UNIVERSITA' DEGLI STUDI DI MILANO

Dipartimento di Scienze dell'Informazione

RAPPORTO INTERNO N° 325-09

Goal Directed Invariant Synthesis in Model-Checking Modulo Theories

Silvio Ghilardi, Silvio Ranise

Goal Directed Invariant Synthesis in Model-Checking Modulo Theories

Silvio Ghilardi[1] and Silvio Ranise[2]
[1]Dipartimento di Scienze dell'Informazione, Università degli Studi di Milano (Italy)
[2]Dipartimento di Informatica, Università degli Studi di Verona (Italy)

April 20, 2008

Abstract

We are interested in automatically proving safety properties of infinite state systems. We present a technique for invariant synthesis which can be incorporated in backward reachability analysis. The main theoretical result ensures that (under suitable hypotheses) our method is guaranteed to find an invariant if one exists. We also discuss heuristics that allow us to derive an implementation of the technique showing remarkable speed-ups on a significant set of safety problems in parametrised systems.

Contents

1 Introduction

Backward reachability analysis has been widely adopted in model checking safety properties of infinite state systems (see, e.g., [1]). This verification procedure repeatedly computes pre-images of a set of unsafe states, usually obtained by complementing a safety property that a system should satisfy. Potentially infinite sets of states are represented by constraints so that pre-image computation can be done symbolically. A key advantage of backward reachability is to be *goal-directed*; the goal being the set of unsafe states from which pre-images are computed. Furthermore, safety properties for some classes of systems (e.g., broadcast protocols [9, 7]) can be decided by backward reachability.

Despite these advantages, backward reachability can unnecessarily explore (large) portions of the symbolic state space of a system which are actually not required to verify the safety property under consideration. Even worse, in some cases the analysis may not detect a fix-point, thereby causing non-termination. In order to avoid visiting irrelevant parts of the symbolic state space during backward reachability, techniques for analyzing pre-images and guessing invariants have been devised (see, e.g., [5, 15, 10, 4, 13] to name a few). The success of these techniques depend crucially on the heuristics used to guess the invariants. Our framework is similar in spirit to [5], but employs techniques which are specific for our different intended application domains.

Along this line of research, we present a technique for interleaving pre-image computation and invariant synthesis which tries to eagerly prune irrelevant parts of the search space. Formally, we work in the framework of the model checking (based on Satisfiability) Modulo Theories approach of [11, 12], where *array-based systems* have been introduced as an abstraction of several classes of infinite state systems (such as parametrized systems, lossy channels, and algorithms manipulating arrays). The **main result** (cf. Theorems 4.7 and 4.9) of the paper ensures that the technique *will find an invariant—provided one exists—under suitable hypotheses*, which are satisfied for important classes of array-based systems (e.g., mutual exclusion algorithms or cache coherence protocols). The key ingredient in the proof of the result is the model-theoretic notion of configuration and configuration ordering (introduced in [1] at an abstract level) which allows us to finitely characterize the search space of candidate invariants. Although the technique is developed for array-based systems, we believe that the underlying idea can be adapted to other symbolic approaches to model checking (e.g., [2, 3]).

Plan of the paper. We briefly introduce the notion of array-based system (Sec. 2). We revisit the backward reachability procedure *as a Tableaux-like calculus* (Sec. 3) so as to give a firm basis for implementation. We show how invariants can help backward reachability (Sec. 4), recall the duality between this and the synthesis of invariants (Sec. 4.1), and describe how to

interleave backward analysis and invariant synthesis (Sec. 4.2) together with some heuristics (Sec. 4.3). Finally (Sec. 5), we discuss how a prototype implementation of our techniques shows remarkable speed-ups. Full proofs and more examples can be found in the Appendix A below.

2 Formal Preliminaries

We assume the usual syntactic (e.g., signature, variable, term, atom, literal, and formula) and semantic (e.g., structure, sub-structure, truth, satisfiability, and validity) notions of first-order logic (see, e.g., [8]). The equality symbol $=$ is included in all signatures considered below. A signature is *relational* if it does not contain function symbols and it is *quasi-relational* if its function symbols are all constants. An *expression* is a term, an atom, a literal, or a formula. Let $\underline{x}$ be a finite tuple of variables and Σ a signature; a $\Sigma(\underline{x})$-expression is an expression built out of the symbols in Σ where at most the variables in $\underline{x}$ may occur free (we will write $E(\underline{x})$ to emphasize that E is a $\Sigma(\underline{x})$-expression). Let $\underline{e}$ be a finite sequence of expressions and σ a substitution; $\underline{e}\sigma$ is the result of applying the substitution σ to each element of the sequence $\underline{e}$.

According to the current practice in the SMT literature [16], a *theory* T is a pair $(\Sigma, \mathcal{C})$, where Σ is a signature and $\mathcal{C}$ is a class of Σ-structures; the structures in $\mathcal{C}$ are the *models* of T. Below, we let $T = (\Sigma, \mathcal{C})$. A Σ-formula ϕ is *T-satisfiable* if there exists a Σ-structure $\mathcal{M}$ in $\mathcal{C}$ such that ϕ is true in $\mathcal{M}$ under a suitable assignment to the free variables of ϕ (in symbols, $\mathcal{M} \models \phi$); it is *T-valid* (in symbols, $T \models \varphi$) if its negation is T-unsatisfiable. Two formulae φ_1 and φ_2 are *T-equivalent* if $\varphi_1 \leftrightarrow \varphi_2$ is *T-valid*. The *satisfiability modulo the theory T* ($SMT(T)$) *problem* amounts to establishing the T-satisfiability of quantifier-free Σ-formulae.

T admits *quantifier elimination* iff for every formula $\varphi(\underline{x})$ one can compute a quantifier-free formula $\varphi'(\underline{x})$ such that $T \models \forall \underline{x}(\varphi(\underline{x}) \leftrightarrow \varphi'(\underline{x}))$. A theory $T = (\Sigma, \mathcal{C})$ is said to be *locally finite* iff Σ is finite and, for every finite set of variables $\underline{x}$, there are finitely many $\Sigma(\underline{x})$-terms $t_1, \ldots, t_{k_{\underline{x}}}$ such that for every further $\Sigma(\underline{x})$-term u, we have that $T \models u = t_i$ (for some $i \in \{1, \ldots, k_{\underline{x}}\}$). The terms $t_1, \ldots, t_{k_{\underline{x}}}$ are called *$\Sigma(\underline{x})$-representative terms*; if they are effectively computable from $\underline{x}$ (and t_i is computable from u), then T is said to be *effectively locally finite* (in the following, when we say 'locally finite', we in fact always mean 'effectively locally finite'). If Σ is relational or quasi-relational, then any Σ-theory T is locally finite. An *enumerated data-type theory* T is a theory in a quasi-relational signature whose class of models contains only a single finite Σ-structure $\mathcal{M} = (M, \mathcal{I})$ such that for every $m \in M$ there exists a constant $c \in \Sigma$ such that $c^{\mathcal{I}} = m$.

A *T-partition* is a finite set $C_1(\underline{x}), \ldots, C_n(\underline{x})$ of quantifier-free formulae such that $T \models$

$\forall \underline{x} \bigvee_{i=1}^{n} C_i(\underline{x})$ and $T \models \bigwedge_{i \neq j} \forall \underline{x} \neg (C_i(\underline{x}) \wedge C_j(\underline{x}))$. A *case-definable extension* $T' = (\Sigma', \mathcal{C}')$ of a theory $T = (\Sigma, \mathcal{C})$ is obtained from T by applying (finitely many times) the following procedure: (i) take a T-partition $C_1(\underline{x}), \ldots, C_n(\underline{x})$ together with Σ-terms $t_1(\underline{x}), \ldots, t_n(\underline{x})$; (ii) let Σ' be $\Sigma \cup \{F\}$, where F is a "fresh" function symbol (i.e. $F \notin \Sigma$) whose arity is equal to the length of $\underline{x}$; (iii) take as $\mathcal{C}'$ the class of Σ'-structures $\mathcal{M}$ whose Σ-reduct is a model of T and such that $\mathcal{M} \models \bigwedge_{i=1}^{n} \forall \underline{x}\ (C_i(\underline{x}) \rightarrow F(\underline{x}) = t_i(\underline{x}))$. Thus a case-definable extension T' of a theory T contains finitely many additional function symbols, called *case-defined functions*. It is not hard to translate any $SMT(T')$ problem into an equivalent $SMT(T)$-problem, by repeatedly applying the following transformation: given the quantifier free formula ϕ to be tested for T'-satisfiability, replace it by $\bigvee_i (C_i \sigma \wedge \phi_i)$, where ϕ_i is a formula obtained from ϕ by replacing each term of the kind $F\sigma$ by $t_i\sigma$ (the C_i's are the partition formulae for the case definition of F and the t_i's are the related 'value' terms).

From now on, we use many-sorted first-order logic. All notions introduced above can be easily adapted to a many-sorted framework. **In the rest of the paper, we fix** (i) a theory $T_I = (\Sigma_I, \mathcal{C}_I)$ for indexes whose only sort symbol is `INDEX`; (ii) a theory $T_E = (\Sigma_E, \mathcal{C}_E)$ for data whose only sort symbol is `ELEM` (the class $\mathcal{C}_E$ of models of this theory is usually a singleton). The **theory** $A_I^E = (\Sigma, \mathcal{C})$ **of arrays with indexes** I **and elements** E is obtained as the combination of T_I and T_E as follows: `INDEX`, `ELEM`, and `ARRAY` are the only sort symbols of A_I^E, the signature is $\Sigma := \Sigma_I \cup \Sigma_E \cup \{\_[\_]\}$ where $\_[\_]$: $\texttt{ARRAY}, \texttt{INDEX} \longrightarrow \texttt{ELEM}$ (intuitively, $a[i]$ denotes the element stored in the array a at index i); a three-sorted structure $\mathcal{M} = (\texttt{INDEX}^{\mathcal{M}}, \texttt{ELEM}^{\mathcal{M}}, \texttt{ARRAY}^{\mathcal{M}}, \mathcal{I})$ is in $\mathcal{C}$ iff $\texttt{ARRAY}^{\mathcal{M}}$ is the set of (total) functions from $\texttt{INDEX}^{\mathcal{M}}$ to $\texttt{ELEM}^{\mathcal{M}}$, the function symbol $\_[\_]$ is interpreted as function application, and $\mathcal{M}_I = (\texttt{INDEX}^{\mathcal{M}}, \mathcal{I}_{|\Sigma_I})$, $\mathcal{M}_E = (\texttt{ELEM}^{\mathcal{M}}, \mathcal{I}_{|\Sigma_E})$ are models of T_I and T_E, respectively (where $\mathcal{I}_{|\Sigma_X}$ is the restriction of the interpretation $\mathcal{I}$ to the symbols in Σ_X for $X \in \{I, E\}$).

Notational conventions. For the sake of brevity, we introduce the following notational conventions: d, e range over variables of sort `ELEM`, a over variables of sort `ARRAY`, i, j, k, and z over variables of sort `INDEX`. An underlined variable name abbreviates a tuple of variables of unspecified (but finite) length and, if $\underline{i} := i_1, \ldots, i_n$, the notation $a[\underline{i}]$ abbreviates the tuple of terms $a[i_1], \ldots, a[i_n]$. Possibly sub/super-scripted expressions of the form $\phi(\underline{i}, \underline{e}), \psi(\underline{i}, \underline{e})$ denote *quantifier-free* $(\Sigma_I \cup \Sigma_E)$*-formulae in which at most the variables* $\underline{i} \cup \underline{e}$ *occur*. Also, $\phi(\underline{i}, \underline{t}/\underline{e})$ (or simply $\phi(\underline{i}, \underline{t})$) abbreviates the substitution of the Σ-terms $\underline{t}$ for the variables $\underline{e}$. Thus, for instance, $\phi(\underline{i}, a[\underline{i}])$ denotes the formula obtained by replacing $\underline{e}$ with $a[\underline{i}]$ in the quantifier-free formula $\phi(\underline{i}, \underline{e})$.

3 Backward Reachability and Tableaux

Following [12], we focus on a particular yet large class of array-based systems corresponding to guarded assignments. A *(guarded assignment) array-based (transition) system (for (T_I, T_E))* is a triple $\mathcal{S} = (a, I, \tau)$ where (i) a is the *state* variable of sort `ARRAY`;[1] (ii) $I(a)$ is the *initial* $\Sigma(a)$-formula; and (iii) $\tau(a, a')$ is the *transition* $(\Sigma \cup \Sigma_D)(a, a')$-formula, where a' is a renamed copy of a and Σ_D is a finite set of case-defined function symbols not in $\Sigma_I \cup \Sigma_E$. Below, we also **assume $I(a)$ to be a $\forall^I$-*formula***, i.e. a formula of the form $\forall \underline{i}.\phi(\underline{i}, a[\underline{i}])$, and $\tau(a, a')$ **to be in *functional form***, i.e. a *disjunction of* formulae of the form

$$\exists \underline{i}\, (\phi_L(\underline{i}, a[\underline{i}]) \wedge \forall j\, a'[j] = F_G(\underline{i}, a[\underline{i}], j, a[j])) \tag{1}$$

where ϕ_L is the *guard* (also called the local component in [11]), and F_G is a case-defined function (called the *global* component). To understand why formulae (1) are in functional form, consider λ-abstraction; then, the sub-formula $\forall j\, a'[j] = F_G(\underline{i}, a[\underline{i}], j, a[j]))$ can be re-written as $a' = \lambda j.F_G(\underline{i}, a[\underline{i}], j, a[j])$. (By abuse of notation, any case-definable extension of A_I^E will be denoted by A_I^E).

Given an array-based system $\mathcal{S} = (a, I, \tau)$ and a formula $U(a)$, (an instance of) the *safety problem* is to establish whether there exists a natural number n such that the formula

$$I(a_0) \wedge \tau(a_0, a_1) \wedge \cdots \wedge \tau(a_{n-1}, a_n) \wedge U(a_n) \tag{2}$$

is A_I^E-satisfiable. If there is no such n, then $\mathcal{S}$ is *safe* (w.r.t. U); otherwise, it is *unsafe* since the A_I^E-satisfiability of (2) implies the existence of a run (of length n) leading the system from a state in I to a state in U. From now on, we **assume $U(a)$ to be a $\exists^I$-*formula***, i.e. a formula of the form $\exists \underline{i}.\phi(\underline{i}, a[\underline{i}])$.

A general approach to solve instances of the safety problem is based on computing the set of backward reachable states. For $n \geq 0$, the *n-pre-image* of a formula $K(a)$ is $Pre^0(\tau, K) := K$ and $Pre^{n+1}(\tau, K) := Pre(\tau, Pre^n(\tau, K))$, where

$$Pre(\tau, K) \quad := \quad \exists a'.(\tau(a, a') \wedge K(a')). \tag{3}$$

Given $\mathcal{S} = (a, I, \tau)$ and $U(a)$, the formula $Pre^n(\tau, U)$ describes the set of backward reachable states in n steps (for $n \geq 0$). At the n-th iteration of the loop, the *basic backward reachability algorithm*, depicted in Figure 1 (a), stores in the variable B the formula $BR^n(\tau, U) := \bigvee_{i=0}^{n} Pre^i(\tau, U)$ representing the set of states which are backward reachable

[1] For simplicity (and without loss of generality), we limit ourselves to array-based systems having just one variable a of sort `ARRAY`. This limitation is however dropped in the examples, where in addition T_E may be many-sorted.

function BReach(U : $\exists^I$-formula)

1 $P \longleftarrow U$; $B \longleftarrow \bot$;
2 **while** ($P \wedge \neg B$ is A_I^E-sat.) **do**
3 **if** ($I \wedge P$ is A_I^E-sat.)
then return unsafe;
4 $B \longleftarrow P \vee B$;
5 $P \longleftarrow Pre(\tau, P)$;
6 **end**
7 **return** (safe, B);

(a)

function SInv(U : $\exists^I$-formula)

1 $P \longleftarrow$ ChooseCover(U); $B \longleftarrow \bot$;
2 **while** ($P \wedge \neg B$ is A_I^E-sat.) **do**
3 **if** ($I \wedge P$ is A_I^E-sat.)
then return failure;
4 $B \longleftarrow P \vee B$;
5 $P \longleftarrow$ ChooseCover($Pre(\tau, P)$);
6 **end**
7 **return** (success, $\neg B$);

(b)

Figure 1: The basic backward reachability (a) and the invariant synthesis (b) algorithms

from the states in U in at most n steps (whereas the variable P stores the formula $Pre^n(\tau, U)$). While computing $BR^n(\tau, U)$, BReach also checks whether the system is unsafe (cf. line 3, which can be read as $I \wedge Pre^n(\tau, U)$ is A_I^E-satisfiable) or a fix-point has been reached (cf. line 2, which can be read as $\neg(BR^n(\tau, U) \rightarrow BR^{n-1}(\tau, U))$ is A_I^E-unsatisfiable or, equivalently, that $(BR^n(\tau, U) \rightarrow BR^{n-1}(\tau, U))$ is A_I^E-valid). When BReach returns the safety of the system (cf. line 7), the variable B stores the formula describing the set of states which are backward reachable from U which is also a fix-point. Indeed, for BReach (Figure 1 (a)) to be a true (possibly non-terminating) procedure, it is mandatory that (i) $\exists^I$-formulae are closed under pre-image computation and (ii) both the A_I^E-satisfiability test for safety (line 3) and that for fix-point (line 2) are effective.

Concerning (i), it is sufficient to recall the following result from [12].

Proposition 3.1. *Let* $K(a) := \exists \underline{k}\, \phi(\underline{k}, a[\underline{k}])$ *and* $\tau(a, a') := \bigvee_{h=1}^{m} \exists \underline{i}\ (\phi_L^h(\underline{i}, a[\underline{i}]) \wedge a' = \lambda j.F_G^h(\underline{i}, a[\underline{i}], j, a[j]))$. *Then,* $Pre(\tau, K)$ *is* A_I^E*-equivalent to an (effectively computable)* $\exists^I$*-formula.*

The proof of Proposition 3.1 (see [12]) consists of applying simple logical manipulations to show that $Pre(\tau_h, K)$ is A_I^E-equivalent to the following $\exists^I$-formula, where τ_h is one of the m disjuncts of τ (cf. Proposition 3.1 above):

$$\exists \underline{i}\, \exists \underline{k}.(\phi_L^h(\underline{i}, a[\underline{i}]) \wedge \phi(\underline{k}, F_G^h(\underline{i}, a[\underline{i}], \underline{k}, a[\underline{k}]))) \tag{4}$$

where $\phi(\underline{k}, F_G^h(\underline{i}, a[\underline{i}], \underline{k}, a[\underline{k}]))$ is the formula obtained from $\phi(\underline{k}, a'[\underline{k}])$ by replacing $a'[k_m]$ with $F_G^h(\underline{i}, a[\underline{i}], k_m, a[k_m])$ for $m = 1, ..., l$ and $\underline{k}$ is the tuple $k_1, \ldots, k_l$ (the F_G^h can then be eliminated as shown in Section 2). Notice that the existentially quantified prefix $\exists\ \underline{k}$ is augmented with

$\exists\ \underline{i}$ in (4) with respect to K. Concerning (ii), observe that the formulae involved in the satisfiability checks are $I \wedge BR^n(\tau, K)$ and $BR^{n+1}(\tau, K) \wedge \neg BR^n(\tau, K)$. Since we have closure under pre-image computation, both formulae are of the form $\exists \underline{a}\ \exists \underline{i}\ \forall \underline{j}\ \psi(\underline{i}, \underline{j}, \underline{a}[\underline{i}], \underline{a}[\underline{j}])$ and are called $\exists^{A,I}\forall^I$*-sentences* [11].

Theorem 3.2 ([11])**.** *The A_I^E-satisfiability of $\exists^{A,I}\forall^I$-sentences is decidable if (i) T_I is locally finite and is closed under substructures; (ii) the $SMT(T_I)$ and $SMT(T_E)$ problems are decidable.*

Hypothesis (i) concerns the *topology* of the system (not the data manipulated by the components of the system) and it is satisfied in many practical cases, e.g., when the models of T_I are all finite sets, linear orders, graphs, forests, etc. For example, the topology of virtually any cache coherence protocol can be formalized by finite sets while that of mutual exclusion protocols by linear orders. Under assumption (i), it is possible to show (see [11]) that an $\exists^{A,I}\forall^I$-sentence is A_I^E-satisfiable iff it is satisfiable in a finite index model of A_I^E (a *finite index model* is a model $\mathcal{M}$ in which the set $\texttt{INDEX}^{\mathcal{M}}$ has finite cardinality). This suggests the following quantifier instantiation algorithm, which is indeed complete [11]. Let $\exists \underline{a}\ \exists \underline{i}\ \forall \underline{j}\ \psi(\underline{i}, \underline{j}, \underline{a}[\underline{i}], \underline{a}[\underline{j}])$ be an $\exists^{A,I}\forall^I$-sentence: first, consider the $\underline{i}$'s as Skolem constants and replace the $\underline{j}$'s with the representative $\underline{i}$-terms (by using the local finiteness of T_I); then, invoke the available SMT solver for checking the A_I^E-satisfiability of the resulting quantifier-free formula. The decidability of the $SMT(A_I^E)$ problem can be shown by using *generic combination techniques* from the decidability of those for $SMT(T_I)$ and $SMT(T_E)$ (see [11] for details).

We summarize our working hypotheses.

Assumption 3.3. We fix an array-based system $\mathcal{S} = (a, I, \tau)$ such that the initial formula I is a $\forall^I$-formula, $\tau(a, a') := \bigvee_{h=1}^{m} \tau_h(a, a')$ where τ_h is a formula in functional form for $h = 1, ..., m$. We also assume that hypotheses (i)-(ii) of Theorem 3.2 are satisfied.

3.1 Tableaux-like Implementation of Backward Reachability

A naive implementation of the algorithm in Figure 1 (a) does not scale up. The main problem is the size of the formula $BR^n(\tau, U)$ which contains many redundant or unsatisfiable subformulae. We now discuss how Tableaux-like techniques can be used to circumvent these difficulties. We need one more definition: an $\exists^I$-formula $\exists i_1 \cdots \exists i_n \phi$ is said to be *primitive* iff ϕ is a conjunction of literals and is said to be *differentiated* iff ϕ contains as a conjunct the negative literal $i_k \neq i_l$ for all $1 \leq k < l \leq n$. By applying various distributive laws together with the rewriting rules

$$\exists j(i = j \wedge \theta) \rightsquigarrow \theta(i/j) \quad \text{and} \quad \theta \rightsquigarrow (\theta \wedge i = j) \vee (\theta \wedge i \neq j) \tag{5}$$

it is possible to transform every $\exists^I$-formula into a disjunction of primitive differentiated ones.

We initialize our tableau with the $\exists^I$-formula $U(a)$ representing the set of unsafe states. The key observation is to revisit the computation of the pre-image as the following inference rule (we use square brackets to indicate the applicability condition of the rule):

$$\frac{K \quad [K \text{ is primitive differentiated}]}{Pre(\tau_1, K) \mid \cdots \mid Pre(\tau_m, K)} \ \mathsf{PreImg}$$

where $Pre(\tau_h, K)$ computes the $\exists^I$-formula which is logically equivalent to the pre-image of K w.r.t. τ_h (this is possible according to Proposition 3.1).

Since the $\exists^I$-formulae labeling the consequents of the rule PreImg may not be primitive and differentiated, we need the following Beta rule

$$\frac{K}{K_1 \mid \cdots \mid K_n} \ \mathsf{Beta}$$

where K is first transformed by eliminating the case-defined functions as explained in Section 2, and then by applying rewriting rules like (5) together with standard distributive laws, in order to get $K_1, \ldots, K_n$ which are primitive, differentiated and whose disjunction is A_I^E-equivalent to K.

