paths have been sampled, the values of $s^{+}$ cannot be further increased and their value corresponds to $Pr^t(s)$ as a consequence of Proposition 4.

We also need to make sure that Random and Max will not get stuck in a local optimum.

**Theorem 3** (Asymptotic convergence). In the limit (for large $N$ or $L$) the probability of sampling the optimal alternative converges to 1.

**Proof**. Consider Max. For each NC node $s$, the probability $p(s')$ of taking a transition to $s' \in \text{child}(s)$ is initialized to $1/|\text{child}(s)| > 0$. When a successful path is sampled, $p(s')$ becomes $c(Q(s')/\sum_{s'' \in \text{child}(s)}(Q(s'')))$. Where $Q(s') = s^{+}/\sum_{s'' \in \text{child}(s)}(Q(s''))$. Furthermore $\sum_{s'' \in \text{child}(s)}(Q(s'')) \leq |\text{child}(s)|$ (since $\forall s'' : 0 < Q(s'') \leq 1$). It follows that $p(s') \geq c/|\text{child}(s)| > 0$ in other words, $p(s')$ is guaranteed to be greater than a positive constant ($h$ does not change the lower bound). Hence, by Borel’s Law of Large Numbers [31], p. 304, it follows that when the number of samples tends to infinity, each possible transition, including the optimal one, is almost surely eventually sampled. For Random, $p(s') \geq 1/|\text{child}(s)| > 0$, and similar considerations apply.

**Pruning** Our techniques collect the full count $(\sum_{s'}(pc_s))$ for each explored symbolic path $(\pi)$. Therefore subsequent explorations of those paths do not yield more information and we can remove those paths from being explored again to speed up the analyses and achieve memory savings. After sampling a path, we mark the leaf in the symbolic execution tree as “explored” and then go up in the tree along the path to mark as “explored” all the nodes for which all of their children have been marked “explored”. Sampling is then performed only from nodes that were not marked as “explored”. When the root is marked “explored”, we are guaranteed that the tree has been fully explored.

**Proposition 2** (Termination of Max and Random with pruning). If pruning is applied, the optimal alternative for each nondeterministic choice will be sampled within $n$ iterations, where $n$ is the total number of symbolic paths.

**Comparison with [20]** We provide here a brief comparison with the statistical algorithm for MDPs from [20]; let us denote it as $\text{Sum}_1$. Max uses as quality $Q$ the expected
maximum probability of reaching the target from the current state (irrespective of current $\sigma$, which is only used to drive sampling). In contrast, $\text{Sum}_1$ uses as quality $Q$ the expected probability of reaching the target from current state, under the current probabilistic scheduler $\sigma$ (i.e. the probabilities from $\sigma$ contribute to $Q$). Therefore $\text{Max}$ does not need to reset the computed $s^+$ with each new $\sigma$ and keeps improving while $\text{Sum}_1$ needs to reset its estimates before each scheduler evaluation. $\text{Max}$ and Random consider the full count of the sampled paths, instead of counting sample by sample as done in $\text{Sum}_1$. Furthermore, $\text{Sum}_1$ needs to sample many times along the same paths to obtain good quality estimates; this makes pruning inapplicable to $\text{Sum}_1$. Finally, $\text{Sum}_1$ needs a determinization step and another round of evaluation for the induced Markov Chain, which are not needed in $\text{Max}$ and Random, because they directly estimate the maximum probabilities.

6. IMPLEMENTATION AND EXPERIMENTS

We have implemented Exact, $\text{Max}$ and Random (with and without pruning) together with the statistical procedure from [20], denoted $\text{Sum}_1$, within a generic framework on top of SPF. The framework can be easily extended with other algorithms for approximate analysis; we plan to make the tool available as open-source. Notable in the tool is the implementation for Monte Carlo sampling. Each sample is performed by one symbolic execution run, as guided by a JPF listener. The listener monitors for choices made during execution. Whenever a path-condition choice is encountered, the decision of exploring the then or the else branch is determined by generating a random number, $x \in [0,1]$, which is then compared with the computed conditional probabilities for the branches. A similar approach is taken for non-deterministic choices; for Random, the likelihood of selecting the choices is uniformly distributed whereas for $\text{Max}$, the probabilities are set according to the learning.

