Incremental Bounded Software Model Checking

Henning Günther  
Vienna University of Technology, Austria  

Georg Weissenbacher  
Vienna University of Technology, Austria

ABSTRACT

Conventional Bounded Software Model Checking tools generate a symbolic representation of all feasible executions of a program up to a predetermined bound. An insufficiently large bound results in missed bugs, and a subsequent increase of the bound necessitates the complete reconstruction of the instance and a restart of the underlying solver. Conversely, exceedingly large bounds result in prohibitively large decision problems, causing the verifier to run out of resources before it can provide a result.

We present an incremental approach to Bounded Software Model Checking, which enables increasing the bound without incurring the overhead of a restart. Further, we provide an LLVM-based open-source implementation which supports a wide range of incremental SMT solvers. We compare our implementation to other traditional non-incremental software model checkers and show the advantages of performing incremental verification by analyzing the overhead incurred on a common suite of benchmarks.

Categories and Subject Descriptors

D.2.4 [Software Engineering]: Software/Program Verification—Bounded Model Checking

General Terms

Experimentation, Performance

Keywords

LLVM, Incremental, SMT, C

1. INTRODUCTION

Bounded Model Checking (BMC) is arguably one of the most successful and widely used formal verification techniques, as witnessed by the TACAS most influential paper award for Biere et al.’s seminal paper [5]. As BMC performs a symbolic exploration of execution traces up to a bounded length only, the primary application of the technique is the detection of bugs. While BMC was initially aimed at hardware designs, it has since become a standard technique for software verification that is implemented in numerous verification tools [13].

We illustrate the inner workings of a typical implementation of BMC for software using the program in Figure 1a. The program implements Wegner’s algorithm [25] to assert that more than 7 bits (or flags) in a bit-vector \( x \) are set if \( x \) matches a certain bit-mask. Bounded software model checking tools such as LLBMC [21] or CBMC [9] unwind the control flow graph (CFG) of the program into a directed acyclic graph (DAG) until a certain user-specified bound is reached, and convert the resulting loop-free code into static single assignment (SSA) form [11]. Figures 1b and 1c illustrate this process for the unwinding depths one and two, respectively. To avoid a blowup of the DAG, the loop exit edges (dashed in Figure 1) are merged after each loop iteration. Since each variable is assigned only once along each path in SSA form, this requires a case split to determine the value of variable \( c \) at node \( u \). (In the SSA representation, this is typically indicated using a \( \phi \) function \( c_3 := \phi(c_1, c_2) \).) For Figure 1b, we obtain the encoding in Figure 2.

By negating the assertion we achieve that any satisfying assignment (provided by a satisfiability checker) of this instance corresponds to a program execution that violates the assertion. The given instance, however, is unsatisfiable, indicating that there is no path that traverses the loop at most one time and violates the assertion. To detect a bug, we need to increment the loop bound and reconstruct the formula (since the disjunctive case split cannot be augmented), or provide a sufficiently large bound in the first place.

For the given program, determining that 3 is the smallest bound admitting an assertion violation is non-trivial unless one understands that the assignment \( y := y \land (y-1) \) resets the right-most bit in \( y \) that is one. Safe over-estimations (e.g., the bit-width of \( x \)) lead to unnecessarily hard problem instances for the satisfiability solver, and under-estimations necessitate expensive restarts.

BMC tools deploy contemporary SAT or SMT solvers and benefit greatly from the impressive advances in this field [6]. A characteristic of most modern SMT solvers is that they solve formulas incrementally, reusing the results of previous calls whenever the formula is augmented with additional conjuncts. Additionally, incremental solvers make it possible to add formulas on a tentative basis and later retract them without requiring a restart.
2. INCREMENTAL BMC

