SAT-Based Methods for Circuit Synthesis

Roderick Bloem¹, Uwe Egly², Patrick Klampfl¹, Robert Könighofer¹, and Florian Lonsing²

¹Institute for Applied Information Processing and Communications, Graz University of Technology, Austria
²Knowledge-Based Systems Group, Institute of Information Systems, Vienna University of Technology, Austria

Abstract—Reactive synthesis supports designers by automatically constructing correct hardware from declarative specifications. Synthesis algorithms usually compute a strategy, and then construct a circuit that implements it. In this work, we study SAT- and QBF-based methods for the second step, i.e., computing circuits from strategies. This includes methods based on QBF-certification, interpolation, and computational learning. We present optimizations, efficient implementations, and experimental results for synthesis from safety specifications, where we outperform BDDs both regarding execution time and circuit size. This is an extended version of [2], with an additional appendix.

I. INTRODUCTION

Synthesis is an ambitious design approach: Instead of checking whether an already constructed system satisfies its specification, a correct implementation is derived automatically from the specification [3]. Synthesis is also used in rapid prototyping, automatic repair [9], and program sketching [14].

Existing work often focuses on finding strategies to satisfy the specification, or only on deciding realizability. However, computing circuits from strategies is computationally demanding as well. System quality (e.g., circuit size and depth) imposes additional challenges. Synthesized strategies usually allow for much implementation freedom, which needs to be exploited cleverly. Algorithms must also be symbolic (operate on formulas rather than enumerating states) to achieve scalability. These symbolic algorithms are usually implemented with BDDs because they offer existential and universal quantification. Recently, SAT-based synthesis algorithms have been proposed [12], [4] as alternative to BDDs and their scalability issues. However, these works do not address circuit extraction.

We thus present and compare several SAT- and QBF-based circuit synthesis algorithms. The basic algorithms are not new, but we present novel optimizations, combinations, efficient implementations for safety synthesis problems, and extensive experiments. This includes methods based on QBF-certification, computational learning (including the first application of incremental QBF solving in synthesis), and interpolation. We achieve the best results by combining ideas from interpolation [8] with learning [7], thereby outperforming BDDs both regarding computation time and circuit size.

Related work. It is argued [7] that many circuit synthesis methods are still outperformed by the simple BDD-based cofactor approach [3]. The same work [7] also proposes learning-based techniques, which are implemented with BDDs. This yields smaller circuits, but is slower. We show how learning can be efficiently realized with SAT- and QBF-solvers, and that this realization can outperform the cofactor approach both regarding circuit size and computation time. SAT-based learning is also used in [4]. However, this work only addresses strategy computation and not circuit synthesis. Jiang et al. [8] propose interpolation for circuit extraction, and show how quantifier alternations can be avoided by temporarily treating outputs as inputs. We combine this idea with learning to compute interpolants, thereby achieving a speedup of several orders of magnitude. QBF certification [13] can derive circuits from a completeness proof of the strategy formula. We show how this method can be applied efficiently for safety synthesis.

II. PRELIMINARIES

We assume familiarity with propositional logic, SAT- and QBF-solving (cf. [1]) but repeat the most important concepts.

Basic Notation. A literal is a Boolean variable or its negation. A clause (cube) is a disjunction (conjunction) of literals, and a Conjunctive Normal Form (CNF) formula is a conjunction of clauses. We denote variables vectors with overlines, corresponding cubes in bold, and propositional formulas with capital letters. E.g., x is a cube over the variable vector \( \overline{x} = (x_1, \ldots, x_n) \), and \( F(\overline{t}) \) is a formula over \( \overline{t} \). If the variables are irrelevant, we simply write \( F \) instead of \( F(\overline{t}) \).