Case Studies We evaluated our implementation on the following multithreaded Java programs. \textbf{Windy}: An example from the reinforcement learning literature; a robot, affected by wind, moves in a grid with start and target positions. We use two versions: \textit{simple} (5 $\times$ 4 grid) and \textit{complex} (9 $\times$ 6 grid). \textbf{Daisy Chain Controller}: An example from previous work [13]: two threads run the actuation procedures for the flap controllers of an aircraft; it also includes a safety check. A wind effect hampers the operation by pushing on the flap’s head or tail. \textbf{MER Arbiter}: An example derived from a flight component for the Mars Exploration Rover developed at NASA JPL; it contains an arbiter and two user threads competing for shared resources. \textbf{Parallel Quick Sort (PQS)}: Three threads sort an array with six elements. It uses complex facilities from java.util.concurrent (e.g. Semaphore and ThreadPoolExecutor). We analyzed two versions based on the granularity with which data is bundled up and passed to the threads (\textit{complex} and \textit{simple}). \textbf{Airline}: Reservation system controlled by five threads with a bug based on data and thread choices. \textbf{Rare}: This is a “pathological” case for approximate analysis (see the code in Figure 4). We provide the source code at: \url{http://people.cs.aau.dk/~luckow/probabilistic/}

The experiments were run on a machine with an Intel Xeon E5-2670 2.60GHz and 64GB of memory.

Results Table 1 shows the results of a first set of experiments, where we compared all the techniques, for a fixed budget of scheduler samples. The best results are marked with bold. We have set the hypothesis $\theta$ according to the best probability obtained with Exact. We used default greediness $\epsilon = 0.5$ and history $h = 0.5$ as these were the best values suggested in [20]. We set restarts $T = 1$, we used a uniform usage profile, and grey paths were treated pessimistically. For each configuration, we conducted five trials and we picked the best result, i.e. the result with the lowest number of scheduler evaluations for verifying the hypothesis, or, if the hypothesis was not verified, the result with the probability closest to $\theta$.

The results indicate that $\text{Sum}_1$ performs poorly both in terms of analysis result and performance: the former is a result of each sample not carrying the full count information as is the case for the other techniques. Performance is a consequence of the required determination step. While exact analysis is tractable for this set of examples, the sampling-based techniques are consistently faster while still finding the optimal scheduler when the state space becomes sufficiently large (Daisy Depth 18 and PQS Simple). For the smaller examples, Random is slightly better than $\text{Max}$. From our results, it is difficult to conclude on good values of $N$ and $L$. Analysis of the larger examples indicates that $N < L$ seem to both verify the hypothesis in less scheduler evaluations or yield a better result regardless of whether pruning is used or not. The effect of pruning is evident; it is consistently better to use pruning for Random and $\text{Max}$. For $\text{Rare}$, the maximum probability of reaching success is easily computed with Exact but very difficult with $\text{Max}$ and Random. This is not surprising since it is known that purely statistical methods are typically ill-suited for “rare” events [39]. Our pruning techniques partially address the problem: in worst case both $\text{Max}_p$ and $\text{Random}_p$ explore all program paths (but not more – Proposition 2) and in general may finish much earlier. For $\text{Rare}$, both $\text{Max}_p$ and $\text{Random}_p$ confirmed the hypothesis (close to worst case), with $\text{Max}_p$ slightly better.

Table 2 shows the results for a second set of experiments, where we run all the techniques to determine the budget required to verify a hypothesis with fixed $\theta$. Here we use larger examples for which the exact analysis is intractable and only show results for the best techniques, namely $\text{Max}$ and Random with pruning. To determine the $\theta$ values we first ran experiments with approx 40K samples and $\theta = 1.0$. The best probability obtained was used as $\theta$ in the table.

Both $\text{Max}$ and Random enable increasing the bound of symbolic execution far beyond what can be analyzed with
Table 1: Exact vs. Max, Random and Sum; ‘P’ denotes pruning. If θ was not verified, values in parentheses after Samples show number of scheduler evaluations to establish the best result. Percentage of experiments where hypothesis was verified is shown next to Results.