2.1 Programs

A program is a directed graph \( \langle \text{Locs}, \text{Stmts} \rangle \) with nodes \( \text{Locs} \) (representing the program locations including the initial location \( l_0 \in \text{Locs} \)) and edges \( \text{Stmts} \) annotated with guarded assignments \( \langle \gamma, x := e \rangle \), where the guard \( \gamma \) is a predicate over the program variables, and \( e \) is an expression assigned to variable \( x \). The guard may be omitted if it is true and the assignment may be omitted if the edge is a conditional jump. The semantics of guarded assignments is determined by the predicate transformer

\[
\text{sp}(\langle \gamma, x := e \rangle, \varphi) \overset{\text{def}}{=} \exists x_i. (\varphi \land \gamma)[x/x_i] \land (x = e[x/x_i]),
\]

where \( i \) is a fresh index and \( \varphi[x/x_i] \) denotes the formula \( \varphi \) with all free occurrences of \( x \) replaced by \( x_i \).

An unwinding of a program \( \langle \text{Locs}, \text{Stmts} \rangle \) is a connected DAG \( (V, E) \) with nodes \( V \) and edges \( E \) such that there exists a mapping \( \ell : V \rightarrow \text{Locs} \) and for every \( \langle u, v \rangle \in E \) we have \( \langle \ell(u), \ell(v) \rangle \in \text{Stmts} \), and each edge \( \langle u, v \rangle \in E \) is accordingly annotated with a guarded assignment \( \text{stmt}(u, \ell(u)) \). Moreover, there is a unique root node \( v_0 \in V \) with \( \ell(v_0) = l_0 \).

Figures 1b and 1c show unwindings for the program in Figure 1a. Given an unwinding \( (V, E) \), the formulas \( \psi_v \) representing reachable states for each node \( v \in V \) are defined inductively:

\[
\psi_v \overset{\text{def}}{=} \begin{cases} 
\text{true} & \text{if } v = v_0 \\
\bigvee_{(u, v) \in E} \text{sp}(\text{stmt}(u, v), \psi_u) & \text{otherwise}
\end{cases}
\tag{1}
\]

This symbolic representation can be derived from the SSA form of an unwinding in a straightforward manner. An assertion \( \text{assert}(\alpha) \) at node \( v \in V \) can be violated if \( \psi_v \land \neg \alpha \) is satisfiable, which can be easily checked using an SMT solver.

2.2 Merge Nodes

The iterative expansion of a given unwinding \( (V, E) \) results in new loop exit edges incident to the node succeeding the loop (node \( u \) in Figure 1, for instance). These nodes, which we call merge nodes, are chosen in a manner such that the resulting expanded unwinding remains cycle-free. Expanding the unwinding increases the in-degree of merge nodes \( v \in V \) and necessitates a modification of the corresponding predicate \( \psi_v \) defined above (1).

While contemporary SMT solvers allow for adding additional conjuncts to the formulas \( \psi_v \) (1), an expansion of the disjunctions for merge nodes \( v \) is not possible, thus requiring a reconstruction of \( \psi_v \) and a restart of the solver.
2.3 Incremental Representation

To avoid the problem described above, we use a symbolic representation of unwinding \((V,E)\) that can be extended on demand. An SSA representation of \((V,E)\) guarantees that exactly one version of each program variable is associated with each node \(v\) (e.g., \(c_2\) and \(y_2\) at \(v_1\) and \(c_2\) at \(u\) in Figure 1b). We use \(x_v\) to denote the SSA version of \(x\) in scope at node \(v\).

For each node \(v\), we introduce a propositional activation variable \(a_v\) which indicates whether the unwinding contains a feasible execution path reaching \(v\). Given an unwinding \((V,E)\) in SSA form, \(a_v\) is constructed as follows:

\[
a_v \equiv \begin{cases} 
\text{true} & \text{if } v = v_0 \\
\forall_{(u,v) \in E} (a_u \land \gamma) \\
\text{where } \text{stmt}(u,v) = ([\gamma], \_)
\end{cases}
\]

For node \(u\) in Figure 1b, for instance, we obtain

\[
a_u = p_u \lor (a_{v_0} \land (y_1 = 0)) \lor (a_{v_1} \land (y_2 = 0)).
\]

The disjunct \(p_u\) is an optional proxy variable which is only introduced at merge nodes. Proxy variables enable us to retroactively introduce additional incoming edges in the encoding. This technique is similar to an encoding used for LTL [17]. The expansion of the unwinding in Figure 1b to the unwinding in Figure 1c results in the constraint \(p_u = (a_{v_0} \land (y_2 = 0) \lor p_v)\), where \(p_v\) is a fresh proxy variable. Whenever we call the SMT solver, “dangling” proxy variables are constrained by adding a retractable formula \(\neg p_u\).