By repeatedly applying the above rules, it is possible to build a tree whose nodes are labelled by $\exists^I$-formulae describing the set of backward reachable states. Indeed, it is not difficult to see that the disjunction of the $\exists^I$-formulae labelling all the nodes in the (potentially infinite) tree is A_I^E-equivalent to the (infinite) disjunction of the formulae $BR^n(\tau, U)$, where $\tau := \bigvee_{h=1}^m \tau_h$. Indeed, there is no need to fully expand our tree. For example, it is useless to apply the rule PreImg to a node ν labelled by an $\exists^I$-formula which is A_I^E-unsatisfiable as all the formulae labelling nodes in the sub-tree rooted at ν will also be A_I^E-unsatisfiable. This observation can be formalized by the following rule closing a branch in the tree (we mark the terminal node of a closed branch by $\times$):

$$\frac{K \quad [K \text{ is } A_I^E\text{-unsatisfiable}]}{\times} \ \mathsf{NotAppl}$$

This rule is effective since $\exists^I$-formulae are a subset of $\exists^{A,I}\forall^I$-sentences and the A_I^E-satisfiability of these formulae is decidable by Theorem 3.2.

According to procedure BReach, there are two more situations in which we can stop expanding a branch in the tree. One terminates the branch because of the safety test (cf. line 3 of Figure 1 (a)):

$$\frac{K \quad [I \wedge K \text{ is } A_I^E\text{-satisfiable}]}{\mathsf{UnSafe}} \ \mathsf{Safety}$$

Interestingly, if we label with τ_h the edge connecting a node labeled with K with that labeled with $Pre(\tau_h, K)$ when applying rule PreImg, then the transitions $\tau_{h_1}, ..., \tau_{h_e}$ labelling the edges in the branch terminated by UnSafe (from the leaf node to the root node) give a *bad trace*, i.e. a sequence of transitions leading the array-based system from a state satisfying I to one satisfying U. Again, rule UnSafe is effective since $I \wedge K$ is equivalent to an $\exists^{A,I}\forall^I$-sentence and its A_I^E-satisfiability is decidable by Theorem 3.2. The other situation in which one can close a branch corresponds to the fix-point test (cf. line 2 of Figure 1 (a))

$$\frac{K \quad [K \wedge \bigwedge\{\neg K' | K' \preceq K\} \text{ is } A_I^E\text{-unsatisfiable}]}{\times}\ \mathsf{FixPoint}$$

where $K' \preceq K$ means that K' is a primitive differentiated $\exists^I$-formula labeling a node preceding the node labeling K (nodes can be ordered according to the strategy for expanding the tree). Once more, this rule is effective since $K \wedge \bigwedge\{\neg K' | K' \preceq K\}$ can be straightforwardly transformed into an $\exists^{A,I}\forall^I$-sentence whose A_I^E-satisfiability is decidable by Theorem 3.2.

From the implementation viewpoint, further heuristics are needed, in order to reduce the instances needed for the satisfiability test of Theorem 3.2 and to trivialize the recognition of the unsatisfiable premise of the rule NotAppl.

4 Invariants and Backward Reachability

Termination of our tableaux calculus (and of the algorithm of Figure 1 (a)) is not guaranteed in general, but follows under certain restrictions covering important applications (see below). In the general case, nothing can be said because safety problems are undecidable.

Theorem 4.1. *The problem: "given an $\exists^I$-formula U, decide whether the array-based system $\mathcal{S}$ is safe w.r.t. U" is undecidable (even if T_E is locally finite).*

It is well-known that invariants are useful for pruning the search space of backward reachability procedures and may help either to obtain or to speed up termination.

Definition 4.2 (Safety invariants)**.** The $\forall^I$-formula $J(a)$ is a *safety invariant* for the safety problem consisting of the array-based system $\mathcal{S} = (a, I, \tau)$ and unsafe $\exists^I$-formula $U(a)$ iff the following conditions hold:

(i) $A_I^E \models \forall a(I(a) \rightarrow J(a))$,

(ii) $A_I^E \models \forall a \forall a'(J(a) \wedge \tau(a, a') \rightarrow J(a'))$, and

(iii) $\exists a.(U(a) \wedge J(a))$ is A_I^E-unsatisfiable.

If we are not given the $\exists^I$-formula $U(a)$ and conditions (i)–(ii) hold, then $J(a)$ is an *invariant for* $\mathcal{S}$.

Checking whether conditions (i), (ii), and (iii) above hold can be reduced, by trivial logical manipulations, to the A_I^E-satisfiability of $\exists^{A,I}\forall^I$-formulae, which is decidable by Theorem 3.2. So, establishing whether a given $\forall^I$-formula $J(a)$ is a safety invariant can be completely automated.

Property 1. *Let U be an $\exists^I$-formula. If there exists a safety invariant for U, then the array-based system $\mathcal{S} = (a, I, \tau)$ is safe with respect to U.*

So, if we are given a suitable safety invariant, Property 1 can be used as the basis of the safety invariant method, which turns out to be more powerful than the basic Backward Reachability algorithm of Figure 1 (a):

Property 2. *Let the procedure* BReach *in Figure 1(a) terminate on the safety problem consisting of the array-based system $\mathcal{S} = (a, I, \tau)$ and unsafe formula $U(a)$. If* BReach *returns* (safe, B)*, then $\neg B$ is a safety invariant for U.*

The converse of Proposition 2 do not hold: there might be a safety invariant even when BReach diverges, as illustrated by the following example.

Example 4.3. Let us consider a simple algorithm for inserting an element $b[0]$ into a sorted array $b[1], \ldots, b[n]$. Let Σ_I consist of one binary relation symbol S and one constant symbol 0 and T_I be the theory whose class of models consists of the substructures of the structure having the naturals as domain, with 0 interpreted in the obvious way, and S interpreted as the graph of the successor function.[2] To simplify the matter, we shall use a two-sorted theory and two array variables. T_E is the two-sorted theory whose class of models consists of the single two-sorted structure given by the Booleans (with the constants $\top, \bot$ interpreted in the obvious way) and the rationals (with the standard ordering $<$). The array variable a is a Boolean flag, whereas the array variable b is the sorted numerical array where $b[0]$ is to be inserted. The initial $\forall^I$-formula is

$$\forall i\,(a[i] = \bot \leftrightarrow i \neq 0) \wedge \forall i_1, i_2\,(S(i_1, i_2) \rightarrow i_1 = 0 \vee b[i_1] \leq b[i_2])$$

[2] We need to take closure under substructures for our Assumption 3.3 to be verified. In these substructures there can be indexes that cannot be reached from 0 by iterated applications of the successor operation, however it is easy to see that nothing can happens during a run in the part of the model containing these indexes (according to the initial and transition formulae below the 'disconnected' cells of the array contain data which are ordered from the very beginning and remain constant).

saying that the elements in the array b, whose corresponding Boolean flag, is set to false are arranged in increasing order (namely, all except that at position 0). The transition has the following guard and global component:

$$\begin{aligned}
&\phi_L(i_1, i_2, a[i_1], a[i_2]) := S(i_1, i_2) \wedge a[i_1] = \top \wedge a[i_2] = \bot \wedge b[i_1] > b[i_2] \\
&F_G(i_1, i_2, a[i_1], a[i_2], b[i_1], b[i_2], j) := \texttt{case of } \{ \quad j = i_1 \ : \ \langle \top, b[i_2] \rangle, \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad j = i_2 \ : \ \langle \top, b[i_1] \rangle, \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad j \neq i_1 \wedge j \neq i_2 \ : \ \langle a[j], b[j] \rangle \ \ \}, \\
\end{aligned}$$

which swaps two elements in the array b if their order is decreasing and sets the Boolean fields appropriately. The obvious correctness property is that there are no two values in decreasing order in the array b whose corresponding Boolean flags do not allow the transition to fire:

$$\exists i_1, i_2 \, (S(i_1, i_2) \wedge \neg(a[i_1] = \top \wedge a[i_2] = \bot) \wedge b[i_1] > b[i_2]). \tag{6}$$

Unfortunately, BReach in Figure 1 (a) applied to (6) diverges. However, it is not difficult to see that a safety invariant for (6) exists and is given by the following formula:

$$\forall i, j.(S(i, j) \rightarrow \neg(a[i] = \bot \wedge a[j] = \top)) \tag{7}$$

saying that two adjacent indexes cannot have their Boolean flags set to $\bot$ and $\top$, respectively.

4.1 Synthesis of Invariants as the Dual of Backward Reachability

The main difficulty to exploit Property 1 is to find suitable $\forall^I$-formulae satisfying conditions (i)—(iii) of Definition 4.2. Unfortunately, the set of $\forall^I$-formulae which are candidates to become safety invariants is infinite. Such a search space can be dramatically restricted when T_E is locally finite, although it is still infinite because there is no bound on the length of the universally quantified prefix. To formalize this, we need to summarize some notions about pre-orders and configurations.

A *pre-order* $(P, \leq)$ is a set endowed with a reflexive and transitive relation; an *upset* of such a pre-order is a subset $U \subseteq P$ such that ($p \in U$ and $p \leq q$ imply $q \in U$). An upset U is *finitely generated* iff it is a finite union of cones, where a *cone* is an upset of the form $\uparrow p = \{q \in P \mid p \leq q\}$ for some $p \in P$. Two elements $p, q \in P$ are *incomparable* (*equivalent*) if neither (both) $p \leq q$ nor (and) $q \leq p$. A pre-order $(P, \leq)$ is a *well-quasi-ordering* (wqo) iff every upset of P is finitely generated (this is equivalent to the standard definition, see [11] for a proof).

An A_I^E*-configuration* (or, briefly, a configuration) is a pair $(s, \mathcal{M})$ such that s is an array of a finite index model $\mathcal{M}$ of A_I^E ($\mathcal{M}$ is omitted whenever it is clear from the context). We associate a Σ_I-structure s_I and a Σ_E-structure s_E with an A_I^E-configuration $(s, \mathcal{M})$ as

follows: the Σ_I-structure s_I is simply the finite structure $\mathcal{M}_I$, whereas s_E is the smallest Σ_E-substructure of $\mathcal{M}_E$ containing the image of s (in other words, if $\texttt{INDEX}^{\mathcal{M}} = \{c_1, \ldots, c_k\}$, then s_E is the smallest Σ_E-substructure containing $\{s(c_1), \ldots, s(c_k)\}$). Let s, s' be configurations: we say that $s' \leq s$ holds iff there are a Σ_I-embedding $\mu : s'_I \longrightarrow s_I$ and a Σ_E-embedding $\nu : s'_E \longrightarrow s_E$ such that the set-theoretical compositions of μ with s and of s' with ν are equal. In [11], termination of BReach is proved under the hypotheses that T_E is locally finite and the configuration order is a wqo. This implies the decidability of the safety problem for, among others, broadcast protocols and lossy channel systems and can be seen as the declarative counterpart of general results formulated within an algebraic framework (see, e.g., [1]). In the following, we show that using the notions of configuration and configuration order, it is possible to design a method for invariant synthesis.

Finitely generated upsets of configurations and $\exists^I$-formulae can be used interchangeably under a suitable assumption. Let $K(a)$ be an $\exists^I$-formula; we let $[\![K]\!] := \{(s, \mathcal{M}) \mid \mathcal{M} \models K(s)\}$.

Proposition 4.4 (Extended version of [11])**.** *Let T_E be locally finite. Finitely generated upsets of A_I^E-configurations coincide with sets of A_I^E-configurations of the kind $[\![K]\!]$, for some $\exists^I$-formula K. In particular, for each A_I^E-configuration s, there exists an $\exists^I$-formula K_s such that $[\![K_s]\!] = \uparrow s$.*

The notion of a basis for a configuration upset will be useful in the following.

Definition 4.5. A *basis* for a finitely generated upset S (resp., for an $\exists^I$-formula K) is a minimal finite set $\{s_1, \ldots, s_n\}$ such that S (resp., $[\![K]\!]$) is equal to $\uparrow s_1 \cup \cdots \cup \uparrow s_n$.[3]

It is easy to see that two bases for the same upset are essentially the same, in the sense that they are formed by pairwise equivalent configurations. Our goal is to integrate the safety invariant method into the basic Backward Reachability algorithm of Figure 1(a). To this end, we introduce the notion of 'sub-reachability'.

Definition 4.6 (Subreachable configurations)**.** Suppose T_E is locally finite and let s be a configuration. A *predecessor* of s is any s' that belongs to a basis for $Pre(\tau, K_s)$. Let s, s' be configurations: s is *sub-reachable* from s' iff there exist configurations $s_0, \ldots, s_n$ such that (i) $s_0 = s$, (ii) $s_n = s'$, and (iii) either $s_{i-1} \leq s_i$ or s_{i-1} is a predecessor of s_i, for each $i = 1, \ldots, n$. If K is an $\exists^I$-formula, s *is sub-reachable from* K iff s is sub-reachable from some s' taken from a basis of K.

The following theorem is our main technical result.

[3]The minimality requirement can be equivalently formulated by saying that $s_1, \ldots, s_n$ are pairwise incomparable.

Theorem 4.7. *Let T_E be locally finite. If there exists a safety invariant for U, then there are finitely many A_I^E-configurations $s_1, \ldots, s_k$ which are sub-reachable from U and such that $\neg(K_{s_1} \vee \cdots \vee K_{s_k})$ is also a safety invariant for U.*

The intuition underlying the theorem is as follows. Let us call 'finitely representable' an upset which is of the kind $[\![K]\!]$ for some $\exists^I$-formula K and let B be the set of backward reachable states. Usually B is infinite and it is finitely representable only in special cases (e.g., when the configuration ordering is a wqo like in the case of broad-cast protocols). Despite this, it may sometimes exist a set $B' \supseteq B$ which is finitely representable and whose complement is an invariant of the system. Theorem 4.7 ensures us to find such a B', if any. This is the case of Example 4.3 where not all configurations satisfying the negation of (7) are in B.

In practice, Theorem 4.7 suggests the following procedure to find the super-set B'. At each iteration of BReach, the algorithm represents symbolically in the variable B the configurations which are backward reachable in n steps; before computing the next pre-image of B, non deterministically replace some of the configurations in a basis of B with some sub-configurations and update B by a symbolic representation of the obtained upset. In this way, if an invariant exists, we are guaranteed to find it; otherwise, the process may diverge. This is so because the search space of the configurations which are sub-reachable in n steps is finite, although this number is infinite if no bound on n is fixed. To illustrate, the negation of (7) in Example 4.3 identifies sub-reachable only configurations. This shows that sub-reachability is crucial for Theorem 4.7 to hold.

The algorithm sketched above can be furtherly refined so as to obtain a completely symbolic method working with formulae without resorting to configurations. The key idea towards this result is to identify an $\exists^I$-formula which is the symbolic counterpart of the (sub-reachable) configurations $s_1, \ldots, s_k$ of the theorem above which can be directly computed from the available safety invariant for U. Formally, we introduce the following definition:

$$Min(\phi, a, \underline{i}) \quad := \quad \phi(\underline{i}, a[\underline{i}]) \wedge \bigwedge_{\sigma} (\phi(\underline{i}\sigma, a[\underline{i}\sigma]) \rightarrow \bigwedge_{i \in \underline{i}} \bigvee_{t} (t\sigma = i))$$

where $\phi(\underline{i}, a[\underline{i}])$ is a quantifier-free formula, t ranges over representative $\Sigma_I(\underline{i})$-terms, and σ ranges over the substitutions with domain $\underline{i}$ and co-domain included in the set of representative $\Sigma_I(\underline{i})$-terms. The formula $\exists \underline{i}.Min(\phi, a, \underline{i})$ is A_I^E-equisatisfiable to the $\exists^I$-formula $\exists \underline{i}.\phi(\underline{i}, a[\underline{i}])$; moreover if (as it often happens in applications) the signature Σ_I is relational and the formula $\phi(\underline{i}, a[\underline{i}])$ is differentiated, $Min(\phi, a, \underline{i})$ is A_I^E-equivalent to $\phi(\underline{i}, a[\underline{i}])$.

Proposition 4.8. *Let T_E be locally finite, $K := \exists \underline{i}.\phi(\underline{i}, a[\underline{i}])$ be an $\exists^I$-formula, and L be a further $\exists^I$-formula. The following two conditions are equivalent:*

(i) *for every s in a basis for K, there exists a configuration s' in a basis for L such that $s \leq s'$;*

(ii) *L is (up to A_I^E-equivalence) of the form $\exists \underline{i}, \underline{j}.\psi(\underline{i}, \underline{j}, a[\underline{i}], a[\underline{j}])$ for a quantifier-free formula ψ and*

$$\text{if } A_I^E \models Min(\psi, a, \underline{i}\,\underline{j}) \rightarrow \theta(\underline{t}, a[\underline{t}]) \quad \text{then} \quad A_I^E \models Min(\phi, a, \underline{i}) \rightarrow \theta(\underline{t}, a[\underline{t}]),$$

for all quantifier free $(\Sigma_E \cup \Sigma_I)$-formula θ and for all tuple of terms $\underline{t}(\underline{i})$ taken from the set of the representative $\Sigma_I(\underline{i})$-terms.

In the following, we will write $K \leq L$ whenever one of the (equivalent) conditions in Proposition 4.8 holds. Under the assumption that T_E is locally finite, it is possible to compute all the finitely many (up to A_I^E-equivalence) $\exists^I$-formulae K such that $K \leq L$.[4] Furthermore, we say that K *covers* L iff both $K \leq L$ and $A_I^E \models L \rightarrow K$. Let $\mathsf{ChooseCover}(L)$ be a procedure that returns (according to some criteria) one of the $\exists^I$-formulae K such that K covers L. We are now ready to give the procedure SInv in Figure 1 (b) for the computation of safety invariants and prove its correctness.

Theorem 4.9. *Let T_E be locally finite. Then, there exists a safety invariant for U iff the procedure* SInv *in Figure 1 (b) returns a safety invariant for U, for a suitable* ChooseCover *function.*

When $\mathsf{ChooseCover}(L) = L$, i.e. ChooseCover is the identity (indeed, L covers L), the procedure SInv is the (exact) dual of BReach in Figure 1 (a) and, hence it can only return (the negation of) a symbolic representation of all backward reachable states as a safety invariant.

4.2 Integrating Invariant Synthesis within Backward Reachability

The main drawback of procedure SInv is the difficulty of defining an appropriate function ChooseCover. Although finite, the number of formulae covering a certain $\exists^I$-formula is so large that makes any implementation of SInv impractical. Instead, we prefer to study how to integrate the synthesis of invariants in the backward reachability algorithm in Figure 1 (a). The idea is to use invariants for the unsafe configuration U so as to prune the search space of the backward reachability algorithm. In our symbolic framework, at the n-th iteration of the loop of the procedure BReach, the set of backward reachable states is represented by the formula stored in the variable B (which is equivalent to $BR^n(\tau, U)$). So, 'pruning the search space of the backward reachability algorithm' amounts to disjoining the negation of the available invariants to B. In this way, the extra information encoded in the invariants

[4] This fact will be formally proved in the Appendix A as Proposition A.8.

makes the satisfiability test at line 2 (for fix-point checking) more likely to be successful and possibly decreasing the number of iterations of the loop.

Indeed, the problem is to synthesize such invariants. A way to do this is to consider the set B of reachable states, to extract an $\exists^I$-formula representing a set of sub-reachable configurations, and then checking whether this is an invariant. We assume the existence of a function ChooseSub that takes an $\exists^I$-formula P and returns a (possibly empty) finite set S of $\exists^I$-formulae such that $K \leq P$ if $K \in S$. The formulae in S represent sub-reachable configurations that may contribute to an invariant in the sense of Theorem 4.7.

To summarize, it is possible to integrate the synthesis of invariants within the backward reachability algorithm by inserting between lines 4 and 5 in Figure 1 (a) the following instructions:

$4'$ **foreach** $CINV \in \mathsf{ChooseSub}(P)$ **do**
if $\mathsf{BReach}(CINV) = (\mathsf{safe}, B_{CINV})$ **then** $B \longleftarrow B \vee \neg B_{CINV}$;

where *CINV* stands for 'candidate invariant.' The resulting procedure will be indicated with BReach+Inv (notice that BReach is used here as a sub-procedure).

Proposition 4.10. *Let T_E be locally finite. If the procedure* BReach+Inv *terminates and returns safe (unsafe), then $\mathcal{S}$ is safe (unsafe) with respect to U.*

The procedure BReach+Inv is incomplete (in the sense that it is not guaranteed to terminate even in case a safety invariant exists), deterministic (no backtracking is required), and highly parallelizable (it is possible to run in parallel as many instances of BReach as formulae in the set returned by ChooseSub), and it performs well, as witnessed by the experimental evidence supplied in the next Section. In this way, invariant synthesis has become a powerful *heuristics* within a sophisticated version of the basic backward reachability algorithm. Furthermore, its integration in the Tableaux calculus of Sec. 3.1 is particularly easy: just use the calculus itself with some bounds on the resources, such as a limit on the depth of the tree to check if a candidate invariant is a true invariant.

4.3 Heuristics

There is a delicate trade-off between the number of candidate invariants produced by the function ChooseSub and their effects in pruning the search space of the basic backward reachability algorithm. More candidate invariants implies a higher probability of finding an invariant and, ultimately, to prune the search space. However, looking at line $4'$, it is evident that more candidate invariants implies many more calls to the basic backward reachability algorithms

to establish if they are invariant or not. Indeed, on "simpler" candidate invariants, the procedure BReach is likely to perform well, i.e. to terminate in few iterations. The following two remarks are helpful in finding the right trade-off.

First, it is possible to limit the resources of the basic backward reachability algorithm BReach when invoking it at line 4′; e.g., it is possible to bound the number of iterations of the loop or its run time. This allows us to avoid slowing down too much each iteration of the main loop in BReach+Inv.

The second remark concerns the implementation of the function ChooseSub when the theories T_I and T_E satisfy some additional requirements, which are often satisfied when modelling classes of parametrised systems such as mutual exclusion algorithms or cache coherence protocols. The goal of this discussion is to design a function ChooseSub returning few "simple" candidate invariants which are likely to become true invariants.

Claim.[5] Let Σ_I be relational and let T_E be locally finite and admit elimination of quantifiers. (When T_I is the theory of all finite sets—this is appropriate for cache coherence protocols—or the theory of linear orders—this is appropriate for mutual exclusion algorithms—and T_E is the theory of an enumerated datatype, these assumptions are satisfied.) Let

$$L := \exists \underline{i}\, \underline{j}.(\psi_E(a[\underline{i}], a[\underline{j}]) \wedge \psi_I(\underline{i}, \underline{j}) \wedge \delta_I(\underline{i})) \tag{8}$$

be a primitive differentiated A_I^E-satisfiable $\exists^I$-formula such that (i) $\underline{i} \cap \underline{j} = \emptyset$, (ii) $\psi_E(\underline{e}, \underline{d})$ is a conjunction of Σ_E-literals; (iii) $\psi_I(\underline{i}, \underline{j})$ is a conjunction of Σ_I-literals; (iv) $\delta_I(\underline{i})$ is a maximal conjunction of $\Sigma_I(\underline{i})$-literals (i.e. for every $\Sigma(\underline{i})$-atom $A(\underline{i})$, δ_I contains either $A(\underline{i})$ or its negation). If

$$K \;:=\; \exists \underline{i}\, (\delta_I(\underline{i}) \wedge \phi_E(a[\underline{i}])), \tag{9}$$

where $\phi_E(\underline{e})$ is T_E-equivalent to $\exists \underline{d}\, \psi_E(\underline{e}, \underline{d})$ (which is guaranteed to exist as T_E admits elimination of quantifiers), then K covers L and in particular $K \leq L$.

When ChooseSub is applied to a disjunction of primitive differentiated $\exists^I$-formulae, we need to transform each disjunct $P := \exists \underline{k}.\theta(\underline{k}, a[\underline{k}])$ to the form of (8) so as to obtain a candidate invariant. To do this, we can decompose $\underline{k}$ into two disjoint sub-sequences $\underline{i}$ and $\underline{j}$ such that $\underline{k} = \underline{i} \cup \underline{j}$ according to some criteria: if the conjunction of $\Sigma_I(\underline{i})$ literals occurring in θ is maximal, we get a candidate invariant by returning the corresponding $\exists^I$-formula (9). This is quite feasible in many concrete cases. For instance, quantifier elimination reduces to a trivial substitution if T_E is an enumerated datatype theory and the Σ_E-literals in θ are all positive. Maximality of θ is guaranteed (by differentiatedness) if T_I is the theory of finite sets;

[5] This Claim will be formally proved in the Appendix A.

maximality of θ is also guaranteed if T_I is the theory of linear orders and $\underline{i} = i_1$ or ($\underline{i} = i_1, i_2$ and θ contains the atom $i_1 < i_2$).

