Boolean Satisfiability with Transitivity Constraints

RANDAL E. BRYANT
MIROSLAV N. VELEV
Carnegie Mellon University

We consider a variant of the Boolean satisfiability problem where a subset $\mathcal{E}$ of the propositional variables appearing in formula F_{sat} encode a symmetric, transitive, binary relation over N elements. Each of these *relational* variables, $e_{i,j}$, for $1 \leq i < j \leq N$, expresses whether or not the relation holds between elements i and j. The task is to either find a satisfying assignment to F_{sat} that also satisfies all transitivity constraints over the relational variables (e.g., $e_{1,2} \wedge e_{2,3} \Rightarrow e_{1,3}$), or to prove that no such assignment exists. Solving this satisfiability problem is the final and most difficult step in our decision procedure for a logic of equality with uninterpreted functions. This procedure forms the core of our tool for verifying pipelined microprocessors.

To use a conventional Boolean satisfiability checker, we augment the set of clauses expressing F_{sat} with clauses expressing the transitivity constraints. We consider methods to reduce the number of such clauses based on the sparse structure of the relational variables.

To use Ordered Binary Decision Diagrams (OBDDs), we show that for some sets $\mathcal{E}$, the OBDD representation of the transitivity constraints has exponential size for all possible variable orderings. By considering only those relational variables that occur in the OBDD representation of F_{sat}, our experiments show that we can readily construct an OBDD representation of the relevant transitivity constraints and thus solve the constrained satisfiability problem.

Categories and Subject Descriptors: F.4.1 [**Mathematical Logic and Formal Languages**]: Mathematical Logic—*Mechanical theorem proving*

General Terms: Algorithms, Verification

Additional Key Words and Phrases: Formal verification, Boolean satisfiability, Decision procedures

1. INTRODUCTION

Consider the following variant of the Boolean satisfiability problem. We are given a Boolean formula F_{sat} over a set of variables $\mathcal{V}$. A subset $\mathcal{E} \subseteq \mathcal{V}$ symbolically encodes a reflexive, symmetric, and transitive binary relation over N elements. Each of these *relational* variables, $e_{i,j}$, where $1 \leq i < j \leq N$, expresses whether or not the relation holds between elements i and j. Typically, $\mathcal{E}$ will be "sparse," containing much fewer than the $N(N-1)/2$ possible variables. Note that when $e_{i,j} \notin \mathcal{E}$ for some value of i and of j, this does not imply that the relation does not hold between elements i and j. It simply indicates

This research was supported by the Semiconductor Research Corporation, Contract 00-DC-068.

Authors' addresses: R. E. Bryant, Computer Science Department, Carnegie Mellon University, Pittsburgh, PA 15213; M. N. Velev, Electrical and Computer Engineering Department, Carnegie Mellon University, Pittsburgh, PA 15213.

that F_{sat} does not directly depend on the relation between elements i and j.

A *transitivity constraint* is a formula of the form

$$e_{[i_1,i_2]} \wedge e_{[i_2,i_3]} \wedge \cdots \wedge e_{[i_{k-1},i_k]} \;\Rightarrow\; e_{[i_1,i_k]} \tag{1}$$

where $e_{[i,j]}$ equals $e_{i,j}$ when $i < j$ and equals $e_{j,i}$ when $i > j$. Let $\mathit{Trans}(\mathcal{E})$ denote the set of all transitivity constraints that can be formed from the relational variables. Our task is to find an assignment $\chi\colon \mathcal{V} \rightarrow \{0,1\}$ that satisfies F_{sat}, as well as every constraint in $\mathit{Trans}(\mathcal{E})$. Goel et al. [1998] have shown this problem is NP-hard, even when F_{sat} is given as an Ordered Binary Decision Diagram (OBDD) [Bryant 1986]. Normally, Boolean satisfiability is trivial given an OBDD representation of a formula.

We are motivated to solve this problem as part of a tool for verifying pipelined microprocessors [Velev and Bryant 1999]. This tool proves that the microprocessor has behavior equivalent to that of an unpipelined, *reference* implementation for all possible instruction sequences. The operations of the datapaths in both processor models are abstracted as a set of uninterpreted functions and uninterpreted predicates operating on symbolic data. The verifier uses the symbolic flushing technique developed by Burch and Dill [1994]. The major computational task is to decide the validity of a formula F_{ver} in a logic of equality with uninterpreted functions [Bryant et al. 1999; Bryant and Velev 2001]. Our decision procedure transforms F_{ver} first by replacing all function application terms with terms over a set of domain variables $\{v_i | 1 \leq i \leq N\}$. Similarly, all predicate applications are replaced by formulas over a set of newly-generated propositional variables. The result is a formula F^*_{ver} containing equations of the form $v_i = v_j$, where $1 \leq i < j \leq N$. Each of these equations is then encoded by introducing a relational variable $e_{i,j}$, similar to the method proposed by Goel et al. [1998]. The result of the translation is a propositional formula $\mathit{encf}(F^*_{\text{ver}})$ expressing the verification condition over both the relational variables and the propositional variables appearing in F^*_{ver}. Let F_{sat} denote $\neg\,\mathit{encf}(F^*_{\text{ver}})$, the complement of the formula expressing the translated verification condition. To capture the transitivity of equality, e.g., that $v_i = v_j \wedge v_j = v_k \;\Rightarrow\; v_i = v_k$, we have transitivity constraints of the form $e_{[i,j]} \wedge e_{[j,k]} \;\Rightarrow\; e_{[i,k]}$. Finding a satisfying assignment to F_{sat} that also satisfies the transitivity constraints will give us a counterexample to the original verification condition F_{ver}. On the other hand, if we can prove that there are no such assignments, then we have proved that F_{ver} is universally valid.

We consider three methods to generate a Boolean formula F_{trans} that encodes the transitivity constraints. The *direct* method enumerates the set of *chord-free* cycles in the undirected graph having an edge (i,j) for each relational variable $e_{i,j} \in \mathcal{E}$. This method avoids introducing additional relational variables but can lead to a formula of exponential size. The *dense* method uses relational variables $e_{i,j}$ for all possible values of i and j such that $1 \leq i < j \leq N$. We can then axiomatize transitivity by forming constraints of the form $e_{[i,j]} \wedge e_{[j,k]} \;\Rightarrow\; e_{[i,k]}$ for all distinct values of i, j, and k. This will yield a formula that is cubic in N. The *sparse* method augments $\mathcal{E}$ with additional relational variables to form a set of variables $\mathcal{E}^+$, such that the resulting graph is *chordal* [Rose 1970]. We then only require transitivity constraints of the form $e_{[i,j]} \wedge e_{[j,k]} \;\Rightarrow\; e_{[i,k]}$ such that $e_{[i,j]}, e_{[j,k]}, e_{[i,k]} \in \mathcal{E}^+$. The sparse method will generate a formula no larger than the dense method, and often it does much better.

To use a conventional Boolean Satisfiability (SAT) procedure to solve our constrained satisfiability problem, we run the checker over a set of clauses encoding both F_{sat} and F_{trans}. A version of the FGRASP SAT checker [Marques-Silva 1999] was able to com-

Table I. Microprocessor Verification Benchmarks. Benchmarks with suffix "t" were modified to require enforcing transitivity.

Circuit		Domain Variables	Propositional Variables	Equations
1×DLX-C		13	42	27
1×DLX-C-t		13	42	37
2×DLX-CA		25	58	118
2×DLX-CA-t		25	58	137
2×DLX-CC		25	70	124
2×DLX-CC-t		25	70	143
100 Buggy 2×DLX-CC	min.	22	56	89
	avg.	25	69	124
	max.	25	77	132

plete all of our benchmarks, although the run times increase significantly when transitivity constraints are enforced.

When using Ordered Binary Decision Diagrams to evaluate satisfiability, we could generate OBDD representations of F_{sat} and F_{trans} and use the APPLY algorithm [Bryant 1986] to compute an OBDD representation of their conjunction. From this OBDD, finding satisfying solutions would be trivial. We show that this approach will not be feasible in general, because the OBDD representation of F_{trans} can be intractable. That is, for some sets of relational variables, the OBDD representation of the transitivity constraint formula F_{trans} will be of exponential size regardless of the variable ordering. The NP-completeness result of Goel, et al. shows that the OBDD representation of F_{trans} may be of exponential size using the ordering previously selected for representing F_{sat} as an OBDD. This leaves open the possibility that there could be some other variable ordering that would yield efficient OBDD representations of both F_{sat} and F_{trans}. Our result shows that transitivity constraints can be intrinsically intractable to represent with OBDDs, independent of the structure of F_{sat}.

We present experimental results on the complexity of constructing OBDDs for the transitivity constraints that arise in actual microprocessor verification. Our results show that the OBDDs can indeed be quite large. We consider two techniques to avoid constructing the OBDD representation of all transitivity constraints. The first of these, proposed by Goel et al. [1998], generates implicants (cubes) of F_{sat} and rejects those that violate the transitivity constraints. Although this method suffices for small benchmarks, we find that the number of implicants generated for our larger benchmarks grows unacceptably large. The second method determines which relational variables actually occur in the OBDD representation of F_{sat}. We can then apply one of our three techniques for encoding the transitivity constraints in order to generate a Boolean formula for the transitivity constraints over this reduced set of relational variables. The OBDD representation of this formula is generally tractable, even for the larger benchmarks.