<table>
<thead>
<tr>
<th>Example</th>
<th>Exact Analysis Result, Approx. Analysis N</th>
<th>L</th>
<th>Result Samples Time, [ms]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MER</strong></td>
<td>Simple Exact Analysis Result, Time, [ms], # of paths</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Random</td>
<td>1,000 –</td>
<td>0.5 (100%)</td>
</tr>
<tr>
<td></td>
<td>Random <em>P</em></td>
<td>1,000 –</td>
<td>0.5 (100%)</td>
</tr>
<tr>
<td></td>
<td>Max</td>
<td>10 100</td>
<td>0.5 (100%)</td>
</tr>
<tr>
<td></td>
<td>Max <em>P</em></td>
<td>10 100</td>
<td>0.5 (100%)</td>
</tr>
<tr>
<td></td>
<td>Sum</td>
<td>10 100</td>
<td>0.5 (100%)</td>
</tr>
<tr>
<td></td>
<td>Random</td>
<td>100 10</td>
<td>0.5 (100%)</td>
</tr>
<tr>
<td></td>
<td>Max <em>P</em></td>
<td>100 10</td>
<td>0.5 (100%)</td>
</tr>
<tr>
<td></td>
<td>Sum</td>
<td>100 10</td>
<td>0.5 (100%)</td>
</tr>
<tr>
<td></td>
<td>Windy Simple Exact Analysis Result, Time, [ms], # of paths</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Random</td>
<td>1,000 –</td>
<td>0.71 (100%)</td>
</tr>
<tr>
<td></td>
<td>Random <em>P</em></td>
<td>1,000 –</td>
<td>0.71 (100%)</td>
</tr>
<tr>
<td></td>
<td>Max</td>
<td>10 100</td>
<td>0.0 (0%)</td>
</tr>
<tr>
<td></td>
<td>Max <em>P</em></td>
<td>10 100</td>
<td>0.71 (100%)</td>
</tr>
<tr>
<td></td>
<td>Sum</td>
<td>10 100</td>
<td>0.71 (100%)</td>
</tr>
<tr>
<td></td>
<td>Random</td>
<td>100 10</td>
<td>0.71 (100%)</td>
</tr>
<tr>
<td></td>
<td>Max <em>P</em></td>
<td>100 10</td>
<td>0.71 (100%)</td>
</tr>
<tr>
<td></td>
<td>Sum</td>
<td>100 10</td>
<td>0.71 (100%)</td>
</tr>
<tr>
<td></td>
<td>Daisy Depth 13 Exact Analysis Result, Time, [ms], # of paths</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Random</td>
<td>1,000 –</td>
<td>0.029919 (%)</td>
</tr>
<tr>
<td></td>
<td>Random <em>P</em></td>
<td>1,000 –</td>
<td>0.029919 (%)</td>
</tr>
<tr>
<td></td>
<td>Max</td>
<td>10 100</td>
<td>0.029919 (%)</td>
</tr>
<tr>
<td></td>
<td>Max <em>P</em></td>
<td>10 100</td>
<td>0.029919 (%)</td>
</tr>
<tr>
<td></td>
<td>Sum</td>
<td>10 100</td>
<td>0.029919 (%)</td>
</tr>
<tr>
<td></td>
<td>Random</td>
<td>100 10</td>
<td>0.026860 (20%)</td>
</tr>
<tr>
<td></td>
<td>Max <em>P</em></td>
<td>100 10</td>
<td>0.026860 (20%)</td>
</tr>
<tr>
<td></td>
<td>Sum</td>
<td>100 10</td>
<td>0.026860 (20%)</td>
</tr>
<tr>
<td></td>
<td>Daisy Depth 18 Exact Analysis Result, Time, [ms], # of paths</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Random</td>
<td>1,000 –</td>
<td>0.024507 (%)</td>
</tr>
<tr>
<td></td>
<td>Random <em>P</em></td>
<td>1,000 –</td>
<td>0.024507 (%)</td>
</tr>
<tr>
<td></td>
<td>Max</td>
<td>10 100</td>
<td>0.027448 (%)</td>
</tr>
<tr>
<td></td>
<td>Max <em>P</em></td>
<td>10 100</td>
<td>0.028625 (20%)</td>
</tr>
<tr>
<td></td>
<td>Sum</td>
<td>10 100</td>
<td>0.025978 (%)</td>
</tr>
<tr>
<td></td>
<td>Random</td>
<td>100 10</td>
<td>0.025684 (%)</td>
</tr>
<tr>
<td></td>
<td>Max <em>P</em></td>
<td>100 10</td>
<td>0.025684 (%)</td>
</tr>
<tr>
<td></td>
<td>Sum</td>
<td>100 10</td>
<td>0.025684 (%)</td>
</tr>
<tr>
<td></td>
<td>Rare Exact Analysis Result, Time, [ms], # of paths</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Random</td>
<td>1,000 –</td>
<td>0.01 (100%)</td>
</tr>
<tr>
<td></td>
<td>Random <em>P</em></td>
<td>1,000 –</td>
<td>0.01 (100%)</td>
</tr>
<tr>
<td></td>
<td>Max</td>
<td>10 100</td>
<td>0.01 (100%)</td>
</tr>
<tr>
<td></td>
<td>Max <em>P</em></td>
<td>10 100</td>
<td>0.01 (100%)</td>
</tr>
<tr>
<td></td>
<td>Sum</td>
<td>10 100</td>
<td>0.01 (100%)</td>
</tr>
<tr>
<td></td>
<td>Random</td>
<td>100 10</td>
<td>0.01 (100%)</td>
</tr>
<tr>
<td></td>
<td>Max <em>P</em></td>
<td>100 10</td>
<td>0.06 (100%)</td>
</tr>
<tr>
<td></td>
<td>Sum</td>
<td>100 10</td>
<td>0.06 (100%)</td>
</tr>
<tr>
<td></td>
<td>PQS Simple Exact Analysis Result, Time, [ms], # of paths</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Random</td>
<td>1,000 –</td>
<td>0.59179 (100%)</td>
</tr>
<tr>
<td></td>
<td>Random <em>P</em></td>
<td>1,000 –</td>
<td>0.89498 (100%)</td>
</tr>
<tr>
<td></td>
<td>Max</td>
<td>10 100</td>
<td>0.64467 (100%)</td>
</tr>
<tr>
<td></td>
<td>Max <em>P</em></td>
<td>10 100</td>
<td>0.994976 (100%)</td>
</tr>
<tr>
<td></td>
<td>Sum</td>
<td>10 100</td>
<td>0.43527 (100%)</td>
</tr>
<tr>
<td></td>
<td>Random</td>
<td>100 10</td>
<td>0.60508 (100%)</td>
</tr>
<tr>
<td></td>
<td>Max <em>P</em></td>
<td>100 10</td>
<td>0.97603 (100%)</td>
</tr>
<tr>
<td></td>
<td>Sum</td>
<td>100 10</td>
<td>0.97603 (100%)</td>
</tr>
<tr>
<td></td>
<td>Random</td>
<td>10,000 –</td>
<td>0.97179 (100%)</td>
</tr>
<tr>
<td></td>
<td>Random <em>P</em></td>
<td>10,000 –</td>
<td>1.0 (100%)</td>
</tr>
<tr>
<td></td>
<td>Max</td>
<td>10 1,000</td>
<td>0.98888 (100%)</td>
</tr>
<tr>
<td></td>
<td>Max <em>P</em></td>
<td>10 1,000</td>
<td>1.0 (100%)</td>
</tr>
<tr>
<td></td>
<td>Max</td>
<td>1,000 10</td>
<td>0.98181 (100%)</td>
</tr>
<tr>
<td></td>
<td>Max <em>P</em></td>
<td>1,000 10</td>
<td>1.0 (100%)</td>
</tr>
<tr>
<td></td>
<td>Sum</td>
<td>1,000 10</td>
<td>0.45450 (100%)</td>
</tr>
</tbody>
</table>
Table 2 Random vs. Max (w/ pruning); Exact runs out of memory.