Unlike in Formula 1, assignments are modeled as separate constraints:

\[
\bigwedge_{x_v} \left( \{ x_v = e \mid (u,v) \in E \land \text{stmt}(u,v) = ([\gamma], \_). \right.
\]

Nodes for which the variable versions of the incoming edges disagree are annotated with \(\phi\) functions in SSA (e.g., \(c_3 = \phi(c_1, c_2)\) for node \(u\) in Figure 1b). A \(\phi\) function for \(x\) at node \(v\) is encoded as

\[
\bigwedge_{(u,v) \in E} ((a_u \land \gamma) \Rightarrow (x_v = x_u)) \text{ (where } \text{stmt}(u,v) = ([\gamma], \_))
\]

(assuming that \(\text{stmt}(u,v)\) does not update \(x_u\)). Formula 3 can be augmented upon expansion of the unwinding. The encoding of \(c_3 = \phi(c_1, c_2)\) at node \(u\) in Figure 1b is \((a_{v_0} \land (y_1 = 0) \Rightarrow (c_3 = c_1)) \land (a_{v_1} \land (y_2 = 0) \Rightarrow (c_3 = c_2))\), to which \(a_{v_2} \land (y_3 = 0) \Rightarrow (c_3 = c_4)\) is added upon further unwinding (Figure 1c).

Assertions are represented using propositional variables \(b_v\) which are constrained with the negated assertion condition and the activation variable of the respective node. The assertion in Figure 1 yields the constraint

\[
b_u = a_u \land ((x\&42 = 42) \land (c_3 \leq 7)).
\]

To check for assertion violations, we assert a disjunction over all assertion variables.

2.4 Pointers and Memory

Dynamic memory accesses are implemented by maintaining a set of memory states \(\text{Mem}\) and a set of pointers \(\text{Ptrs}\). Each memory state represents the state of the memory at a certain point of program execution and contains a set of all the allocated memory objects. Each memory object is represented by a bitvector SMT-variable and has a unique identifier. For a memory-state \(m \in \text{Mem}\), we write \(m(i)\) to refer to the memory object identified by \(i\). Every pointer \(p \in \text{Ptrs}\) has two attributes:

- A set of object identifiers \(\text{points-to}(p)\) which keeps track of all the objects the pointer \(p\) can potentially point to. This is required to limit the number of case splits over the objects the pointer can actually point to, which reduces the strain on the SMT solver.
- The SMT representation of the actual object identifier the pointer points to, referred to as \(\text{repr}(p)\). This can be any SMT expression such that it evaluates to one of the object identifiers in its \(\text{points-to}\) set, i.e.,

\[
\bigvee_{i \in \text{points-to}(p)} \text{repr}(p) = i
\]

always holds.

In the following, we introduce a set of memory instructions which we use to encode constraints over \(\text{Mem}, \text{Ptrs}\), and the program variables. As the program is unwound incrementally, the program statements are converted into memory instructions, which are then applied to successively add the corresponding constraints to the encoding.

- **connect** \(c m_1 m_2\) enforces the conditional equivalence of the memory states \(m_1\) and \(m_2\). This is achieved by generating constraints such that

\[
c \Rightarrow (\forall i. m_1(i) = m_2(i))
\]

holds. Note that the quantifier can be expanded, since the number of objects \(i\) is finite.

