Mona Reimplemented: WS1S Logic with Mata

Michal Šedý

Email: xsedym02@stud.fit.vutbr.cz;

Abstract

This paper focuses on the reimplementation of the decision procedure for WS1S logic, a second-order logic that can be decided using finite automata. The well known tool for WS1S logic decision, Mona, employs automata with transitions represented through binary decision diagrams (BDDs). Due to the integration of BDDs in automata operations, tasks like reversal cannot be executed in the conventional manner of reverting individual edges. Instead, the reversal of each BDD must be computed, potentially resulting in an exponential blowup. Motivated by these limitations, Pavel Bednar reimplemented Mona using a pure automata approach with the Mata library. This work optimizes the automata methodology, resulting in a significant speedup, up to ten times faster, in WS1S decision compared to Bednar's original reimplementation.

Keywords: Finite Automata, Binary Decision Diagrams, WS1S, MONA, MATA

1 Introduction

The most well-known decision procedures are SAT and SMT [1], which are widely used in various applications such as verification (e.g., predicate abstraction), test generation, hardware synthesis, minimization, artificial intelligence, etc. The SAT (satisfiability) problem is a decision problem that asks whether a given propositional formula is satisfiable. The SMT (satisfiability modulo theories) problem extends the SAT problem to the satisfiability of first-order formulas with equality and atoms from various first-order theories. There are various higher-order decision procedures such as WS1S, WS2S, WSkS, S1S, etc.

This work focuses on WS1S, the weak monadic second-order theory of the first successor. The term "weak" refers to finite sets, "monadic" indicates unary relations, "second-order" allows the usage of quantifiers over the relations, and "first successor" means that there is only one successor (e.g., the structure is linear). WS1S [2] has an extremely simple syntax and semantics: it is variation of predicate logic with first-order variable that denote natural numbers and second-order variables that denote finite sets of natural numbers, it has a single function symbol, which denotes the successor function and has usual comparison operators such as $\leq$, $=$, $\in$ and $\supseteq$. Richard Büchi presented approach how to decide WS1S using finite automata in [3] The main idea is to recursively transform each subformula of the main WS1S formula into deterministic finite automata (DFA) representing feasible interpretations and simulate boolean operations via the automata operations.

The most commonly used tool for deciding WS1S and WS2S is Mona[1], which employs Büchi's recursion approach for the construction of finite automata with binary

[1] accessible at https://www.brics.dk/mona/index.html

decision diagrams (BDD) to represent all automaton transitions. The use of BDD makes the decision faster, but at the cost of making some automata operations, such as reversion, expensive (potentially resulting in exponential blowup). Despite this limitation, Mona is widely utilized in various fields of program verification, including the verification of programs with complex dynamic data structures [4, 5], string analysis [6], parametrized systems [7], distributed systems [8], automatic synthesis [9], hardware verification [10], and many others.

The previously mentioned problem with hard-to-compute automata operations when using BDDs motivated Bc. Pavel Bednář's master's thesis [11]. He reimplemented Mona's decision of WS1S by using a pure automata-based approach with the Mata automata library[2]. The special type of edge, the *jumping edge* has been introduced. The jumping edge contains information about how many variables can be jumped over. The primary idea behind introducing the jumping edge was to enable jumps not only over inner states but also over automaton states, with no upper limit on the maximal jump. However, despite this innovation, the jumping edge did not yield significant improvements in terms of space or time compression. Furthermore, it appears that jumping edges led to an overcomplication of algorithms.

In our approach, we reimplemented Bednář's solution by enhancing each automaton state with an index corresponding to the variable ID, mirroring the indexing strategy used for each inner node in the ordered BDD employed by Mona. This index information allows us to determine the length of a jump based on the indices of the source and destination states in the automaton's transition. Due to the indexing sequence on states follows a pattern of $0, 1, \ldots, n-1, 0, 1, \ldots, n-1, 0, \ldots$, the longest jump can only reach to the next state with an index of 0. While this might appear to be a step backward from Bednář's approach, the limitation on the jump length simplifies all algorithms. Surprisingly, it results in a significantly faster decision of the input formula, up to 10 times faster, compared to the variant with jumping edges.