2. BENCHMARKS

Our benchmarks [Velev and Bryant 1999] are based on applying our verifier [Velev 2001] to a set of high-level microprocessor designs. Each is based on the DLX RISC processor described by Hennessy and Patterson [1996]:

1×DLX-C. is a single-issue, five-stage pipeline capable of fetching up to one new instruction every clock cycle. It implements six instruction types: register-register, registerimmediate, load, store, branch, and jump. The pipeline stages are: Fetch, Decode, Execute, Memory, and Write-Back. An interlock causes the instruction immediately following a load to stall one cycle if it requires the loaded result. Branches and jumps are predicted as not-taken, with up to 3 instructions squashed when there is a misprediction. This example is comparable to the DLX example first verified by Burch and Dill [1994].

2×DLX-CA. has a complete first pipeline, capable of executing the six instruction types, and a second pipeline capable of executing arithmetic instructions. Between 0 and 2 new instructions are issued on each cycle, depending on their types and source registers, as well as the types and destination registers of the preceding instructions. This example is comparable to one verified by Burch [1996].

2×DLX-CC. has two complete pipelines, i.e., each can execute any of the six instruction types. There are four load interlocks—between a load in Execute in either pipeline and an instruction in Decode in either pipeline. On each cycle, between 0 and 2 instructions can be issued.

In all of these examples, the domain variables v_i, with $1 \leq i \leq N$, in F^*_{ver} encode register identifiers. As described in [Bryant et al. 1999; Bryant and Velev 2001], we can encode the symbolic terms representing program data and addresses as distinct values, avoiding the need to have equations among these variables. Equations arise in modeling the read and write operations of the register file, the bypass logic implementing data forwarding, the load interlocks, and the pipeline issue logic.

Our original processor benchmarks can be verified without enforcing any transitivity constraints. The unconstrained formula F_{sat} is unsatisfiable in every case. We are nonetheless motivated to study the problem of constrained satisfiability for two reasons. First, other processor designs might rely on transitivity, e.g., due to more sophisticated issue logic. Second, to aid designers in debugging their pipelines, it is essential that we generate counterexamples that satisfy all transitivity constraints. Otherwise the designer will be unable to determine whether the counterexample represents a true bug or a weakness of our verifier.

To create more challenging benchmarks, we generated variants of the circuits that require enforcing transitivity in the verification. For example, the normal forwarding logic in the Execute stage of 1×DLX-C must determine whether to forward the result from the Memory stage instruction as either one or both operand(s) for the Execute stage instruction. It does this by comparing the two source registers $\mathtt{ESrc1}$ and $\mathtt{ESrc2}$ of the instruction in the Execute stage to the destination register $\mathtt{MDest}$ of the instruction in the memory stage. In the modified circuit, we changed the bypass condition $\mathtt{ESrc1} = \mathtt{MDest}$ to be $\mathtt{ESrc1} = \mathtt{MDest} \vee (\mathtt{ESrc1} = \mathtt{ESrc2} \wedge \mathtt{ESrc2} = \mathtt{MDest})$. Given transitivity, these two expressions are equivalent. For each pipeline, we introduced four such modifications to the forwarding logic, with different combinations of source and destination registers. These modified circuits are named 1×DLX-C-t, 2×DLX-CA-t, and 2×DLX-CC-t.

To study the problem of counterexample generation for buggy circuits, we generated 105 variants of 2×DLX-CC, each containing a small modification to the control logic. Of these, 5 were found to be functionally correct, e.g., because the modification caused the processor to stall unnecessarily, yielding a total of 100 benchmark circuits for counterexample generation.

Table I gives some statistics for the benchmarks. The number of domain variables N ranges between 13 and 25, while the number of equations ranges between 27 and 143.

The verification condition formulas F^*_{ver} also contain between 42 and 77 propositional variables expressing the operation of the control logic. These variables plus the relational variables comprise the set of variables $\mathcal{V}$ in the propositional formula F_{sat}. The circuits with modifications that require enforcing transitivity yield formulas containing up to 19 additional equations. The final three lines summarize the complexity of the 100 buggy variants of 2×DLX-CC. We apply a number of simplifications during the generation of formula F_{sat}, and hence small changes in the circuit can yield significant variations in the formula complexity.

3. GRAPH FORMULATION

Our definition of $\mathit{Trans}(\mathcal{E})$ (Equation 1) places no restrictions on the length or form of the transitivity constraints, and hence there can be an infinite number. We show that we can construct a graph representation of the relational variables and identify a reduced set of transitivity constraints that, when satisfied, guarantees that all possible transitivity constraints are satisfied. By introducing more relational variables, we can alter this graph structure, further reducing the number of transitivity constraints that must be considered.

For variable set $\mathcal{E}$, define the undirected graph $G(\mathcal{E})$ as containing a vertex i for $1 \leq i \leq N$, and an edge (i, j) for each variable $e_{i,j} \in \mathcal{E}$. For an assignment χ of Boolean values to the relational variables, define the labeled graph $G(\mathcal{E}, \chi)$ to be the graph $G(\mathcal{E})$ with each edge (i, j) labeled as a *1-edge* when $\chi(e_{i,j}) = 1$, and as a *0-edge* when $\chi(e_{i,j}) = 0$.

A *path* is a sequence of vertices $[i_1, i_2, \ldots, i_k]$ having edges between successive elements. That is, each element i_p of the sequence ($1 \leq p \leq k$) denotes a vertex: $1 \leq i_p \leq N$, while each successive pair of elements i_p and i_{p+1} ($1 \leq p < k$) forms an edge (i_p, i_{p+1}). We consider each edge (i_p, i_{p+1}) for $1 \leq p < k$ to also be part of the path. A *cycle* is a path of the form $[i_1, i_2, \ldots, i_k, i_1]$.

PROPOSITION 3.1. *An assignment χ to the variables in $\mathcal{E}$ violates transitivity if and only if some cycle in $G(\mathcal{E}, \chi)$ contains exactly one 0-edge.*

PROOF. *If.* Suppose there is such a cycle. Letting i_1 be the vertex at one end of the 0-edge, we can trace around the cycle, giving a sequence of vertices $[i_1, i_2, \ldots, i_k]$, where i_k is the vertex at the other end of the 0-edge. The assignment has $\chi(e_{[i_j, i_{j+1}]}) = 1$ for $1 \leq j < k$, and $\chi(e_{[i_1, i_k]} = 0)$, and hence it violates Equation 1.

Only If. Suppose the assignment violates a transitivity constraint given by Equation 1. Then, we construct a cycle $[i_1, i_2, \ldots, i_k, i_1]$ of vertices such that only edge (i_k, i_1) is a 0-edge. □

A path $[i_1, i_2, \ldots, i_k]$ is said to be *acyclic* when $i_p \neq i_q$ for all $1 \leq p < q \leq k$. A cycle $[i_1, i_2, \ldots, i_k, i_1]$ is said to be *simple* when its prefix $[i_1, i_2, \ldots, i_k]$ is acyclic.

PROPOSITION 3.2. *An assignment χ to the variables in $\mathcal{E}$ violates transitivity if and only if some* simple *cycle in $G(\mathcal{E}, \chi)$ contains exactly one 0-edge.*

PROOF. The "if" portion of this proof is covered by Proposition 3.1. For the "only if" portion, suppose the construction shown in the proof of Proposition 3.1 yields a cycle C containing exactly one 0-edge. If C is not simple, then it can be partitioned into a set of simple cycles $C_1, C_2, \ldots, C_m$. One of these cycles must contain the 0-edge of C. □

Define a *chord* of a simple cycle to be an edge that connects two vertices that are not adjacent in the cycle. More precisely, for a simple cycle $[i_1, i_2, \ldots, i_k, i_1]$, a chord is an

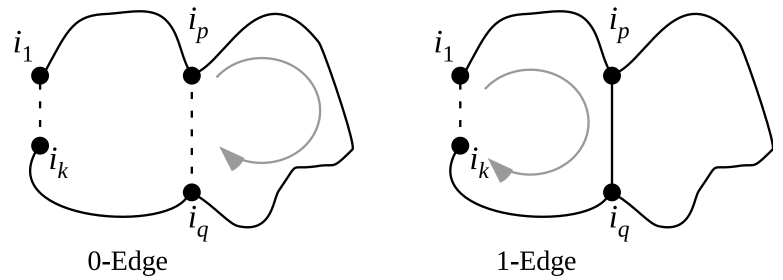


Fig. 1. Case Analysis for Proposition 3.3. 0-Edges are shown as dashed lines. When a cycle representing a transitivity violation contains a chord, we can find a smaller cycle that also represents a transitivity violation.

edge (i_p, i_q) in $G(\mathcal{E})$ such that $1 \leq p < q \leq k$, with $p+1 < q$, and either $p \neq 1$ or $q \neq k$. A cycle is said to be *chord-free* if it is simple and has no chords.

PROPOSITION 3.3. *An assignment χ to the variables in $\mathcal{E}$ violates transitivity if and only if some* chord-free *cycle in $G(\mathcal{E}, \chi)$ contains exactly one 0-edge.*

PROOF. The “if” portion of this proof is covered by Proposition 3.1.

The “only if” portion is proved by induction on the number of variables in the transitivity constraint, i.e., the value of k in Equation 1. The induction hypothesis is: if a transitivity constraint with k variables is violated, then there must be a chord-free cycle in $G(\mathcal{E}, \chi)$ containing exactly one 0-edge. Clearly this holds when $k \leq 2$, since nontrivial transitivity constraints must have at least 3 variables.