- **connect_ptr** \(c p_1 p_2\) connects the pointers \(p_1\) and \(p_2\) if the condition \(c\) holds. The memory model must generate constraints to make \(c \Rightarrow \text{repr}(p_1) = \text{repr}(p_2)\) and \(\forall i \in \text{points-to}(p_1), i \in \text{points-to}(p_2)\) true.

- **alloc** \(m p s m_2\) allocates a new object of size \(s\) and creates a new state \(m_2\), which contains the new object and all previous objects of \(m_1\). The pointer \(p\) is initialized to point to the new object. Accordingly, for the fresh object identifier \(i\) and the SMT bitvector variable \(v\) representing the new object, the instruction yields the following:

\[
\forall i' \neq i, m_2(i') = m_1(i'), \\
m_2(i) = v, \text{repr}(p) = i, \text{ and} \\
\text{points-to}(p) = \{i\}.
\]

- **null** \(p\) constrains the pointer \(p\) to point to the null object. The representation of the null object is 0 and the points-to set is empty:

\[
(\text{repr}(p) = 0) \land (\text{points-to}(p) = \emptyset)
\]

- **load** \(m p r\) assigns the content of pointer \(p\) in state \(m\) into the SMT variable \(r\). The encoding guarantees that if the representation of the pointer \(p\) matches an object identifier \(i\) then the result \(r\) will be the memory object \(m(i):\)

\[
\bigwedge_{i \in \text{points-to}(p)} (\text{repr}(p) = i \Rightarrow (r = m(i))).
\]
The constraint

\[ m_2(i) = \begin{cases} 
  v & \text{if } i \in \text{points-to}(p_1) \land \text{repr}(p) = i \\
  m_1(i) & \text{otherwise}
\end{cases} \]

is maintained for all objects \( i \).

- **connect \( p_1 \) \( p_2 \) \( r \)** compares the pointer \( p_1 \) and \( p_2 \) for equality and stores the result in the SMT variable \( r \), such that \( r = (\text{repr}(p_1) = \text{repr}(p_2)) \) holds.

Since the points-to sets of pointers can change due to new connect-instructions, load and store instructions from or to these changed pointers have to be augmented to take the newly reachable objects into account. Consider the example given in Figure 3. Every node \( v \) in the CFG has a memory state \( m_v \) associated with it. Since the assignment \( p_0 := q_0 \) does not manipulate the dynamically allocated memory, we have \( m_{p_0} = m_{q_0} \). At the \((a,b)\) edge, the address of \( q_0 \) gets assigned to \( p_0 \), so we use \( q_0 \) instead of introducing an alias pointer.

To realize the edge \((b,g)\), we must first connect the pointer \( q_0 \) to the pointer \( p_3 \) (associated with node \( g \)). This means that we have to initialize the points-to set for \( p_3 \) with the one of \( q_0 \). Suppose that \( q_0 \) can point to two object identifiers \( i_0 \) and \( i_1 \), which are represented in \( m_{q_0} \) by the objects \( m_{q_0}(i_0) \) and \( m_{q_0}(i_1) \). We obtain points-to\((p_3) = \{i_0, i_1\} \). We also get the following constraint for the SMT instance: \( c_b \Rightarrow \text{repr}(p_3) = \text{repr}(q_0) \).

Then we have to connect the memory state \( m_{p_0} \) to \( m_{q_0} \), which yields \( c_b \Rightarrow m_{q_0}(i_0) = m_{p_0}(i_0) \) and \( c_b \Rightarrow m_{q_0}(i_1) = m_{p_0}(i_1) \).

Suppose that \( p_1 \) can only point to the object identified by \( i_0 \). Storing 15 to this pointer creates a new memory state \( m_{p_1} \) in which \( m_{p_1}(i_0) = 15 \). Connecting \( p_1 \) to \( p_3 \) does not change the points-to set of \( p_3 \) since \( i_0 \) is already contained in it. However, we get the new SMT constraint \( c_d \Rightarrow \text{repr}(p_3) = \text{repr}(p_1) \).