The first section introduces basic notations, definition of finite automata, binary decision diagrams, and WS1S. In the second section, we delve into the background of automata construction from WS1S formulas. The third section provides a detailed description of algorithms for intersection, union, complement, determinization, and minimization of automata with indexes. Moving to the fourth section, we present a comparison of decision times between the Mona tool, automata with jumping edges, and automata with indexes. The experiments are divided into two parts. Initially, automata operations are tested separately on the automata generated during Mona computation. Following that, the comparison is executed on the entire input formula.

2 Preliminaries

In this section, we briefly introduce the definitions of nondeterministic and deterministic automata, binary decision diagrams, and the WS1S logic.

2.1 Automata

Definition 1. *A deterministic finite automaton is a 5-tuple* $M = (Q, \Sigma, \delta, q_0, F)$*, where its components are:*

- Q *is a finite nonempty set of states,*
- Σ *is an alphabet,*
- $\delta : Q \times \Sigma \to Q$ *is a transition function,*
- $q \in Q$ *is an initial state, and*
- $F \subseteq Q$ *is a set of final states.*

Definition 2. *A nondeterministic finite automaton is a 5-tuple* $M = (Q, \Sigma, \delta, Q_0, F)$*, where* Q*,* Σ*, and* F *are defined identically as for the DFA. The transition function* δ *is defined as* $\delta : Q \times \Sigma \to 2^Q$ *and* $Q_0 \subseteq Q$ *is a nonempty set of initial states.*

[2] available at: https://github.com/VeriFIT/mata

Nondeterminism allows the automaton to make transitions to more than one successor based on the current state and the read input symbol. In contrast, its deterministic variant can transition to at most one state. Nondeterminism keeps the automaton more compact, but certain operations such as complementation cannot be performed directly on NFA. Therefore determinization is required beforehand.

2.2 Binary Decision Diagrams

Representation of the boolean function ϕ with n logical variables leads to 2^n transitions for each automaton state in order to cover every possible combination of logical values. This exponential number of transitions can be reduced using Binary Decision Diagrams (BDDs). Binary Decision Diagrams provide a compact and, most importantly, canonical representation for logical functions in the form $\phi : \{0,1\}^* \to \{0,1\}$.

Definition 3. *The binary decision diagram [12] is rooted, directed, connected, and acyclic graph defined as a 7-tuple* $G = (N, T, var, low, high, root, val)$ *where:*

- N *is finite set on non-terminal (inner) nodes,*
- T *is a finite set of terminal nodes (leaves) such that* $N \cap T = \emptyset$*,*
- $var : N \to N \cup T$ *defines the low and high successors of the inner nodes,*
- $root \in N \cup T$ *is the root node, and*
- $val : T \to \{0,1\}$ *assignes logical value to the leaves.*

The size of the BDD is not determined only by the number of logical variables used within the function ϕ but also by the ordering of the variables in the BDD. The best variable ordering can result in a BDD with a linear (in the number of variables) number of nodes, while the worst ordering can lead to an exponential size.

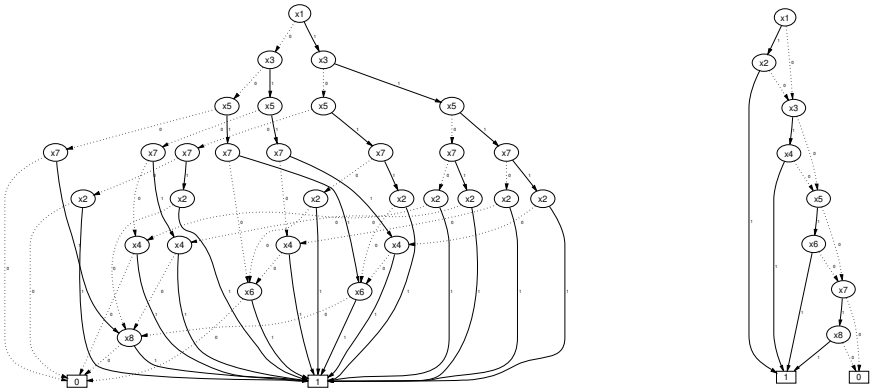


Fig. 1: Two bdds for the function $f(x1, \ldots, x_{2n}) = x_1x_2 + x_3x_4 + \cdots, x_{2n-1}x_{2n}$ with bad variable ordering (on the left) and good variable ordering (on the right).