5 Experiments and Discussion

To test the practical viability of our approach, we have implemented MCMT, a prototype tool which uses Yices (`http://yices.csl.sri.com`) as the backhand SMT solver. MCMT is the successor of the system in [12] which is not capable of solving almost any of the problems considered here. The starting point of our implementation is the Tableaux-like calculus of Section 3.1. As Yices is guaranteed to behave as a decision procedure on quantifier-free formulae only, universally quantified variables in $\exists^{A,I}\forall^{I}$-sentences are instantiated according to the procedure sketched after Theorem 3.2: this is required for the application of rules NotAppl, Safety, FixPoint. Invariants have been integrated in the basic backward reachability algorithm along the lines of Section 4.2.

As benchmarks, we have derived safety problems in our format from two sets of benchmarks in [2]: one is of mutual exclusion protocols (with 7 problems, cf. Table 1) and the other is of cache coherence protocols (with 9 problems, cf. Table 2).[6] We used the theory of finite linear orders as T_I for mutual exclusion algorithms and the theory of finite sets as T_I for cache coherence protocols. The theory T_E for the various systems is the combination of an enumerated datatype theory for the control locations with theories for the data manipulated by the processes. A difficulty in the translation was the presence of global (i.e. universally quantified) guards which are not directly supported by our formalism. It is possible to eliminate universal quantifiers in guards (see [12] for details) by adopting the well-known *stopping failure model* (see, e.g., [14]) which is quite close to the approximate model in [2, 3]. This is without loss of generality since establishing a safety property for the stopping failures model of a system trivially implies that the same property is enjoyed by the original system. The elimination of global guards can be easily mechanized as it is purely syntactic.

Columns 2-5 of both Tables report the statistics of our implementation of the procedure BReach while columns 6-10 show the results for BReach+Inv. (All timings are in seconds and obtained on a Pentium Dual-Core 3.4 GHz with 2 Gb Sdram). Table 1 clearly shows the usefulness of invariant search as the size of the problem grows. Table 2 seems to suggest that invariant search is useless or even detrimental to performances on cache coherence protocols. However, we remark that all these problems, except the German, are quite small and a brute force search of the tiny search space (see the column '#nodes') is likely to be more successful.

[6] The files containing such specifications and an executable of the tool are available at `http://homes.dsi.unimi.it/\char126\relaxghilardi/mcmt`.

	depth	#nodes	#calls	time	depth	#nodes	#calls	#inv	time
Bakery	9	29	221	0.104	7	8	129	5	**0.052**
Burns	14	57	497	0.216	2	2	59	3	**0.016**
Java M-lock	9	23	353	**0.156**	9	22	2390	1	0.772
Dijkstra	13	40	392	0.148	2	1	41	2	**0.012**
Dijkstra (rv)	14	138	6905	5.756	2	1	57	2	**0.016**
Szymanski	17	143	3266	2.208	11	22	1185	8	**0.288**
Szymanski (a)	23	2358	902017	24m19s	16	90	8547	16	**5.188**

Table 1: Mutual exclusion algorithms

	depth	#nodes	#calls	time	depth	#nodes	#calls	#inv	time
Berkeley	2	1	102	**0.020**	2	1	190	0	0.032
Mesi	3	2	175	**0.032**	3	2	231	0	0.036
Moesi	3	2	304	**0.048**	3	2	384	0	0.052
Dec Firefly	4	4	163	**0.052**	4	4	222	0	0.068
Xerox P.D.	7	13	607	**0.288**	7	13	1059	0	0.432
Illinois	4	8	998	**0.196**	4	8	1114	0	0.216
Futurebus	4	19	1318	**0.460**	4	19	3824	0	1.096
German	26	2985	322335	**8m39s**	26	2856	544429	10	10m37s
German (pfs)	42	26004	3062165	176m51s	42	22808	2656282	40	**173m42s**

Table 2: Cache coherence protocols

Furthermore, the overhead of searching for invariants can be eliminated by implementing a parallel version of the tool. Interestingly, there is some gain in using invariant synthesis on the last problem in this set (a difficult version of the German protocol [15], which is well-known to be a significant benchmark for verification tools). Although a comparative analysis is somewhat difficult in lack of a standard for the specifications of safety problems, we report that MCMT performs comparably with the model checker PFS [2] on small to medium sized problems and outperforms the latter on larger instances.

References

[1] P. A. Abdulla, K. Cerans, B. Jonsson, and Y.-K. Tsay. General decidability theorems for infinite-state systems. In *Proc. of LICS*, pages 313–321, 1996.

[2] P. A. Abdulla, G. Delzanno, N. B. Henda, and A. Rezine. Regular model checking without transducers. In *TACAS*, volume 4424 of *LNCS*, pages 721–736, 2007.

[3] P. A. Abdulla, G. Delzanno, and A. Rezine. Parameterized verification of infinite-state processes with global conditions. In *CAV*, volume 4590 of *LNCS*, pages 145–157, 2007.

[4] D. Beyer, T. A. Henzinger, R. Majumdar, and A. Rybalchenko. Invariant Synthesis for Combined Theories. In *VMCAI'07*, volume 4349 of *LNCS*, 2007.

[5] Aaron R. Bradley and Zohar Manna. Property-Directed Incremental Invariant Generation. *Formal Aspects of Computing*, 2009. To appear.

[6] Chen-Chung Chang and Jerome H. Keisler. *Model Theory*. North-Holland, Amsterdam-London, third edition, 1990.

[7] G. Delzanno, J. Esparza, and A. Podelski. Constraint-based analysis of broadcast protocols. In *Proc. of CSL*, volume 1683 of *LNCS*, pages 50–66, 1999.

[8] Herbert B. Enderton. *A Mathematical Introduction to Logic*. Academic Press, New York-London, 1972.

[9] J. Esparza, A. Finkel, and R. Mayr. On the verification of broadcast protocols. In *Proc. of LICS*, pages 352–359. IEEE Computer Society, 1999.

[10] C. Flanagan and S. Qadeer. Predicate abstraction for software verification. In *Proc. of POPL'02*, pages 191–202. ACM, 2002.

[11] S. Ghilardi, E. Nicolini, S. Ranise, and D. Zucchelli. Towards SMT Model-Checking of Array-based Systems. In *Proc. of IJCAR*, LNCS, 2008.

[12] S. Ghilardi, S. Ranise, and T. Valsecchi. Light-Weight SMT-based Model-Checking. In *Proc. of AVOCS 07-08*, ENTCS, 2008.

[13] S. K. Lahiri and R. E. Bryant. Predicate Abstraction with Indexed Predicate. *ACM Trans. on Comp. Logic*, 9(1), 2007.

[14] Nancy A. Lynch. *Distributed Algorithms*. Morgan Kaufmann, 1996.

[15] A. Pnueli, S. Ruath, and L. D. Zuck. Automatic deductive verification with invisible invariants. In *Proc. of TACAS 2001*, volume 2031 of *LNCS*, 2001.

[16] S. Ranise and C. Tinelli. The SMT-LIB Standard: Version 1.2. Technical report, Dep. of Comp. Science, Iowa, 2006. Available at `http://www.SMT-LIB.org/papers`.

A Appendix

Here, we collect the proofs of the main results of the paper.

A.1 Theorem 4.1: undecidability

We make a rather straightforward reduction from the reachability problem of Minsky machines.

A *two registers Minsky machine* is a finite set $\mathbf{P}$ of instructions (also called a program) for manipulating configurations seen as triples (q, m, n) where m, n are natural numbers representing the registers content and q represents the machine location state (q varies on a fixed finite set Q). There are four possible kinds of instructions, inducing transformations on the configurations as explained in Table 3. A $\mathbf{P}$-transformation is a transformation in-

N.	Instruction	Transformation
I	$q \to (r, 1, 0)$	$(q, m, n) \to (r, m+1, n)$
II	$q \to (r, 0, 1)$	$(q, m, n) \to (r, m, n+1)$
III	$q \to (r, -1, 0)[r']$	`if` $m \neq 0$ `then` $(q, m, n) \to (r, m-1, n)$ `else` $(q, m, n) \to (r', m, n)$
IV	$q \to (r, 0, -1)[r']$	`if` $n \neq 0$ `then` $(q, m, n) \to (r, m, n-1)$ `else` $(q, m, n) \to (r', m, n)$

Table 3: Instructions and related transformations for (two-registers) Minsky Machines

duced by an instruction of $\mathbf{P}$ on a certain configuration. For a Minsky machine $\mathbf{P}$, we write $(q, m, n) \to^{\star}_{\mathbf{P}} (q', m', n')$ to say that it is possible to reach configuration (q', m', n') from (q, m, n) by applying finitely many $\mathbf{P}$-transformations. Given a Minsky machine $\mathbf{P}$ and an initial configuration (q_0, m_0, n_0), the problem of checking whether a configuration (q', m', n') is reachable from (q_0, m_0, n_0) (i.e., if $(q_0, m_0, n_0) \to^{\star}_{\mathbf{P}} (q', m', n')$ holds or not) is called *the (second) reachability (configuration) problem*. It is well-known[7] that there exists a (two-register) Minsky machine $\mathbf{P}$ and a configuration (q_0, m_0, n_0) such that the second reachability configuration problem is undecidable. To simplify the matter, we assume that $m_0 = 0$ and $n_0 = 0$: there is no loss of generality in that, because one can add to the program $\mathbf{P}$ more states and instructions (precisely $m_0 + n_0$ further states and instructions of type I-II) for the initialization to m_0, n_0.

[7]For details and further references, see for instance A. Chagrov and M. Zakharyaschev *Modal Logic*, Clarendon Press, Oxford, 1997.

We build a locally finite array-based system $\mathcal{S}_{\mathbf{P}} = (a, I_{\mathbf{P}}, \tau_{\mathbf{P}})$ and an $\exists^I$-formula $U_{q,m,n}$ such that $\mathcal{S}$ is unsafe w.r.t. $U_{q,m,n}$ iff the machine $\mathbf{P}$ reaches the configuration (q, m, n). We take as Σ_I the signature having two constants o, o' and a binary relation S; models of T_I are the Σ_I-structures satisfying the axioms

$$\forall i\, \neg S(i, o), \qquad \forall i\, \forall j_1\, \forall j_2\, (S(i, j_1) \wedge S(i, j_2) \rightarrow j_1 = j_2),$$
$$S(o, o'), \qquad \forall i_1\, \forall i_2\, \forall j\, (S(i_1, j) \wedge S(i_2, j) \rightarrow i_1 = i_2),$$

saying that S is a an injective partial function having o in the domain but not in the range. As Σ_E is take the enumerated datatype theory relative to the finite set $Q \times \{0, 1\} \times \{0, 1\}$. Notice that T_I, T_E are both locally finite; in addition, T_I is closed under substructures and T_E has quantifier elimination.

The idea is that of encoding a configuration (q, m, n) as any configuration s (in our formal sense!) satisfying the following conditions:

(i) the support of s_I contains a substructure of the kind

$$o = i_0 \rightarrow_S o' = i_1 \rightarrow_S i_2 \cdots \rightarrow_S i_K$$

for some $K > m, n$ (we write $i \rightarrow_S j$ to means that (i, j) is in the interpretation of the relational symbol S in s_I).

(ii) for all i in the support of s_I, if $s(i) = \langle r, u, v\rangle$ then (a) $r = q$; (b) $u = 1$ iff $i = i_k$ for $k \leq m$; (c) $v = 1$ iff $i = i_k$ for $k \leq n$.

In case the above conditions (i)-(ii) hold, we say that s *bi-simulates* (q, m, n).

The initial formula I is

$$\forall i((i \neq 0 \wedge a[i] = \langle q_0, 0, 0\rangle) \vee (i = 0 \wedge a[i] = \langle q_0, 1, 1\rangle)).$$

Clearly for every model $\mathcal{M}$ and for every $s \in \texttt{ARRAY}^{\mathcal{M}}$, the following happens:

(α) $\mathcal{M} \models I(s)$ iff s bi-simulates the initial machine configuration $(q_0, 0, 0)$.

We write the transition τ in such a way that for every model $\mathcal{M}$ and for every $s, s' \in \texttt{ARRAY}^{\mathcal{M}}$, the following happens:

(β) if s bi-simulates (q, m, n), then $\mathcal{M} \models \tau(s, s')$ iff there is (q', m', n') such that s' bi-simulates (q', m', n') and $(q, m, n) \rightarrow_{\mathbf{P}} (q', m', n')$.

This goal is obtained by taking τ to be a disjunction of T-formulae corresponding to the instructions for $\mathbf{P}$. The T-formula corresponding to the first kind of instructions $q \to (r, 1, 0)$ is the following:[8]

$$\begin{aligned}\exists i_1\, \exists i_2\, \exists i_3 \quad & (S(i_1, i_2) \wedge S(i_2, i_3) \wedge pr_1(a[i_1]) = q \wedge \\ & \wedge pr_2(a[i_1]) = 1 \wedge pr_2(a[i_2]) = 0 \wedge pr_2(a[i_3]) = 0 \wedge a' = \lambda j\, F)\end{aligned}$$

where

$$\begin{aligned}F \;:=\; \texttt{case of}\ \{ \quad & j = i_2 : \ \langle r, 1, pr_3(a[j])\rangle; \\ & j \neq i_2 : \ \langle r, pr_2(a[j]), pr_3(a[j])\rangle; \}\end{aligned}$$

Instructions $q \to (r, -1, 0)[r']$ of the kind (III) are simulated by the following T-formula

$$\exists i_1\, \exists i_2\, (S(i_1, i_2) \wedge pr_1(a[i_1]) = q \wedge pr_2(a[i_1]) = 1 \wedge pr_2(a[i_2]) = 0)$$

where

$$\begin{aligned}F \;:=\; \texttt{case of}\ \{ \quad & i_1 \neq o \wedge j = i_1 \ : \ \langle r, 0, pr_3(a[j])\rangle; \\ & i_1 \neq o \wedge j \neq i_1 \ : \ \langle r, pr_2(a[j]), pr_3(a[j])\rangle; \\ & i_1 = o \qquad\quad : \ \langle r', pr_2(a[j]), pr_3(a[j])\rangle; \}\end{aligned}$$

T-formulae for instructions of kind (II) and (IV) are defined accordingly.

We write the unsafe states formula $U_{q,m,n}$ in such a way that for every model $\mathcal{M}$ and for every $s \in \texttt{ARRAY}^{\mathcal{M}}$, the following happens:

(γ) if $\mathcal{M} \models U_{q,m,n}(s)$ and s bi-simulates some machine configuration, then it bi-simulates (q, m, n).

This goal is achieved by taking $U_{q,m,n}$ to be the following formula (suppose $m \geq n$, the case $n \leq m$ is symmetric):

$$\begin{aligned}\exists i_0 \cdots \exists i_{m+1} \quad & (i_0 = o \wedge \textstyle\bigwedge_{0 \leq k \leq m} S(i_k, i_{k+1}) \wedge \bigwedge_{0 \leq k \leq n} a[i_k] = \langle q, 1, 1\rangle \wedge \\ & \wedge \textstyle\bigwedge_{n < k \leq m} a[i_k] = \langle q, 1, 0\rangle \wedge a[i_{m+1}] = \langle q, 0, 0\rangle).\end{aligned}$$

From (α)-(β)-(γ) above it is clear that $\mathbf{P}$ reaches the configuration (q, m, n) iff $\mathcal{S}$ is unsafe w.r.t. $U_{q,m,n}$,[9] so that the latter is not decidable. □

[8] For simplicity, we assume that the signature Σ_E is 4-sorted and endowed with the three projection functions: there is no need of this assumption, but without it one should make a lot of case distinctions more.

[9] For the left to right implication, take a run in a model with a large enough S-chain starting with o.

A.2 Background for results from Section 4.1

Results of Section 4.1 needs some background from the extended version of [11]: we report this background here for the sake of completeness.

Proposition A.1. *For every $\exists^I$-formula $K(a)$, the set $[\![K]\!]$ is upward closed; for every $\exists^I$-formulae K_1, K_2, we have that $[\![K_1]\!] \subseteq [\![K_2]\!]$ iff $A_I^E \models K_1 \to K_2$.*

Proof. Let's first show that the set $[\![K]\!]$ is upward closed. By using disjunctive normal forms and by distributing existential quantifiers over disjunctions, we can freely suppose that $K(a)$ is of the kind $\exists \underline{i} \phi(\underline{i}, a[\underline{i}])$,[10] where ϕ is a conjunction of $\Sigma_I \cup \Sigma_E$-literals. If we also separate Σ_I- and Σ_E-literals, we can suppose that $\phi(\underline{i}, a[\underline{i}])$ is of the kind $\phi_I(\underline{i}) \wedge \phi_E(a[\underline{i}])$, where ϕ_I is a conjunction of Σ_I-literals and ϕ_E is a conjunction of Σ_E-literals. Suppose now that $(\mathcal{M}, s)$ and $(\mathcal{N}, t)$ are configurations such that $s \leq t$ and $\mathcal{M} \models K(s)$: we wish to prove that $\mathcal{N} \models K(t)$. From $\mathcal{M} \models K(s)$, it follows that there are elements $\underline{i}$ from $\mathtt{INDEX}^{\mathcal{M}}$ such that $\mathcal{M} \models \phi_I(\underline{i}) \wedge \phi_E(s[\underline{i}])$, i.e. such that $s_I \models \phi_I(\underline{i})$ and $s_E \models \phi_E(s(\underline{i}))$ (to infer the latter, recall that the operations $a[\underline{i}]$ are interpreted as functional applications in our models and also that truth of quantifier free formulae is preserved when passing to substructures). Now $s \leq t$ says that there are embeddings $\mu : s_I \longrightarrow t_I$ and $\nu : s_E \longrightarrow t_E$ such that $\nu \circ s = t \circ \mu$. Since truth of quantifier free formulae is preserved when passing to superstructures, we get $t_I \models \phi_I(\mu(\underline{i}))$ and $t_E \models \phi_E(\nu(s(\underline{i}))$ (that is, $t_E \models \phi_E(t(\mu(\underline{i})))$ and also $\mathcal{N} \models \phi_I(\mu(\underline{i})) \wedge \phi_E(t[\mu(\underline{i})])$, which implies $\mathcal{N} \models K(t)$, as desired.

Let's now prove the second claim of the Proposition. That $A_E^I \models K_1 \to K_2$ implies $[\![K_1]\!] \subseteq [\![K_2]\!]$ is trivial. Suppose conversely that $A_E^I \not\models K_1 \to K_2$, which means that $K_1(a) \wedge \neg K_2(a)$ is A_E^I-satisfiable: since this implies that $K_1(a) \wedge \neg K_2(a)$ is satisfiable in a finite index model of A_E^I,[11] we immediately get that $[\![K_1]\!] \not\subseteq [\![K_2]\!]$. □

Before continuing, we need some standard model-theoretic background on Robinson diagrams [6]. Let $\mathcal{M} = (M, \mathcal{I})$ be a Σ-structure which is generated by $G \subseteq M$. Let's take a free variable x_g for every $g \in G$[12] and let us call G_x the set $\{x_g \mid g \in G\}$. The *Σ_G-diagram $\delta_{\mathcal{M}}(G)$ of $\mathcal{M}$* is the set of all $\Sigma(G_x)$-literals L such $\mathcal{M}, \mathtt{a} \models L$, where $\mathtt{a}$ is the assignment mapping x_g to g.

[10] Notice that a union of upsets is an upset.

[11] An $\exists^{A,I}\forall^I$-sentence is A_I^E-satisfiable iff it is satisfiable in a finite index model of A_I^E. This result follows from the proof of Theorem 3.2 and is formally stated and proved as Theorem A.1(i)-(ii) in the extended version of [11].

[12] One may complain because there are only countable many variables and G may not be countable: this trouble can be disposed of either by using free constants instead of variables (this is the standard approach), or by realizing that we won't need in the paper an uncountable G (actually, in all our applications, G is always finite).

The following celebrated result [6] is simple, but nevertheless very powerful.

Lemma A.2 (Robinson Diagram Lemma)**.** *Let $\mathcal{M} = (M, \mathcal{I})$ be a Σ-structure which is generated by $G \subseteq M$ and let $\mathcal{N} = (N, \mathcal{J})$ be a further Σ-structure. Then there is a bijective correspondence given by*

$$\mu(g) = \mathtt{a}(x_g) \tag{10}$$

(for all $g \in G$)[13] *between assignments $\mathtt{a}$ on N such that $\mathcal{N}, \mathtt{a} \models \delta_{\mathcal{M}}(G)$ and Σ-embeddings $\mu : \mathcal{M} \longrightarrow \mathcal{N}$.*

The diagram $\delta_{\mathcal{M}}(G)$ usually contains infinitely many literals, however there are important cases where we can keep it finite.

Lemma A.3. *Suppose that $\mathcal{M}$ is a Σ-structure (where Σ is a finite signature), whose support M is finite; then for every set of generators $G \subseteq M$, there are finitely many literals from $\delta_{\mathcal{M}}(G)$ having all remaining literals of $\delta_{\mathcal{M}}(G)$ as a logical consequence.*

Proof. Choose $\Sigma(G_x)$-terms $t_1, \ldots, t_n$ such that (under the assignment $\mathtt{a} : x_g \mapsto g$), M is equal to the set of the elements assigned by $\mathtt{a}$ to $t_1, \ldots, t_n$ (this is possible because the elements of G are generators and M is finite); we also include the x_g varying $g \in G$ among the $t_1, \ldots, t_n$. We can get the desired finite set S of literals by taking the set of atoms of the form

$$R(t_{i_1}, \ldots, t_{i_k}), \quad f(t_{i_1}, \ldots, t_{i_k}) = t_{i_{k+1}}$$

(as well as their negations), which are true in $\mathcal{M}$ under the assignment $\mathtt{a}$. In fact, modulo S, it is easy to see by induction on u that every $\Sigma(G_x)$-term u is equal to some t_i; it follows that every literal from $\delta_{\mathcal{M}}(G)$ is a logical consequence of S. □

Whenever the conditions of the above Lemma are true, we can take a finite conjunction and treat $\delta_{\mathcal{M}}(G)$ as a single formula: notice that we are allowed to do so whenever G is finite and $\mathcal{M}$ is a model of a locally finite theory.

Proposition 4.4 (Extended version of [11]) *Let T_E be locally finite. The following hold:*

(i) *with every A_I^E-configuration $(\mathcal{M}, s)$ one can effectively associate an $\exists^I$-formula K_s such that $[\![K_s]\!] = {\uparrow} s$;*

(ii) *with every $\exists^I$-formula K one can effectively associate a finite set $\{s_1, \ldots, s_n\}$ of A_I^E-configurations such that K is A_I^E-equivalent to $K_{s_1} \vee \cdots \vee K_{s_n}$.*

[13] In other words, (10) can be used to define μ from $\mathtt{a}$ and conversely. Notice that an embedding $\mu : \mathcal{M} \longrightarrow \mathcal{N}$ is uniquely determined, in case it exists, by the image of the set of generators G: this is because the fact that G generates $\mathcal{M}$ implies (and is equivalent to) the fact that every $c \in M$ is of the kind $t^{\mathcal{I}}(\underline{g})$, for some term t and some $\underline{g}$ from G.