Now assume our hypothesis holds as long for all constraints containing fewer than k variables and suppose assignment χ violates Equation 1. If there are no values of p and q such that there is a variable $e_{[i_p,i_q]} \in \mathcal{E}$ with $p+1 < q$ and either $p \neq 1$ or $q \neq k$, then the cycle denoted by this constraint is chord-free. If such values of p and q exist, then consider the two cases illustrated in Figure 1, where 0-edges are shown as dashed lines, 1-edges are shown as solid lines, and the wavy lines represent sequences of 1-edges. Case 1: Edge (i_p, i_q) is a 0-edge (shown on the left). Then the transitivity constraint:

$$e_{[i_p,i_{p+1}]} \wedge \cdots \wedge e_{[i_{q-1},i_q]} \;\Rightarrow\; e_{[i_p,i_q]}$$

is violated and has fewer than k variables. Case 2: Edge (i_p, i_q) is a 1-edge (shown on the right). Then the transitivity constraint:

$$e_{[i_1,i_2]} \wedge \cdots \wedge e_{[i_{p-1},i_p]} \wedge e_{[i_p,i_q]} \wedge e_{[i_q,i_{q+1}]} \wedge \cdots \wedge e_{[i_{k-1},i_k]} \;\Rightarrow\; e_{[i_1,i_k]}$$

is violated and has fewer than k variables. In either case our induction hypothesis applies, and hence there must be some chord-free cycle in $G(\mathcal{E}, \chi)$ containing exactly one 0-edge. □

Each length k cycle $[i_1, i_2, \ldots, i_k, i_1]$ yields k constraints, given by the following clauses. Each clause is derived by expressing Equation 1 as a disjunction.

$$\begin{array}{l}
\neg e_{[i_1,i_2]} \vee \cdots \vee \neg e_{[i_{k-1},i_k]} \vee e_{[i_k,i_1]} \\
\neg e_{[i_2,i_3]} \vee \cdots \vee \neg e_{[i_{k-1},i_k]} \vee \neg e_{[i_k,i_1]} \vee e_{[i_1,i_2]} \\
\quad \cdots \\
\neg e_{[i_k,i_1]} \vee \neg e_{[i_1,i_2]} \vee \cdots \vee \neg e_{[i_{k-2},i_{k-1}]} \vee e_{[i_{k-1},i_k]}
\end{array} \tag{2}$$

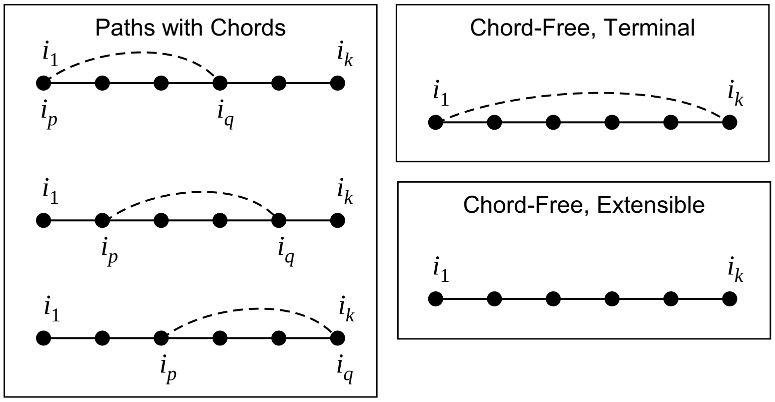


Fig. 2. Different Types of Paths. Those on the left contain chords (shown as dashed arcs), while those on the right are chord-free. A chord-free path with an edge between its endpoints is terminal, and otherwise it is extensible.

For a set of relational variables $\mathcal{E}$, we define $F_{\text{trans}}(\mathcal{E})$ to be the conjunction of all transitivity constraints for all chord-free cycles in the graph $G(\mathcal{E})$.

THEOREM 3.4. *An assignment to the relational variables $\mathcal{E}$ will satisfy all of the transitivity constraints given by Equation 1 if and only if it satisfies $F_{trans}(\mathcal{E})$.*

This theorem follows directly from Proposition 3.3 and the encoding given by Equation 2.

3.1 Enumerating Chord-Free Cycles

To enumerate the chord-free cycles of a graph, we exploit the following properties. An acyclic path $[i_1, i_2, \ldots, i_k]$ is said to have a chord when there is an edge (i_p, i_q) in $G(\mathcal{E})$ such that $1 \leq p < q \leq k$ with $p + 1 < q$, and either $p \neq 1$ or $q \neq k$. The left hand side of Figure 2 illustrates several types of paths with chords. We classify a chord-free path as *terminal* when (i_k, i_1) is in $G(\mathcal{E})$, and as *extensible* otherwise. These are shown on the right hand side of Figure 2. Observe that a terminal, chord-free path consists of all but one edge of a chord-free cycle.

PROPOSITION 3.5. *A path $[i_1, i_2, \ldots, i_k]$ is chord-free and terminal if and only if the cycle $[i_1, i_2, \ldots, i_k, i_1]$ is chord-free.*

This follows by noting that the conditions imposed on a chord-free path are identical to those for a chord-free cycle, except that the latter includes a closing edge (i_k, i_1).

A *proper prefix* of path $[i_1, i_2, \ldots, i_k]$ is a path $[i_1, i_2, \ldots, i_j]$ such that $1 \leq j < k$.

PROPOSITION 3.6. *Every proper prefix of a chord-free path is chord-free and extensible.*

PROOF. Clearly, any prefix of a chord-free path is also chord-free. Let $[i_1, i_2, \ldots, i_j]$ be a prefix of a chord-free path $[i_1, i_2, \ldots, i_j, \ldots, i_k]$ with $j < k$. If this prefix were terminal, then the edge (i_j, i_1) would form a chord of $[i_1, i_2, \ldots, i_j, \ldots, i_k]$. □

Given these properties, we can enumerate the set of all chord-free paths by breadth first expansion. As we enumerate these paths, we also generate C, the set of all chord-free

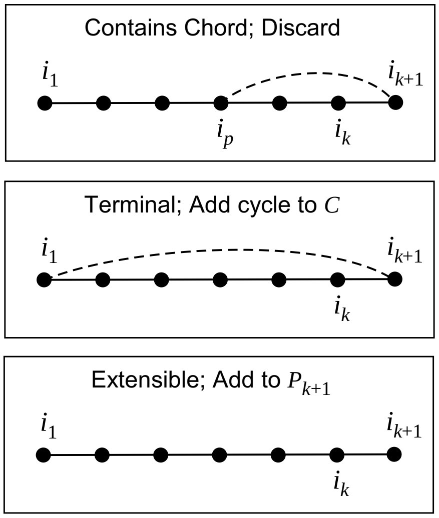


Fig. 3. Possible Actions Taken after Extending Path with an Additional Edge. The resulting path $[i_1, \ldots, i_k, i_{k+1}]$, may have a chord. Otherwise, if it is terminal then we have found a chord-free cycle, while if it is extensible, it is retained for further extension.

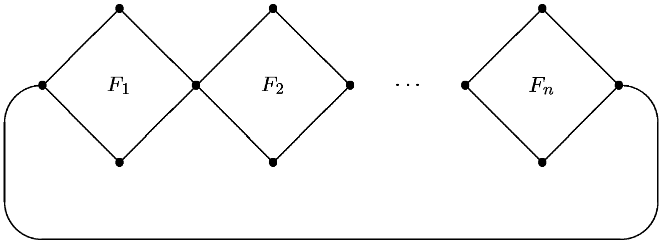


Fig. 4. Class of Graphs with Many Chord-Free Cycles. For a graph with n diamond-shaped faces, there are $2^n + n$ chord-free cycles.

cycles. Define P_k to be the set of all extensible, chord-free paths having k vertices, for $1 \leq k \leq N$. Initially we have $P_1 = \{[i] | 1 \leq i \leq N\}$, $P_k = \emptyset$ for $k > 1$, and $C = \emptyset$.

Given set P_k, we generate set P_{k+1} and add some cycles of length $k + 1$ to C. For each path $\pi = [i_1, i_2, \ldots, i_k] \in P_k$, we consider the path $\pi' = [i_1, i_2, \ldots, i_k, i_{k+1}]$ for each edge (i_k, i_{k+1}) in $G(\mathcal{E})$, such that $i_{k+1} \neq i_{k-1}$. We are guaranteed that $i_{k+1} \neq i_p$ for any $1 \leq p \leq k$, or else π would not have been chord-free and extensible. The possible actions taken with path π' are illustrated in Figure 3. If there is an edge (i_{k+1}, i_p) in $G(\mathcal{E})$ for some $1 < p < k$, then we can discard π', since it has a chord. Otherwise, if there is an edge (i_{k+1}, i_1) in $G(\mathcal{E})$, we add the cycle $[i_1, i_2, \ldots, i_k, i_{k+1}, i_1]$ to C. If both of these conditions fail, then we can add π' to P_{k+1}.

After generating all of these paths, we can use the set C to generate the set of all chord-free cycles. For each terminal, chord-free cycle having k vertices, there will be $2k$ members of C—each of the k edges of the cycle can serve as the closing edge, and a cycle can traverse the closing edge in either direction. To generate the set of clauses given by Equation 2, we simply need to choose one element of C for each closing edge, e.g., by considering only cycles $[i_1, \ldots, i_k, i_1]$ for which $i_1 < i_k$.

As Figure 4 indicates, there can be an exponential number of chord-free cycles in a graph. In particular, this figure illustrates a family of graphs with $3n + 1$ vertices. Con-

Table II. Cycles in Original and Augmented Benchmark Graphs. Results are given for the three different methods of encoding transitivity constraints.