By connecting \( m_{p_0} \) to \( m_{p_1} \), we only get one constraint, namely \( c_d \Rightarrow m_{p_0}(i_0) = m_{p_1}(i_0) \), since \( m_{p_0} \) does not contain \( i_1 \).

Loading from pointer \( p_3 \) at edge \((g,h)\) entails adding a constraint for each object identifier in points-to\((p_3)\): \( \text{repr}(p_3) = i_0 \Rightarrow r = m_{q_0}(i_0) \) and \( \text{repr}(p_3) = i_1 \Rightarrow r = m_{q_0}(i_1) \).

Now the third incoming edge is added in step 2; suppose that \( m_{p_2} \) is empty, so the allocation creates a fresh variable \( v \) of 4 bytes and a fresh identifier \( i_2 \) such that \( m_f(i_2) = v \).

The pointer \( p_2 \) is created with the singleton points-to set points-to\((p_2) = \{i_2\} \) and the representation \( \text{repr}(p_2) = i_2 \). Connecting the pointers \( p_2 \) and \( p_3 \) now adds the new object identifier \( i_2 \) into the points-to set of \( p_3 \), so we have to augment the SMT formulas generated by the load instruction from \( p_3 \) by the following formula: \( \text{repr}(p_3) = i_2 \Rightarrow r = m_{q_0}(i_2) \).

The constraints \( c_f \Rightarrow \text{repr}(p_3) = \text{repr}(p_2) \) and \( c_f \Rightarrow m_f(i_2) \) are added as before. After adding these constraints \( r \) now represents every possible loading result of the three incoming edges.

### 2.5 Catching Memory Bugs

To detect invalid memory accesses (either loads from or stores to null-pointers), we must generate an assertion \( \text{repr}(p) \neq 0 \) for every memory instruction \textit{load} \( m \) \( p \) \( r \) or \textit{store} \( m \) \( v \) \( p \) \( m_2 \). However, oftentimes we can actually statically infer that \( p \) can never be a null pointer. We can accomplish this by introducing a special object identifier \( i_{null} \) which identifies no allocated object but instead its presence in a points-to set signifies that the pointer can potentially be null. With this in place, we only have to generate the assertions for pointer with \( i_{null} \in \text{points-to}(p) \).

### 2.6 Extending the Memory Model

The memory model described above is very limited and only able to handle very simple programs without arrays, pointer indirections, casts or structs. We informally describe the various extensions implemented in Nbis to handle more complex programs here:

- **Pointer stores and loads.** To enable the memory model to store and load pointers to/from other pointers we need to extend each memory object with a points-to set. Whenever a pointer is loaded from a memory object, it inherits its points-to information from the memory object. Similarly, storing a pointer transfers its points-to information to the memory-object.

- **Structures.** Instead of representing each memory model with one single SMT variable, we can allow a memory object to be composed of multiple SMT variables, where each variable represents a field in structure data type.

- **Arrays.** While arrays of a constant size can be handled by creating an SMT variable for each array element, arrays with a variable size require more thought. We can represent arrays of dynamic size using the SMT theory of arrays with McCarthy’s \textbf{select} and \textbf{update} functions to manipulate arrays. Each array is represented by an SMT array variable representing the content of the array and a bitvector variable storing the size of the array for error checking (if the array index is larger than the size variable, we detect a memory access violation).
Since LLVM handles all arrays as heap objects, we have to augment the symbolic representation of pointers. Instead of having the pointer representation only identify the object the pointer is pointing to, we split the pointer representation into two parts: The first part of the pointer represents the object identifier, as before, while the second half of the pointer representation can be used to represent a potential offset into the object. To avoid having to check for all possible offsets into a given object, we can also augment the points-to set of pointers with a set of offsets that the pointer can potentially represent.

- **Global variables.** Since global variables are implemented in LLVM as pointers to pre-allocated objects, a global variable \( v \) can be represented by an object identifier \( i_v \) which is present in every memory state and a pointer \( p_v \) which only points to the object identified by \( i_v \). We generate a memory instruction \( \text{alloc} m_0 p_v s m_{\text{start}} \) at the beginning of the unrolling where \( s \) is the size of the global variable and \( m_{\text{start}} \) is the initial memory state for the program.