As a consequence of (i)-(ii)*, finitely generated upsets of A_I^E-configurations coincide with sets of A_I^E-configurations of the kind $[\![K]\!]$, for some $\exists^I$-formula K.*

Proof. Ad (i): we take G, G' to be the support of s_I and the image of the support of s_I under the function s, respectively; clearly G is a set of generators for s_I and G' is a set of generators for s_E. Let us call the set of variables G_x, G'_x as $\underline{i} := \{i_1, \ldots, i_n\}$ and $\underline{e} := \{e_1, \ldots, e_n\}$, respectively. We take K_s to be

$$\exists \underline{i} \, (\delta_{s_I}(\underline{i}) \wedge \delta_{s_E}(a_0[\underline{i}])) \tag{11}$$

(in other words, we take the diagrams $\delta_{s_I}(G), \delta_{s_E}(G')$, make in the latter the replacement $\underline{e} \mapsto a_0[\underline{i}]$, take conjunction, and quantify existentially over the $\underline{i}$). For every configuration $(\mathcal{N}, t)$, we have that $t \in [\![K_s]\!]$ iff $\delta_{s_I}(\underline{i}) \wedge \delta_{s_E}(a_0[\underline{i}])$ is true in $\mathcal{N}$ under some assignment $\mathtt{a}$ mapping the array variable a_0 to t, that is iff that there are embeddings $\mu : s_I \longrightarrow t_I$ and $\nu : s_E \longrightarrow t_E$ as prescribed by the Robinson Diagram Lemma. These embeddings map the generators G onto the indexes assigned to the $\underline{i}$ by $\mathtt{a}$ and the generators G' to the elements assigned by $\mathtt{a}$ to the terms $a_0[\underline{i}]$, which means precisely that $t \circ \mu = \nu \circ s$. Thus $t \in [\![K_s]\!]$ is equivalent to $s \leq t$, as wanted.

Ad (ii): modulo taking disjunctive normal forms, we can suppose that $K(a_0)$ is $\exists \underline{i} \bigvee_k (\phi_k(\underline{i}) \wedge \psi_k(a_0[\underline{i}]))$ (where the ϕ_k are Σ_I-formulae, the ψ_k are Σ_E-formulae and we let, for instance, $\underline{i}$ be $i_1, \ldots, i_m$). Since T_I is locally finite, we can assume that for every representative $\underline{i}$-term t there is an $i_s \in \underline{i}$ such that $t = i_s$ is an A_E^I-logical consequence of ϕ_k, for all k: this is achieved by conjoining (just once!) equations like $i_k = t$ with ϕ_k - here the i_s are new existentially quantified variables and t is a representative Σ_I-term in which only the original existentially quantified variables occur. In this way, all elements in a substructure generated by the $\underline{i}$ are named explicitly and so are their a_0-images $a_0[\underline{i}]$ (otherwise said, modulo $\phi_k(\underline{i})$, for every $\Sigma_I(\underline{i})$-term t, we have that $a_0[t]$ is equal to some of the $a_0[\underline{i}]$).

Now, in a locally finite theory, every quantifier free formula θ having at most m free variables, is equivalent to a disjunction of diagram formulae $\delta_{\mathcal{M}}(G)$, where $\mathcal{M}$ is a substructure of a model of the theory and G is a set of generators for $\mathcal{M}$ of cardinality at most m.[14] If we apply this to both T_I and T_E, we get that our $K(a_0)$ can be rewritten as

$$\bigvee_{\mathcal{A},\mathcal{B}} \exists \underline{i} \, (\delta_{\mathcal{A}}(\underline{i}) \wedge \delta_{\mathcal{B}}(a_0[\underline{i}]))$$

[14] Since the theory is locally finite, there are finitely many atoms whose free variables are included in a given set of cardinality m. Maximal conjunctions of literals built on these atoms are either inconsistent (modulo the theory) of satisfiable in an m-generated substructure of a model of the theory. By maximality, these maximal conjunctions must be diagrams.

where $\mathcal{A}$ ranges over the m-generated models of T_I and $\mathcal{B}$ over the m-generated sub-models of T_E.[15] Every such pair $(\mathcal{A}, \mathcal{B})$ is either A_E^I-inconsistent (in case some equality among the generators of $\mathcal{A}$ is not satisfied by the corresponding generators of $\mathcal{B}$) or it gives rise to a configuration a such that $\exists \underline{i}\,(\delta_{\mathcal{A}}(\underline{i}) \wedge \delta_{\mathcal{B}}(a_0[\underline{i}]))$ is precisely K_a. □

The formula K_s will be called *the diagram formula* for the configuration s.

A.3 Proof of the results in Section 4.1

Here we prove the main results of the paper justifying our methodology for invariant synthesis.

First, we give the easy justification of *Proposition 2.* Suppose that the Algorithm of Figure 1 exits the main loop at the k-th iteration and returns B; then B is $\bigvee_{i=0}^{k} Pre^i(\tau, U)$,[16] the formula $Pre^{k+1}(\tau, U) \wedge \neg B$ is A_E^I-inconsistent and the formulae $I \wedge Pre^i(\tau, U)$ (for $i = 0, \ldots, k$) are also A_E^I-inconsistent. The latter means that $A_I^E \models \forall a(I(a) \rightarrow \neg B(a))$; for $i = 0$ (since $Pre^0(\tau, U)$ is U), we also get that $\exists a.(U(a) \wedge \neg B(a))$ is A_I^E-unsatisfiable. To claim that $\neg B(a)$ is an invariant, we only need to check that $A_I^E \models \forall a \forall a'(\neg B(a) \wedge \tau(a, a') \rightarrow \neg B(a'))$, i.e. that $A_I^E \models \forall a(Pre(\tau, B(a)) \rightarrow B(a))$, which is trivial by the fact that $Pre(\tau, B)$ is $Pre^{k+1}(\tau, U) \vee B$. □

We now prove in detail also *the claim of Property 1.* For reductio, suppose that there is a safety invariant for U, but that the array-based system $\mathcal{S} = (a, I, \tau)$ is not safe w.r.t. U. This means that the formula

$$I(a_0) \wedge \tau(a_0, a_1) \wedge \cdots \wedge \tau(a_{n-1}, a_n) \wedge U(a_n) \tag{12}$$

is A_E^I consistent; using Definition 4.2(i)-(ii), we get that $J(a_n) \wedge U(a_n)$ is A_E^I-consistent, in contrast to Definition 4.2(iii). □

We first reformulate set-theoretically the conditions of Definition 4.2.

Lemma A.4. *Let J be a $\forall^I$-formula; the conditions (i), (ii), and (iii) of Definition 4.2 are equivalent to the following three conditions on (sets of) configurations:*

$$[\![I]\!] \cap [\![H]\!] = \emptyset \tag{13}$$

$$[\![Pre(\tau, H)]\!] \subseteq [\![H]\!] \tag{14}$$

$$[\![U]\!] \subseteq [\![H]\!], \tag{15}$$

where H is the $\exists^I$-formula which is logically equivalent to the negation of J.

[15] Recall that T_I is closed under substructures.

[16] Notice that the disjunction of $\exists^I$-formulae is (up to logical equivalence) an $\exists^I$-formula, so B is itself an $\exists^I$-formula.

Proof. For (13), we have:

$$\begin{aligned}
\text{(i) of Def. 4.2} &\Leftrightarrow A_I^E \models \forall a.(I(a) \rightarrow J(a)) \Leftrightarrow \\
&\Leftrightarrow \neg\forall a.(I(a) \rightarrow J(a)) \text{ is } A_I^E\text{-unsat.} \Leftrightarrow \\
&\Leftrightarrow \exists a.(I(a) \wedge \neg J(a)) \text{ is } A_I^E\text{-unsat.} \Leftrightarrow \\
&\Leftrightarrow \exists a.(I(a) \wedge H(a)) \text{ is } A_I^E\text{-unsat.} \Leftrightarrow \\
&\Leftrightarrow [\![I]\!] \cap [\![H]\!] = \emptyset.
\end{aligned}$$

For (14), we have:

$$\begin{aligned}
\text{(ii) of Def. 4.2} &\Leftrightarrow A_I^E \models \forall a, a'.(J(a) \wedge \tau(a, a') \rightarrow J(a')) \Leftrightarrow \\
&\Leftrightarrow \exists a, a'.\neg(J(a) \wedge \tau(a, a') \rightarrow J(a')) \text{ is } A_I^E\text{-unsat.} \Leftrightarrow \\
&\Leftrightarrow \exists a, a'.(J(a) \wedge \tau(a, a') \wedge \neg J(a')) \text{ is } A_I^E\text{-unsat.} \Leftrightarrow \\
&\Leftrightarrow \exists a.(J(a) \wedge \exists a'.(\tau(a, a') \wedge \neg J(a'))) \text{ is } A_I^E\text{-unsat.} \Leftrightarrow \\
&\Leftrightarrow \exists a.(J(a) \wedge \exists a'.(\tau(a, a') \wedge H(a'))) \text{ is } A_I^E\text{-unsat.} \Leftrightarrow \\
&\Leftrightarrow \exists a.(J(a) \wedge Pre(\tau, H)(a)) \text{ is } A_I^E\text{-unsat.} \Leftrightarrow \\
&\Leftrightarrow A_I^E \models \forall a.(\neg J(a) \vee \neg Pre(\tau, H)(a)) \Leftrightarrow \\
&\Leftrightarrow A_I^E \models \forall a.(H(a) \vee \neg Pre(\tau, H)(a)) \Leftrightarrow \\
A_I^E \models \forall a.(Pre(\tau, H)(a) \rightarrow H(a)) &\Leftrightarrow [\![Pre(\tau, H)]\!] \subseteq [\![H]\!].
\end{aligned}$$

For (15), we have:

$$\begin{aligned}
\text{(iii) of Def. 4.2} &\Leftrightarrow \exists a.(U(a) \wedge J(a)) \text{ is } A_I^E\text{-unsat.} \Leftrightarrow \\
&\exists a.\neg(\neg U(a) \vee \neg J(a)) \text{ is } A_I^E\text{-unsat.} \Leftrightarrow \\
&\Leftrightarrow A_I^E \models \forall a.(U(a) \rightarrow \neg J(a)) \Leftrightarrow \\
A_I^E \models \forall a.(U(a) \rightarrow H(a)) &\Leftrightarrow [\![U]\!] \subseteq [\![H]\!].
\end{aligned}$$

□

Theorem 4.7 *Let T_E be locally finite. If there exists a safety invariant for U, then there exist finitely many A_I^E-configurations $s_1, \ldots, s_k$ which are sub-reachable from U and such that $\neg(K_{s_1} \vee \cdots \vee K_{s_k})$ is also a safety invariant for U.*

Proof. Our goal is to replace an $\exists^I$-formula H satisfying the three conditions of Lemma A.4 with an $\exists^I$-formula L whose negation is still a safety invariant for U and whose basis is formed by configurations which are all sub-reachable from U. To this end, we consider a function $\gamma(S)$ where S is an $\exists^I$-formula such that $[\![S]\!] \subseteq [\![H]\!]$: the function $\gamma(S)$ returns an $\exists^I$-formula

$K_{a_1} \vee \cdots \vee K_{a_n}$, where $\{a_1, \ldots, a_n\} \subseteq [\![H]\!]$ is a minimal set of configurations taken from a basis of H such that $[\![S]\!] \subseteq \uparrow a_1 \cup \cdots \cup \uparrow a_n$. (Notice that this implies that $\{a_1, \ldots, a_n\}$ is a basis of $\gamma(S)$ and $[\![S]\!] \subseteq [\![\gamma(S)]\!]$.)[17]

Now, define the following sequence of $\exists^I$-formulae L_i: (i) $L_0 := \gamma(U)$ and (ii) $L_{i+1} := L_i \vee \gamma(Pre(\tau, L_i))$. (The definition is well given because $[\![L_i]\!] \subseteq [\![H]\!]$ is a consequence of (15) and (14).) What remains to be shown is that the sequence becomes stable and its fix-point is the desired L, i.e. a safety invariant for U whose basis is formed by configurations which are sub-reachable from U.

We first show, by induction on k, that every configuration b that belongs to a basis of L_k is sub-reachable from U:

- if $k = 0$, we have that $\{a_1, \ldots, a_n\}$ is a minimal set of configurations taken from a basis of H such that $[\![U]\!] \subseteq \uparrow a_1 \cup \cdots \cup \uparrow a_n$ and $b = a_j$ for some $j = 1, \ldots, n$. By minimality, there is s from a basis of U such that $s \notin \uparrow a_1 \cup \cdots \cup \uparrow a_{j-1} \cup \uparrow a_{j+1} \cup \uparrow a_n$, which means that $s \in \uparrow a_j$, that is $a_j \leq s$ and $a_j = b$ is sub-reachable from U.

- Suppose now $k = i + 1 > 0$. A basis for $L_i \vee \gamma(Pre(\tau, L_i))$ is obtained by joining two bases— one for L_i and one for $\gamma(Pre(\tau, L_i))$—and then by discarding non-minimal elements. As a consequence, if b is in a basis for L_k, then b is either in a basis for L_i or in a basis for $\gamma(Pre(\tau, L_i))$ (or in both). In the former case, we just apply induction. If b is in a basis for $\gamma(Pre(\tau, L_i))$, the same argument used in the case $k = 0$ shows that $b \leq s$ for an s that belongs to a basis for $Pre(\tau, L_i)$. Now, if $c_{i1}, \ldots, c_{ik_i}$ is a basis of L_i, the formula $Pre(\tau, L_i)$ is A_I^E-equivalent to the disjunction of the $Pre(\tau, K_{c_{ij}})$ and consequently s must be in a basis of one of the latter (that is, s is a predecessor of some c_{ij}); since the c_{ij} are sub-reachable by induction hypothesis and $b \leq s$, the definition of sub-reachability guarantees that b is sub-reachable from U.

The increasing chain

$$[\![L_0]\!] \subseteq [\![L_1]\!] \subseteq \cdots$$

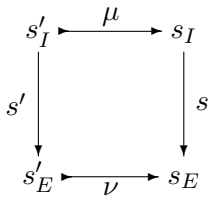
becomes stationary, because at each step only configurations from a basis of H can be added and bases are (unique and) finite by definition. Thus, we have $[\![L_i]\!] = [\![L_{i+1}]\!]$ for some i: let L be L_i for such i.

[17] There might be many functions γ satisfying the above specification, we just take one of them. This can be done (by choice axiom) because, given S such that $[\![S]\!] \subseteq [\![H]\!]$, there always exists a a minimal set of configurations $\{a_1, \ldots, a_n\}$ taken from a basis of H such that $[\![S]\!] \subseteq \uparrow a_1 \cup \cdots \cup \uparrow a_n$ (just take any basis for H and throw out configurations from it until minimality is acquired).

The fact that L is a safety invariant is straightforward: condition $[\![I]\!] \cap [\![L]\!] = \emptyset$ follows from (13) and the fact that $[\![L]\!] \subseteq [\![H]\!]$, whereas conditions $[\![U]\!] \subseteq [\![L]\!]$ and $[\![Pre(\tau, L)]\!] \subseteq [\![L]\!]$ follow directly from the above definitions of L_0 and L_{i+1} (we have $[\![U]\!] \subseteq [\![\gamma(U)]\!] = [\![L_0]\!] \subseteq [\![L]\!]$ and for all $i \geq 0$, $[\![Pre(\tau, L_i)]\!] \subseteq [\![\gamma(Pre(\tau, L_i))]\!] \subseteq [\![L_{i+1}]\!] \subseteq [\![L]\!]$). □

Let us now give a closer look to the equivalence relation among configurations: recall that s is said to be equivalent to t (written $s \approx t$) iff $s \leq t$ and $t \leq s$.

Proposition A.5. *We have that $s \approx t$ holds iff there are a Σ_I-isomorphism μ and a Σ_E-isomorphism ν such that such that the set-theoretical compositions of μ with s and of s' with ν are equal.*[18]



Proof. The supports of s_I and of t_I are finite, hence the existence of embeddings $s_I \xrightarrow{\mu_1} t_I \xrightarrow{\mu_2} s_I$ means (for cardinality reasons) that μ_1, μ_2 are bijections, hence isomorphisms. Since the images of s and of t are finite sets of generators for s_E and t_E, we have embeddings $s_E \xrightarrow{\nu_1} t_E \xrightarrow{\nu_2} s_E$ mapping generators into generators: again for cardinality reasons, ν_1, ν_2 restrict to bijections among generators, which means that they are isomorphisms. □

Lemma A.6. *A configuration s belongs to a basis for an $\exists^I$-formula K iff $s \in [\![K]\!]$ and for every s' ($s' \leq s$ and $s' \in [\![K]\!]$) imply that $s \approx s'$.*

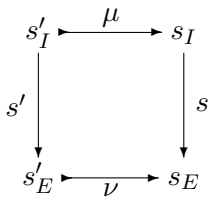
Proof. Let B be a basis for K and let also $s \in B$, $s' \leq s$ and $s' \in [\![K]\!]$; then s' is bigger than some configuration from B, which must be s, because elements from B are incomparable: $s \approx s'$ follows immediately. Conversely, suppose that $s \in [\![K]\!]$ and for every s', $s' \leq s$ and $s' \in [\![K]\!]$ imply that $s \approx s'$. Then we have $s \approx b$ for some b from a basis B of K: it is now clear that we can get another basis for K by replacing in B the configuration b with s. □

The following Lemma explains the semantic meaning of the formula $Min(\phi, a, \underline{i})$ of Proposition 4.8:

[18] Notice that, since the image of s is a set of generators for s_E, it is not difficult to see that ν is uniquely determined from μ (i.e., given μ, there might be no ν such that the above square commutes, but in case one such exists, it is unique). Observe also that, if s comes from the finite index model $\mathcal{M}$ and t comes from the finite index model $\mathcal{N}$, the fact that $s \approx t$ holds does not mean that $\mathcal{M}$ and $\mathcal{N}$ are isomorphic: their Σ_I-reducts are Σ_I-isomorphic, but their Σ_E-reducts need not be Σ_E-isomorphic (only the Σ_E-substructures s_E and t_E are Σ_E-isomorphic).

Lemma A.7. *Consider an $\exists^I$-formula $K \equiv \exists \underline{i}\, \phi(\underline{i}, a[\underline{i}])$, an A_E^I-model $\mathcal{M}$ and a variable assignment* $\mathtt{a}$ *in $\mathcal{M}$ such that $(\mathcal{M}, \mathtt{a}) \models \phi(\underline{i}, a[\underline{i}])$. We have that $(\mathcal{M}, \mathtt{a}) \models Min(\phi, a, \underline{i})$ iff the configuration s obtained by restricting $\mathtt{a}(a)$ to the Σ_I-substructure generated by the $\mathtt{a}(\underline{i})$'s belongs to a basis of K.*[19]

Proof. Suppose that $(\mathcal{M}, \mathtt{a}) \models Min(\phi, a, \underline{i})$ (for simplicity, we shall directly call $\underline{i}, a$ the elements assigned by $\mathtt{a}$ to $\underline{i}, a$, respectively). In view of Proposition A.5 and Lemma A.6, it is sufficient to prove the following. Consider $s' \leq s$ such that $s' \in [\![K]\!]$: we show that the embeddings μ, ν witnessing the relation $s' \leq s$ and making the square



to commute are isomorphisms (in fact, it is sufficient to show only that μ is bijective, because the images of s' and s are Σ_E-generators and the square commutes). Without loss of generality, we can assume that μ is an inclusion; the domain of s' is then formed by elements of the form $t^{(\mathcal{M},\mathtt{a})}$ for suitable (representative) $\Sigma_I(\underline{i})$-terms t and the fact that $s' \in [\![K]\!]$ means then that $(\mathcal{M}, \mathtt{a}) \models \phi(\underline{i}\sigma, a[\underline{i}\sigma])$ holds for a substitution σ whose domain is $\underline{i}$ and whose range is contained into the set of those representative $\Sigma_I(\underline{i})$-terms u such that $u^{(\mathcal{M},\mathtt{a})}$ is in the support of s'_I. Since $(\mathcal{M}, \mathtt{a}) \models Min(\phi, a, \underline{i})$ holds, for every $i \in \underline{i}$ there is a representative $\Sigma_I(\underline{i})$-term t such that $(\mathcal{M}, \mathtt{a}) \models t\sigma = i$ holds. The latter means that i is in the support of s'_I, hence the inclusion μ is onto.

Conversely, if s belongs to a basis of of K, then no $s' \leq s$ is in $[\![K]\!]$, unless s' is equivalent to s, by Lemma A.6. Suppose that $(\mathcal{M}, \mathtt{a}) \models \phi(\underline{i}\sigma, a[\underline{i}\sigma])$ holds for a substitution σ whose domain is $\underline{i}$ and whose range is included into the set of representative $\Sigma_I(\underline{i})$-terms. For reductio, suppose that $(\mathcal{M}, \mathtt{a}) \models t\sigma = i$ does not hold for some $i \in \underline{i}$ and all representative $\Sigma_I(\underline{i})$-terms t; we can restrict the array a to the Σ_I-substructure given by the elements of the kind $t\sigma^{(\mathcal{M},\mathtt{a})}$, thus getting a configuration $s' \leq s$ such that $s' \in [\![K]\!]$. Since the finite support of s'_I has smaller cardinality than the support of s_I (because $\mathtt{a}(i)$ does not belong to it), we cannot have $s' \approx s$, contradiction. □

Let us now prove Proposition 4.8:

[19] To make the statement of the lemma precise, one should define not just s but also the finite index model where s is taken from. In detail, we take the A_E^I-model $\mathcal{N}$ whose Σ_I-reduct is the restriction of $\mathcal{M}_I$ to the Σ_I-substructure generated by the $\mathtt{a}(\underline{i})$'s and whose Σ_E-reduct is equal to $\mathcal{M}_E$. Within this model, we can define the array s to be the restriction of $\mathtt{a}(a)$ to $\mathtt{INDEX}^{\mathcal{N}} \subseteq \mathtt{INDEX}^{\mathcal{M}}$. The pair $(s, \mathcal{N})$ is now a configuration in the sense defined in Section 4.1.

Proposition 4.8 *Suppose that T_E is locally finite. Let $K := \exists \underline{i}\, \phi(\underline{i}, a[\underline{i}])$ be an $\exists^I$-formula and let L be a further $\exists^I$-formula. The following two conditions are equivalent:*

(i) *for every s in a basis for K there exists a configuration s' in a basis for L such that $s \leq s'$;*

(ii) *L is (up to A_E^I-equivalence) of the form $\exists \underline{i} \exists \underline{j} \psi(\underline{i}, \underline{j}, a[\underline{i}], a[\underline{j}])$ for a quantifier-free formula ψ and*

$$\text{if } A_I^E \models Min(\psi, a, \underline{i}\,\underline{j}) \rightarrow \theta(\underline{t}, a[\underline{t}]) \quad \text{ then } \quad A_I^E \models Min(\phi, a, \underline{i}) \rightarrow \theta(\underline{t}, a[\underline{t}]).$$

for all quantifier free $(\Sigma_E \cup \Sigma_I)$-formula θ and for all tuple of terms $\underline{t}(\underline{i})$ taken from the set of the representative $\Sigma_I(\underline{i})$-terms.

Proof. Assume (i). We first apply a syntactic transformation to L as follows. Let B, B' be bases for K, L, respectively; we know that for every $(s, \mathcal{M}_s) \in B$ there is $(s^L, \mathcal{M}_s^L) \in B'$ such that $s \leq s^L$: the relationship $s \leq s^L$ is due to the existence of a pair of embeddings (μ_s, ν_s) as required by the configuration ordering definition. For every $s \in B$ and for every assignment $\mathtt{a}$ such that $\mathtt{a}(a) = s$ and $(\mathcal{M}_s, \mathtt{a}) \models \phi(\underline{i}, a[\underline{i}])$, we build the diagram formula $K_{\mathtt{a}}$ for s^L given by

$$\exists \underline{i}\, \exists \underline{k}\, (\delta_{s_I^L}(\underline{i}, \underline{k}) \wedge \delta_{s_E^L}(a[\underline{i}], a[\underline{k}])) \tag{16}$$

where the variables $\underline{k}$ are names for the elements in the complement subset $supp(s_I^L) \backslash \mu_s(\mathtt{a}(\underline{i}))$ (here $supp(s_I^L)$ is the support of the Σ_I-structure s_I^L). Notice that the formula (16) is nothing but the formula (11) used in the proof of Proposition 4.4(i).[20] Since, for a configuration t, the fact that $t \in [\![K_{\mathtt{a}}]\!]$ means that there are suitable embeddings witnessing that $s^L \leq t$, we have that $[\![L]\!] = [\![L \vee \bigvee_{\mathtt{a}} K_{\mathtt{a}}]\!]$, hence by Proposition A.1 the formula L is A_E^I-equivalent to $L \vee \bigvee_{\mathtt{a}} K_{\mathtt{a}}$.[21] Up to logical equivalence, we can move the existentially quantified variables outside the disjunctions so that L is equivalent to a prenex existential formula of the kind $\exists \underline{i} \exists \underline{j} \psi$. With this new syntactic form, the following property holds: for every $s \in B$ and for every assignment $\mathtt{a}$ such that $\mathtt{a}(a) = s$ and $(\mathcal{M}_s, \mathtt{a}) \models \phi(\underline{i}, a[\underline{i}])$, there is an assignment $\mathtt{a}_L$ such that (i) $(\mathcal{M}_s^L, \mathtt{a}^L) \models \psi(\underline{i}, \underline{j}, a[\underline{i}], a[\underline{j}])$, (ii) $\mathtt{a}^L(\underline{i}) = \mu_s(\mathtt{a}(\underline{i}))$, and (iii) $\mathtt{a}^L(a) = s^L$. Since s^L is in a basis of L, from Lemma A.7, it follows also that $(\mathcal{M}_s^L, \mathtt{a}^L) \models Min(\psi, a, \underline{i}\,\underline{j})$.