Consider the Boolean function $f(x_1, \ldots, x_{2n}) = x_1x_2 + x_3x_4 + \cdots + x_{2n-1}x_{2n}$. Using the variable ordering $x_1 < x_3 < \cdots < x_{2n-1} < x_2 < x_4 < \cdots < x_{2n}$, the Binary Decision Diagram (BDD) requires 2^{n+1} nodes to represent the function. Using the ordering $x_1 < x_2 < x_3 < x_4 < \cdots < x_{2n-1} < x_{2n}$, the BDD consists of $2n + 2$ nodes. An example of such orderings is shown in Figure 1. The problem of finding the best variable ordering is NP-hard [13]. However, various heuristics exist to address this challenge [14].

Definition 4. *Let* $\prec$ *be a given ordering on logical variables* Var*, a Binary Decision Diagram (BDD)* G *is ordered (OBDD) with respect to* $\prec$ *if, for every* $n \in \mathbb{N}$*, the following conditions hold:*

1. $low(n) \in N \implies var(n) \prec var(low(n))$
2. $high(n) \in N \implies var(n) \prec var(high(n))$

Definition 5. *The OBDD $G = (N, T, var, low, high, root, val)$ is a Reduced OBDD (ROBDD) if the following conditions are satisfied:*

1. $\forall t_1, t_2 \in T : val(t_1) \neq val(t_2)$
2. *There are no isomorphic subgraphs in G*
3. $\forall n_1, n_2 \in N : low(n_1) \neq low(n_2) \vee high(n_1) \neq high(n_2)$

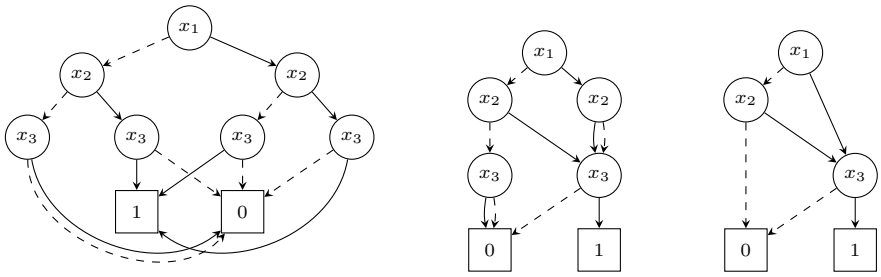


Fig. 2: From left to right, an OBDD satisfies the first, second, and third conditions as specified in the definition of ROBDD.

Theorem 1. *For every Boolean function ϕ over some set of variables Var and every variable ordering $\prec$ on Var, there is a unique (up to isomorphism) reduced OBDD (with respect to $\prec$) G_ϕ which represents ϕ. [12]"*

Based on Theorem 1, checking the equivalence of two functions, ϕ_1 and ϕ_2, represented by Reduced OBDDs (ROBDDs) G_1 and G_2 is equivalent to checking the isomorphism of G_1 and G_2.

Moreover, if several Boolean functions are represented with one shared ROBDD with multiple roots, as Mona does, the equivalence checking is reduced from isomorphism checking to simply checking the identity of the BDD roots.

2.3 WS1S

Richard Büchi showed that WS1S is equivalent to regular expressions and can therefore be represented by finite automata [3]. In this subsection, the simplification of the WS1S formula and its semantics will be presented, followed by the transformation of atomic formulae to automata. The main source for this subsection was [15].

Formula simplification

First-order terms are encoded as second-order terms since a first-order value can be seen as a singleton second-order value. Also, booleans can be encoded using the first position in the input automaton string.

All second-order terms are 'flattened' by introducing new variables that contain the values of all subterms. For example, the formula $A = (B \cup C) \cap D$ will be transformed into the form $\exists V : A = V \cap D \wedge V = B \cup C$, where V is a new variable.