<table>
<thead>
<tr>
<th>Example</th>
<th>Hypothesis</th>
<th>Approx. Analysis</th>
<th>Samples</th>
<th>Time [ms]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windy</td>
<td>$P_r(P) \geq \max P_r$</td>
<td>Random $P_r$</td>
<td>23</td>
<td>8,688</td>
</tr>
<tr>
<td>Complex</td>
<td>0.71</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Daisy</td>
<td>$P_r(P) \geq \max P_r$</td>
<td>Random $P_r$</td>
<td>136</td>
<td>38,261</td>
</tr>
<tr>
<td>Depth 20</td>
<td>0.028723</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Daisy</td>
<td>$P_r(P) \geq \max P_r$</td>
<td>Random $P_r$</td>
<td>129</td>
<td>43,347</td>
</tr>
<tr>
<td>Depth 30</td>
<td>0.029409</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PQS</td>
<td>$P_r(P) \geq \max P_r$</td>
<td>Random $P_r$</td>
<td>3,075</td>
<td>1,273,642</td>
</tr>
<tr>
<td>Complex</td>
<td>1.0</td>
<td></td>
<td>12,047</td>
<td>3,914,474</td>
</tr>
<tr>
<td>Airline</td>
<td>$P_r(P) \geq \max P_r$</td>
<td>Random $P_r$</td>
<td>169</td>
<td>40,851</td>
</tr>
</tbody>
</table>

Exact; increasing the bound naturally reveals more information about the paths. For example, for Daisy Chain Controller at depth limit 20, we can find a scheduler with a better probability for success than the exact analysis shown in Table 1. These results furthermore demonstrate the benefits of reinforcement learning as compared to Random when the state space is large (see all cases except Windy Complex).