Suppose now that $A_E^I \not\models Min(\phi, a, \underline{i}) \rightarrow \theta(\underline{t}(\underline{i}), a[\underline{t}(\underline{i})])$; by Lemma A.7 (and by the fact that ϕ, θ are quantifier-free) this means that there are a configuration $(s, \mathcal{M}_s) \in B$ and an

[20] It might happen here that duplicate variables are used because the $\mathtt{a}(\underline{i})$ need not be distinct. This is not a problem: if different index variables (say i_1, i_2) naming the same element are employed, the diagram formula will contain a conjunct like $i_1 = i_2$. The embedding property of Robinson Diagram Lemma is not affected by these duplications.

[21] The assignments are infinite, but only finitely many variables are really involved in them, so that only finitely many formulae $K_{\mathtt{a}}$ can be produced.

assignment $\mathtt{a}$ such that $(\mathcal{M}_s, \mathtt{a}) \models \phi(\underline{i}, a[\underline{i}])$ and $(\mathcal{M}_s, \mathtt{a}) \not\models \theta(\underline{t}, a[\underline{t}])$. Since θ is quantifier-free, taking the assignment $\mathtt{a}^L$ satisfying (i)-(ii)-(iii) above, we get that $(\mathcal{M}_s^L, \mathtt{a}^L) \not\models \theta(\underline{t}, a[\underline{t}])$, thus also $(\mathcal{M}_s^L, \mathtt{a}^L) \not\models Min(\psi, a, \underline{i}\,\underline{j}) \rightarrow \theta(\underline{t}, a[\underline{t}])$.

Conversely, assume (ii). Fix s in a basis B for K and an assignment $\mathtt{a}$ such that $(\mathcal{M}_s, \mathtt{a}) \models \phi(\underline{i}, a[\underline{i}])$; by Lemma A.7, $(\mathcal{M}_s, \mathtt{a}) \models Min(\phi, a, \underline{i})$ follows. Let $\theta(\underline{t}(\underline{i}), a[\underline{t}(\underline{i})])$ be the negation of the formula $\delta_{s_I}(\underline{t}(\underline{i})) \wedge \delta_{s_E}(a[\underline{t}(\underline{i})])$.[22] We have $(\mathcal{M}_s, \mathtt{a}) \not\models Min(\phi, a, \underline{i}) \rightarrow \theta(\underline{t}, a[\underline{t}])$, hence there are $\mathcal{N}$ and $\mathtt{b}$ such that $(\mathcal{N}, \mathtt{b}) \not\models Min(\psi, a, \underline{i}\,\underline{j}) \rightarrow \theta(\underline{t}, a[\underline{t}])$. By restricting the support of $\mathcal{N}_I$ if needed, we can suppose that $\mathcal{N}$ is a finite index model and that $\mathcal{N}_I$ is generated by the elements assigned by $\mathtt{b}$ to the $\underline{i}, \underline{j}$. Let s' be $\mathtt{b}(a)$: from Lemma A.7 it follows that s' is in a basis for L; also, from the fact that $(\mathcal{N}, \mathtt{b}) \not\models \theta(\underline{t}, a[\underline{t}])$, we can conclude that $s \leq s'$, as wanted. □

As an application of Proposition 4.8, we now *justify the claim in Section 4.3.* Let Σ_I be a relational signature and let T_E be locally finite and admit quantifier elimination; we show that $K \leq L$ holds in case

- L is the A_E^I-consistent primitive differentiated $\exists^I$-formula $\exists \underline{i}\, \exists \underline{j}\, (\delta_I(\underline{i}) \wedge \psi_I(\underline{i}, \underline{j}) \wedge \psi_E(a[\underline{i}], a[\underline{j}]))$, where δ_I, ψ_I, ψ_E satisfy the conditions (i)-(iv) of the claim in Section 4.3.
- K is $\exists \underline{i}\, (\delta_I(\underline{i}) \wedge \phi_E(a[\underline{i}]))$, where $\phi_E(\underline{e})$ is T_E-equivalent to $\exists \underline{d}\, \psi_E(\underline{e}, \underline{d})$.

We use Proposition 4.8(ii): as remarked in Section 4, since L and K are differentiated, we can avoid mentioning the corresponding formulae Min in the condition of Proposition 4.8(ii) and just prove that

$$A_E^I \not\models \quad \delta_I(\underline{i}) \wedge \phi_E(a[\underline{i}]) \rightarrow \theta(\underline{i}, a[\underline{i}]) \quad \Rightarrow$$
$$\Rightarrow \quad A_E^I \not\models \delta_I(\underline{i}) \wedge \psi_I(\underline{i}, \underline{j}) \wedge \psi_E(a[\underline{i}], a[\underline{j}]) \rightarrow \theta(\underline{i}, a[\underline{i}])$$

(notice that, since Σ_I is relational, the only $\Sigma_I(\underline{i})$-terms are the $\underline{i}$). Pick a model $\mathcal{M}$ and an assignment $\mathtt{a}$ such that $(\mathcal{M}, \mathtt{a}) \models \delta_I(\underline{i}) \wedge \phi_E(a[\underline{i}])$ and $(\mathcal{M}, \mathtt{a}) \not\models \theta(\underline{i}, a[\underline{i}])$. We can freely assume that that the support of $\mathcal{M}_I$ is a Σ_I-structure generated by the $\mathtt{a}(\underline{i})$; by modifying the value of $\mathtt{a}$ on the element variables $\underline{d}$, if needed, we can also assume that $(\mathcal{M}, \mathtt{a}) \models \psi_E(a[\underline{i}], \underline{d})$ (this is because $\phi_E(\underline{e})$ is T_E-equivalent to $\exists \underline{d}\, \psi_E(\underline{e}, \underline{d})$). Since L is consistent, there are also a model $\mathcal{N}$ and an assignment $\mathtt{b}$ such that $(\mathcal{N}, \mathtt{b}) \models \delta_I(\underline{i}) \wedge \psi_I(\underline{i}, \underline{j}) \wedge \psi_E(a[\underline{i}], a[\underline{j}])$. Again, we can assume

[22] Again, this is the conjunction of two Robinson diagram formulae, it is the same as the formula (11) used in the proof of Proposition 4.4(i): the only difference is that now the $\underline{i}$ at our disposal are only generators for s_I - they do not name the whole support of s_I. As a consequence, we use $\underline{t}(\underline{i})$ and $a[\underline{t}(\underline{i})]$ (varying $\underline{t}$ among representative $\Sigma_I(\underline{i})$-terms) as generators for s_I and s_E (the former choice is redundant, but the latter is not, as the $a[\underline{i}]$ are not sufficient anymore to generate s_E).

that the support of $\mathcal{N}_I$ is a Σ_I-structure generated by the $\mathtt{a}(\underline{i},\underline{j})$; since $\delta_I(\underline{i})$ is maximal, it is a diagram formula, hence (up to an isomorphism) $\mathcal{M}_I$ is a substructure of $\mathcal{N}_I$. Let us now take the model $\mathcal{N}'$, whose Σ_I-reduct is $\mathcal{N}_I$ and whose Σ_E-reduct is $\mathcal{M}_E$. Let $\mathtt{b}'$ be the assignment which is like $\mathtt{b}$ as far as the index variables $\underline{i},\underline{j}$ are concerned and which associates with the variable a the array whose $\mathtt{b}'(\underline{i})$-values are the $\mathtt{b}'(\underline{i}) = \mathtt{a}(\underline{i})$-values of $\mathtt{a}(a)$ and whose $\mathtt{b}'(\underline{j})$-values are the $\underline{d}$ (notice that this is correct because by differentiatedness of L the $\mathtt{b}'(\underline{i}\underline{j})$ are all distinct). It turns out that $(\mathcal{N}',\mathtt{b}') \not\models \delta_I(\underline{i}) \wedge \psi_I(\underline{i},\underline{j}) \wedge \psi_E(a[\underline{i}],a[\underline{j}]) \rightarrow \theta(\underline{i},a[\underline{i}])$, as desired. □

Proposition 4.8 is mainly used as a theoretical tool in order to justify heuristics like that mentioned in Section 4.2 (which is based on the claim in Section 4.3). Nevertheless, it is important to remark the following fact mentioned in Section 4.1:

Proposition A.8. *Given an $\exists^I$-formula L, there are only finitely many $\exists^I$-formulae K such that $K \leq L$ and all such K can be effectively computed.*

Proof. This claim can be justified by using both the criterion of Proposition 4.8(i) and the criterion of Proposition 4.8(ii). Let us show in detail *how to use the latter* (which is entirely symbolic): let L be given. Suppose that L is $\exists\underline{k}\gamma$: to use the criterion of Proposition 4.8(ii) in an effective way, we only have to find a bound for the length of the tuples $\underline{i}$ and $\underline{j}$. In fact, once that bound is known the search space for the formulae $\exists\underline{i}\,\exists\underline{j}\,\psi$ and $\exists\underline{i}\,\phi$ satisfying the conditions (to be tested by the algorithm of Theorem 3.2)

$$A^I_E \models \exists\underline{k}\gamma \leftrightarrow \exists\underline{i}\,\exists\underline{j}\,\psi, \qquad \text{and for all } \theta(\underline{t}(\underline{i}),a[\underline{t}(\underline{i})])$$
$$A^I_E \models Min(\psi,a,\underline{i}\,\underline{j}) \rightarrow \theta(\underline{t},a[\underline{t}]) \quad \Rightarrow \quad A^I_E \models Min(\phi,a,\underline{i}) \rightarrow \theta(\underline{t},a[\underline{t}]).$$

is finite: this is because T_I and T_E are both locally finite and hence there are only finitely many non A^I_E-equivalent quantifier-free formulae of the required type involving a fixed number of index variables. The proof of Proposition 4.8 shows that the sum of the lengths of $\underline{i}$ and $\underline{j}$ can be bounded by the maximum cardinality N of the support of s_I, where s_I is a configuration that belongs to a basis for $L \equiv \exists\underline{k}\,\gamma$: this means that N cannot exceed the number of the representative $\Sigma_I(\underline{k})$-terms. □

We now prove our main Theorem, justifying the algorithm for invariant synthesis:

Theorem 4.9 *Suppose that T_E is locally finite. There exists a safety invariant for U iff (for a suitable* ChooseCover *function) the Algorithm of Figure 1 (b) returns the negation of a safety invariant for U.*

Proof. Suppose that the Algorithm returns B after $k+1$ iterations of the loop: we show that

$\neg B$ is a safety invariant. Notice that B is a disjunction $P_0 \vee \cdots \vee P_k$ of $\exists^I$-formulae such that for all $i = 0, \ldots, k$,

(I) the formula $I \wedge P_i$ is not A_E^I-satisfiable;

also P_i covers $Pre(\tau, P_{i-1})$ and P_0 covers U, which means in particular that

(II) $A_E^I \models \forall a\,(Pre(\tau, P_{i-1})(a) \rightarrow P_i(a))$ and $A_E^I \models \forall a\,(U(a) \rightarrow P_0(a))$.

Finally, the Algorithm could exit the loop because for some P_{k+1} covering $Pre(\tau, P_k)$, it happened that $P_{i+1} \wedge \neg B$ was not A_E^I-consistent: these two conditions entail that

(III) $A_E^I \models \forall a\,(Pre(\tau, P_k)(a) \rightarrow B(a))$.

Conditions (i) and (iii) of Definition 4.2 now easily follows from (I) and (II); we only need to check condition (ii) of Definition 4.2, namely (up to logical equivalence) that $A_I^E \models \forall a\,(Pre(\tau, B)(a) \rightarrow B(a))$: since $Pre(\tau, B)$ is logically equivalent to the disjunction $\bigvee_{i=0}^{n} Pre(\tau, P_i)$, the claim follows immediately from (II)-(III).

Let us now prove the converse, i.e. that in case a safety invariants exists, the Algorithm of Figure 1 (b) is able to produce one. Recall the proof of Theorem 4.7: given the negation H of a safety invariant for U, another negation L of a safety invariant for U is produced in the following way. Define the sequence of $\exists^I$-formulae L_i: (i) $L_0 := \gamma(U)$ and (ii) $L_{i+1} := L_i \vee \gamma(Pre(\tau, L_i))$. Our L is the smallest i for which we have that L_{i+1} is A_E^I-equivalent to L_i (the proof of Theorem 4.7 guarantees that such i exists).

The above recursive definitions for L_i are based on the function γ, which is defined (non symbolically) by making use of configurations. Actually, for an $\exists^I$-formula S such that $[\![S]\!] \subseteq [\![H]\!]$, the function $\gamma(S)$ returns an $\exists^I$-formula $K_{a_1} \vee \cdots \vee K_{a_n}$, where $\{a_1, \ldots, a_n\} \subseteq [\![H]\!]$ is a minimal set of configurations taken from a basis of H such that $[\![S]\!] \subseteq \uparrow a_1 \cup \cdots \cup \uparrow a_n$. Using Proposition 4.8, we can see that the minimality condition implies that $\gamma(S) \leq S$: in fact, condition $[\![S]\!] \subseteq \uparrow a_1 \cup \cdots \cup \uparrow a_n$ says that for every s in a basis for S there is a_i in the basis $\{a_1, \ldots, a_n\}$ for $\gamma(S)$ such that $a_i \leq s$, but the converse must hold too, by minimality.[23] Thus $\gamma(S)$ is such that $\gamma(S) \leq S$ and $A_E^I \models S \rightarrow \gamma(S)$, i.e. $\gamma(S)$ covers S.

It is then clear that an appropriate choice of the function ChooseCover in the Algorithm of Figure 1 (b) can produce precisely the formulae L_i for assignment to the variable B at the ith-loop of the Algorithm, thus justifying the claim of the Theorem. □

[23] In more detail: after dropping a_i, the relation

$$[\![S]\!] \subseteq \uparrow a_1 \cup \cdots \cup \uparrow a_{i-1} \cup \uparrow a_{i+1} \cup \cdots \cup \uparrow a_n$$

does not hold, hence there is s from a basis of S such that $a_j \not\leq s$ for all $j = 1, \ldots, i-1, i+1, \ldots n$. Since on the contrary $[\![S]\!] \subseteq \uparrow a_1 \cup \cdots \cup \uparrow a_n$ holds, we must conclude that $a_i \leq s$. Hence for every a_i there is s in a basis of S such that $a_i \leq s$.

A.4 Proof of the results in Section 4.2

We only miss the proof of the following soundness result:

Proposition 4.10 *Suppose that T_E is locally finite. If the procedure* BReach+Inv *terminates and returns safe (resp. unsafe), then $\mathcal{S}$ is safe (resp. unsafe) with respect to U.*

Proof. The claim for the unsafe case is trivial. Suppose that the Algorithm terminates by displaying a safety message at the $(k+1)$-th iteration of the main loop. Observe that, at this $(k+1)$-th iteration of the main loop, the content of the variable B is

$$Pre^0(\tau, U) \vee Pre^1(\tau, U) \vee \cdots \vee Pre^k(\tau, U) \vee H_1 \vee \cdots \vee H_m \tag{17}$$

where $H_1, \ldots, H_m$ are negations of invariants (see Property 2). For reductio, suppose that the system is unsafe: this means that for some n the formula (2)

$$I(a_n) \wedge \tau(a_n, a_{n-1}) \wedge \cdots \wedge \tau(a_1, a_0) \wedge U(a_0)$$

is consistent. Let it be satisfied by the arrays $s_n, \ldots, s_0$ in a model of A_E^I: we say that $s_n, \ldots, s_0$ are a *bad trace*, let they be a bad trace of shortest length. Since the formulae $I \wedge Pre^0(\tau, U), I \wedge Pre^1(\tau, U), \ldots I \wedge Pre^k(\tau, U)$ are all A_E^I-inconsistent (see Line 3 of BReach+Inv), n must be bigger than k. Let us now focus on s_{k+1}; since the Algorithm displays a safety message at step $k+1$, it must have exited the loop because the formula in the current value of P (which is $Pre^{k+1}(\tau, U)$) is not A_E^I-consistent with the negation of the formula in the current value of B (which is (17)). Thus s_{k+1} (which satisfies $Pre^{k+1}(\tau, U)$) must satisfy either some Pre^l (for $l < k+1$) or some H_i, but both alternative are impossible. In fact, the former would yield a shorter bad trace, whereas the latter is in contrast to the fact that s_{k+1} is forward reachable from a state satisfying I and, as such, it should satisfy the invariant $\neg H_i$. □

B A tricky example

We include a hand-made example which is instructive because it clearly explains the difference between the fully symbolic approach of MTMC and that underlying other state-of-the art tools like PFS and UNDIP. One may think that the main difference between MTMC and these tools lies just in the technology for constraint satisfiability: MTMC would simply use an SMT-solver where other tools use efficient but dedicated algorithm. This is not the case: MTMC produces much less nodes in the backward search tree because *it represents symbolically the system topology*. To illustrate this fundamental aspect we employ an example.

Let T_I is the theory of linear orders and T_E be an enumerated datatype with 15 constants denoted by the numeral from 1 to 15. Consider the following parametrized system having 7 transitions and 15 control locations:

- transition 1 allows process i to move from location 1 to location 2 provided there is a process j to the right of i (i.e. $i < j$ holds) which is on location 9;
- similarly, transition 2 allows process i to move from location 2 to location 3 provided there is a process j to the right of i which is on location 10, and so on (the last transition allows process i to move from location 7 to location 8 provided there is a process j to the right of i which is on location 15).

Initially, all processes are in location 1. We consider the following safety problem: is it possible for a process to reach location 8? The answer is obviously no.

MCMT solves the problem by generating 7 nodes in only 0.03 sec. On the contrary, PFS takes about 4 minutes and generates thousands of constraints.

Why is this so? The point is that tools like PFS based on some form of rewriting semantics for transitions do not symbolically represent the system topology and need to specify the relative positions of all the involved processes. In contrast, MTMC can handle partial information like "there exists 7 processes to the right of i whose locations are from 9 to 15, respectively" just because it is based on an entirely deductive symbolic engine (the SMT solver). The gain is dramatic because there is no need of listing all permutations!

Thus, MTMC represents a fully declarative approach to infinite state model checking that, if coupled with appropriate heuristics, should pave the way to the verification of systems with ever more complex topologies that other tools (like PFS) cannot handle.

C A worked out example: Szymanski

Below, we show how MCMT solves the safety problem for the Szymanski algorithm ensuring mutual exclusion. Most of the text below is automatically generated by our tool. We have added some explanations about our techniques for invariant synthesis (this text is in *slanted*). Figures 2 and 3 are also automatically generated by our tool. It outputs the tree (defined in Section 3.10 in the dot format of GraphViz which is then used to generate the figures. Figure 4 has been manually derived from a comparison between the previous two (however, also this operation can be automated).

First (Section C.1), we present the formalization of Szymanski algorithm as an array-based system and then we show the formulae representing the set of backward reachable states without (Section C.2)/with (Section C.3) using invariants.

Remark. The output below has been obtained with the version 0.1 of MCMT with the default setting (which applies a flexible instantiation strategy). So, more recent releases of the tool and different settings may give different results. The point we would like to make below is the dramatic gains that one may obtain by using automatically derived invariants to prune the search space of the tool.

C.1 Szymanski algorithm as an array-based system

Auxiliary declarations

There are 8 *distinct control locations for each process. In particular, control location* `8` *corresponds to the 'crash' state.*

- `(define-type locations (subrange 1 8))`

Array variables

The state of the algorithm is composed of three arrays; `a` *for the program counter,* `s` *and* `w` *for two Boolean flags. Intuitively, this formalizes a parametrized system where each process has three local variables: one storing the control locations and two containing Boolean flags.*

- `a : int` $\longrightarrow$ `locations` (program counter)
- `s : int` $\longrightarrow$ `bool`
- `w : int` $\longrightarrow$ `bool`

Initial states

At the beginning, all processes are at control location `1` *and the two Boolean flags are set to false.*

$$I(\mathtt{a},\mathtt{s},\mathtt{w}) \;:=\; \forall \mathtt{x}.(\wedge\ (\mathtt{a[x]=1})\ (\mathtt{s[x]}=\bot)\ (\mathtt{w[x]}=\bot))$$

A conjunction of literals

$$L_1 \wedge \cdots \wedge L_n \quad \textit{is written as} \quad (\wedge\ L_1 \ldots L_n)$$

for $n \geq 1$.