Circuit		Direct			Dense			Sparse		
		Edges	Cycles	Clauses	Edges	Cycles	Clauses	Edges	Cycles	Clauses
1×DLX-C		27	90	360	78	286	858	33	40	120
1×DLX-C-t		37	95	348	78	286	858	42	68	204
2×DLX-CA		118	2,393	9,572	300	2,300	6,900	172	697	2,091
2×DLX-CA-t		137	1,974	7,944	300	2,300	6,900	178	695	2,085
2×DLX-CC		124	2,567	10,268	300	2,300	6,900	182	746	2,238
2×DLX-CC-t		143	2,136	8,364	300	2,300	6,900	193	858	2,574
100 Buggy	min.	89	1,446	6,360	231	1,540	4,620	132	430	1,290
2×DLX-CC	avg.	124	2,562	10,270	300	2,300	6,900	182	750	2,244
	max.	132	3,216	12,864	299	2,292	6,877	196	885	2,655
M_4		24	24	192	120	560	1,680	42	44	132
M_5		40	229	3,056	300	2,300	6,900	77	98	294
M_6		60	3,436	61,528	630	7,140	21,420	131	208	624
M_7		84	65,772	1,472,184	1,176	18,424	55,272	206	408	1,224
M_8		112	1,743,247	48,559,844	2,016	41,664	124,992	294	662	1,986

sider the cycles passing through the n diamond-shaped faces as well as the edge along the bottom. For each diamond-shaped face F_i, a cycle can pass through either the upper vertex or the lower vertex. Thus there are 2^n such cycles. In addition, the edges forming the perimeter of each face F_i create a chord-free cycle, giving a total of $2^n + n$ chord-free cycles.

The columns labeled "Direct" in Table II show results for enumerating the chord-free cycles for our benchmarks. For each correct microprocessor, we have two graphs: one for which transitivity constraints played no role in the verification, and one (indicated with a "t" at the end of the name) modified to require enforcing transitivity constraints. We summarize the results for the transitivity constraints in our 100 buggy variants of 2×DLX-CC in terms of the minimum, the average, and the maximum of each measurement. We also show results for five synthetic benchmarks consisting of $n \times n$ planar meshes M_n, with n ranging from 4 to 8, where the mesh for $n = 6$ is illustrated in Figure 5. For all of the circuit benchmarks, the number of cycles, although large, appears to be manageable. Moreover, the cycles have at most 4 edges. The synthetic benchmarks, on the other hand, demonstrate the exponential growth predicted as worst case behavior. The number of cycles grows quickly as the meshes grow larger. Furthermore, the cycles can be much longer, causing the number of clauses to grow even more rapidly.

3.2 Adding More Relational Variables

Enumerating the transitivity constraints based on the set of relational variables $\mathcal{E}$ appearing in formula F_{sat} runs the risk of generating a Boolean formula of exponential size.

We can guarantee polynomial growth by considering a larger set of relational variables. In general, let $\mathcal{E}'$ be some set of relational variables such that $\mathcal{E} \subseteq \mathcal{E}' \subseteq \{e_{i,j} | 1 \leq i < j \leq N\}$, and let $F_{\text{trans}}(\mathcal{E}')$ be the transitivity constraint formula generated by enumerating the chord-free cycles in the graph $G(\mathcal{E}')$.

THEOREM 3.7. *If $\mathcal{E}$ is the set of relational variables in F_{sat} and $\mathcal{E} \subseteq \mathcal{E}'$, then the formula $F_{sat} \wedge F_{trans}(\mathcal{E})$ is satisfiable if and only if $F_{sat} \wedge F_{trans}(\mathcal{E}')$ is satisfiable.*

We introduce a series of lemmas to prove this theorem. For a propositional formula F over a set of variables $\mathcal{A}$ and an assignment $\chi \colon \mathcal{A} \rightarrow \{0, 1\}$, define the *valuation* of F under χ, denoted $[F]_\chi$, to be the result of evaluating formula F according to assignment χ. We first prove that we can extend any assignment over a set of relational variables to one over a superset of these variables yielding identical valuations for both transistivity constraint formulas.

LEMMA 3.8. *For any sets of relational variables $\mathcal{E}_1$ and $\mathcal{E}_2$ such that $\mathcal{E}_1 \subseteq \mathcal{E}_2$, and for any assignment $\chi_1\colon \mathcal{E}_1 \rightarrow \{0,1\}$, such that $[F_{trans}(\mathcal{E}_1)]_{\chi_1} = 1$, there is an assignment $\chi_2\colon \mathcal{E}_2 \rightarrow \{0,1\}$ such that $[F_{trans}(\mathcal{E}_2)]_{\chi_2} = 1$.*

PROOF. We consider the case where $\mathcal{E}_2 = \mathcal{E}_1 \cup \{e_{i,j}\}$. The general statement of the proposition then holds by induction on $|\mathcal{E}_2| - |\mathcal{E}_1|$.

Define assignment χ_2 to be:

$$\chi_2(e) \;=\; \begin{cases} \chi_1(e), & e \neq e_{i,j} \\ 1, & \text{Graph } G(\mathcal{E}_1, \chi) \text{ has a path of 1-edges from node } i \text{ to node } j. \\ 0, & \text{otherwise} \end{cases}$$

We consider two cases:

(1) If $\chi_2(e_{i,j}) = 0$, then any cycle in $G(\mathcal{E}_2, \chi_2)$ through $e_{i,j}$ must contain a 0-edge other than $e_{i,j}$. Hence adding this edge does not introduce any transitivity violations.

(2) If $\chi_2(e_{i,j}) = 1$, then there must be some path π_1 of 1-edges between nodes i and j in $G(\mathcal{E}_1, \chi_1)$. In order for the introduction of 1-edge $e_{i,j}$ to create a transitivity violation, there must also be some path π_2 between nodes i and j in $G(\mathcal{E}_1, \chi_1)$ containing exactly one 0-edge. But then we could concatenate paths π_1 and π_2 to form a cycle in $G(\mathcal{E}_1, \chi_1)$ containing exactly one 0-edge, implying that $[F_{\text{trans}}(\mathcal{E}_1)]_{\chi_1} = 0$. We conclude therefore that adding 1-edge $e_{i,j}$ does not introduce any transitivity violations.

□

LEMMA 3.9. *For $\mathcal{E}_1 \subseteq \mathcal{E}_2$ and assignment $\chi\colon \mathcal{E}_2 \rightarrow \{0,1\}$, such that $[F_{trans}(\mathcal{E}_2)]_{\chi} = 1$, we also have $[F_{trans}(\mathcal{E}_1)]_{\chi} = 1$.*

PROOF. We note that any cycle in $G(\mathcal{E}_1, \chi)$ must be present in $G(\mathcal{E}_2, \chi)$ and have the same edge labeling. Thus, if $G(\mathcal{E}_2, \chi)$ has no cycle with a single 0-edge, then neither does $G(\mathcal{E}_1, \chi)$. □

We now return to the proof of Theorem 3.7.

PROOF. Suppose that $F_{\text{sat}} \wedge F_{\text{trans}}(\mathcal{E})$ is satisfiable, i.e., there is some assignment χ such that $[F_{\text{sat}}]_{\chi} = 1$ and $[F_{\text{trans}}(\mathcal{E})]_{\chi} = 1$. Then by Lemma 3.8 we can find an assignment χ' such that $[F_{\text{trans}}(\mathcal{E}')]_{\chi'} = 1$. Furthermore, since the construction of χ' by Lemma 3.8 preserves the values assigned to all variables in $\mathcal{E}$, and these are the only relational variables occurring in F_{sat}, we can conclude that $[F_{\text{sat}}]_{\chi'} = 1$. Therefore $F_{\text{sat}} \wedge F_{\text{trans}}(\mathcal{E}')$ is satisfiable.

Suppose on the other hand that $F_{\text{sat}} \wedge F_{\text{trans}}(\mathcal{E}')$ is satisfiable, i.e., there is some assignment χ' such that $[F_{\text{sat}}]_{\chi'} = [F_{\text{trans}}(\mathcal{E}')]_{\chi'} = 1$. Then by Lemma 3.9 we also have $[F_{\text{trans}}(\mathcal{E})]_{\chi'} = 1$, and hence $F_{\text{sat}} \wedge F_{\text{trans}}(\mathcal{E})$ is satisfiable. □

Our goal then is to add as few relational variables as possible in order to reduce the size of the transitivity formula. We will continue to use our path enumeration algorithm to generate the transitivity formula.

3.3 Dense Enumeration

For the *dense* enumeration method, let $\mathcal{E}_N$ denote the set of variables $e_{i,j}$ for all values of i and j such that $1 \leq i < j \leq N$. Graph $G(\mathcal{E}_N)$ is a complete, undirected graph. In this graph, any cycle of length greater than three must have a chord. Hence our algorithm will enumerate transitivity constraints of the form $e_{[i,j]} \wedge e_{[j,k]} \Rightarrow e_{[i,k]}$, for all distinct values of i, j, and k. The graph has $N(N-1)/2$ edges and $N(N-1)(N-2)/6$ chord-free cycles, yielding a total of $N(N-1)(N-2)/2 = \Theta(N^3)$ transitivity constraints.

The columns labeled "Dense" in Table II show the complexity of this method for the benchmark circuits. For the smaller graphs 1×DLX-C, 1×DLX-C-t, M_4 and M_5, this method yields more clauses than direct enumeration of the cycles in the original graph. For the larger graphs, however, it yields fewer clauses. The advantage of the dense method is most evident for the mesh graphs, where the cubic complexity is far superior to exponential.

3.4 Sparse Enumeration

We can improve on both of these methods by exploiting the sparse structure of $G(\mathcal{E})$. We want to introduce additional relational variables, giving a set of variables $\mathcal{E}^+$, such that the resulting graph $G(\mathcal{E}^+)$ becomes *chordal* [Rose 1970]. That is, the graph has the property that every cycle of length greater than three has a chord. We can then generate a sufficient set of transitivity constraints by enumerating the triangles in $G(\mathcal{E}^+)$. Our hope is that the number of constraints will be much smaller than is generated by the dense enumeration method.