Subformulae are simplified to contain fewer operators. As a result, only basic operations have to be implemented by the solver. The abstract syntax for simplified WS1S formulas can be defined by the following grammar:

$$\phi := \neg\phi' | \phi' \wedge \phi'' | \exists P_i : \phi' | P_i \subseteq P_j | P_i = P_j \setminus P_k | P_i = P_j + 1$$

Semantic

Given the main formula ϕ_0, we define its semantic inductively relative to a string w over the alphabet $\mathbb{B}^k$, where $\mathbb{B} = 0, 1$ and k is the number of variables in ϕ_0. Assume every variable of ϕ_0 is assigned a unique number in the range $1, 2, \ldots, k$, called the *variable index*. The string w now determines an interpretation $w(P_i)$ of P_i, defined as the finite

set $j, |,$ the jth bit in the P_i-track is 1. For example, the formula $\phi_0 \equiv \exists C : A = B \setminus C$ has variables A, B, and C, which are assigned the indices 1, 2, and 3, respectively. A typical string w over $\mathbb{B}^3$ looks like:

$$\begin{matrix} A \\ B \\ C \end{matrix} \quad \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

It's important to note that w with the suffix $(0^*)^T$ defines the same interpretation as w. Therefore, the minimum w is such a string that there is no such non-empty suffix. The semantics of a formula ϕ is defined inductively:

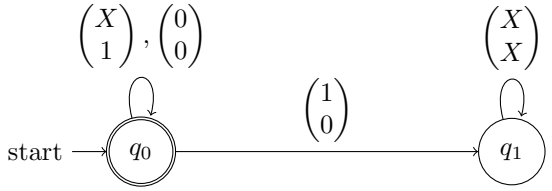
$$\begin{array}{lll} w \vDash \neg\phi' & \text{iff} & w \nvDash \phi' \\ w \vDash \phi' \wedge \phi'' & \text{iff} & w \vDash \phi' \wedge w \vDash \phi'' \\ w \vDash \exists P_i : \phi' & \text{iff} & \exists finite(M) \subseteq \mathbb{N} : w[P_i \mapsto M] \vDash \phi' \\ w \vDash P_i \subseteq P_j & \text{iff} & w(P_i) \subseteq w(P_j) \\ w \vDash P_i = P_j \setminus P_k & \text{iff} & w(P_i) = w(P_j) \setminus w(P_k) \\ w \vDash P_i = P_j + 1 & \text{iff} & w(P_i) = \{j + 1 \,|\, j \in w(P_j)\} \end{array}$$

where we use the notation $w[P_i \mapsto M]$ for the shortest string w' that interprets all variables P_j, $j \neq i$, as w does but interprets P_i as M. Note that if we assume that w is minimum, then w' decomposes into $w' = w \cdot w''$, where w'' is a string of letters of the form $(0^*X0^*)^T$, and the ith component is the only one that may be different from 0.

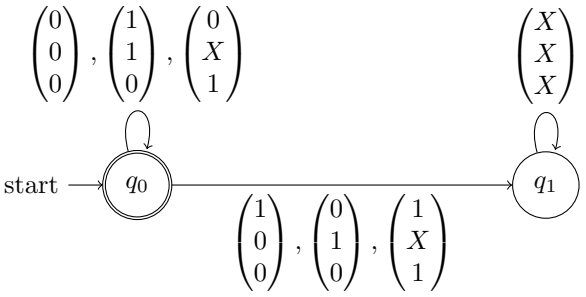
Automaton construction

The input formula ϕ is recursively transformed into the deterministic finite automaton that represents the set of satisfying strings $L(\phi) = w, |, w \vDash \phi$. The translation of atomic and composite formulae to deterministic finite automata follows:

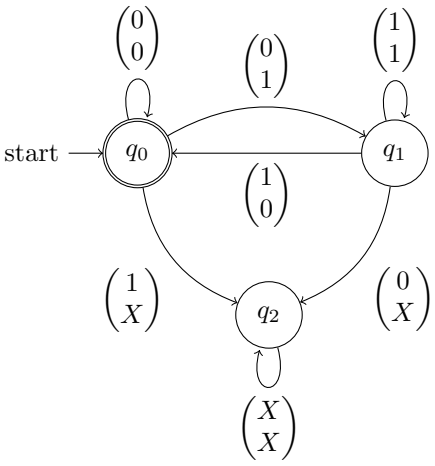
- $\phi = P_1 \subseteq P_2$:



- $\phi = P_1 = P_2 \setminus P_3$:



- $\phi = P_1 = P_2 + 1$:



- $\phi = \neg\phi'$: Negation of a formula corresponds to automaton complementation. If we have already calculated A' such that $L(\phi') = L(A')$, then $L(\neg\phi') = \complement L(\phi') = \complement L(A') = L(\complement A')$, where $\complement$ denotes both language complementation and automata complementation. If the automaton is complete and deterministic, then complementation can be done by swapping accepting and non-accepting states.
- $\phi = \phi' \wedge \phi''$: Conjunction corresponds to language intersection, $L(\phi' \wedge \phi'') = L(\phi') \cap L(\phi'')$. So, the resulting automaton A is obtained by the production of automata $A' \times A''$, where $L(\phi') = L(A')$ and $L(\phi'') = L(A'')$.
- $\phi = \exists P_i : \phi'$: Intuitively, the desired automaton A acts as the automaton A' for ϕ' except that it is allowed to guess the bits on the P_i-track. The resulting automaton A is nondeterministic. It is necessary to apply determinization and adjust the automaton A in such a way that each $w \in L(A)$ is minimal.

3 Automata representation

This section presents three different approaches on how to incorporate BDDs into finite automata. First, Mona's approach using shared BDDs is shown, followed by approaches that utilize jumping edges or state indexing.

3.1 Mona

Mona represents the transition function not only using a single BDD (as in the case of Kripke structures) but with a *shared multi-terminal* BDD (SMTBDD). The main difference from standard BDDs is that the leaves of SMTBDD do not contain boolean values 0 or 1 but rather states of the automaton.

Definition 6. *Let $M = (Q, \Sigma, \delta, q_0, F)$ be DFA. The SMTBDD is defined as a 7-tuple $G = (N, T, var, low, high, R, val)$ where:*

- *N is finite set on non-terminal (inner) nodes,*
- *T is a finite set of terminal nodes (leaves) such that $N \cap T = \emptyset$,*
- *$var : N \to N \cup T$ defines the low and high successors of the inner nodes,*
- *$R \subseteq N \cup T$ is nonempty set of rules, and*
- *$val : T \to Q$ assignes states to the leaves.*

For example, let the formula $\phi \equiv \exists p, q : p \neq q \wedge p \in X \cap Y \wedge q \in X \cap Y$ be represented by the automaton M in Figure 3, where each state r, s, and t contains information about whether it is accepting or not and points to its root node in the SMTBDD describing its transition relation. The data structure also contains a pointer to the initial state.

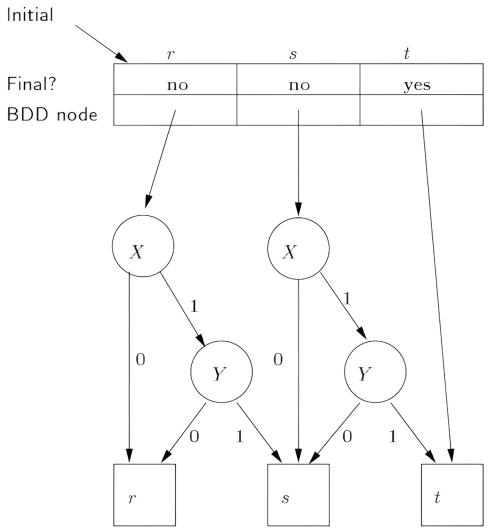


Fig. 3: Mona automaton for the formula $\phi \equiv \exists p, q : p \neq q \wedge p \in X \cap Y \wedge q \ \in X \cap Y$.