Unsafe states

An unsafe state is one where two processes at control location `7` *which corresponds to the critical section.*

$$U(\mathtt{a},\mathtt{s},\mathtt{w}) \;:=\; \exists \mathtt{x},\mathtt{y}.(\wedge\ \mathtt{(a[x]=7)}\ \mathtt{(x<y)}\ \mathtt{(a[y]=7)})$$

Transitions

Roughly, there are two cases describing the behavior of the system. First, if a process i fires transitions τ_1 and τ_2 while the other processes remain in the initial states. Since these processes are at control location `1`*, transition τ_3 is enabled for process i. After taking τ_3, process i is at control location* `5`*, τ_1 is disabled for all processes $j \neq i$ since the Boolean flag* `s` *is set to true. Then, i can fire τ_6 followed by τ_7, thereby accessing the critical section (i.e. going to control location* `7`*). Finally, process i moves back to control location* `1`*, and resets the flag* `s` *to false, thus enabling transition τ_1 for all the other processes.*

The second case is the following. Some processes may fire transition τ_2 and then τ_3 while all the other remain at control location `1`*. If process i fires τ_3, then τ_3 becomes disabled for all other processes at control location* `3`*. At the same time, process i is blocked at control location* `5` *since the processes not at control location* `1` *have set* `w` *to true thus disabling transition τ_6. However, for processes at control location* `3` *both transitions τ_4 and τ_5 are enabled. The process i (at control location* `5` *with* `s` *set to true and* `w` *set to false) is blocked until such processes will go to control location* `5`*. In this case, all processes can move to control location* `6`*. Then, among all processes at control location* `6`*, only the leftmost process can fire transition τ_7.*

$$\tau(\mathtt{a},\mathtt{s},\mathtt{w},\mathtt{a}',\mathtt{s}',\mathtt{w}') \;:=\; \bigvee_{h=1}^{8} \tau_h(\mathtt{a},\mathtt{s},\mathtt{w},\mathtt{a}',\mathtt{s}',\mathtt{w}')$$

where

- $\tau_1(\mathtt{a},\mathtt{s},\mathtt{w},\mathtt{a}',\mathtt{s}',\mathtt{w}') \;:=$

$$\exists \mathtt{x}.\left(\begin{array}{l} G_1(\mathtt{x},\mathtt{a[x]},\mathtt{s[x]},\mathtt{w[x]}) \quad \wedge \\ (\mathtt{a}',\mathtt{s}',\mathtt{w}') = \lambda \mathtt{j}.\overline{F_1}(\mathtt{x},\mathtt{j},\mathtt{a[x]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[j]}) \end{array}\right)$$

where

$$
\begin{aligned}
G_1(\mathtt{x},\mathtt{a[x]},\mathtt{s[x]},\mathtt{w[x]}) &:= \mathtt{(= a[x]\ 1)} \\
F_1(\mathtt{x},\mathtt{j},\mathtt{a[x]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[j]}) &:= \mathtt{case\ of\ \ \{} \\
\mathtt{(= j\ x)} &: (2,\mathtt{s[j]},\mathtt{w[j]}) \\
\mathtt{(= s[j]}\ \bot\mathtt{)} &: (\mathtt{a[j]},\mathtt{s[j]},\mathtt{w[j]}) \\
\mathtt{(}\neg\mathtt{(= s[j]}\ \bot\mathtt{))} &: (8,\mathtt{s[j]},\mathtt{w[j]}) \\
&\}
\end{aligned}
$$

- $\tau_2(\mathtt{a},\mathtt{s},\mathtt{w},\mathtt{a}',\mathtt{s}',\mathtt{w}') :=$

$$\exists \mathtt{x}.\left(\begin{array}{l} G_2(\mathtt{x},\mathtt{a[x]},\mathtt{s[x]},\mathtt{w[x]}) \ \ \wedge \\ (\mathtt{a}',\mathtt{s}',\mathtt{w}') = \lambda \mathtt{j}.\overline{F_2}(\mathtt{x},\mathtt{j},\mathtt{a[x]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[j]}) \end{array}\right)$$

where

$$
\begin{aligned}
G_2(\mathtt{x},\mathtt{a[x]},\mathtt{s[x]},\mathtt{w[x]}) &:= \mathtt{(= a[x]\ 2)} \\
F_2(\mathtt{x},\mathtt{j},\mathtt{a[x]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[j]}) &:= \mathtt{case\ of\ \ \{} \\
\mathtt{(= j\ x)} &: (3,\top,\top) \\
\mathtt{(}\neg\mathtt{(= j\ x))} &: (\mathtt{a[j]},\mathtt{s[j]},\mathtt{w[j]}) \\
&\}
\end{aligned}
$$

- $\tau_3(\mathtt{a},\mathtt{s},\mathtt{w},\mathtt{a}',\mathtt{s}',\mathtt{w}') :=$

$$\exists \mathtt{x}.\left(\begin{array}{l} G_3(\mathtt{x},\mathtt{a[x]},\mathtt{s[x]},\mathtt{w[x]}) \ \ \wedge \\ (\mathtt{a}',\mathtt{s}',\mathtt{w}') = \lambda \mathtt{j}.\overline{F_3}(\mathtt{x},\mathtt{j},\mathtt{a[x]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[j]}) \end{array}\right)$$

where

$$
\begin{aligned}
G_3(\mathtt{x},\mathtt{a[x]},\mathtt{s[x]},\mathtt{w[x]}) &:= \mathtt{(= a[x]\ 3)} \\
F_3(\mathtt{x},\mathtt{j},\mathtt{a[x]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[j]}) &:= \mathtt{case\ of\ \ \{} \\
\mathtt{(= j\ x)} &: (5,\mathtt{s[j]},\bot) \\
\mathtt{(= a[j]\ 1)} &: (\mathtt{a[j]},\mathtt{s[j]},\mathtt{w[j]}) \\
\mathtt{(}\neg\mathtt{(= a[j]\ 1))\ (= w[j]}\ \top\mathtt{)} &: (\mathtt{a[j]},\mathtt{s[j]},\mathtt{w[j]}) \\
\mathtt{(}\neg\mathtt{(= a[j]\ 1))\ (}\neg\mathtt{(= w[j]}\ \top\mathtt{))} &: (8\ ,\mathtt{s[j]},\mathtt{w[j]}) \\
&\}
\end{aligned}
$$

- $\tau_4(\mathtt{a},\mathtt{s},\mathtt{w},\mathtt{a}',\mathtt{s}',\mathtt{w}') :=$

$$\exists \mathtt{x},\mathtt{y}.\left(\begin{array}{l} G_4(\mathtt{x},\mathtt{y},\mathtt{a[x]},\mathtt{a[y]},\mathtt{s[x]},\mathtt{s[y]},\mathtt{w[x]},\mathtt{w[y]}) \ \ \wedge \\ (\mathtt{a}',\mathtt{s}',\mathtt{w}') = \lambda \mathtt{j}.\overline{F_4}(\mathtt{x},\mathtt{y},\mathtt{j},\mathtt{a[x]},\mathtt{a[y]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[y]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[y]},\mathtt{w[j]}) \end{array}\right)$$

where

$$G_4(\mathtt{x},\mathtt{y},\mathtt{a[x]},\mathtt{a[y]},\mathtt{s[x]},\mathtt{s[y]},\mathtt{w[x]},\mathtt{w[y]}) :=$$
$$\mathtt{(= a[x]\ 3)}\ \ \mathtt{(\neg(= x\ y))}\ \ \mathtt{(\neg(= a[y]\ 1))}\ \ \mathtt{(= w[y]}\ \bot\mathtt{)}\ \ \mathtt{(\neg(= a[y]\ 8))}$$

$$\begin{array}{rcl} F_4(\mathtt{x},\mathtt{y},\mathtt{j},\mathtt{a[x]},\mathtt{a[y]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[y]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[y]},\mathtt{w[j]}) & := & \mathtt{case\ of\ \ \{} \\ \mathtt{(= j\ x)} & : & (4,\bot,\mathtt{w[j]}) \\ \mathtt{(\neg(= j\ x))} & : & (\mathtt{a[j]},\mathtt{s[j]}\ ,\mathtt{w[j]}\ ) \\ & & \mathtt{\}} \end{array}$$

- $\tau_5(\mathtt{a},\mathtt{s},\mathtt{w},\mathtt{a}',\mathtt{s}',\mathtt{w}') :=$

$$\exists \mathtt{x},\mathtt{y}.\left(\begin{array}{l} G_5(\mathtt{x},\mathtt{y},\mathtt{a[x]},\mathtt{a[y]},\mathtt{s[x]},\mathtt{s[y]},\mathtt{w[x]},\mathtt{w[y]}) \ \ \wedge \\ (\mathtt{a}',\mathtt{s}',\mathtt{w}') = \lambda \mathtt{j}.\overline{F_5}(\mathtt{x},\mathtt{y},\mathtt{j},\mathtt{a[x]},\mathtt{a[y]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[y]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[y]},\mathtt{w[j]}) \end{array}\right)$$

where

$$G_5(\mathtt{x},\mathtt{y},\mathtt{a[x]},\mathtt{a[y]},\mathtt{s[x]},\mathtt{s[y]},\mathtt{w[x]},\mathtt{w[y]}) :=$$
$$\mathtt{(= a[x]\ 4)}\ \ \mathtt{(\neg(= x\ y))}\ \ \mathtt{(= s[y]}\ \top\mathtt{)}\ \ \mathtt{(= w[y]}\ \bot\mathtt{)}\ \ \mathtt{(\neg(= a[y]\ 8))}$$

$$\begin{array}{rcl} F_5(\mathtt{x},\mathtt{y},\mathtt{j},\mathtt{a[x]},\mathtt{a[y]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[y]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[y]},\mathtt{w[j]}) & := & \mathtt{case\ of\ \ \{} \\ \mathtt{(= j\ x)} & : & (5,\top,\bot) \\ \mathtt{(\neg(= j\ x))} & : & (\mathtt{a[j]},\mathtt{s[j]},\mathtt{w[j]}) \\ & & \mathtt{\}} \end{array}$$

- $\tau_6(\mathtt{a},\mathtt{s},\mathtt{w},\mathtt{a}',\mathtt{s}',\mathtt{w}') :=$

$$\exists \mathtt{x}.\left(\begin{array}{l} G_6(\mathtt{x},\mathtt{a[x]},\mathtt{s[x]},\mathtt{w[x]}) \ \ \wedge \\ (\mathtt{a}',\mathtt{s}',\mathtt{w}') = \lambda \mathtt{j}.\overline{F_6}(\mathtt{x},\mathtt{j},\mathtt{a[x]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[j]}) \end{array}\right)$$

where

$$\begin{array}{rcl} G_6(\mathtt{x},\mathtt{a[x]},\mathtt{s[x]},\mathtt{w[x]}) & := & \mathtt{(= a[x]\ 5)} \\ F_6(\mathtt{x},\mathtt{j},\mathtt{a[x]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[j]}) & := & \mathtt{case\ of\ \ \{} \\ \mathtt{(= j\ x)} & : & (6\ ,\mathtt{s[j]},\mathtt{w[j]}) \\ \mathtt{(= w[j]}\ \bot\mathtt{)} & : & (\mathtt{a[j]},\mathtt{s[j]},\mathtt{w[j]}) \\ \mathtt{(\neg(= w[j]}\ \bot\mathtt{))} & : & (8,\mathtt{s[j]},\mathtt{w[j]}) \\ & & \mathtt{\}} \end{array}$$

- $\tau_7(\mathtt{a},\mathtt{s},\mathtt{w},\mathtt{a}',\mathtt{s}',\mathtt{w}') :=$

$$\exists \mathtt{x}.\left(\begin{array}{l} G_7(\mathtt{x},\mathtt{a[x]},\mathtt{s[x]},\mathtt{w[x]}) \quad \wedge \\ (\mathtt{a}',\mathtt{s}',\mathtt{w}') = \lambda \mathtt{j}.\overline{F_7}(\mathtt{x},\mathtt{j},\mathtt{a[x]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[j]}) \end{array}\right)$$

where

$$\begin{array}{rcl} G_7(\mathtt{x},\mathtt{a[x]},\mathtt{s[x]},\mathtt{w[x]}) & := & \mathtt{(=\ a[x]\ 6)} \\ F_7(\mathtt{x},\mathtt{j},\mathtt{a[x]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[j]}) & := & \mathtt{case\ of\ \ \{} \\ \mathtt{(=\ j\ x)} & : & (7,\mathtt{s[j]},\mathtt{w[j]}) \\ \mathtt{(<\ x\ j)} & : & (\mathtt{a[j]},\mathtt{s[j]},\mathtt{w[j]}) \\ \mathtt{(<\ j\ x)\ (=\ s[j]}\ \bot\mathtt{)} & : & (\mathtt{a[j]},\mathtt{s[j]},\mathtt{w[j]}) \\ \mathtt{(<\ j\ x)\ (\neg(=\ s[j]}\ \bot\mathtt{))} & : & (8,\mathtt{s[j]},\mathtt{w[j]}) \\ \multicolumn{3}{r}{\}} \end{array}$$

- $\tau_8(\mathtt{a},\mathtt{s},\mathtt{w},\mathtt{a}',\mathtt{s}',\mathtt{w}') :=$

$$\exists \mathtt{x}.\left(\begin{array}{l} G_8(\mathtt{x},\mathtt{a[x]},\mathtt{s[x]},\mathtt{w[x]}) \quad \wedge \\ (\mathtt{a}',\mathtt{s}',\mathtt{w}') = \lambda \mathtt{j}.\overline{F_8}(\mathtt{x},\mathtt{j},\mathtt{a[x]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[j]}) \end{array}\right)$$

where

$$\begin{array}{rcl} G_8(\mathtt{x},\mathtt{a[x]},\mathtt{s[x]},\mathtt{w[x]}) & := & \mathtt{(=\ a[x]\ 7)} \\ F_8(\mathtt{x},\mathtt{j},\mathtt{a[x]},\mathtt{a[j]},\mathtt{s[x]},\mathtt{s[j]},\mathtt{w[x]},\mathtt{w[j]}) & := & \mathtt{case\ of\ \ \{} \\ \mathtt{(=\ j\ x)} & : & (1,\bot,\mathtt{w[j]}) \\ \mathtt{(\neg(=\ j\ x))} & : & (\mathtt{a[j]},\mathtt{s[j]},\mathtt{w[j]}) \\ \multicolumn{3}{r}{\}} \end{array}$$

C.2 Szymanski without invariants

List of reachable nodes

The sequence of transitions $(\tau_1;...;\tau_m)$ is written as $(\tau_m;...;\tau_1;\epsilon)^{-1}$ and ϵ denotes the empty sequence. The $\exists^I$-formula labelling node i is obtained by applying the sequence $(\tau_1;...;\tau_m)$ of transitions as follows: $Pre_{\tau_m}(\cdots(Pre_{\tau_1}(U)\cdots)$. In the following we shall use the notation $\tau_i(z_j)$ or the notation `t_`i`_`j *to mean that when applying the transition* `t_`i *we identify the quantified variable* `x` *with* `zj` *(similarly the notations $\tau_i(z_j,z_k)$ and* `t_`i`_`j`_`k *mean that when applying the transition* `t_`i *we identify the quantified variable* `x` *with* `zj` *and the quantified variable* `y` *with* `zk`*). These identifications arise not only from the fact we use canonical names*

z1, z2,... for the existentially quantified variables in our labeling $\exists^I$-formulae, but also from the fact that the labeling $\exists^I$-formulae are kept differentiated. Notice that quite often, after computing preimages, the existential quantifiers prefix in the labeling formula does not grow or grows less than expected (i.e. the increment is lower than the number of the existentially quantified variables appearing in the guard of the transition). This phenomenon is explained analytically in [12].

The $\exists^I$-formulae listed below have been slightly edited to improve readability. Notice however that these formulae may contain redundant information (e.g., duplicated literals): in the new version 0.2 of MCMT *a better simplification routine avoids this.*

- Node 0 at depth 0 generated by applying the sequence of transitions ϵ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.(\wedge\ \mathtt{(a[z1]=7)\ (z1<z2)\ (a[z2]=7))}$$

- Node 1 at depth 1 generated by applying the sequence of transitions $(\tau_7(\mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.(\wedge\ \mathtt{(a[z1]=6)\ (z1<z2)\ (a[z2]=7))}$$

- Node 2 at depth 1 generated by applying the sequence of transitions $(\tau_7(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.(\wedge\ \mathtt{(a[z2]=6)\ (z1<z2)\ (s[z1]=\bot)\ (a[z1]=7))}$$

- Node 3 at depth 2 generated by applying the sequence of transitions $(\tau_6(\mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.(\wedge\ \mathtt{(a[z1]=5)\ (z1<z2)\ (w[z2]=\bot)\ (a[z2]=7))}$$

- Node 4 at depth 2 generated by applying the sequence of transitions $(\tau_7(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.(\wedge\ \mathtt{(a[z2]=6)\ (z1<z2)\ (s[z1]=\bot)\ (a[z1]=6))}$$

- Node 5 at depth 2 generated by applying the sequence of transitions $(\tau_6(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.(\wedge\ \mathtt{(a[z2]=5)\ (z1<z2)\ (w[z1]=\bot)\ (s[z1]=\bot)\ (a[z1]=7))}$$

- Node 6 at depth 3 generated by applying the sequence of transitions $(\tau_5(\texttt{z1}, \texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z1]=4)}\ \texttt{(z1<z2)}\ \texttt{(s[z2]=}\top\texttt{)}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z2]=8))}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(a[z2]=7))}$$

- Node 7 at depth 3 generated by applying the sequence of transitions $(\tau_5(\texttt{z1}, \texttt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ \texttt{(a[z1]=4)}\ \texttt{(}\neg\texttt{(z1=z3))}\ \texttt{(s[z3]=}\top\texttt{)}\ \texttt{(w[z3]=}\bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z3]=8))}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(a[z2]=7))}$$

- Node 8 at depth 3 generated by applying the sequence of transitions $(\tau_7(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z2]=6)}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\bot\texttt{)}\ \texttt{(a[z1]=5)}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(z1<z2))}$$

- Node 9 at depth 3 generated by applying the sequence of transitions $(\tau_6(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z2]=5)}\ \texttt{(w[z1]=}\bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\bot\texttt{)}\ \texttt{(a[z1]=6)}\ \texttt{(z1<z2))}$$

- Node 10 at depth 3 generated by applying the sequence of transitions $(\tau_5(\texttt{z2}, \texttt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ \texttt{(a[z2]=4)}\ \texttt{(}\neg\texttt{(z2=z3))}\ \texttt{(s[z3]=}\top\texttt{)}\ \texttt{(w[z3]=}\bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z3]=8))}\ \texttt{(w[z1]=}\bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\bot\texttt{)}\ \texttt{(a[z1]=7))}$$

- Node 11 at depth 4 generated by applying the sequence of transitions $(\tau_4(\texttt{z1}, \texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z1]=3)}\ \texttt{(}\neg\texttt{(a[z2]=1))}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z2]=8))}\ \texttt{(s[z2]=}\ \top\texttt{)}\ \texttt{(w[z2]=}\ \bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z2]=8))}\ \texttt{(w[z2]=}\ \bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(a[z2]=7))}$$

- Node 12 at depth 4 generated by applying the sequence of transitions $(\tau_7(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z2]=6)}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\bot\texttt{)}\ \texttt{(a[z1]=4)}\ \texttt{(s[z2]=}\top\texttt{)}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(w[z2]=}\bot\texttt{))}$$

- Node 13 at depth 4 generated by applying the sequence of transitions $(\tau_4(\mathtt{z1}, \mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.$ (∧ (a[z1]=3) (¬(a[z2]=1)) (w[z2]=⊥) (¬(a[z2]=8)) (¬(z1=z3)) (s[z3]= ⊤) (w[z3]= ⊥) (¬(a[z3]=8)) (w[z2]= ⊥) (z1<z2) (a[z2]=7))

- Node 14 at depth 4 generated by applying the sequence of transitions $(\tau_7(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.$ (∧ (a[z2]=6) (z1<z2) (s[z1]=⊥) (z2<z3) (a[z1]=4) (¬(z1=z3)) (s[z3]=⊤) (w[z3]=⊥) (¬(a[z3]=8)) (w[z2]=⊥) (z1<z2))

- Node 15 at depth 4 generated by applying the sequence of transitions $(\tau_6(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$\exists \mathtt{z1}, \mathtt{z2}.$ (∧ (a[z2]=5)(w[z1]=⊥) (z1<z2) (s[z1]=⊥) (a[z1]=5) (w[z2]=⊥) (z1<z2))

- Node 16 at depth 4 generated by applying the sequence of transitions $(\tau_5(\mathtt{z2}, \mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.$ (∧ (a[z2]=4) (¬(z2=z3)) (s[z3]=⊤) (w[z3]=⊥) (¬(a[z3]=8)) (w[z1]=⊥) (z1<z2) (s[z1]=⊥) (a[z1]=6) (z1<z2))

- Node 17 at depth 4 generated by applying the sequence of transitions $(\tau_4(\mathtt{z2}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.$ (∧ (a[z2]=3) (¬(z2=z1)) (¬(a[z1]=1)) (w[z1]=⊥) (¬(a[z1]=8)) (¬(z2=z3)) (s[z3]= ⊤) (w[z3]= ⊥) (¬(a[z3]=8)) (w[z1]= ⊥) (z1<z2) (s[z1]= ⊥) (a[z1]=7) (z1<z2))

- Node 18 at depth 5 generated by applying the sequence of transitions $(\tau_2(\mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$\exists \mathtt{z1}, \mathtt{z2}.$ (∧ (a[z1]=2) (¬(a[z2]=1)) (w[z2]=⊥) (¬(a[z2]=8)) (s[z2]= ⊤) (w[z2]= ⊥) (¬(a[z2]=8)) (w[z2]= ⊥) (z1<z2) (a[z2]=7))

- Node 19 at depth 5 generated by applying the sequence of transitions $(\tau_7(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$\exists \mathtt{z1}, \mathtt{z2}.$ (∧ (a[z2]=6) (z1<z2) (s[z1]=⊥) (a[z1]=3) (w[z2]=⊥) (s[z2]= ⊤) (w[z2]= ⊥) (w[z2]= ⊥) (z1<z2))

- Node 20 at depth 5 generated by applying the sequence of transitions $(\tau_4(\texttt{z1}, \texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z1]=3)}\ (\neg\texttt{(a[z2]=1)})\ \texttt{(w[z2]=}\bot\texttt{)}\ (\neg\texttt{(a[z2]=8)})\ \texttt{(a[z2]=6)}\ \texttt{(z1<z2)}\ \texttt{(s[z2]=}\ \top\texttt{)}\ \texttt{(w[z2]=}\ \bot\texttt{)}\ \texttt{(w[z2]=}\ \bot\texttt{)}\ \texttt{(z1<z2))}$$

- Node 21 at depth 5 generated by applying the sequence of transitions $(\tau_6(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z2]=5)}\ \texttt{(w[z1]=}\bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\bot\texttt{)}\ \texttt{(a[z1]=4)}\ \texttt{(s[z2]=}\top\texttt{)}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(z1<z2))}$$

- Node 22 at depth 5 generated by applying the sequence of transitions $(\tau_2(\texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ \texttt{(a[z1]=2)}\ (\neg\texttt{(a[z2]=1)})\ \texttt{(w[z2]=}\bot\texttt{)}\ (\neg\texttt{(a[z2]=8)})\ (\neg\texttt{(z1=z3)})\ \texttt{(s[z3]=}\ \top\texttt{)}\ \texttt{(w[z3]=}\ \bot\texttt{)}\ (\neg\texttt{(a[z3]=8)})\ \texttt{(w[z2]=}\ \bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(a[z2]=7))}$$

- Node 23 at depth 5 generated by applying the sequence of transitions $(\tau_7(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ \texttt{(a[z2]=6)(z1<z2)}\ \texttt{(s[z1]=}\bot\texttt{)}\ \texttt{(z2<z3)}\ \texttt{(a[z1]=3)}\ \texttt{(w[z2]=}\bot\texttt{)}\ (\neg\texttt{(z1=z3)})\ \texttt{(s[z3]=}\ \top\texttt{)}\ \texttt{(w[z3]=}\ \bot\texttt{)}\ (\neg\texttt{(a[z3]=8)})\ \texttt{(w[z2]=}\ \bot\texttt{)}\ \texttt{(z1<z2))}$$

- Node 24 at depth 5 generated by applying the sequence of transitions $(\tau_4(\texttt{z1}, \texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ \texttt{(a[z1]=3)}\ (\neg\texttt{(a[z2]=1)})\ \texttt{(w[z2]=}\bot\texttt{)}\ (\neg\texttt{(a[z2]=8)})\ \texttt{(a[z2]=6)(z1<z2)}\ \texttt{(z2<z3)}\ (\neg\texttt{(z1=z3)})\ \texttt{(s[z3]=}\ \top\texttt{)}\ \texttt{(w[z3]=}\ \bot\texttt{)}\ (\neg\texttt{(a[z3]=8)})\ \texttt{(w[z2]=}\ \bot\texttt{)}\ \texttt{(z1<z2))}$$

- Node 25 at depth 5 generated by applying the sequence of transitions $(\tau_6(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ (\texttt{a[z2]=5})(\texttt{w[z1]=}\bot)\ (\texttt{w[z3]=}\bot)\ (\texttt{z1<z2})$$
$$(\texttt{s[z1]=}\bot)\ (\texttt{z2<z3})\ (\texttt{a[z1]=4})\ (\neg(\texttt{z1=z3}))$$
$$(\texttt{s[z3]=}\top)\ (\texttt{w[z3]=}\bot)\ (\neg(\texttt{a[z3]=8}))$$
$$(\texttt{w[z2]=}\bot)\ (\texttt{z1<z2}))$$

- Node 26 at depth 5 generated by applying the sequence of transitions $(\tau_5(\texttt{z2}, \texttt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\quad (\wedge\ (\texttt{a[z2]=4})\ (\neg(\texttt{z2=z3}))\ (\texttt{s[z3]=}\top)$$
$$(\texttt{w[z3]=}\bot)\ (\neg(\texttt{a[z3]=8}))\ (\texttt{w[z1]=}\bot)$$
$$(\texttt{z1<z2})\ (\texttt{s[z1]=}\bot)\ (\texttt{a[z1]=5})\ (\texttt{z1<z2}))$$

- Node 27 at depth 5 generated by applying the sequence of transitions $(\tau_4(\texttt{z2}, \texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ (\texttt{a[z2]=3})\ (\neg(\texttt{z2=z1}))\ (\neg(\texttt{a[z1]=1}))$$
$$(\texttt{w[z1]=}\bot)\ (\neg(\texttt{a[z1]=8}))$$
$$(\neg(\texttt{z2=z3}))\ (\texttt{s[z3]=}\ \top)\ (\texttt{w[z3]=}\ \bot)$$
$$(\neg(\texttt{a[z3]=8}))\ (\texttt{w[z1]=}\ \bot)\ (\texttt{z1<z2})$$
$$(\texttt{s[z1]=}\ \bot)\ (\texttt{a[z1]=6})\ (\texttt{z1<z2}))$$