Decision Procedures. A SAT-solver checks if a CNF is satisfiable. We write \( (\text{sat}, x) := P\text{SAT}(F(\overline{t})) \) for a SAT-solver call, where \( \text{sat} \) is assigned true iff the CNF \( F \) is satisfiable, and \( x \) is a satisfying assignment given as cube over \( \overline{t} \). Let \( x \) be a cube. We write \( y := P\text{CORE}(x, F) \) to denote the extraction of an unsatisfiable core: Given that \( x \land F \) is unsatisfiable, \( y \) will be a sub-cube of \( x \) such that \( y \land F \) is still unsatisfiable. Let \( A(\overline{t}, \overline{y}) \) and \( B(\overline{t}, \overline{z}) \) be two CNFs such that \( A \land B \) is unsatisfiable, and \( \overline{y} \) and \( \overline{z} \) are disjoint. An interpolant is a formula \( I(\overline{t}) \) such that \( A \Rightarrow I \Rightarrow \neg B \). Interpolants can be computed from the unsatisfiability proof of \( A \land B \) [6]. We denote this computation by \( I := \text{Int}(A, B) \). A Quantified Boolean Formula (QBF) is a formula \( Q_1(\overline{t}) . Q_2(\overline{t}) \ldots . F(\overline{t}, \overline{y}, \ldots) \), where \( Q_i \in \{\forall, \exists\} \) and \( F \) is a CNF. The quantifiers have their expected semantics. A QBF-solver checks if a QBF is satisfiable. We write \( (\text{sat}, a) := Q\text{SAT}(\exists \exists \ldots Q_1(\overline{t}) . Q_2(\overline{t}) \ldots . F(\overline{t}, \overline{y}, \ldots)) \) for QBF-solver calls. The satisfying assignment \( a \) can only be extracted for variables that are quantified existentially on the outermost level. Finally, we write \( b := Q\text{CORE}(a, \exists \exists \ldots Q_1(\overline{t}) . Q_2(\overline{t}) \ldots . F(\overline{t}, \overline{y}, \ldots)) \) to denote the extraction of an unsatisfiable core.

This work was supported in part by the Austrian Science Fund (FWF) through the national research network RiSE (S11406-N23, S11409-N23) and the project QUAINIT (I774-N23), as well as by the European Commission through project STANCE (317753).
As long as $N'$ is not yet $\neg W'$, i.e., $W' \land \neg N'$ is still satisfiable, we refine $N'$ with a clause that excludes the cube $x$ witnessing this insufficiency. By taking the unsatisfiable core, the clause eliminates also other counterexamples. Since clauses are only added, NegLearn is suitable for incremental SAT solving.

Using incremental SAT solving, we also simplify $W$ by removing literals and clauses as long as $W$ does not change semantically. This is applied to all following methods as well.

## B. QBF-Based Learning

In [1], several learning-based circuit synthesis algorithms are presented and implemented using BDDs. Here, we discuss an efficient implementation of the CNF-learning algorithm using a QBF-solver. Since QBF-solvers operate on CNFs, this algorithm is particularly suitable. It can be defined as follows.

1. procedure SYLearnQBF($S(x, i, \overline{s}, \overline{p})$) 
   2. $\overline{S} := \overline{(x, i, \overline{s}, \overline{p})}$ 
   3. for $v \in \overline{p}$ do 
      4. $v_a := \overline{v} \setminus \{v\}$, $v := v \cup v_a$, $f_v := \text{true}$, $R := v \land \neg S$ 
      5. while sat, with $(\text{sat}, u) := \text{QSat}(\overline{v}, \overline{v_a}, \overline{p_e}, R)$ do 
         6. $u := \text{QCore}(u, \overline{v}, \overline{v_a}, \overline{p_e}, \overline{p}, -v \land \neg S)$ 
         7. $f_v := f_v \land \neg u_2$, $R := R \land \neg u_2$ 
      8. dumpCircuit($v$, $f_v$), $S := S \lor (v \leftrightarrow f_v)$

SYLearnQBF builds up circuits in $f_v$ for each $v \in \overline{p}$ after the other. Initially, $f_v = \text{true}$, i.e., the circuit always outputs true. While there exists an input $u$ for which $v$ must be false (the QBF in line 5 is satisfiable), $f_v$ is refined with a clause that maps $u$ to false. By taking the core in line 6 other inputs are also mapped to false as long as false is allowed by $S$. The final solution $f_v$ is dumped, and $S$ is refined with the implementation of $v$ before the next circuit is computed. The final $f_v$ are in CNF, so the circuits have a depth of only two. Even after optimizations and mapping to standard cells, the depth usually remains low [7], which enables fast clock rates.