Chordal graphs have been studied extensively in the context of sparse Gaussian elimination. In fact, the problem of finding a minimum set of variables to add to our set is identical to the problem of finding an elimination ordering for Gaussian elimination that minimizes the amount of fill-in. Although this problem is NP-complete [Yannakakis 1981], there are good heuristic solutions. In particular, our implementation proceeds as a series of elimination steps, starting with graph $G_0 = G(\mathcal{E})$. On elimination step i, we create a graph G_i that is identical to G_{i-1}, except that some vertex m_i and its incident edges are removed and new edges are possibly added. In particular, for every pair of distinct, vertices j and k such that G_{i-1} contains edges (m_i, j) and (m_i, k), we add an edge (j, k) to G_i if it does not already exist. This process continues until we reach empty graph G_N. Now let G be a graph identical to $G(\mathcal{E})$, plus all of the edges that were added during the elimination process. G has an edge set $\cup_{i=0,N} E_i$, where E_i is the set of edges in graph G_i. It can be shown that G is a chordal graph [Rose 1970]. To choose which vertex to eliminate on a given step, our implementation uses the simple heuristic of choosing the vertex with minimum degree. If more than one vertex has minimum degree, we choose one that minimizes the number of new edges added. Thus, we can let $\mathcal{E}^+$ consist of the variables in $\mathcal{E}$ plus a variable $e_{[j,k]}$ for each edge (j, k) that was added at some step in the elimination process.

The columns in Table II labeled "Sparse" show the effect of making the benchmark graphs chordal by this method. Observe that this method gives superior results to either of the other two methods. In our implementation we have therefore used the sparse method to generate all of the transitivity constraint formulas.

4. SAT-BASED DECISION PROCEDURES

Most Boolean satisfiability (SAT) checkers take as input a formula expressed in clausal form. Each clause is a set of *literals*, where a literal is either a variable or its complement.

Table III. Performance of FGRASP on Benchmark Circuits. Results are given both without and with transitivity constraints.

Circuit		C_{sat}		$C_{\text{trans}} \cup C_{\text{sat}}$		Ratio
		Satisfiable?	Secs.	Satisfiable?	Secs.	
1×DLX-C		No	3	No	4	1.4
1×DLX-C-t		Yes	1	No	9	N.A.
2×DLX-CA		No	176	No	1,275	7.2
2×DLX-CA-t		Yes	3	No	896	N.A.
2×DLX-CC		No	5,035	No	9,932	2.0
2×DLX-CC-t		Yes	4	No	15,003	N.A.
100 Buggy	min.	Yes	1	Yes	1	0.2
2×DLX-CC	avg.	Yes	125	Yes	1,517	2.3
	max.	Yes	2,186	Yes	43,817	69.4

A clause denotes the disjunction of its literals. The task of the checker is to either find an assignment to the variables that satisfies all of the clauses or to determine that no such assignment exists. We can solve the constrained satisfiability problem using a conventional SAT checker by generating a set of clauses C_{trans} representing $F_{\text{trans}}(\mathcal{E}^+)$ and a set of clauses C_{sat} representing the formula F_{sat}. We then run the checker on the combined clause set $C_{\text{sat}} \cup C_{\text{trans}}$ to find satisfying solutions to $F_{\text{sat}} \wedge F_{\text{trans}}(\mathcal{E}^+)$.

In experimenting with a number of Boolean satisfiability checkers, we have found that FGRASP [Marques-Silva and Sakallah 1999] has the best overall performance. The most recent version can be directed to periodically restart the search using a randomly-generated variable assignment [Marques-Silva 1999]. This is the first SAT checker we have tested that can complete all of our benchmarks. All of our experiments were conducted on a 336 MHz Sun UltraSPARC II with 1.2GB of primary memory. We show only the times required for the satisfiability program, but all other processing steps required only a negligible (well under 1.0 second) amount of time.

As indicated by Table III, we ran FGRASP on clause sets C_{sat} and $C_{\text{trans}} \cup C_{\text{sat}}$, i.e., both without and with transitivity constraints. For benchmarks 1×DLX-C, 2×DLX-CA, and 2×DLX-CC, the formula F_{sat} is unsatisfiable. As can be seen, including transitivity constraints increases the run time significantly. For benchmarks 1×DLX-C-t, 2×DLX-CA-t, and 2×DLX-CC-t, the formula F_{sat} is satisfiable, but only because transitivity is not enforced. When we add the clauses for F_{trans}, the formula becomes unsatisfiable. For the buggy circuits, the run times for C_{sat} range from under one second to over 36 minutes. The run times for $C_{\text{trans}} \cup C_{\text{sat}}$ range from less than one second to over 12 hours. In some cases, adding transitivity constraints actually decreased the CPU time (by as much as a factor of 5), but in most cases the CPU time increased (by as much as a factor of 69). On average (using the geometric mean) adding transitivity constraints increased the CPU time by a factor of 2.3. We therefore conclude that satisfiability checking with transitivity constraints is more difficult than conventional satisfiability checking, but the added complexity is not overwhelming.

5. OBDD-BASED DECISION PROCEDURES

A simple-minded approach to solving satisfiability with transitivity constraints using OBDDs would be to generate separate OBDD representations of F_{trans} and F_{sat}. We could then use the APPLY operation [Bryant 1986] to generate an OBDD for $F_{\text{trans}} \wedge F_{\text{sat}}$, and then either find a satisfying assignment or determine that the function is unsatisfiable. We

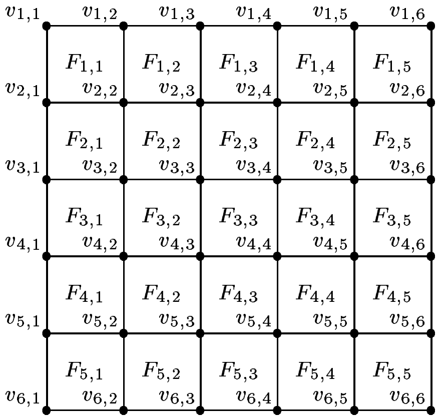


Fig. 5. Mesh Graph M_6.

show that for some sets of relational variables $\mathcal{E}$, the OBDD representation of $F_{\text{trans}}(\mathcal{E})$ can be too large to represent and manipulate.

5.1 Lower Bound on the OBDD Representation of $F_{\text{trans}}(\mathcal{E})$

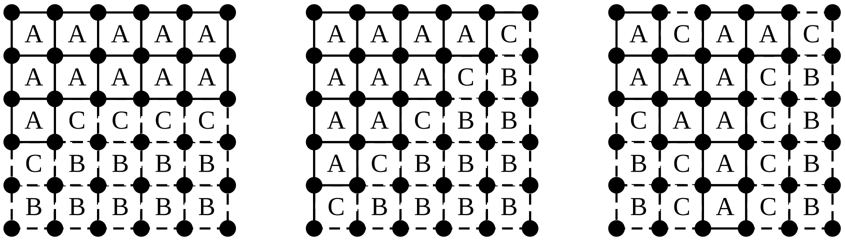
We prove that for some sets $\mathcal{E}$, the OBDD representation of $F_{\text{trans}}(\mathcal{E})$ may be of exponential size for all possible variable orderings. As mentioned earlier, the NP-completeness result proved by Goel et al. [1998] has implications for the complexity of representing $F_{\text{trans}}(\mathcal{E})$ as an OBDD. They showed that given an OBDD G_{sat} representing formula F_{sat}, the task of finding a satisfying assignment of F_{sat} that also satisfies the transitivity constraints in $\mathit{Trans}(\mathcal{E})$ is NP-complete in the size of G_{sat}. By this, assuming $P \neq NP$, we can infer that the OBDD representation of $F_{\text{trans}}(\mathcal{E})$ may be of exponential size when using the same variable ordering as is used in G_{sat}. Our result extends this lower bound to arbitrary variable orderings and is independent of the P vs. NP problem.

Let M_n denote a planar mesh consisting of a square array of $n \times n$ vertices. For example, Figure 5 shows the graph for $n = 6$. Being a planar graph, the edges partition the plane into *faces*. As shown in Figure 5 we label these $F_{i,j}$ for $1 \leq i, j \leq n-1$. There are a total of $(n-1)^2$ such faces. One can see that the set of edges forming the border of each face forms a chord-free cycle. As shown in Table II, many other cycles are also chord-free, e.g., the perimeter of any rectangular region having height and width greater than one face, but we will consider only the cycles corresponding to single faces.

Define $\mathcal{E}_{n\times n}$ to be a set of relational variables corresponding to the edges in M_n. $F_{\text{trans}}(\mathcal{E}_{n\times n})$ is then an encoding of the transitivity constraints for these variables.

THEOREM 5.1. *Any OBDD representation of $F_{trans}(\mathcal{E}_{n\times n})$ must have $\Omega(2^{n/8})$ vertices.*

To prove this theorem, consider any ordering of the variables representing the edges in M_n. Let A denote those in the first half of the ordering, and B denote those in the second half. Our proof follows the general scheme outlined in [Bryant 1991]. We will show that there are $k \geq (n-3)/8$ variable pairs of the form (ea_i, eb_i) with $ea_i \in A$ and $eb_i \in B$, as



a = 11, b = 9, c = 5 a = 10, b = 10, c = 5 a = 10, b = 6, c = 9

Fig. 6. Partitioning Edges into Sets A (solid) and B (dashed). Each face can then be classified as type A (all solid), B (all dashed), or C (mixed).

well as an assignment of values to the other variables in A and B, such that $F_{\text{trans}}(\mathcal{E}_{n\times n})$ will evaluate to 1 if and only if the variables in each pair (ea_i, eb_i) are assigned identical values. Each variable pair (ea_i, eb_i) will be two edges of a face of M_n. The OBDD representation of the function must have at least 2^k nodes to encode the values assigned to the variables ea_i in A, for all values of i, in order to correctly determine whether their counterparts eb_i in B are assigned identical values. By proving a lower bound on the number of these pairs for any partitioning of the variables, we prove an exponential lower bound for any OBDD representation.