- Node 28 at depth 5 generated by applying the sequence of transitions $(\tau_5(\texttt{z3}, \texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ (\texttt{a[z3]=4})\ (\neg(\texttt{z3=z2}))\ (\texttt{s[z2]=}\top)$$
$$(\texttt{w[z2]=}\bot)\ (\neg(\texttt{a[z2]=8}))\ (\texttt{a[z2]=4})$$
$$(\neg(\texttt{z2=z3}))\ (\texttt{w[z1]=}\bot)\ (\texttt{z1<z2})$$
$$(\texttt{s[z1]=}\bot)\ (\texttt{a[z1]=6})\ (\texttt{z1<z2}))$$

- Node 29 at depth 5 generated by applying the sequence of transitions $(\tau_2(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{s[z3]=}\top)\ (\mathtt{w[z3]=}\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=7})\ (\mathtt{z1<z2}))$$

- Node 30 at depth 6 generated by applying the sequence of transitions $(\tau_7(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\ \ (\wedge\ (\mathtt{a[z2]=6})(\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=2})\ (\mathtt{w[z2]=}\bot)\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 31 at depth 6 generated by applying the sequence of transitions $(\tau_6(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\ \ (\wedge\ (\mathtt{a[z2]=5})(\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=3})\ (\mathtt{w[z2]=}\bot)\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 32 at depth 6 generated by applying the sequence of transitions $(\tau_2(\mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\ \ (\wedge\ (\mathtt{a[z1]=2})\ (\neg(\mathtt{a[z2]=1}))\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=6})(\mathtt{z1<z2})\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 33 at depth 6 generated by applying the sequence of transitions $(\tau_6(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\ \ (\wedge\ (\mathtt{a[z2]=5})(\mathtt{w[z1]=}\bot)\ (\mathtt{a[z1]=3})\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 34 at depth 6 generated by applying the sequence of transitions $(\tau_5(\mathtt{z2},\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1},\mathtt{z2},\mathtt{z3}.\quad (\wedge\ (\mathtt{a[z2]=4})\ (\neg(\mathtt{z2=z3}))\ (\mathtt{s[z3]}=\top)\ (\mathtt{w[z3]}=\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z1]}=\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]}=\bot)\ (\mathtt{a[z1]=4})\ (\mathtt{z1<z2}))$$

- Node 35 at depth 6 generated by applying the sequence of transitions $(\tau_7(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1},\mathtt{z2},\mathtt{z3}.\quad (\wedge\ (\mathtt{a[z2]=6})(\mathtt{z1<z2})\ (\mathtt{s[z1]}=\bot)\ (\mathtt{z2<z3})\ (\mathtt{a[z1]=2})\ (\mathtt{w[z2]}=\bot)\ (\neg(\mathtt{z1=z3}))\ (\mathtt{s[z3]}=\top)\ (\mathtt{w[z3]}=\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z2]}=\bot)\ (\mathtt{z1<z2}))$$

- Node 36 at depth 6 generated by applying the sequence of transitions $(\tau_6(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1},\mathtt{z2},\mathtt{z3}.\quad (\wedge\ (\mathtt{a[z2]=5})(\mathtt{w[z1]}=\bot)\ (\mathtt{w[z3]}=\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]}=\bot)\ (\mathtt{z2<z3})\ (\mathtt{a[z1]=3})\ (\mathtt{w[z2]}=\bot)\ (\neg(\mathtt{z1=z3}))\ (\mathtt{s[z3]}=\top)\ (\mathtt{w[z3]}=\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z2]}=\bot)\ (\mathtt{z1<z2}))$$

- Node 37 at depth 6 generated by applying the sequence of transitions $(\tau_2(\mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1},\mathtt{z2},\mathtt{z3}.\quad (\wedge\ (\mathtt{a[z1]=2})\ (\neg(\mathtt{a[z2]=1}))\ (\mathtt{w[z2]}=\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=6})(\mathtt{z1<z2})\ (\mathtt{z2<z3})\ (\neg(\mathtt{z1=z3}))\ (\mathtt{s[z3]}=\top)\ (\mathtt{w[z3]}=\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z2]}=\bot)\ (\mathtt{z1<z2}))$$

- Node 38 at depth 6 generated by applying the sequence of transitions $(\tau_6(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1},\mathtt{z2},\mathtt{z3}.\quad (\wedge\ (\mathtt{a[z2]=5})(\mathtt{w[z1]}=\bot)\ (\mathtt{w[z3]}=\bot)\ (\mathtt{a[z1]=3})\ (\mathtt{w[z2]}=\bot)\ (\mathtt{z1<z2})\ (\mathtt{z2<z3})\ (\neg(\mathtt{z1=z3}))\ (\mathtt{s[z3]}=\top)\ (\mathtt{w[z3]}=\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z2]}=\bot)\ (\mathtt{z1<z2}))$$

- Node 39 at depth 6 generated by applying the sequence of transitions $(\tau_3(\mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z1]=3})\ (\neg(\mathtt{a[z2]=1}))\ (\mathtt{w[z2]}=\top)$$
$$(\mathtt{a[z3]=1})\ (\mathtt{a[z2]=4})\ (\neg(\mathtt{z2=z3}))$$
$$(\mathtt{s[z3]}=\top)\ (\mathtt{w[z3]}=\bot)\ (\neg(\mathtt{a[z3]=8}))$$
$$(\mathtt{z1<z2})\ (\mathtt{s[z1]}=\bot)\ (\mathtt{z1<z2}))$$

- Node 40 at depth 6 generated by applying the sequence of transitions $(\tau_4(\mathtt{z2}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))$$
$$(\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8}))$$
$$(\neg(\mathtt{z2=z3}))\ (\mathtt{s[z3]}=\top)\ (\mathtt{w[z3]}=\bot)$$
$$(\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z1]}=\bot)\ (\mathtt{z1<z2})$$
$$(\mathtt{s[z1]}=\bot)\ (\mathtt{a[z1]=5})\ (\mathtt{z1<z2}))$$

- Node 41 at depth 6 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3}, \mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]}=\top)$$
$$(\mathtt{w[z2]}=\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=4})$$
$$(\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]}=\bot)\ (\mathtt{z1<z2})$$
$$(\mathtt{s[z1]}=\bot)\ (\mathtt{a[z1]=5})\ (\mathtt{z1<z2}))$$

- Node 42 at depth 6 generated by applying the sequence of transitions $(\tau_2(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))$$
$$(\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8}))$$
$$(\neg(\mathtt{z2=z3}))\ (\mathtt{s[z3]}=\top)\ (\mathtt{w[z3]}=\bot)$$
$$(\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z1]}=\bot)\ (\mathtt{z1<z2})$$
$$(\mathtt{s[z1]}=\bot)\ (\mathtt{a[z1]=6})\ (\mathtt{z1<z2}))$$

- Node 43 at depth 6 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3}, \mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]}=\top)$$
$$(\mathtt{w[z2]}=\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=3})$$
$$(\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))$$
$$(\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))$$
$$(\mathtt{w[z1]}=\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]}=\ \bot)$$
$$(\mathtt{a[z1]=6})\ (\mathtt{z1<z2}))$$

- Node 44 at depth 7 generated by applying the sequence of transitions $(\tau_6(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\quad (\wedge\ (\mathtt{a[z2]=5})(\mathtt{w[z1]}=\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]}=\bot)$$
$$(\mathtt{a[z1]=2})\ (\mathtt{w[z2]}=\bot)\ (\mathtt{s[z2]}=\ \top)\ (\mathtt{w[z2]}=\ \bot)$$
$$(\mathtt{w[z2]}=\ \bot)\ (\mathtt{z1<z2}))$$

- Node 45 at depth 7 generated by applying the sequence of transitions $(\tau_5(\mathtt{z2}, \mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\quad (\wedge\ (\mathtt{a[z2]=4})\ (\neg(\mathtt{z2=z3}))\ (\mathtt{s[z3]}=\top)$$
$$(\mathtt{w[z3]}=\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z1]}=\bot)$$
$$(\mathtt{z1<z2})\ (\mathtt{s[z1]}=\bot)\ (\mathtt{a[z1]=3})\ (\mathtt{z1<z2}))$$

- Node 46 at depth 7 generated by applying the sequence of transitions $(\tau_6(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\ \ (\wedge\ (\mathtt{a[z2]=5})(\mathtt{w[z1]}=\bot)\ (\mathtt{a[z1]=2})\ (\mathtt{w[z2]}=\bot)$$
$$(\mathtt{z1<z2})\ (\mathtt{s[z2]}=\ \top)\ (\mathtt{w[z2]}=\ \bot)\ (\mathtt{w[z2]}=\ \bot)$$
$$(\mathtt{z1<z2}))$$

- Node 47 at depth 7 generated by applying the sequence of transitions $(\tau_5(\mathtt{z2}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\ \ (\wedge\ (\mathtt{a[z2]=4})\ (\neg(\mathtt{z2=z1}))\ (\mathtt{s[z1]}=\top)$$
$$(\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{w[z1]}=\bot)$$
$$(\mathtt{a[z1]=3})\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 48 at depth 7 generated by applying the sequence of transitions $(\tau_4(\mathtt{z2},\mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1},\mathtt{z2},\mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{s[z3]=}\top)\ (\mathtt{w[z3]=}\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=4})\ (\mathtt{z1<z2}))$$

- Node 49 at depth 7 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3},\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1},\mathtt{z2},\mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=4})\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=4})\ (\mathtt{z1<z2}))$$

- Node 50 at depth 7 generated by applying the sequence of transitions $(\tau_6(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1},\mathtt{z2},\mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z2]=5})(\mathtt{w[z1]=}\bot)\ (\mathtt{w[z3]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{z2<z3})\ (\mathtt{a[z1]=2})\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{z1=z3}))\ (\mathtt{s[z3]=}\top)\ (\mathtt{w[z3]=}\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 51 at depth 7 generated by applying the sequence of transitions $(\tau_6(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1},\mathtt{z2},\mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z2]=5})(\mathtt{w[z1]=}\bot)\ (\mathtt{w[z3]=}\bot)\ (\mathtt{a[z1]=2})\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{z2<z3})\ (\neg(\mathtt{z1=z3}))\ (\mathtt{s[z3]=}\top)\ (\mathtt{w[z3]=}\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 52 at depth 7 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad \begin{array}{c} (\wedge\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z1}))\ (\mathtt{s[z1]}=\top) \\ (\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z2]=5}) \\ (\mathtt{w[z1]}=\bot)\ (\mathtt{a[z1]=3})\ (\mathtt{w[z2]}=\bot)\ (\mathtt{z1<z2}) \\ (\mathtt{z2<z3})\ (\neg(\mathtt{z1=z3}))\ (\mathtt{w[z2]=}\ \bot) \\ (\mathtt{z1<z2})) \end{array}$$

- Node 53 at depth 7 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3}, \mathtt{z4});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}. \quad \begin{array}{c} (\wedge\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z4}))\ (\mathtt{s[z4]}=\top) \\ (\mathtt{w[z4]}=\bot)\ (\neg(\mathtt{a[z4]=8}))\ (\mathtt{a[z2]=5}) \\ (\mathtt{w[z1]}=\bot)\ (\mathtt{a[z1]=3})\ (\mathtt{w[z2]}=\bot)\ (\mathtt{z1<z2}) \\ (\mathtt{z2<z3})\ (\neg(\mathtt{z1=z3}))\ (\mathtt{w[z2]=}\ \bot) \\ (\mathtt{z1<z2})) \end{array}$$

- Node 54 at depth 7 generated by applying the sequence of transitions $(\tau_4(\mathtt{z2}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad \begin{array}{c} (\wedge\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1})) \\ (\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8})) \\ (\mathtt{a[z1]=3})\ (\mathtt{w[z2]}=\top)\ (\mathtt{a[z3]=1})\ (\neg(\mathtt{z2=z3})) \\ (\mathtt{s[z3]=}\ \top)\ (\mathtt{w[z3]=}\ \bot)\ (\neg(\mathtt{a[z3]=8})) \\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\ \bot)\ (\mathtt{z1<z2}) \end{array}$$

- Node 55 at depth 7 generated by applying the sequence of transitions $(\tau_4(\mathtt{z2}, \mathtt{z4});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}. \quad \begin{array}{c} (\wedge\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z4}))\ (\neg(\mathtt{a[z4]=1})) \\ (\mathtt{w[z4]}=\bot)\ (\neg(\mathtt{a[z4]=8})) \\ (\mathtt{a[z1]=3})\ (\mathtt{w[z2]}=\top)\ (\mathtt{a[z3]=1})\ (\neg(\mathtt{z2=z3})) \\ (\mathtt{s[z3]=}\ \top)\ (\mathtt{w[z3]=}\ \bot)\ (\neg(\mathtt{a[z3]=8})) \\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\ \bot)\ (\mathtt{z1<z2}) \end{array}$$

- Node 56 at depth 7 generated by applying the sequence of transitions $(\tau_2(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{s[z3]=}\top)\ (\mathtt{w[z3]=}\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=5})\ (\mathtt{z1<z2}))$$

- Node 57 at depth 7 generated by applying the sequence of transitions $(\tau_3(\mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z1]=3})\ (\neg(\mathtt{a[z2]=1}))\ (\mathtt{w[z2]=}\top)\ (\mathtt{a[z3]=1})\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{s[z3]=}\top)\ (\mathtt{w[z3]=}\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 58 at depth 7 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3}, \mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=5})\ (\mathtt{z1<z2}))$$

- Node 59 at depth 7 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=4})\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=5})\ (\mathtt{z1<z2}))$$

- Node 60 at depth 7 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3}, \mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]}=\top)\ (\mathtt{w[z2]}=\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]}=\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]}=\bot)\ (\mathtt{a[z1]=6})\ (\mathtt{z1<z2}))$$

- Node 61 at depth 7 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]}=\top)\ (\mathtt{w[z2]}=\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]}=\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]}=\bot)\ (\mathtt{a[z1]=6})\ (\mathtt{z1<z2}))$$

- Node 62 at depth 8 generated by applying the sequence of transitions $(\tau_5(\mathtt{z2}, \mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z2]=4})\ (\neg(\mathtt{z2=z3}))\ (\mathtt{s[z3]}=\top)\ (\mathtt{w[z3]}=\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z1]}=\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]}=\bot)\ (\mathtt{a[z1]=2})\ (\mathtt{z1<z2}))$$

- Node 63 at depth 8 generated by applying the sequence of transitions $(\tau_4(\mathtt{z2}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{s[z3]}=\top)\ (\mathtt{w[z3]}=\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z1]}=\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]}=\bot)\ (\mathtt{a[z1]=3})\ (\mathtt{z1<z2}))$$

- Node 64 at depth 8 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3}, \mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]}=\top)$$
$$(\mathtt{w[z2]}=\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=4})$$
$$(\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]}=\bot)\ (\mathtt{z1<z2})$$
$$(\mathtt{s[z1]}=\bot)\ (\mathtt{a[z1]=3})\ (\mathtt{z1<z2}))$$

- Node 65 at depth 8 generated by applying the sequence of transitions $(\tau_5(\mathtt{z2}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\ \ (\wedge\ (\mathtt{a[z2]=4})\ (\neg(\mathtt{z2=z1}))\ (\mathtt{s[z1]}=\top)$$
$$(\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{w[z1]}=\bot)$$
$$(\mathtt{a[z1]=2})\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 66 at depth 8 generated by applying the sequence of transitions $(\tau_4(\mathtt{z2}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\ \ (\wedge\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))$$
$$(\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8}))$$
$$(\neg(\mathtt{z2=z1}))\ (\mathtt{s[z1]}=\top)\ (\mathtt{w[z1]}=\bot)$$
$$(\neg(\mathtt{a[z1]=8}))\ (\mathtt{w[z1]}=\bot)\ (\mathtt{a[z1]=3})$$
$$(\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 67 at depth 8 generated by applying the sequence of transitions $(\tau_2(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))$$
$$(\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8}))$$
$$(\neg(\mathtt{z2=z3}))\ (\mathtt{s[z3]}=\top)\ (\mathtt{w[z3]}=\bot)$$
$$(\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z1]}=\bot)\ (\mathtt{z1<z2})$$
$$(\mathtt{s[z1]}=\bot)\ (\mathtt{a[z1]=4})\ (\mathtt{z1<z2}))$$

- Node 68 at depth 8 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3}, \mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]}=\top)$$
$$(\mathtt{w[z2]}=\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=3})$$
$$(\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))$$
$$(\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))$$
$$(\mathtt{w[z1]}=\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]}=\bot)$$
$$(\mathtt{a[z1]=4})\ (\mathtt{z1<z2}))$$

- Node 69 at depth 8 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1}))$$
$$(\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8}))$$
$$(\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]}=\top)\ (\mathtt{w[z2]}=\bot)$$
$$(\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=4})\ (\neg(\mathtt{z2=z3}))$$
$$(\mathtt{w[z1]}=\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]}=\bot)$$
$$(\mathtt{a[z1]=4})\ (\mathtt{z1<z2}))$$

- Node 70 at depth 8 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3}, \mathtt{z4});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}.\ \ (\wedge\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z4}))\ (\mathtt{s[z4]}=\top)$$
$$(\mathtt{w[z4]}=\bot)\ (\neg(\mathtt{a[z4]=8}))\ (\mathtt{a[z2]=5})$$
$$(\mathtt{w[z1]}=\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]}=\bot)\ (\mathtt{z2<z3})$$
$$(\mathtt{a[z1]=2})\ (\mathtt{w[z2]}=\bot)\ (\neg(\mathtt{z1=z3}))$$
$$(\mathtt{w[z2]}=\bot)\ (\mathtt{z1<z2}))$$

- Node 71 at depth 8 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z1}))\ (\mathtt{s[z1]}=\top)$$
$$(\mathtt{w[z1]}=\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z2]=5})$$
$$(\mathtt{w[z1]}=\bot)\ (\mathtt{a[z1]=2})\ (\mathtt{w[z2]}=\bot)\ (\mathtt{z1<z2})$$
$$(\mathtt{z2<z3})\ (\neg(\mathtt{z1=z3}))\ (\mathtt{w[z2]}=\bot)$$
$$(\mathtt{z1<z2}))$$

- Node 72 at depth 8 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1}))$$
$$(\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))$$
$$(\neg(\mathtt{z3=z1}))\ (\mathtt{s[z1]=}\top)\ (\mathtt{w[z1]=}\bot)$$
$$(\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z2]=5})(\mathtt{w[z1]=}\bot)$$
$$(\mathtt{a[z1]=3})\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{z2<z3})$$
$$(\neg(\mathtt{z1=z3}))\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 73 at depth 8 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}.\ \ (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1}))$$
$$(\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))$$
$$(\neg(\mathtt{z3=z4}))\ (\mathtt{s[z4]=}\top)\ (\mathtt{w[z4]=}\bot)$$
$$(\neg(\mathtt{a[z4]=8}))\ (\mathtt{a[z2]=5})(\mathtt{w[z1]=}\bot)$$
$$(\mathtt{a[z1]=3})\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{z2<z3})$$
$$(\neg(\mathtt{z1=z3}))\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 74 at depth 8 generated by applying the sequence of transitions $(\tau_2(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1})$$
$$(\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))$$
$$(\mathtt{a[z1]=3})\ (\mathtt{a[z3]=1})\ (\neg(\mathtt{z2=z3}))$$
$$(\mathtt{s[z3]=}\top)\ (\mathtt{w[z3]=}\bot)\ (\neg(\mathtt{a[z3]=8}))$$
$$(\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 75 at depth 8 generated by applying the sequence of transitions $(\tau_2(\mathtt{z2});\ \epsilon)^{-1}$ and

labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}, \texttt{z4}.\ \ (\wedge\ \texttt{(a[z2]=2)}\ (\neg\texttt{(z2=z4)})\ (\neg\texttt{(a[z4]=1)}\ \texttt{(w[z4]=}\bot\texttt{)}\ (\neg\texttt{(a[z4]=8))}\ \texttt{(a[z1]=3)}\ \texttt{(a[z3]=1)}\ (\neg\texttt{(z2=z3))}\ \texttt{(s[z3]=}\ \top\texttt{)}\ \texttt{(w[z3]=}\ \bot\texttt{)}\ (\neg\texttt{(a[z3]=8))}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\ \bot\texttt{)}\ \texttt{(z1<z2))}$$

- Node 76 at depth 8 generated by applying the sequence of transitions $(\tau_3(\texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ \texttt{(a[z1]=3)}\ (\neg\texttt{(a[z2]=1))}\ \texttt{(w[z2]=}\top\texttt{)}\ \texttt{(a[z3]=1)}\ \texttt{(a[z2]=2)}\ (\neg\texttt{(z2=z1))}\ (\neg\texttt{(z2=z3))}\ \texttt{(s[z3]=}\ \top\texttt{)}\ \texttt{(w[z3]=}\ \bot\texttt{)}\ (\neg\texttt{(a[z3]=8))}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\ \bot\texttt{)}\ \texttt{(z1<z2))}$$

- Node 77 at depth 8 generated by applying the sequence of transitions $(\tau_5(\texttt{z3}, \texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ \texttt{(a[z3]=4)}\ (\neg\texttt{(z3=z2))}\ \texttt{(s[z2]=}\top\texttt{)}\ \texttt{(w[z2]=}\bot\texttt{)}\ (\neg\texttt{(a[z2]=8))}\ \texttt{(a[z2]=2)}\ (\neg\texttt{(z2=z1))}\ (\neg\texttt{(a[z1]=1))}\ \texttt{(w[z1]=}\bot\texttt{)}\ (\neg\texttt{(a[z1]=8))}\ (\neg\texttt{(z2=z3)}\ \texttt{(w[z1]=}\ \bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\ \bot\texttt{)}\ \texttt{(a[z1]=5)}\ \texttt{(z1<z2))}$$

- Node 78 at depth 8 generated by applying the sequence of transitions $(\tau_2(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ \texttt{(a[z2]=2)}\ \texttt{(a[z1]=3)}\ \texttt{(a[z3]=1)}\ (\neg\texttt{(z2=z1)}\ (\neg\texttt{(z2=z3))}\ \texttt{(s[z3]=}\ \top\texttt{)}\ \texttt{(w[z3]=}\ \bot\texttt{)}\ (\neg\texttt{(a[z3]=8))}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\ \bot\texttt{)}\ \texttt{(z1<z2))}$$

- Node 79 at depth 8 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z1})\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=5})\ (\mathtt{z1<z2}))$$

- Node 80 at depth 8 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=4})\ (\neg(\mathtt{z2=z3})\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=5})\ (\mathtt{z1<z2}))$$

- Node 81 at depth 8 generated by applying the sequence of transitions $(\tau_1(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z2]=1})(\mathtt{s[z1]=}\bot)\ (\mathtt{s[z3]=}\bot)\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3})\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=6})\ (\mathtt{z1<z2}))$$

- Node 82 at depth 8 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$

and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z1})\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=6})\ (\mathtt{z1<z2}))$$

- Node 83 at depth 8 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z1})\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=6})\ (\mathtt{z1<z2}))$$

- Node 84 at depth 9 generated by applying the sequence of transitions $(\tau_4(\mathtt{z2}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{s[z3]=}\top)\ (\mathtt{w[z3]=}\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=2})\ (\mathtt{z1<z2}))$$

- Node 85 at depth 9 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3}, \mathtt{z2});\ \epsilon)^{-1}$

and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)$$
$$(\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=4})$$
$$(\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})$$
$$(\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=2})\ (\mathtt{z1<z2}))$$

- Node 86 at depth 9 generated by applying the sequence of transitions $(\tau_2(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1})$$
$$(\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))$$
$$(\neg(\mathtt{z2=z3}))\ (\mathtt{s[z3]=}\ \top)\ (\mathtt{w[z3]=}\ \bot)$$
$$(\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})$$
$$(\mathtt{s[z1]=}\ \bot)\ (\mathtt{a[z1]=3})\ (\mathtt{z1<z2}))$$

- Node 87 at depth 9 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3}, \mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)$$
$$(\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=3})$$
$$(\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))$$
$$(\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3})$$
$$(\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\ \bot)$$
$$(\mathtt{a[z1]=3})\ (\mathtt{z1<z2}))$$