Once $S$ is available in CNF, the algorithm only adds clauses to existing CNFs (i.e., to $R$ and $f_v$). Only for the resubstitution in line 1 a CNF encoding of $\neg f_v$ is needed.

### II. Circuit Synthesis Algorithms

#### A. QBF-Certification

An implementation can be computed as Skolem functions for the signals $\overline{s}$ and $\overline{p}$ in the QBF $\forall \overline{x}, \overline{p}, \exists \overline{v}, S(x, i, \overline{s}, \overline{p})$. QBFCert [13] computes such functions using DepQBF [10].

### Optimization for Safety Specifications

We need to find Skolem functions for $\overline{s}$ in $\forall \overline{x}, \overline{p}, \exists \overline{v}, \neg(W \lor (T \land W'))$. Yet, we achieve better results with QBFCert by computing Herbrand functions in the unsatisfiable QBF $\exists \overline{v}, \forall \overline{s}, \exists \overline{p}, W \land T \land \neg W'$. This works because $T$ is deterministic and complete. In our setting, $W$ is in CNF, so the conjunctions in the latter formulation are simpler to realize in CNF. Also, the clause resolution proofs required for unsatisfiable QBFs are usually less expensive than the cube resolution proofs for satisfiable ones. Still, the intermediate files produced by QBFCert can grow large (hundreds of GB). One reason is that a straightforward CNF encoding of $\neg W'$ requires many auxiliary variables and clauses. We could reduce the size of the files by up to a factor of 30 by learning a CNF representation of $\neg W'$ without introducing auxiliary variables using the following algorithm:

1. procedure NegLearn($W'$), returns: $\neg W'$
   2. $N' := \text{true}$
   3. while sat, with $(\text{sat}, x) := \text{PSat}(W' \land N')$ do 
      4. $N' := N' \land \neg \text{PCore}(x, \neg W')$
   5. return $N'$

1.i.e., $\forall x, i, \overline{s}, \overline{p}, T(x, i, \overline{s}, \overline{p}), T$ can always be made complete: if some input is not allowed by the original specification, $T$ can allow for arbitrary outputs; if some output is not allowed originally, $T$ can visit an unsafe state.

2.i.e., $\forall x, i, \overline{s}, \overline{p}, \overline{p_e}, (T(x, i, \overline{s}, \overline{p}))) \land T(x, i, \overline{s}, \overline{p})) \Rightarrow (\overline{p} = \overline{p})$.

3.Skolem functions define existentially quantified variables as a function over the universally quantified ones such that the QBF becomes true.

4.Herbrand functions define universally quantified variables as a function over the existentially quantified ones such that the QBF becomes false.

### C. Interpolation

Jiang et al. [8] present two interpolation-based approaches to synthesize circuits for one $v \in \overline{p}$ after the other. The first one
expands \( S \) over \( \tau \). We consider this intractable in our setting.

The second approach circumvents the quantifier alternation and expansion by temporarily treating output signals as inputs:

1. **procedure** \( \text{SYINT}(S(\pi, \tau, \pi')) \)
2. \( \overline{\alpha} := \alpha \cup \tau \cup \sigma \cup \pi' \), \( \tau : = \emptyset \)
3. for \( v \in \overline{\alpha} \) do
4. \( \overline{\alpha} := \overline{\alpha} \setminus \{v\}, \pi : = \pi \cup \{v\} \)
5. \( \overline{\tau}_1, \overline{\tau}_2, \overline{\tau}_3, \overline{\tau}_4 : = \text{create4FreshCopies}(\overline{\tau}) \)
6. \( M_1(\overline{\alpha}, \overline{\tau}_1, \overline{\tau}_2) := (S \lor v)[\overline{v} \leftarrow \overline{\tau}_1] \land (\neg S \land \neg v)[\overline{v} \leftarrow \overline{\tau}_2] \)
7. \( M_0(\overline{\alpha}, \overline{\tau}_3, \overline{\tau}_4) := (S \lor v)[\overline{v} \leftarrow \overline{\tau}_3] \land (\neg S \land \neg v)[\overline{v} \leftarrow \overline{\tau}_4] \)
8. \( f_v(\overline{\alpha}) := \text{INT}(M_1(\overline{\alpha}, \overline{\tau}_1, \overline{\tau}_2), M_0(\overline{\alpha}, \overline{\tau}_3, \overline{\tau}_4)) \)
9. **DUMP**\( \text{CIRCUIT}(v, f_v) \), \( S : = S \land (v \leftarrow f_v) \)

In each iteration, \( \overline{\alpha} \) contains all variables on which the implementation of the current \( v \in \tau \) can depend, and \( \pi \) contains the rest. For \( \tau = (v_1, \ldots, v_n) \), \( v_1 \) can depend not only on \( \pi \) but also on \( (v_2, \ldots, v_n) \), \( v_2 \) can depend on \( \pi \) and \( (v_3, \ldots, v_n) \), etc. Yet, when the circuits for all \( v \in \tau \) are built together, the signals \( \pi \) effectively depend on \( \pi \) only. The formulas \( M_1 \) and \( M_0 \) characterize the \( \overline{\alpha} \)-vectors for which \( v \) must be set to true and false respectively. The syntax \( \tau \leftarrow \overline{\tau} \) means that the variables \( \overline{\tau} \) are renamed by fresh copies \( \overline{\tau} \), Line 8 computes an interpolant between \( M_1 \) and \( M_0 \). The property \( M_1 \rightarrow f_v \rightarrow \neg M_0 \) of the interpolant ensures that (a) \( f_v \) is true whenever it must be true, and (b) whenever \( f_v \) is true then it does not have to be false. The renaming of the variables \( \tau \) has the effect that \( f_v \) can only depend on the shared signals \( \overline{\alpha} \).

**Optimizations for Safety Specifications.** In order to avoid double-negations of \( W \) in \( S \) by negating \( S \), we compute

\[
M_1 := (T \land W' \lor v)[\overline{v} \leftarrow \overline{\tau}_1] \land (T \land \neg v \land W \land \neg W')[\overline{v} \leftarrow \overline{\tau}_2] \\
M_0 := (T \land W' \land \neg v)[\overline{v} \leftarrow \overline{\tau}_3] \land (T \land v \land W \land \neg W')[\overline{v} \leftarrow \overline{\tau}_4] 
\]

Note the difference to a plain substitution of \( S = T \land (W \lor W') \) and \( S = T \land W \land 
\neg W' \) in \( \text{SYINT} \): \( \neg W \land W' \) reduces to \( W' \) due to the conjunction with \( W \) from \( \neg S \). This is fortunate because disjunctions are expensive in CNF. Since \( \text{SYINT} \) allows \( v_i \) to depend on other \( v_j \) with \( j > i \), it is sensitive to the variable order, both regarding execution time and circuit size. We exploit this insight with the following optimization. Once \( v_i \) has been synthesized, we analyze on which \( v_j \) it actually depends. If \( v_j \) does not depend on a particular \( v_i \), then \( v_j \) is allowed to depend on \( v_i \). This gives an increased flexibility without introducing circular dependencies. We simplify all computed interpolants with \texttt{ABC}. As long as there exists some \( d \) for which \( f \) is true but must be false, i.e., \( M_0 \land f \) is satisfiable, we refine \( f \) with an additional clause that excludes the cube \( d \) witnessing this insufficiency. By taking the unsatisfiable core, other inputs are also mapped to false as long as false is allowed.