3.2 Automata with Skip Edges

The main idea of Bednář's skip edges [11] is to integrate BDD nodes directly into the transitions of the automaton. This can be easily noted, as BDD has an automata-like structure. To simulate the functionality of a BDD, where each node has an assigned variable, it is necessary to use skip edges.

Definition 7. *Let $M = (Q, \Sigma, \delta, Q_0, F)$ be an NFA, then automaton with skip edges $N = (Q, \Sigma, \delta', Q_0, F)$ has transition function defined as $\delta' : Q \times \Sigma \to 2^{\mathbb{N} \times Q}$.*

The transition function in the automaton with skip edges provides information about target states and the number of variables that have been jumped over. The skip edge with a length of 1 is a special case that has the same functionality as edges in NFA. $(n, r) \in \delta'(q, a)$ denotes that the automaton can move from state q to r after reading a symbol a and then jump over $n - 1$ variables.

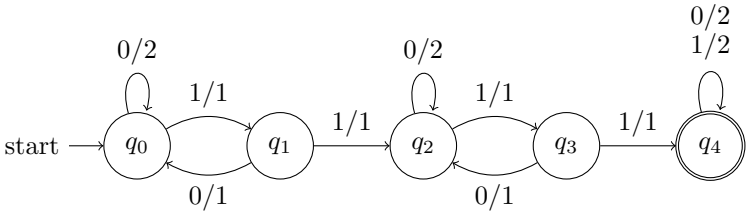


Fig. 4: An automaton with skip edges representing the language from Figure 3. A skip edge labeled with a/n can be interpreted as a transition of length n reading symbol a.

The potential benefit of skip edges is derived from the fact that the length of the jump edge is not limited. Therefore, the jump edge can traverse over many BDDs and automaton states. The demonstration of this benefit is shown in Figure 5. However, it has to be mentioned that this approach overcomplicated algorithms and did not show improvement in space or time.

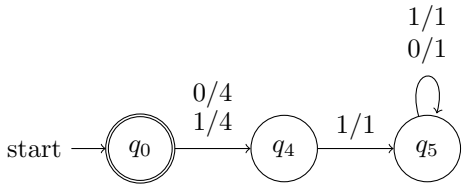


Fig. 5: Automaton with skip edges and a variable X representing formula $3 \in X$.

3.3 Automata with Indexed States

The approach of an automaton with indexed states has been the main focus of the reimplementation. This automaton integrates BDDs directly while maintaining the indexes on its nodes (automaton states).

Definition 8. *Let $M = (Q, \Sigma, \delta, Q_0, F)$ be an NFA. The automaton M is called an automaton with indexing if there exists an index function $\iota : Q \to \mathbb{N}_0$ such that the following conditions hold:*

1. $\forall q \in Q_0 : \iota(q) = 0$
2. $\forall q \in F : \iota(q) = 0$
3. $\forall q, r \in Q : \nexists a \in \Sigma : r \in \delta(q, a) \wedge \iota(r) \neq 0 \wedge \iota(q) \geq \iota(r)$

The first and second conditions reflect the fact that only roots or leaves in the BDD can be initial and final states, respectively. The third condition demands that the part of the automaton simulating the BDD must be acyclic, with the exception of the root nodes/states with index 0.

The index information determines the length of a jump based on the indices of the source and destination states in the automaton's transition. Due to the indexing sequence following a pattern of $0, 1, \ldots, n-1, 0, 1, \ldots, n-1, 0, \ldots$, the longest jump can only reach to the next state with an index of 0. Although it might seem like a step back from Bednář's method, the restriction on jump length actually simplifies all algorithms. Interestingly, this leads to a noticeably faster evaluation of the input formula, up to 10 times faster when compared to the version incorporating skip edges.

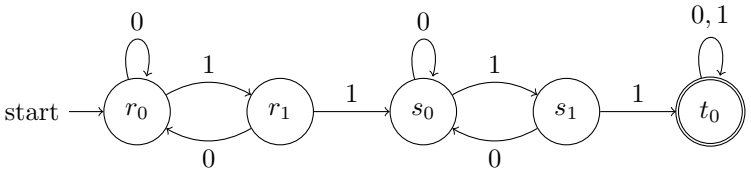


Fig. 6: Automaton with indexed states representing the language from Figure 3.