- **Pointer casts.** Since the C-language allows almost every possible conversion between pointers, care has to be taken to incorporate pointer casts into the memory model. For example, if the program casts a pointer to a 64-bit integer into a byte-array and accesses the pointer using a dynamic offset, the loading instruction has to generate a case split over all the byte components of the integer.

2.7 Optimizations

Since increasing the bound may add new incoming edges to merge nodes, it is not possible to safely infer information about the values of variables from a given unrolling. Accordingly, optimizations such as constant-propagation, elimination of overflow-checks, etc. can only be applied by performing an up-front static analysis of the program. We perform an approximate static analysis to infer the following information: (a) lower and upper bounds of variables to remove redundant array-bounds checks, (b) access and alignment information for data structures to simplify load and store instructions, (c) alias information to remove redundant checks for null-pointer accesses.

3. EVALUATION

To evaluate our approach, we implemented it in a tool called Nbis, written in Haskell. Nbis uses the intermediate representation of the LLVM compiler framework [19], which simplifies the handling of the complex semantics of the C programming language. Our implementation supports a range of SMT solvers such as Z3 [12], MathSAT [8], STP [16], CVC4 [2], Yices [14], and others supporting the SMT-LIB standard [3]. The implementation is available under the terms of the GNU public license version 3 (GPL3) on github (https://github.com/hgunther/nbis).

To demonstrate the feasibility of incremental verification, we evaluated Nbis on the programs in the bitvector category of the SV-COMP 2013. First, we compared Nbis in non-incremental mode to the state-of-the-art tools CBMC [9], ESBMC [10], and LLBMC [21]. Since CBMC relies on bit-blasting and a SAT-solver, we compared it to Nbis running with the STP [16] backend. We also compared Nbis in this configuration with LLBMC, since it also uses STP as its backend. ESBMC, on the other hand, uses Z3 [12] as a solver, so we used the same solver as the backend in our comparison. Figure 4 shows the running times of these tools plotted with a logarithmic time-scale. The performance of Nbis running with STP is comparable (and often even better) than CBMC and only slightly worse than LLBMC. Comparing Nbis with ESBMC, we can see that Nbis fares better on every benchmark.

To measure the performance overhead of incremental BMC, we ran Nbis on every benchmark with different SMT-backends and compared the performance to the running time in non-incremental mode. A fair comparison between incremental and non-incremental BMC is difficult, because the run-time is influenced by the following parameters:

1. **Unwinding depth.** In the presence of a bug, the non-incremental approach is at a disadvantage if the unwinding depth significantly exceeds the depth at which the bug manifests itself.

2. **Check interval.** By default, Nbis checks for bugs after each unwinding, resulting in a significant overhead if each unwinding step only adds a small number of constraints to the instance. By increasing the number of unwindings after which a check is performed to the unwinding depth, we can enforce that only one SAT query is made, which is equal to the non-incremental algorithm.

Since it is always possible to tweak these parameters in favor of either incremental or non-incremental BMC, we measure the worst case for incremental verification:

- The bound for the non-incremental is set to the minimal depth where the bug appears. If no bug is present and a completeness threshold can be computed, it is used as the bound. Otherwise a bound of 10 is selected.

- The incremental algorithm checks for bugs after each unwinding step.

Table 1 shows the overhead of running the incremental algorithm on the problem instances, where an overhead of \( n \) means that the incremental version took \( n \) times as long to complete. Missing entries indicate a time-out, which was set to 30 seconds. The smallest overhead is highlighted.

We make the following observations:

1. The performance of incremental verification is contingent on the solver: There are many examples—such as “gcd 3”—where some solvers perform significantly better than the rest.

2. Many examples from the bitvector benchmark suite show a less-than twofold increase in execution time, even under the worst possible circumstances. This is very encouraging, as it suggests that the approach is indeed viable for a wide range of examples.