**Optimizations.** We use two SAT solver instances, one for line [3] and one for line [4]. A new incremental session is started upon each call of \texttt{INTLEARN}. Using activation variables to set \( \tau \)-variables to true, false, or equal to their renamed copy, whenever it must be

\[
\text{DUMP CIRCUIT}(v, f_v), \quad S := S \land (v \leftarrow f_v) 
\]

In order to avoid double-negations of \( W \) in \( S \) by negating \( S \), we compute

\[
M_1 := (T \land W' \lor v)[\overline{v} \leftarrow \overline{\tau}_1] \land (T \land \neg v \land W \land \neg W')[\overline{v} \leftarrow \overline{\tau}_2] \\
M_0 := (T \land W' \land \neg v)[\overline{v} \leftarrow \overline{\tau}_3] \land (T \land v \land W \land \neg W')[\overline{v} \leftarrow \overline{\tau}_4] 
\]

As long as there exists some \( d \) for which \( f \) is true but must be false, i.e., \( M_0 \land f \) is satisfiable, we refine \( f \) with an additional clause that excludes the cube \( d \) witnessing this insufficiency. By taking the unsatisfiable core, other inputs are also mapped to false as long as false is allowed.

**Optimizations.** We use two SAT solver instances, one for line [3] and one for line [4]. A new incremental session is started upon each call of \texttt{INTLEARN}. Using activation variables to set \( \tau \)-variables to true, false, or equal to their renamed copy, whenever it must be

\[
\text{DUMP CIRCUIT}(v, f_v), \quad S := S \land (v \leftarrow f_v) 
\]

In order to avoid double-negations of \( W \) in \( S \) by negating \( S \), we compute

\[
M_1 := (T \land W' \lor v)[\overline{v} \leftarrow \overline{\tau}_1] \land (T \land \neg v \land W \land \neg W')[\overline{v} \leftarrow \overline{\tau}_2] \\
M_0 := (T \land W' \land \neg v)[\overline{v} \leftarrow \overline{\tau}_3] \land (T \land v \land W \land \neg W')[\overline{v} \leftarrow \overline{\tau}_4] 
\]

As long as there exists some \( d \) for which \( f \) is true but must be false, i.e., \( M_0 \land f \) is satisfiable, we refine \( f \) with an additional clause that excludes the cube \( d \) witnessing this insufficiency. By taking the unsatisfiable core, other inputs are also mapped to false as long as false is allowed.

**Optimizations.** We use two SAT solver instances, one for line [3] and one for line [4]. A new incremental session is started upon each call of \texttt{INTLEARN}. Using activation variables to set \( \tau \)-variables to true, false, or equal to their renamed copy, whenever it must be

\[
\text{DUMP CIRCUIT}(v, f_v), \quad S := S \land (v \leftarrow f_v) 
\]
MathSAT, which supports several interpolation schemes. We use McMillan’s scheme (see [6]), but the performance is similar with other schemes. We also implemented our own interpolation engine by processing proofs produced by PicoSat. However, the proof files grew prohibitively large.

The limitations of our implementation are that it can only handle safety specifications in AIGER format, it can produce circuit only in AIGER format, and it runs under Linux only.

B. Benchmarks

We use the same benchmarks as [4], but report here only results for the interesting ones. The benchmarks amba\_ij specify an arbiter for ARM’s AMBA AHB bus \[3\], where \(i\) is the number of masters, and \(j \in \{c,b,f\}\) indicates the method used to transform the original benchmark \[3\] into our input format \[4\]. The benchmarks genbuf\_ij, again with \(j \in \{c,b,f\}\), define a generalized buffer \[3\] connecting \(i\) senders to two receivers. The specifications addi and multi denote \(i\)-bit combinational adders and multipliers.

C. Results and Discussion

Fig. 2 summarizes our results with cactus plots. The y-axis gives the execution time or circuit size, and the x-axis gives the number of benchmarks that can be solved within this time or size limit. Concrete numbers and more plots can be found in the appendix and in the downloadable archive. All experiments were performed on an Intel Xeon E5430 CPU running a 64 bit Linux at 2.66 GHz. The memory limit was set to 8 GB, the time-out to 10 000 seconds. All circuits have been successfully model checked.