Our approximate algorithms are well suited for exploring systems with large state spaces but that are well structured, i.e. they may have multiple components running the same or similar algorithms and have few interactions points between components (e.g. MER, Daisy, Windy). Common examples include planning and scheduling for robots, control software for aircrafts and many critical applications of interest. However, for unstructured systems (e.g. Rare) the approximate algorithms require scheduling decisions to be made on all states, thus defeating their purpose. This is confirmed by the related literature [39, 20] and more research is needed to address the issue.

Non-Uniform Usage Profiles To see how our approach applies for non-uniform usage profiles, let us revisit the Daisy Chain Controller and consider two different scenarios where the wind effect is weak ($UP_w$) and strong ($UP_s$), respectively (see Figure 3). In particular, the weak and strong wind usage profiles are defined as the case where respectively 5% and 15% of the input values yield wind $> 10$. We would expect that under the conditions of $UP_w$, the flap controller is more likely to operate successfully because the flap is less likely to exceed the goal position. We use a symbolic variable, up, constrained such that $1 \leq up \leq 100$, for controlling the distribution of the input values for the wind variable.

Listing 1 and Listing 2 show how $UP_w$ and $UP_s$ are encoded as preconditions, i.e. assume statements in the code. The assume statements are implemented using the built-in Debug.assume() method from SPF. With the usage profiles, we ran Exact and obtained $Pr_{UP_w} = 0.048387$ which is indeed better than $Pr_{UP_s} = 0.024037$.

7. RELATED WORK

In previous work [15] we defined the probabilistic symbolic analysis for Java programs that forms the basis of our work here. However in [15] we only discuss exact algorithms and multithreading is treated by computing probabilities along linear schedules. As we already explained in Section 2 this is insufficient in general. In recent work we have investigated approximate procedures for the probabilistic analysis of floating-point programs [6] and for the scalable probabilistic symbolic execution of sequential code [16]. However none of these approaches address sampling for nondeterministic programs and hence the challenge of computing (near)optimal schedulers.

Other related work includes probabilistic abstract interpretation [25], probabilistic static analysis [10, 9] and probabilistic model checking [3, 17, 2]. In particular the program analysis from [3] is relevant here as it performs aggressive pruning, but not for symbolic execution. Again none of these works address sampling in the presence of nondeterminism which is one of the main contributions here.

Statistical verification techniques [27, 25, 36, 13] perform sampling over the analyzed state spaces, but aside from the work in [20], there are very few other approaches that study nondeterminism, e.g. [20, 9]. In [26] random sampling is exploited to search for a near-optimal scheduler, whose quality is again evaluated by a statistical approach. However, the iterative use of the conservative Chernoff-Hoeffding bound [21] to determine the necessary number of samples might require an impractically large number of them. The work in [4] studies partial order reductions for MDPs to reduce nondeterminism, and thus it is orthogonal to ours. Our work is also generally related to planning for MDPs [23, 34, 37]. In the future we plan to investigate whether our techniques are applicable to planning as well.

8. CONCLUSIONS AND FUTURE WORK

We presented exact and approximate symbolic execution techniques for the probabilistic analysis of nondeterministic programs. We implemented and evaluated them showing improvement over established techniques.

In the future we plan to investigate replacing the exact model counting with approximate quantification (e.g. QCorel [9] for floating-point constraints). We would need to revise our theoretical results but we note that one of our main results (Proposition 2) would hold too.

The sampling process is highly parallelizable. We implemented a parallel prototype and results show improvement in performance, even though some overhead due to thread contention is inevitable; e.g. distributing the workload to two clients for Example 1, reduces the analysis runtime by 30%. More experimentation is planned for the future.
REFERENCES


[29] J. Musa. The operational profile. In S. Özekici, editor,