4 Automata operations

4.1 Complement

4.2 Union

4.3 Intersection

4.4 Revert

4.5 Determinization

4.6 Minimization

4.7 Projection

5 Experimental results

5.1 Operations performance

5.2 WS1S formulae

6 Conclusion

References

[1] Vojnar Tomáš: Lecture notes in Static Analysis and Verification: SAT and SMT Solving. BUT - Faculty of Information Technology (2023). https://www.fit.vutbr.cz/study/courses/SAV/public/Lectures/sav-lecture-10.pdf

[2] Klarlund, N.: A theory of restrictions for logics and automata. In: Computer Aided Verification, CAV '99. LNCS, vol. 1633

[3] Büchi, J.R.: Weak second-order arithmetic and finite automata. Mathematical Logic Quarterly **6**(1-6), 66–92 (1960) https://doi.org/10.1002/malq.19600060105

[4] Møller, A., Schwartzbach, M.I.: The pointer assertion logic engine. In: Proceedings of the ACM SIGPLAN 2001 Conference on Programming Language Design and Implementation. PLDI '01, pp. 221–231. Association for Computing Machinery, New York, NY, USA (2001). https://doi.org/10.1145/378795.378851

[5] Madhusudan, P., Parlato, G., Qiu, X.: Decidable logics combining heap structures and data. SIGPLAN Not. **46**(1), 611–622 (2011) https://doi.org/10.1145/1925844.1926455

[6] Tateishi, T., Pistoia, M., Tripp, O.: Path- and index-sensitive string analysis based on monadic second-order logic. ACM Trans. Softw. Eng. Methodol. **22**(4) (2013) https://doi.org/10.1145/2522920.2522926

[7] Baukus, K., Bensalem, S., Lakhnech, Y., Stahl, K., Equation, V.: Abstracting ws1s systems to verify parameterized networks. (2001). https://doi.org/10.1007/3-540-46419-0_14

[8] Klarlund, N., Nielsen, M., Sunesen, K.: A case study in verification based on trace abstractions. In: Broy, M., Merz, S., Spies, K. (eds.) Formal Systems Specification, pp. 341–373. Springer, Berlin, Heidelberg (1996)

[9] Sandholm, A., Schwartzbach, M.I.: Distributed safety controllers for web services. In: Astesiano, E. (ed.) Fundamental Approaches to Software Engineering, pp. 270–284. Springer, Berlin, Heidelberg (1998)

[10] Basin, D., Klarlund, N.: Automata based symbolic reasoning in hardware verification. Form. Methods Syst. Des. **13**(3), 255–288 (1998) https://doi.org/10.1023/A:1008644009416

[11] Pavel, B.: Rozhodování ws1s pomocí symbolických automatů [online]. Diplomová práce, Vysoké učení technické v BrněBrno (2023 [cit. 2024-01-20]). SUPERVISOR:. https://theses.cz/id/kq7t5j/

[12] Vojnar Tomáš: Lecture notes in Static Analysis and Verification: Binary Decision Diagrams. BUT - Faculty of Information Technology (2023). https://www.fit.vutbr.cz/study/courses/SAV/public/Lectures/sav-lecture-07.pdf

[13] Bollig, B., Wegener, I.: Improving the variable ordering of obdds is np-complete. IEEE Transactions on Computers **45**(9), 993–1002 (1996) https://doi.org/10.1109/12.537122

[14] Rice, M., Kulhari, S.: A Survey of Static Variable Ordering Heuristics for Efficient BDD/MDD Construction, Technical Report. http://www.cs.ucr.edu/~skulhari/StaticHeuristics.pdf (2008)

[15] Klarlund, N., Møller, A.: MONA Version 1.4 User Manual. BRICS, Department of Computer Science, Aarhus University, (2001). BRICS, Department of Computer Science, Aarhus University. Notes Series NS-01-1. Available from http://www.brics.dk/mona/. Revision of BRICS NS-98-3