We can classify each face of M_n according to the four edges forming its border:

A: All are in A.

B: All are in B.

C: Some are in A, while others are in B. These are called “split” faces.

Observe that we cannot have a type A face adjacent to a type B face, since their shared edge cannot be in both A and B. Therefore there must be split faces separating any region of type A faces from any region of type B faces.

For example, Figure 6 shows three possible partitionings of the edges of M_6 and the resulting classification of the faces. If we let a, b, and c denote the number of faces of each respective type, we see that we always have $c \geq 5 = n - 1$. In particular, a minimum value for c is achieved when the partitioning of the edges corresponds to a partitioning of the graph into a region of type A faces and a region of type B faces, each having nearly equal size, with the split faces forming the boundary between the two regions.

LEMMA 5.2. *For any partitioning of the edges of mesh graph M_n into equally-sized sets A and B, there must be at least $(n-3)/2$ split faces.*

Note that this lower bound is somewhat weak—it seems clear that we must have $c \geq n - 1$. However, this weaker bound will suffice to prove an exponential lower bound on the OBDD size.

PROOF. Our proof is an adaptation of a proof by Leighton [1992, Theorem 1.21] that M_n has a bisection bandwidth of at least n. That is, one would have to remove at least n edges to split the graph into two parts of equal size.

Observe that M_n has n^2 vertices and $2n(n-1)$ edges. These edges are split so that $n(n-1)$ are in A and $n(n-1)$ are in B.

Let M_n^D denote the planar dual of M_n. That is, it contains a vertex $u_{i,j}$ for each face $F_{i,j}$ of M_n, and edges between pairs of vertices for which the corresponding faces in M_n have a common edge. In fact, one can readily see that this graph is isomorphic to M_{n-1}.

Partition the vertices of M_n^D into sets U_a, U_b, and U_c according to the types of their corresponding faces. Let a, b, and c denote the number of elements in each of these sets. Our objective is to prove that $c \geq (n-3)/2$. Our strategy will be to embed a bipartite graph G in M_n^D with each edge of the G being a path in M_n^D, and with each such path containing at least one vertex in U_c. By showing a lower bound on the number of edges in G and an upper bound on the number of paths cut when a single vertex from U_c is removed, we prove a lower bound on the size of U_c.

First, we can obtain upper bounds on a and b as follows. Each face of M_n has four bordering edges, and each edge is the border of at most two faces. Thus, as an upper bound on a, we must have $4a \leq 2n(n-1)$, giving $a \leq n(n-1)/2$, and similarly for b. In addition, since a face of type A cannot be adjacent in M_n to one of type B, no vertex in U_a can be adjacent in M_n^D to one in U_b.

Consider the complete, directed, bipartite graph having as vertices the set $U_a \cup U_b$, and as edges the set $(U_a \times U_b) \cup (U_b \times U_a)$. There is a total of $2ab$ edges. Given the bounds: $a + b = (n-1)^2 - c$, $a \leq n(n-1)/2$, and $b \leq n(n-1)/2$, the minimum value of $2ab$ is achieved when either $a = n(n-1)/2$ and $b = (n-1)^2 - (n-1)n/2 - c = (n-1)(n-2)/2 - c$, or vice-versa, giving a lower bound:

$$\begin{aligned} 2ab &\geq 2[n(n-1)/2] \cdot [(n-1)(n-2)/2 - c] \\ &= n(n-1)^2(n-2)/2 \; - \; cn(n-1) \end{aligned}$$

We can embed this bipartite graph in M_n^D by forming a path from vertex $u_{i,j}$ to vertex $u_{i',j'}$, where either $u_{i,j} \in U_a$ and $u_{i',j'} \in U_b$, or vice-versa. By convention, we will use the path that first follows vertical edges to $u_{i',j}$ and then follows horizontal edges to $u_{i',j'}$. We must have at least one vertex in U_c along each such path, and therefore removing the vertices in U_c would cut all $2ab$ paths.

For each vertex $u_{i,j} \in U_c$, we can bound the total number of paths passing through it by separately considering paths that enter from the bottom, the top, the left, and the right. For those entering from the bottom, there are at most $n-i-1$ source vertices and $i(n-1)$ destination vertices, giving at most $i(n-i-1)(n-1)$ paths. This quantity is maximized for $i = (n-1)/2$, giving an upper bound of $(n-1)^3/4$. A similar argument shows that there are at most $(n-1)^3/4$ paths entering from the top of any vertex. For the paths entering from the left, there are at most $(j-1)(n-1)$ source vertices and $(n-j)$ destinations, giving at most $(j-1)(n-j)(n-1)$ paths. This quantity is maximized when $j = (n-1)/2$, giving an upper bound of $(n-1)^3/4$. This bound also holds for those paths entering from the right. Thus, removing a single vertex would cut at most $(n-1)^3$ paths.

Combining the lower bound on the number of paths $2ab$, the upper bound on the number of paths cut by removing a single vertex, and the fact that we are removing c vertices, we have:

$$c(n-1)^3 \quad \geq \quad 2ab \quad \geq \quad n(n-1)^2(n-2)/2 - cn(n-1).$$

From this we can derive

$$\begin{aligned} c(n-1)^3 &\geq n(n-1)^2(n-2)/2 - cn(n-1) \\ c(n-1)^2 + cn &\geq n(n-1)(n-2)/2 \end{aligned}$$

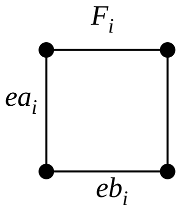


Fig. 7. Split Face F_i in Proof of Theorem 5.1. The variable for edge ea_i is from set A, while that for edge eb_i is from set B.

$$c(n^2 - n + 1) \;\geq\; n(n-1)(n-2)/2$$

We can rewrite $n(n-1)(n-2)$ as $(n^2 - n + 1)(n-3) + n^2 - 2n + 3$. Observing that $n^2 - 2n + 3 > 0$ for all values of n, and that $n^2 - n + 1 > 0$, we have:

$$\begin{aligned} c(n^2 - n + 1) &\geq (n^2 - n + 1)(n-3)/2 + (n^2 - 2n + 3)/2 \\ c(n^2 - n + 1) &\geq (n^2 - n + 1)(n-3)/2 \\ c &\geq (n-3)/2 \end{aligned}$$

□

Define a set of faces as *independent* if no two of them share a vertex.

LEMMA 5.3. *For any partitioning of the edges of mesh graph M_n into equal-sized sets A and B, there must be an independent set of split faces containing at least $(n-3)/8$ elements.*

PROOF. Partition the set of split faces into four sets: EE, EO, OE, and OO, where face $F_{i,j}$ is assigned to a set according to the values of i and j:

EE: Both i and j are even.
EO: i is even and j is odd.
OE: i is odd and j is even.
OO: Both i and j are odd.

Each of these sets is independent. At least one of the sets must contain at least $1/4$ of the elements. Since there are at least $(n-3)/2$ split faces, one of the sets must contain at least $(n-3)/8$ vertex-independent split faces. □

We can now complete the proof of Theorem 5.1.

PROOF. Suppose there is an independent set $\mathcal{F} \doteq \{F_1, \ldots, F_k\}$ of split faces. As illustrated in Figure 7, for each face F_i, we can choose a face edge ea_i from A, and a face edge eb_i from B. Although not necessary for the proof here, we can assume that ea_i and eb_i are adjacent.

Let $\vec{x}, \vec{y} \in \{0,1\}^k$ denote two Boolean vectors of length k. We define assignment $\alpha_{\vec{x}}: A \rightarrow \{0,1\}$ as follows:

(1) If $e = ea_i$ for some $F_i \in \mathcal{F}$, then $\alpha_{\vec{x}}(e) = x_i$.
(2) If $e \in A$ is some other edge in some face $F_i \in \mathcal{F}$, then $\alpha_{\vec{x}}(e) = 1$.
(3) Otherwise $\alpha_{\vec{x}}(e) = 0$.

Similarly, we define assignment $\beta_{\vec{y}}: B \rightarrow \{0,1\}$ as follows:

(1) If $e = eb_i$ for some $F_i \in \mathcal{F}$, then $\beta_{\vec{y}}(e) = y_i$.

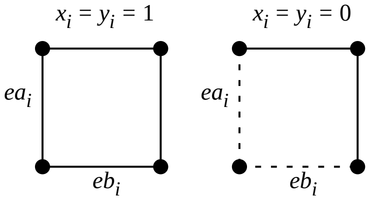


Fig. 8. Possible Edge Types for Face F_i when $x_i = y_i$. 1-edges are shown as solid lines, while 0-edges are shown as dashed lines. In either case, there are no transitivity violations.

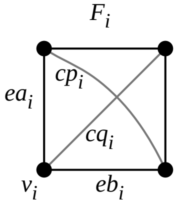


Fig. 9. Split Face F_i in Proof of Corollary 5.4. The graph may also contain diagonal edges across the face. These are labeled cp_i and cq_i.

(2) If $e \in B$ is some other edge in some face $F_i \in \mathcal{F}$, then $\beta_{\vec{y}}(e) = 1$.