Method SL achieves the best results both regarding execution time and circuit size. The dependency optimization (SL vs. SLN) is very beneficial for add and multi, but slower for amba and genbuf. QC, QL, and SI do not perform so well. Using incremental QBF solving in QL gives an average speedup of factor 3.5. The speedup factor compared to using the QBF preprocessor Bloquer is even 21. Still, QL is not very competitive. BDD is much better, but still outperformed by SL.

In particular, SL outperforms SL by many orders of magnitude. Hence, our idea of implementing the interpolation procedure with computational learning is very beneficial. Execution time and circuit size are not in conflict but rather correlate. The time for optimization with ABC is usually insignificant, but only yields moderate size reductions (around 25 % for SL). Using method SLN, Demigurge won a track of SyntComp 2014. One reason was the small circuit size compared to other tools.

V. Conclusion

We compared several SAT- and QBF-based methods to synthesize circuits from strategies, and presented optimizations and efficient implementations for safety specifications. Our SAT-based learning method combines the quantifier elimination approach by Jiang et al. [8] with computational learning as proposed by Ehlers et al. [7], and outperforms BDDs both regarding execution time and circuit size in our experiments.

Future research includes preprocessing for incremental QBF solving, exploiting unreachable states, and parallelization.
APPENDIX

Table I contains more performance results. “T” indicates a time-out of 10,000 seconds. The suffix k stands for a multiplication with 1000. The size column \( G \) gives the number of AIGER gates defining \( T \). The column “files” in QC gives the size of the intermediate files (the QBF trace) produced by \( \text{QBFCert} \); we aborted at 20GB. “M” indicates that \( ABC \) ran out of memory (because QC produces huge circuits). More details can be found in the downloadable archive.

<table>
<thead>
<tr>
<th>Size</th>
<th>BDD</th>
<th>QC</th>
<th>QL</th>
<th>SI</th>
<th>SL</th>
<th>SLN</th>
</tr>
</thead>
</table>

| | | | | | | |

Table I

**Performance Results.**

<table>
<thead>
<tr>
<th>[1]</th>
<th>[1]</th>
<th>[1]</th>
<th>[1]</th>
<th>[1]</th>
<th>[1]</th>
<th>[1]</th>
</tr>
</thead>
</table>

| | | | | | | |

**Additional Details:**

- \( \text{genbuf1c} \) contains more performance results.
- “T” indicates a time-out of 10,000 seconds.
- The suffix k stands for a multiplication with 1000.
- The size column \( G \) gives the number of AIGER gates defining \( T \).
- The column “files” in QC gives the size of the intermediate files (the QBF trace) produced by \( \text{QBFCert} \).
- We aborted at 20GB. “M” indicates that \( ABC \) ran out of memory (because QC produces huge circuits). More details can be found in the downloadable archive.

### Additional Tables

<table>
<thead>
<tr>
<th>Size</th>
<th>BDD</th>
<th>QC</th>
<th>QL</th>
<th>SI</th>
<th>SL</th>
<th>SLN</th>
</tr>
</thead>
</table>

| | | | | | | |

**Additional Details:**

- \( \text{genbuf1c} \) contains more performance results.
- “T” indicates a time-out of 10,000 seconds.
- The suffix k stands for a multiplication with 1000.
- The size column \( G \) gives the number of AIGER gates defining \( T \).
- The column “files” in QC gives the size of the intermediate files (the QBF trace) produced by \( \text{QBFCert} \).
- We aborted at 20GB. “M” indicates that \( ABC \) ran out of memory (because QC produces huge circuits). More details can be found in the downloadable archive.