3. Large overheads (such as the 12-fold increase of running time in the “modulus safe” benchmark) are owed to the fact that incremental BMC prevents constant propagation in the unwinding. This problem can be mitigated by performing an up-front static analysis to detect constants. We will add this feature in a future version of Nbis.
Figure 4: Non-incremental verification times

Figure 5: Runtime comparison on the “s3 clnt 2 safe” benchmark

Figure 5 illustrates the runtime variation resulting from the different performance characteristics of the SMT solvers: We ran Z3 and STP on the “s3 clnt 2 safe”-benchmark and compared the running times for each unwinding depth. While STP has a linear increase in running time both in incremental and non-incremental mode, Z3 shows a much steeper curve in incremental mode. As of yet, the reasons for these differences between solvers are unknown to the authors.

Figure 5 also illustrates that the additional cost of incremental verification amortizes quickly once the non-incremental solver is restarted for the first time: For the given example, the overhead of the incremental algorithm is never larger than the cost of restarting the non-incremental algorithm.

4. RELATED WORK

A number of verification tools, such as CBMC [9], ESBMC [10], and LLBMC [21], F-Soft [18], SMT-BMC [1] are based on non-incremental BMC. CBMC performs bit-blasting and uses the SAT solver MINISAT [15] to solve the resulting propositional problem, while SMT-BMC and ESBMC deploy an SMT solver. ESBMC and CBMC use the same front-end for parsing C-files. F-Soft stands out as it performs several static analyses on the program in order to simplify the resulting unwinding instance. LLBMC bears the closest similarity with NBIS, since it also uses the LLVM internal representation. None of these tools allow the bound to be increased incrementally.
Table 1: Incremental verification time overhead