(3) Otherwise $\beta_{\vec{y}}(e) = 0$.

The combined assignment $\alpha_{\vec{x}} \cdot \beta_{\vec{y}}$ assigns values to all variables in $\mathcal{E}_{n\times n}$. We claim that $F_{\text{trans}}(\mathcal{E}_{n\times n})$ evaluates to 1 under this assignment if and only if $\vec{x} = \vec{y}$. We argue this by examining the possible cycles in the graph $G(\mathcal{E}_{n\times n}, \alpha_{\vec{x}} \cdot \beta_{\vec{y}})$.

First consider the case where $\vec{x} = \vec{y}$. The two possible cases for face F_i are illustrated in Figure 8. The cycle forming the face's perimeter will have no 0-edges when $x_i = y_i = 1$ and two 0-edges when $x_i = y_i = 0$. Any other cycle in the graph must contain at least two edges that are not part of any face in $\mathcal{F}$, and these two will be 0-edges. Hence, $F_{\text{trans}}(\mathcal{E}_{n\times n})$ evaluates to 1 under this assignment.

Suppose, on the other hand, that $x_i = 1$ and $y_i = 0$ for some i. Then the edges forming the perimeter of face F_i will have exactly one 0-edge, causing the function to evaluate to 0. A similar result holds when $x_i = 0$ and $y_i = 1$.

Thus, the set of assignments $\{\alpha_{\vec{x}} | \vec{x} \in \{0,1\}^k\}$ forms an *OBDD fooling set*, as defined in [Bryant 1991]. That is, for each distinct pair of assignments $\alpha_{\vec{x}}$ and $\alpha_{\vec{x}'}$, there is an assignment β (namely $\beta_{\vec{x}}$), such that the combined assignment $\alpha_{\vec{x}} \cdot \beta$ causes the function to evaluate to 1, while the assignment $\alpha_{\vec{x}'} \cdot \beta$ causes the function to evaluate to 0. As is shown in [Bryant 1991], this implies that the OBDD must have at least $2^k \geq 2^{(n-3)/8} = \Omega(2^{n/8})$ vertices. □

We have seen that adding relational variables can reduce the number of cycles and therefore simplify the transitivity constraint formula. This raises the question of how adding relational variables affects the BDD representation of the transitivity constraints. Unfortunately, the exponential lower bound still holds.

COROLLARY 5.4. *For any set of relational variables $\mathcal{E}$ such that $\mathcal{E}_{n\times n} \subseteq \mathcal{E}$, any OBDD representation of $F_{trans}(\mathcal{E})$ must contain $\Omega(2^{n/8})$ vertices.*

PROOF. The proof is similar to that for Theorem 5.1. The extra edges in $\mathcal{E}$ introduce complications, because they form chords across faces and create cycles containing edges from different faces.

Consider any ordering of the variables. We partition these into two sets A and B such that the variables in A come before those in B, and such that the number of variables that

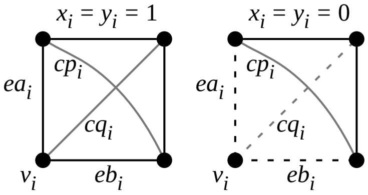


Fig. 10. Possible Edge Types for Face F_i when $x_i = y_i$. 1-edges are shown as solid lines, while 0-edges are shown as dashed lines. In either case, there are no transitivity violations, even in the presence of diagonal edges.

are in $\mathcal{E}_{n\times n}$ are equally split between A and B. Let $\mathcal{F} \doteq \{F_1, \ldots, F_k\}$ be an independent set of split faces. For each such face F_i, we can select edges $ea_i \in A$, and $eb_i \in B$, such that they are adjacent, i.e., they share a common vertex v_i, as illustrated in Figure 9. The graph can potentially contain edges that form diagonals across the face. We label these cp_i (not incident on v_i) and cq_i (incident on v_i).

For Boolean vector $\vec{x} \in \{0,1\}^k$ we define assignment $\alpha_{\vec{x}}$ to the variables in A as follows:

(1) If $e = ea_i$ for some $F_i \in \mathcal{F}$, then $\alpha_{\vec{x}}(e) = x_i$.
(2) If $e \in A$ is some other edge in some face $F_i \in \mathcal{F}$, then $\alpha_{\vec{x}}(e) = 1$.
(3) If e is some other edge in $\mathcal{E}_{n\times n}$, then $\alpha_{\vec{x}}(e) = 0$.
(4) If $e = cq_i$ for some face $F_i \in \mathcal{F}$, then $\alpha_{\vec{x}}(e) = x_i$.
(5) If $e = cp_i$ for some face $F_i \in \mathcal{F}$, then $\alpha_{\vec{x}}(e) = 1$.
(6) For any other edge e, $\alpha_{\vec{x}}(e) = 0$.

For Boolean vector $\vec{y} \in \{0,1\}^k$, we define assignment $\beta_{\vec{y}}$ to the variables in B as follows:

(1) If $e = eb_i$ for some $F_i \in \mathcal{F}$, then $\beta_{\vec{y}}(e) = y_i$.
(2) If $e \in A$ is some other edge in some face $F_i \in \mathcal{F}$, then $\beta_{\vec{y}}(e) = 1$.
(3) If e is some other edge in $\mathcal{E}_{n\times n}$, then $\beta_{\vec{y}}(e) = 0$.
(4) If $e = cq_i$ for some face $F_i \in \mathcal{F}$, then $\beta_{\vec{y}}(e) = y_i$.
(5) If $e = cp_i$ for some face $F_i \in \mathcal{F}$, then $\beta_{\vec{y}}(e) = 1$.
(6) For any other edge e, $\beta_{\vec{y}}(e) = 0$.

We claim that for the combined assignment $\alpha_{\vec{x}} \cdot \beta_{\vec{y}}$, $F_{\text{trans}}(\mathcal{E}_{n\times n})$ evaluates to 1 if and only if $\vec{x} = \vec{y}$. We argue this by examining the possible cycles in the graph $G(\mathcal{E}, \alpha_{\vec{x}} \cdot \beta_{\vec{y}})$.

First, consider the case where $\vec{x} = \vec{y}$. Figure 10 illustrates the possible cases for face F_i. For this face, we must consider its perimeter, plus possibly cycles including one of the diagonal edges. As before, the perimeter will contain either no 0-edges ($x_i = 1$), or two 0-edges ($x_i = 0$). If edge cp_i is present, then there will be two triangles: one containing cp_i, ea_i and eb_i, which will have either zero or two 0-edges, and one containing cp_i and the other edges of the face, which will have no 0-edges. If edge cq_i is present, then there will be two triangles: one containing cq_i, ea_i, and some other face edge, and one containing cq_i, eb_i, and some other face edge. Each of these triangles will contain either no 0-edges ($x_i = 1$), or two 0-edges ($x_i = 0$). Any other cycle in the graph must contain at least two edges that are neither part of any face in $\mathcal{F}$, nor diagonal edges of some face in $\mathcal{F}$. These two edges must be 0-edges. Thus, $F_{\text{trans}}(\mathcal{E}_{n\times n})$ evaluates to 1.

For the case where $\vec{x} \neq \vec{y}$, the same argument as used in the proof of Theorem 5.1 shows that $F_{\text{trans}}(\mathcal{E}_{n\times n})$ evaluates to 0.

Table IV. Graphs for Reduced Transitivity Constraints. Results are given for the three different methods of encoding transitivity constraints based on the variables in the true support of F_{sat}.

Circuit		Verts.	Direct			Dense			Sparse		
			Edges	Cycles	Clauses	Edges	Cycles	Clauses	Edges	Cycles	Clauses
1×DLX-C-t		9	18	14	45	36	84	252	20	19	57
2×DLX-CA-t		17	44	101	395	136	680	2,040	49	57	171
2×DLX-CC-t		17	46	108	417	136	680	2,040	52	66	198
100 Buggy	min.	3	2	0	0	3	1	3	2	0	0
2×DLX-CC	avg.	12	17	19	75	73	303	910	21	14	42
	max.	19	52	378	1,512	171	969	2,907	68	140	420

Thus, the set of assignments $\{\alpha_{\vec{y}} | \vec{y} \in \{0,1\}^k\}$ forms an OBDD fooling set, implying that the OBDD must have at least $2^k \geq 2^{(n-3)/8} = \Omega(2^{n/8})$ vertices. □

Our lower bounds are fairly weak, and there is no reason to believe that the graphs encountered in real-life examples will resemble rectangular meshes. Still, these theoretical results show the inherent intractability of applying OBDDs to transitivity constraints. We have found in practice that the OBDDs do indeed perform poorly for representing large sets of transitivity constraints. The OBDDs representing the transitivity constraints from our benchmarks tend to be large relative to those generated during the evaluation of F_{sat}. For example, although the OBDD representation of $F_{\text{trans}}(\mathcal{E}^+)$ for benchmark 1×DLX-C-t is just 2,692 nodes (a function over 42 variables), we could not construct the OBDD representations of this function for either 2×DLX-CA-t (178 variables) or 2×DLX-CC-t (193 variables) despite running for over 24 hours.

5.2 Enumerating and Eliminating Violations

Goel et al. [1998] proposed a method that generates implicants (cubes) of the function F_{sat} from its OBDD representation. Each implicant is examined and discarded if it violates a transitivity constraint. In our experiments, we have found this approach works well for the normal, correctly-designed pipelines (i.e., circuits 1×DLX-C, 2×DLX-CA, and 2×DLX-CC) since the formula F_{sat} is unsatisfiable and hence has no implicants. For all 100 of our buggy circuits, the first implicant generated contained no transitivity violation and hence was a valid counterexample.