### Additional Tables

<table>
<thead>
<tr>
<th>Size</th>
<th>BDD</th>
<th>QC</th>
<th>QL</th>
<th>SI</th>
<th>SL</th>
<th>SLN</th>
</tr>
</thead>
</table>

| | | | | | | |

**Additional Details:**

- \( \text{genbuf1c} \) contains more performance results.
- “T” indicates a time-out of 10,000 seconds.
- The suffix k stands for a multiplication with 1000.
- The size column \( G \) gives the number of AIGER gates defining \( T \).
- The column “files” in QC gives the size of the intermediate files (the QBF trace) produced by \( \text{QBFCert} \).
- We aborted at 20GB. “M” indicates that \( ABC \) ran out of memory (because QC produces huge circuits). More details can be found in the downloadable archive.

### Additional Tables

<table>
<thead>
<tr>
<th>Size</th>
<th>BDD</th>
<th>QC</th>
<th>QL</th>
<th>SI</th>
<th>SL</th>
<th>SLN</th>
</tr>
</thead>
</table>

| | | | | | | |

**Additional Details:**

- \( \text{genbuf1c} \) contains more performance results.
- “T” indicates a time-out of 10,000 seconds.
- The suffix k stands for a multiplication with 1000.
- The size column \( G \) gives the number of AIGER gates defining \( T \).
- The column “files” in QC gives the size of the intermediate files (the QBF trace) produced by \( \text{QBFCert} \).
- We aborted at 20GB. “M” indicates that \( ABC \) ran out of memory (because QC produces huge circuits). More details can be found in the downloadable archive.

### Additional Tables

<table>
<thead>
<tr>
<th>Size</th>
<th>BDD</th>
<th>QC</th>
<th>QL</th>
<th>SI</th>
<th>SL</th>
<th>SLN</th>
</tr>
</thead>
</table>

| | | | | | | |

**Additional Details:**

- \( \text{genbuf1c} \) contains more performance results.
- “T” indicates a time-out of 10,000 seconds.
- The suffix k stands for a multiplication with 1000.
- The size column \( G \) gives the number of AIGER gates defining \( T \).
- The column “files” in QC gives the size of the intermediate files (the QBF trace) produced by \( \text{QBFCert} \).
- We aborted at 20GB. “M” indicates that \( ABC \) ran out of memory (because QC produces huge circuits). More details can be found in the downloadable archive.

### Additional Tables

<table>
<thead>
<tr>
<th>Size</th>
<th>BDD</th>
<th>QC</th>
<th>QL</th>
<th>SI</th>
<th>SL</th>
<th>SLN</th>
</tr>
</thead>
</table>

| | | | | | | |

**Additional Details:**

- \( \text{genbuf1c} \) contains more performance results.
- “T” indicates a time-out of 10,000 seconds.
- The suffix k stands for a multiplication with 1000.
- The size column \( G \) gives the number of AIGER gates defining \( T \).
- The column “files” in QC gives the size of the intermediate files (the QBF trace) produced by \( \text{QBFCert} \).
- We aborted at 20GB. “M” indicates that \( ABC \) ran out of memory (because QC produces huge circuits). More details can be found in the downloadable archive.

### Additional Tables

<table>
<thead>
<tr>
<th>Size</th>
<th>BDD</th>
<th>QC</th>
<th>QL</th>
<th>SI</th>
<th>SL</th>
<th>SLN</th>
</tr>
</thead>
</table>

| | | | | | | |

**Additional Details:**

- \( \text{genbuf1c} \) contains more performance results.
- “T” indicates a time-out of 10,000 seconds.
- The suffix k stands for a multiplication with 1000.
- The size column \( G \) gives the number of AIGER gates defining \( T \).
- The column “files” in QC gives the size of the intermediate files (the QBF trace) produced by \( \text{QBFCert} \).
- We aborted at 20GB. “M” indicates that \( ABC \) ran out of memory (because QC produces huge circuits). More details can be found in the downloadable archive.