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>S</th>
<th>STP</th>
<th>MathSAT</th>
<th>Boolector</th>
<th>CVC</th>
<th>Yices</th>
</tr>
</thead>
<tbody>
<tr>
<td>byte add 1</td>
<td>6.8</td>
<td>7.6</td>
<td>54.9</td>
<td>11.5</td>
<td>11.5</td>
<td>10.7</td>
</tr>
<tr>
<td>byte add 2</td>
<td>6.5</td>
<td>8.2</td>
<td>39.1</td>
<td>15.0</td>
<td>12.6</td>
<td>14.8</td>
</tr>
<tr>
<td>byte add u</td>
<td>5.1</td>
<td>5.8</td>
<td>9.2</td>
<td>47.0</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>gcd 1</td>
<td>1.1</td>
<td>1.0</td>
<td>3.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>gcd 2</td>
<td>–</td>
<td>5.7</td>
<td>3.0</td>
<td>–</td>
<td>1.3</td>
<td>–</td>
</tr>
<tr>
<td>gcd 3</td>
<td>–</td>
<td>7.8</td>
<td>2.7</td>
<td>–</td>
<td>–</td>
<td>1.3</td>
</tr>
<tr>
<td>gcd 4</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>interl. bits</td>
<td>1.3</td>
<td>1.1</td>
<td>1.1</td>
<td>1.2</td>
<td>1.1</td>
<td>1.0</td>
</tr>
<tr>
<td>jain 1</td>
<td>1.1</td>
<td>1.3</td>
<td>1.0</td>
<td>1.1</td>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>jain 2</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.3</td>
<td>1.0</td>
<td>1.1</td>
</tr>
<tr>
<td>jain 3</td>
<td>1.3</td>
<td>1.0</td>
<td>1.1</td>
<td>1.4</td>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>jain 4</td>
<td>1.0</td>
<td>1.1</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.1</td>
</tr>
<tr>
<td>jain 5</td>
<td>1.3</td>
<td>1.1</td>
<td>1.0</td>
<td>1.3</td>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>jain 6</td>
<td>1.2</td>
<td>1.0</td>
<td>1.0</td>
<td>1.1</td>
<td>1.1</td>
<td>1.0</td>
</tr>
<tr>
<td>jain 7</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>modulus</td>
<td>11.7</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>num conv. 1</td>
<td>1.1</td>
<td>1.1</td>
<td>1.0</td>
<td>1.1</td>
<td>1.1</td>
<td>1.0</td>
</tr>
<tr>
<td>num conv. 2</td>
<td>1.2</td>
<td>1.0</td>
<td>1.1</td>
<td>1.1</td>
<td>1.1</td>
<td>1.0</td>
</tr>
<tr>
<td>parity</td>
<td>14.9</td>
<td>14.4</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>s3 clnt 1 s</td>
<td>5.2</td>
<td>6.7</td>
<td>10.5</td>
<td>2.6</td>
<td>–</td>
<td>2.5</td>
</tr>
<tr>
<td>s3 clnt 1 u</td>
<td>1.7</td>
<td>2.3</td>
<td>2.3</td>
<td>1.4</td>
<td>–</td>
<td>1.8</td>
</tr>
<tr>
<td>s3 clnt 2 s</td>
<td>1.8</td>
<td>1.1</td>
<td>2.0</td>
<td>2.0</td>
<td>8.5</td>
<td>1.2</td>
</tr>
<tr>
<td>s3 clnt 2 u</td>
<td>2.7</td>
<td>4.7</td>
<td>6.9</td>
<td>1.9</td>
<td>–</td>
<td>2.2</td>
</tr>
<tr>
<td>s3 clnt 3 s</td>
<td>5.7</td>
<td>7.68</td>
<td>13.5</td>
<td>2.2</td>
<td>–</td>
<td>2.0</td>
</tr>
<tr>
<td>s3 clnt 3 u</td>
<td>1.3</td>
<td>2.3</td>
<td>1.6</td>
<td>1.4</td>
<td>–</td>
<td>1.6</td>
</tr>
<tr>
<td>s3 srvr 1</td>
<td>1.7</td>
<td>1.3</td>
<td>1.6</td>
<td>1.9</td>
<td>6.5</td>
<td>1.5</td>
</tr>
<tr>
<td>s3 srvr 2</td>
<td>3.1</td>
<td>4.3</td>
<td>1.6</td>
<td>1.9</td>
<td>–</td>
<td>1.9</td>
</tr>
<tr>
<td>s3 srvr 3</td>
<td>3.5</td>
<td>1.8</td>
<td>4.6</td>
<td>1.1</td>
<td>–</td>
<td>1.3</td>
</tr>
<tr>
<td>soft float 1</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>soft float 2</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>soft float 3</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.23</td>
<td>1.0</td>
</tr>
<tr>
<td>soft float 4</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>soft float 5</td>
<td>1.0</td>
<td>1.1</td>
<td>1.1</td>
<td>1.1</td>
<td>1.1</td>
<td>1.1</td>
</tr>
</tbody>
</table>

5. CONCLUSION AND FUTURE WORK

We introduced a BMC approach which takes advantage of incremental SMT solvers in order to perform a gradual unwinding of the program. Incremental BMC is favorable if the specified unwinding depth significantly exceeds the depth of the bug and relieves the user of the burden to determine an adequate bound. In addition, an incremental BMC can report partial results for bug-free programs even if the specified unwinding depth is not reached.

As the presented benchmarks show, the performance of incremental bounded model checking is encouraging on many examples. We are confident that the overhead for the remaining examples can be addressed with additional optimizations (such as an up-front static analysis enabling constant propagation) in future versions of Nbis.

In addition, incremental BMC enables additional optimizations typically used in symbolic simulation: the ability to perform a query at any point during the unwinding process enables the verification tool to prune infeasible traces. This optimization will be incorporated into a future version of Nbis.

6. ACKNOWLEDGEMENTS

This work was supported by the Austrian National Research Network S11403-N23 (RISe) of the Austrian Science Fund (FWF) and by the Vienna Science and Technology Fund (WWTF) through grant VRG11-005.

7. REFERENCES