For circuits that do require enforcing transitivity constraints, we have found this approach impractical. For example, in verifying 1×DLX-C-t by this means, we generated 253,216 implicants, requiring a total of 35 seconds of CPU time (vs. 0.2 seconds for 1×DLX-C). For benchmarks 2×DLX-CA-t and 2×DLX-CC-t, our program ran for over 24 hours without having generated all of the implicants. By contrast, circuits 2×DLX-CA and 2×DLX-CC can be verified in 11 and 29 seconds, respectively. Our implementation could be improved by making sure that we generate only implicants that are irredundant and prime. In general, however, we believe that a verifier that generates individual implicants will not be very robust. The complex control logic for a pipeline can lead to formulas F_{sat} containing very large numbers of implicants, even when transitivity plays only a minor role in the correctness of the design.

5.3 Enforcing a Reduced Set of Transitivity Constraints

One advantage of OBDDs over other representations of Boolean functions is that we can readily determine the *true support* of the function, i.e., the set of variables on which the function depends. This leads to a strategy of computing an OBDD representation of F_{sat}

Table V. OBDD-based Verification. Transitivity constraints were generated for a reduced set of variables $\hat{\mathcal{E}}$.

Circuit		OBDD Nodes			CPU
		F_{sat}	$F_{\text{trans}}(\hat{\mathcal{E}}^{+})$	$F_{\text{sat}} \wedge F_{\text{trans}}(\hat{\mathcal{E}}^{+})$	Secs.
1×DLX-C		1	1	1	0.2
1×DLX-C-t		530	344	1	2
2×DLX-CA		1	1	1	11
2×DLX-CA-t		22,491	10,656	1	109
2×DLX-CC		1	1	1	29
2×DLX-CC-t		17,079	7,168	1	441
100 Buggy	min.	20	1	20	7
2×DLX-CC	avg.	3,173	1,483	25,057	107
	max.	15,784	93,937	438,870	2,466

and intersecting its support with $\mathcal{E}$ to give a set $\hat{\mathcal{E}}$ of relational variables that could potentially lead to transitivity violations. We then augment these variables to make the graph chordal, yielding a set of variables $\hat{\mathcal{E}}^{+}$ and generate an OBDD representation of $F_{\text{trans}}(\hat{\mathcal{E}}^{+})$. We compute $F_{\text{sat}} \wedge F_{\text{trans}}(\hat{\mathcal{E}}^{+})$ and, if it is satisfiable, generate a counterexample.

Table IV shows the complexity of the graphs generated by this method for our benchmark circuits. Comparing these with the full graphs shown in Table II, we see that we typically reduce the number of relational vertices (i.e., edges) by a factor of 3 for the benchmarks modified to require transitivity and by an even greater factor for the buggy circuit benchmarks. The resulting graphs are also very sparse. For example, we can see that both the direct and sparse methods of encoding transitivity constraints greatly outperform the dense method.

Table V shows the complexity of applying the OBDD-based method to all of our benchmarks. In our experiments, we use the CUDD OBDD package [Somenzi 2001] with dynamic variable reordering by sifting. Our measured times include all steps of the decision procedure, although everything except BDD processing required a negligible amount of time. The original circuits 1×DLX-C, 2×DLX-CA, and 2×DLX-CC yielded formulas F_{sat} that were unsatisfiable, and hence no transitivity constraints were required. The 3 modified circuits 1×DLX-C-t, 2×DLX-CA-t, and 2×DLX-CC-t are more interesting. The reduction in the number of relational variables makes it feasible to generate an OBDD representation of the transitivity constraints. Compared to benchmarks 1×DLX-C, 2×DLX-CA, and 2×DLX-CC, we see there is a significant, although tolerable, increase in the computational requirement to verify the modified circuits.

For the 100 buggy variants of 2×DLX-CC, F_{sat} depends on up to 52 relational variables, with an average of 17. This yielded OBDDs for $F_{\text{trans}}(\hat{\mathcal{E}}^{+})$ ranging up to 93,937 nodes, with an average of 1,483. The OBDDs for $F_{\text{sat}} \wedge F_{\text{trans}}(\hat{\mathcal{E}}^{+})$ ranged up to 438,870 nodes (average 25,057), showing that adding transitivity constraints does significantly increase the complexity of the OBDD representation. However, this is just one OBDD at the end of a sequence of OBDD operations. In the worst case, imposing transitivity constraints increased the total CPU time by a factor of 2, but the average increase was only 2%. The memory required to generate F_{sat} ranged from 9.8 to 50.9 MB (average 15.5), but even in the worst case the total memory requirement increased by only 2%.

6. CONCLUSION

By formulating a graphical interpretation of the relational variables, we have shown that we can generate a set of clauses expressing the transitivity constraints that exploits the sparse structure of the relation. Adding relational variables to make the graph chordal eliminates the theoretical possibility of there being an exponential number of clauses and also works well in practice. A conventional SAT checker can then solve constrained satisfiability problems, although the run times increase significantly compared to unconstrained satisfiability. Our best results were obtained using OBDDs. By considering only the relational variables in the true support of F_{sat}, we can enforce transitivity constraints with only a small increase in CPU time.

In more recent work [Velev and Bryant 2001], we have found that the SAT solver CHAFF [Moskewicz et al. 2001] is particularly effective at dealing with the additional clauses expressing transitivity constraints. This program uses techniques that avoid the repeated scanning of the entire clause database as done by other SAT solvers. In conjunction with the sparse enumeration technique described here, CHAFF has allowed our verifier to operate on much more complex processor designs than either we or anyone else could handle before.

We have also conducted some preliminary studies of some superscalar execution units employing out-of-order issue [Hennessy and Patterson 1996]. We have found that transitivity constraints must be enforced to verify these designs, because the logic used to avoid write-after-write hazards relies on this property. In addition, we have found that the OBDDs representing the reduced set of transivity constraints can be too large to generate. Overall, we have found that verifying out-of-order issue processors is much more demanding computationally than is the case for in-order processors.

REFERENCES

BRYANT, R. E. 1986. Graph-based algorithms for Boolean function manipulation. *IEEE Trans. Comput. C-35,* 8 (Aug.), 677–691.

BRYANT, R. E. 1991. On the complexity of VLSI implementations and graph representations of Boolean functions with application to integer multiplication. *IEEE Trans. Comput. 40,* 2 (Feb.), 205–213.

BRYANT, R. E., GERMAN, S., AND VELEV, M. N. 1999. Exploiting positive equality in a logic of equality with uninterpreted functions. In *Computer-Aided Verification*, N. Halbwachs and D. Peled, Eds. Lecture Notes in Computer Science, vol. 1633. Springer-Verlag, 470–482.

BRYANT, R. E. AND VELEV, M. N. 2001. Processor verification using efficient reductions of the logic of uninterpreted functions to propositional logic. *ACM Transactions on Computational Logic 2,* 1 (Jan.).

BURCH, J. R. 1996. Techniques for verifying superscalar microprocessors. In *33rd Design Automation Conference*. 552–557.

BURCH, J. R. AND DILL, D. L. 1994. Automated verification of pipelined microprocessor control. In *Computer-Aided Verification,* D. L. Dill, Ed. Lecture Notes in Computer Science, vol. 818. Springer-Verlag, 68–80.

GOEL, A., SAJID, K., ZHOU, H., AZIZ, A., AND SINGHAL, V. 1998. BDD based procedures for a theory of equality with uninterpreted functions. In *Computer-Aided Verification*, A. J. Hu and M. Y. Vardi, Eds. Lecture Notes in Computer Science, vol. 1427. Springer-Verlag, 244–255.

HENNESSY, J. L. AND PATTERSON, D. A. 1996. *Computer Architecture: A Quantitative Approach, 2nd edition*. Morgan-Kaufmann.

LEIGHTON, F. T. 1992. *An Introduction to Parallel Algorithms and Architectures: Arrays, Trees, and Hypercubes*. Morgan Kaufmann.

MARQUES-SILVA, J. P. 1999. The impact of branching heuristics in propositional satisfiability algorithms. In *9th Portugese Conference on Artificial Intelligence*.

Marques-Silva, J. P. and Sakallah, K. A. 1999. GRASP: A search algorithm for propositional satisfiability. *IEEE Trans. Comput. 48,* 5 (May), 506–521.

Moskewicz, M. W., Madigan, C. F., Zhao, Y., Zhang, L., and Malik, S. 2001. Chaff: Engineering an efficient SAT solver. In *38th Design Automation Conference*.

Rose, D. 1970. Triangulated graphs and the elimination process. *Journal of Mathematical Analysis and Applications 32*, 597–609.

Somenzi, F. 2001. CU decision diagram package. Available from http://vlsi.colorado.edu/~fabio.

Velev, M. N. 2001. EVC: A validity checker for the logic of equality with uinterpred functions and memories, exploiting positive equality and conservative transformations. In *Computer-Aided Verification*, G. Berry, Ed. Lecture Notes in Computer Science. Springer-Verlag.

Velev, M. N. and Bryant, R. E. 1999. Superscalar processor verification using efficient reductions of the logic of equality with uninterpreted functions. In *Correct Hardware Design and Verification Methods*, L. Pierre and T. Kropf, Eds. Vol. 1703. Springer-Verlag, 37–53.

Velev, M. N. and Bryant, R. E. 2001. Effective use of Boolean satisifiability solvers in the formal verification of superscalar and VLIW microprocessors. In *38th Design Automation Conference*.

Yannakakis, M. 1981. Computing the minimum fill-in is NP-complete. *SIAM Jorunal of Algebraic and Discrete Mathematics 2*, 77–79.

Received August 2000; revised May 2001; accepted August 2001;