### Additional Tables

<table>
<thead>
<tr>
<th>Size</th>
<th>BDD</th>
<th>QC</th>
<th>QL</th>
<th>SI</th>
<th>SL</th>
<th>SLN</th>
</tr>
</thead>
</table>

| | | | | | | |

**Additional Details:**

- \( \text{genbuf1c} \) contains more performance results.
- “T” indicates a time-out of 10,000 seconds.
- The suffix k stands for a multiplication with 1000.
- The size column \( G \) gives the number of AIGER gates defining \( T \).
- The column “files” in QC gives the size of the intermediate files (the QBF trace) produced by \( \text{QBFCert} \).
- We aborted at 20GB. “M” indicates that \( ABC \) ran out of memory (because QC produces huge circuits). More details can be found in the downloadable archive.

### Additional Tables

<table>
<thead>
<tr>
<th>Size</th>
<th>BDD</th>
<th>QC</th>
<th>QL</th>
<th>SI</th>
<th>SL</th>
<th>SLN</th>
</tr>
</thead>
</table>

| | | | | | | |

**Additional Details:**

- \( \text{genbuf1c} \) contains more performance results.
- “T” indicates a time-out of 10,000 seconds.
- The suffix k stands for a multiplication with 1000.
- The size column \( G \) gives the number of AIGER gates defining \( T \).
- The column “files” in QC gives the size of the intermediate files (the QBF trace) produced by \( \text{QBFCert} \).
- We aborted at 20GB. “M” indicates that \( ABC \) ran out of memory (because QC produces huge circuits). More details can be found in the downloadable archive.

### Additional Tables

<table>
<thead>
<tr>
<th>Size</th>
<th>BDD</th>
<th>QC</th>
<th>QL</th>
<th>SI</th>
<th>SL</th>
<th>SLN</th>
</tr>
</thead>
</table>

| | | | | | | |

**Additional Details:**

- \( \text{genbuf1c} \) contains more performance results.
- “T” indicates a time-out of 10,000 seconds.
- The suffix k stands for a multiplication with 1000.
- The size column \( G \) gives the number of AIGER gates defining \( T \).
- The column “files” in QC gives the size of the intermediate files (the QBF trace) produced by \( \text{QBFCert} \).
- We aborted at 20GB. “M” indicates that \( ABC \) ran out of memory (because QC produces huge circuits). More details can be found in the downloadable archive.

### Additional Tables

<table>
<thead>
<tr>
<th>Size</th>
<th>BDD</th>
<th>QC</th>
<th>QL</th>
<th>SI</th>
<th>SL</th>
<th>SLN</th>
</tr>
</thead>
</table>

| | | | | | | |

**Additional Details:**

- \( \text{genbuf1c} \) contains more performance results.
- “T” indicates a time-out of 10,000 seconds.
- The suffix k stands for a multiplication with 1000.
- The size column \( G \) gives the number of AIGER gates defining \( T \).
- The column “files” in QC gives the size of the intermediate files (the QBF trace) produced by \( \text{QBFCert} \).
- We aborted at 20GB. “M” indicates that \( ABC \) ran out of memory (because QC produces huge circuits). More details can be found in the downloadable archive.
Fig. 3 contains cactus plots summarizing the execution time and circuit size per benchmark. For `mult`, the dependency optimization has an even stronger positive impact than for `add`, both regarding execution time and circuit size (`SL` vs. `SLN`). For `genbuf`, it results in smaller circuits, but is slower. For `amba`, it is not beneficial in either metric. The interpolation-based method `SI` is competitive for `add`, but has troubles with the other benchmarks. The difference in circuit size can grow very large (more than three orders of magnitude). Our a-posteriori circuit minimization using ABC can only compensate an insignificant fraction of this difference. Investing more effort in post-processing can be expensive, especially for large circuits. We therefore conclude that circuit size is best considered during the synthesis process already. The fact that circuit size and execution time correlate is not surprising. Most of our methods compute circuits for one output signal after the other. The strategy is refined with the circuit for one signal before continuing with the next one. This is necessary in order to prevent uncoordinated choices. If the computed circuits are complicated, then this re-substitution makes the strategy formula for the next output complicated, which results in higher computation times. This may also explain why implementing an interpolation procedure with computational learning is very beneficial (`SL` vs. `SI`): computational learning seems to find smaller circuits, and this also pays off in terms of the overall computation time.