- Node 88 at depth 9 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})$$
$$(\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))$$
$$(\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\ \top)\ (\mathtt{w[z2]=}\ \bot)$$
$$(\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=4})\ (\neg(\mathtt{z2=z3})$$
$$(\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\ \bot)$$
$$(\mathtt{a[z1]=3})\ (\mathtt{z1<z2}))$$

- Node 89 at depth 9 generated by applying the sequence of transitions $(\tau_1(\texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ (\texttt{a[z1]=1})\ (\texttt{s[z2]=}\bot)\ (\texttt{a[z2]=4})\ (\neg(\texttt{z2=z1})\ (\texttt{s[z1]=}\top)\ (\texttt{w[z1]=}\bot)\ (\texttt{w[z1]=}\bot)\ (\texttt{z1<z2})\ (\texttt{z1<z2}))$$

- Node 90 at depth 9 generated by applying the sequence of transitions $(\tau_4(\texttt{z2}, \texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ (\texttt{a[z2]=3})\ (\neg(\texttt{z2=z1}))\ (\neg(\texttt{a[z1]=1})\ (\texttt{w[z1]=}\bot)\ (\neg(\texttt{a[z1]=8}))\ (\neg(\texttt{z2=z1}))\ (\texttt{s[z1]=}\top)\ (\texttt{w[z1]=}\bot)\ (\neg(\texttt{a[z1]=8}))\ (\texttt{w[z1]=}\bot)\ (\texttt{a[z1]=2})\ (\texttt{z1<z2})\ (\texttt{z1<z2}))$$

- Node 91 at depth 9 generated by applying the sequence of transitions $(\tau_2(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ (\texttt{a[z2]=2})\ (\neg(\texttt{z2=z1}))\ (\neg(\texttt{a[z1]=1})\ (\texttt{w[z1]=}\bot)\ (\neg(\texttt{a[z1]=8}))\ (\neg(\texttt{z2=z1}))\ (\texttt{s[z1]=}\top)\ (\texttt{w[z1]=}\bot)\ (\neg(\texttt{a[z1]=8}))\ (\texttt{w[z1]=}\bot)\ (\texttt{a[z1]=3})\ (\texttt{z1<z2})\ (\texttt{z1<z2}))$$

- Node 92 at depth 9 generated by applying the sequence of transitions $(\tau_5(\texttt{z3}, \texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ (\texttt{a[z3]=4})\ (\neg(\texttt{z3=z2}))\ (\texttt{s[z2]=}\top)\ (\texttt{w[z2]=}\bot)\ (\neg(\texttt{a[z2]=8}))\ (\texttt{a[z2]=2})\ (\neg(\texttt{z2=z1}))\ (\neg(\texttt{a[z1]=1}))\ (\texttt{w[z1]=}\bot)\ (\neg(\texttt{a[z1]=8}))\ (\neg(\texttt{z2=z3})\ (\texttt{w[z1]=}\bot)\ (\texttt{z1<z2})\ (\texttt{s[z1]=}\bot)\ (\texttt{a[z1]=4})\ (\texttt{z1<z2}))$$

- Node 93 at depth 9 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z1})\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=4})\ (\mathtt{z1<z2}))$$

- Node 94 at depth 9 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=4})\ (\neg(\mathtt{z2=z3})\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=4})\ (\mathtt{z1<z2}))$$

- Node 95 at depth 9 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}. \quad (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z4}))\ (\mathtt{s[z4]=}\top)\ (\mathtt{w[z4]=}\bot)\ (\neg(\mathtt{a[z4]=8}))\ (\mathtt{a[z2]=5})(\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{z2<z3})\ (\mathtt{a[z1]=2})\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{z1=z3}))\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 96 at depth 9 generated by applying the sequence of transitions $(\tau_1(\mathtt{z1});\ \epsilon)^{-1}$ and

labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z1]=1})\ (\mathtt{s[z2]}{=}\bot)\ (\mathtt{s[z3]}{=}\bot)\ (\mathtt{a[z3]=4})$$
$$(\neg(\mathtt{z3=z1}))\ (\mathtt{s[z1]}{=}\top)\ (\mathtt{w[z1]}{=}\bot)$$
$$(\mathtt{a[z2]=5})(\mathtt{w[z1]}{=}\bot)\ (\mathtt{w[z2]}{=}\bot)\ (\mathtt{z1<z2})$$
$$(\mathtt{z2<z3})\ (\neg(\mathtt{z1=z3}))\ (\mathtt{w[z2]}{=}\ \bot)$$
$$(\mathtt{z1<z2}))$$

- Node 97 at depth 9 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})$$
$$(\mathtt{w[z1]}{=}\bot)\ (\neg(\mathtt{a[z1]=8}))$$
$$(\neg(\mathtt{z3=z1}))\ (\mathtt{s[z1]}{=}\ \top)\ (\mathtt{w[z1]}{=}\ \bot)$$
$$(\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z2]=5})(\mathtt{w[z1]}{=}\ \bot)$$
$$(\mathtt{a[z1]=2})\ (\mathtt{w[z2]}{=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{z2<z3})$$
$$(\neg(\mathtt{z1=z3}))\ (\mathtt{w[z2]}{=}\ \bot)\ (\mathtt{z1<z2}))$$

- Node 98 at depth 9 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})$$
$$(\mathtt{w[z1]}{=}\bot)\ (\neg(\mathtt{a[z1]=8}))$$
$$(\neg(\mathtt{z3=z1}))\ (\mathtt{s[z1]}{=}\ \top)\ (\mathtt{w[z1]}{=}\ \bot)$$
$$(\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z2]=5})(\mathtt{w[z1]}{=}\ \bot)$$
$$(\mathtt{a[z1]=3})\ (\mathtt{w[z2]}{=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{z2<z3})$$
$$(\neg(\mathtt{z1=z3}))\ (\mathtt{w[z2]}{=}\ \bot)\ (\mathtt{z1<z2}))$$

- Node 99 at depth 9 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}.\ \ (\wedge\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})$$
$$(\mathtt{w[z1]}{=}\bot)\ (\neg(\mathtt{a[z1]=8}))$$
$$(\neg(\mathtt{z3=z4}))\ (\mathtt{s[z4]}{=}\ \top)\ (\mathtt{w[z4]}{=}\ \bot)$$
$$(\neg(\mathtt{a[z4]=8}))\ (\mathtt{a[z2]=5})(\mathtt{w[z1]}{=}\ \bot)$$
$$(\mathtt{a[z1]=3})\ (\mathtt{w[z2]}{=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{z2<z3})$$
$$(\neg(\mathtt{z1=z3}))\ (\mathtt{w[z2]}{=}\ \bot)\ (\mathtt{z1<z2}))$$

- Node 100 at depth 9 generated by applying the sequence of transitions $(\tau_1(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z2]=1})(\mathtt{s[z1]=}\bot)\ (\mathtt{s[z3]=}\bot)\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3})\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\ \bot)\ (\mathtt{a[z1]=5})\ (\mathtt{z1<z2}))$$

- Node 101 at depth 9 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\ \top)\ (\mathtt{w[z2]=}\ \bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z1})\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\ \bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\ \bot)\ (\mathtt{a[z1]=5})\ (\mathtt{z1<z2}))$$

- Node 102 at depth 9 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\ \top)\ (\mathtt{w[z2]=}\ \bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z1})\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\ \bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\ \bot)\ (\mathtt{a[z1]=5})\ (\mathtt{z1<z2}))$$

- Node 103 at depth 9 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$

and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad \begin{array}{c} \mathtt{(\wedge\ (a[z3]=3)\ (\neg(z3=z1))\ (\neg(a[z1]=1)} \\ \mathtt{(w[z1]=\bot)\ (\neg(a[z1]=8))} \\ \mathtt{(a[z2]=1)(s[z1]=\ \bot)\ (\neg(z3=z2))} \\ \mathtt{(s[z2]=\ \top)\ (w[z2]=\ \bot)\ (\neg(z2=z1))} \\ \mathtt{(\neg(a[z1]=1))\ (w[z1]=\ \bot)\ (\neg(a[z1]=8)} \\ \mathtt{(\neg(z2=z3))\ (w[z1]=\ \bot)} \\ \mathtt{(z1<z2)\ (s[z1]=\ \bot)\ (a[z1]=6)\ (z1<z2))} \end{array}$$

- Node 104 at depth 9 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad \begin{array}{c} \mathtt{(\wedge\ (a[z3]=2)\ (\neg(z3=z1))\ (\neg(a[z1]=1)} \\ \mathtt{(w[z1]=\bot)\ (\neg(a[z1]=8))} \\ \mathtt{(\neg(z3=z2))\ (s[z2]=\ \top)\ (w[z2]=\ \bot)} \\ \mathtt{(\neg(a[z2]=8))\ (a[z2]=2)\ (\neg(z2=z1)} \\ \mathtt{(\neg(a[z1]=1))\ (w[z1]=\ \bot)} \\ \mathtt{(\neg(a[z1]=8))\ (\neg(z2=z3))} \\ \mathtt{(w[z1]=\ \bot)\ (z1<z2)\ (s[z1]=\ \bot)\ (a[z1]=6)} \\ \mathtt{(z1<z2))} \end{array}$$

- Node 105 at depth 10 generated by applying the sequence of transitions $(\tau_2(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad \begin{array}{c} \mathtt{(\wedge\ (a[z2]=2)\ (\neg(z2=z1))\ (\neg(a[z1]=1)} \\ \mathtt{(w[z1]=\bot)\ (\neg(a[z1]=8))} \\ \mathtt{(\neg(z2=z3))\ (s[z3]=\ \top)\ (w[z3]=\ \bot)} \\ \mathtt{(\neg(a[z3]=8))\ (w[z1]=\ \bot)\ (z1<z2)} \\ \mathtt{(s[z1]=\ \bot)\ (a[z1]=2)\ (z1<z2))} \end{array}$$

- Node 106 at depth 10 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3}, \mathtt{z2});\ \epsilon)^{-1}$

and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ (\texttt{a[z3]=4})\ (\neg(\texttt{z3=z2}))\ (\texttt{s[z2]=}\top)$$
$$(\texttt{w[z2]=}\bot)\ (\neg(\texttt{a[z2]=8}))\ (\texttt{a[z2]=3})$$
$$(\neg(\texttt{z2=z1}))\ (\neg(\texttt{a[z1]=1}))$$
$$(\texttt{w[z1]=}\bot)\ (\neg(\texttt{a[z1]=8}))\ (\neg(\texttt{z2=z3})$$
$$(\texttt{w[z1]=}\ \bot)\ (\texttt{z1<z2})\ (\texttt{s[z1]=}\ \bot)$$
$$(\texttt{a[z1]=2})\ (\texttt{z1<z2}))$$

- Node 107 at depth 10 generated by applying the sequence of transitions $(\tau_4(\texttt{z3}, \texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ (\texttt{a[z3]=3})\ (\neg(\texttt{z3=z1}))\ (\neg(\texttt{a[z1]=1})$$
$$(\texttt{w[z1]=}\bot)\ (\neg(\texttt{a[z1]=8}))$$
$$(\neg(\texttt{z3=z2}))\ (\texttt{s[z2]=}\ \top)\ (\texttt{w[z2]=}\ \bot)$$
$$(\neg(\texttt{a[z2]=8}))\ (\texttt{a[z2]=4})\ (\neg(\texttt{z2=z3})$$
$$(\texttt{w[z1]=}\ \bot)\ (\texttt{z1<z2})\ (\texttt{s[z1]=}\ \bot)$$
$$(\texttt{a[z1]=2})\ (\texttt{z1<z2}))$$

- Node 108 at depth 10 generated by applying the sequence of transitions $(\tau_5(\texttt{z3}, \texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ (\texttt{a[z3]=4})\ (\neg(\texttt{z3=z2}))\ (\texttt{s[z2]=}\top)$$
$$(\texttt{w[z2]=}\bot)\ (\neg(\texttt{a[z2]=8}))\ (\texttt{a[z2]=2})$$
$$(\neg(\texttt{z2=z1}))\ (\neg(\texttt{a[z1]=1}))$$
$$(\texttt{w[z1]=}\bot)\ (\neg(\texttt{a[z1]=8}))\ (\neg(\texttt{z2=z3})$$
$$(\texttt{w[z1]=}\ \bot)\ (\texttt{z1<z2})\ (\texttt{s[z1]=}\ \bot)$$
$$(\texttt{a[z1]=3})\ (\texttt{z1<z2}))$$

- Node 109 at depth 10 generated by applying the sequence of transitions $(\tau_4(\texttt{z3}, \texttt{z1});\ \epsilon)^{-1}$

and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z1})\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=3})\ (\mathtt{z1<z2}))$$

- Node 110 at depth 10 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=4})\ (\neg(\mathtt{z2=z3})\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=3})\ (\mathtt{z1<z2}))$$

- Node 111 at depth 10 generated by applying the sequence of transitions $(\tau_4(\mathtt{z2}, \mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z3}))\ (\neg(\mathtt{a[z3]=1})\ (\mathtt{w[z3]=}\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{a[z1]=1})\ (\neg(\mathtt{z2=z1}))\ (\mathtt{s[z1]=}\top)\ (\mathtt{w[z1]=}\bot)\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 112 at depth 10 generated by applying the sequence of transitions $(\tau_1(\mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}. \quad (\wedge\ (\mathtt{a[z1]=1})\ (\mathtt{s[z2]=}\bot)\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z1})\ (\neg(\mathtt{=\ 2\ 1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{z2=z1}))\ (\mathtt{s[z1]=}\top)\ (\mathtt{w[z1]=}\bot)\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 113 at depth 10 generated by applying the sequence of transitions $(\tau_2(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\ \ (\wedge\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z1}))\ (\mathtt{s[z1]=}\top)\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{a[z1]=2})\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 114 at depth 10 generated by applying the sequence of transitions $(\tau_1(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z2]=1})(\mathtt{s[z1]=}\bot)\ (\mathtt{s[z3]=}\bot)\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3})\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=4})\ (\mathtt{z1<z2}))$$

- Node 115 at depth 10 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z1})\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=4})\ (\mathtt{z1<z2}))$$

- Node 116 at depth 10 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$

and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z3]=2) (}\neg\texttt{(z3=z1)) (}\neg\texttt{(a[z1]=1)}$$
$$\texttt{(w[z1]=}\bot\texttt{) (}\neg\texttt{(a[z1]=8))}$$
$$\texttt{(}\neg\texttt{(z3=z2)) (s[z2]=}\ \top\texttt{) (w[z2]=}\ \bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(a[z2]=8)) (a[z2]=3) (}\neg\texttt{(z2=z1)}$$
$$\texttt{(}\neg\texttt{(a[z1]=1)) (w[z1]=}\ \bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(a[z1]=8)) (}\neg\texttt{(z2=z3))}$$
$$\texttt{(w[z1]=}\ \bot\texttt{) (z1<z2) (s[z1]=}\ \bot\texttt{) (a[z1]=4)}$$
$$\texttt{(z1<z2))}$$

- Node 117 at depth 10 generated by applying the sequence of transitions $(\tau_2(\texttt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}, \texttt{z4}. \quad \texttt{(}\wedge\ \texttt{(a[z3]=2) (}\neg\texttt{(z3=z1)) (}\neg\texttt{(a[z1]=1)}$$
$$\texttt{(w[z1]=}\bot\texttt{) (}\neg\texttt{(a[z1]=8))}$$
$$\texttt{(}\neg\texttt{(z3=z4)) (s[z4]=}\ \top\texttt{) (w[z4]=}\ \bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(a[z4]=8)) (a[z2]=5)(w[z1]=}\ \bot\texttt{)}$$
$$\texttt{(z1<z2) (s[z1]=}\ \bot\texttt{) (z2<z3) (a[z1]=2)}$$
$$\texttt{(w[z2]=}\ \bot\texttt{) (}\neg\texttt{(z1=z3)) (w[z2]=}\ \bot\texttt{)}$$
$$\texttt{(z1<z2))}$$

- Node 118 at depth 10 generated by applying the sequence of transitions $(\tau_4(\texttt{z3}, \texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z3]=3) (}\neg\texttt{(z3=z2)) (}\neg\texttt{(a[z2]=1)}$$
$$\texttt{(w[z2]=}\bot\texttt{) (}\neg\texttt{(a[z2]=8))}$$
$$\texttt{(a[z1]=1) (s[z2]=}\ \bot\texttt{) (}\neg\texttt{(z3=z1))}$$
$$\texttt{(s[z1]=}\ \top\texttt{) (w[z1]=}\ \bot\texttt{) (a[z2]=5)(w[z1]=}\ \bot\texttt{)}$$
$$\texttt{(w[z2]=}\ \bot\texttt{) (z1<z2) (z2<z3) (}\neg\texttt{(z1=z3)}$$
$$\texttt{(w[z2]=}\ \bot\texttt{) (z1<z2))}$$

- Node 119 at depth 10 generated by applying the sequence of transitions $(\tau_2(\texttt{z3});\ \epsilon)^{-1}$

and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z3]=2) (}\neg\texttt{(z3=z1)) (}\neg\texttt{(a[z1]=1)}$$
$$\texttt{(w[z1]=}\bot\texttt{) (}\neg\texttt{(a[z1]=8))}$$
$$\texttt{(}\neg\texttt{(z3=z1)) (s[z1]=}\ \top\texttt{) (w[z1]=}\ \bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(a[z1]=8)) (a[z2]=5)(w[z1]=}\ \bot\texttt{)}$$
$$\texttt{(a[z1]=2) (w[z2]=}\ \bot\texttt{) (z1<z2) (z2<z3)}$$
$$\texttt{(}\neg\texttt{(z1=z3)) (w[z2]=}\ \bot\texttt{) (z1<z2))}$$

- Node 120 at depth 10 generated by applying the sequence of transitions $(\tau_3(\texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z1]=3) (a[z2]=1) (}\neg\texttt{(a[z3]=1))}$$
$$\texttt{(w[z3]=}\top\texttt{) (a[z2]=1)(s[z1]=}\bot\texttt{) (s[z3]=}\bot\texttt{)}$$
$$\texttt{(a[z3]=4) (}\neg\texttt{(z3=z2)) (s[z2]=}\top\texttt{)}$$
$$\texttt{(w[z2]=}\bot\texttt{) (}\neg\texttt{(z2=z1)) (}\neg\texttt{(z2=z3)}$$
$$\texttt{(z1<z2) (s[z1]=}\ \bot\texttt{) (z1<z2))}$$

- Node 121 at depth 10 generated by applying the sequence of transitions $(\tau_4(\texttt{z3}, \texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z3]=3) (}\neg\texttt{(z3=z1)) (}\neg\texttt{(a[z1]=1)}$$
$$\texttt{(w[z1]=}\bot\texttt{) (}\neg\texttt{(a[z1]=8))}$$
$$\texttt{(a[z2]=1)(s[z1]=}\ \bot\texttt{) (}\neg\texttt{(z3=z2))}$$
$$\texttt{(s[z2]=}\ \top\texttt{) (w[z2]=}\ \bot\texttt{) (}\neg\texttt{(z2=z1))}$$
$$\texttt{(}\neg\texttt{(a[z1]=1)) (w[z1]=}\ \bot\texttt{) (}\neg\texttt{(a[z1]=8)}$$
$$\texttt{(}\neg\texttt{(z2=z3)) (w[z1]=}\ \bot\texttt{)}$$
$$\texttt{(z1<z2) (s[z1]=}\ \bot\texttt{) (a[z1]=5) (z1<z2))}$$

- Node 122 at depth 10 generated by applying the sequence of transitions $(\tau_2(\texttt{z3});\ \epsilon)^{-1}$

and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad \begin{array}{c} \mathtt{(\wedge\ (a[z3]=2)\ (\neg(z3=z1))\ (\neg(a[z1]=1)} \\ \mathtt{(w[z1]=\bot)\ (\neg(a[z1]=8))} \\ \mathtt{(\neg(z3=z2))\ (s[z2]=\top)\ (w[z2]=\bot)} \\ \mathtt{(\neg(a[z2]=8))\ (a[z2]=2)\ (\neg(z2=z1)} \\ \mathtt{(\neg(a[z1]=1))\ (w[z1]=\bot)} \\ \mathtt{(\neg(a[z1]=8))\ (\neg(z2=z3))} \\ \mathtt{(w[z1]=\bot)\ (z1<z2)\ (s[z1]=\bot)\ (a[z1]=5)} \\ \mathtt{(z1<z2))} \end{array}$$

- Node 123 at depth 10 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad \begin{array}{c} \mathtt{(\wedge\ (a[z3]=2)\ (\neg(z3=z1))\ (\neg(a[z1]=1)} \\ \mathtt{(w[z1]=\bot)\ (\neg(a[z1]=8))} \\ \mathtt{(a[z2]=1)(s[z1]=\bot)\ (\neg(z3=z2))} \\ \mathtt{(s[z2]=\top)\ (w[z2]=\bot)\ (\neg(z2=z1))} \\ \mathtt{(\neg(a[z1]=1))\ (w[z1]=\bot)\ (\neg(a[z1]=8)} \\ \mathtt{(\neg(z2=z3))\ (w[z1]=\bot)} \\ \mathtt{(z1<z2)\ (s[z1]=\bot)\ (a[z1]=6)\ (z1<z2))} \end{array}$$

- Node 124 at depth 11 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3}, \mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad \begin{array}{c} \mathtt{(\wedge\ (a[z3]=4)\ (\neg(z3=z2))\ (s[z2]=\top)} \\ \mathtt{(w[z2]=\bot)\ (\neg(a[z2]=8))\ (a[z2]=2)} \\ \mathtt{(\neg(z2=z1))\ (\neg(a[z1]=1))} \\ \mathtt{(w[z1]=\bot)\ (\neg(a[z1]=8))\ (\neg(z2=z3)} \\ \mathtt{(w[z1]=\bot)\ (z1<z2)\ (s[z1]=\bot)} \\ \mathtt{(a[z1]=2)\ (z1<z2))} \end{array}$$

- Node 125 at depth 11 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$

and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z3]=3) (}\neg\texttt{(z3=z1)) (}\neg\texttt{(a[z1]=1)}$$
$$\texttt{(w[z1]=}\bot\texttt{) (}\neg\texttt{(a[z1]=8))}$$
$$\texttt{(}\neg\texttt{(z3=z2)) (s[z2]=}\top\texttt{) (w[z2]=}\bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(a[z2]=8)) (a[z2]=3) (}\neg\texttt{(z2=z1)}$$
$$\texttt{(}\neg\texttt{(a[z1]=1)) (w[z1]=}\bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(a[z1]=8)) (}\neg\texttt{(z2=z3))}$$
$$\texttt{(w[z1]=}\bot\texttt{) (z1<z2) (s[z1]=}\bot\texttt{) (a[z1]=2)}$$
$$\texttt{(z1<z2))}$$

- Node 126 at depth 11 generated by applying the sequence of transitions $(\tau_2(\texttt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z3]=2) (}\neg\texttt{(z3=z1)) (}\neg\texttt{(a[z1]=1)}$$
$$\texttt{(w[z1]=}\bot\texttt{) (}\neg\texttt{(a[z1]=8))}$$
$$\texttt{(}\neg\texttt{(z3=z2)) (s[z2]=}\top\texttt{) (w[z2]=}\bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(a[z2]=8)) (a[z2]=4) (}\neg\texttt{(z2=z3)}$$
$$\texttt{(w[z1]=}\bot\texttt{) (z1<z2) (s[z1]=}\bot\texttt{)}$$
$$\texttt{(a[z1]=2) (z1<z2))}$$

- Node 127 at depth 11 generated by applying the sequence of transitions $(\tau_1(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z2]=1)(s[z1]=}\bot\texttt{) (s[z3]=}\bot\texttt{) (a[z3]=4)}$$
$$\texttt{(}\neg\texttt{(z3=z2)) (s[z2]=}\top\texttt{) (w[z2]=}\bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(z2=z1)) (}\neg\texttt{(a[z1]=1))}$$
$$\texttt{(w[z1]=}\bot\texttt{) (}\neg\texttt{(a[z1]=8)) (}\neg\texttt{(z2=z3)}$$
$$\texttt{(w[z1]=}\bot\texttt{) (z1<z2) (s[z1]=}\bot\texttt{)}$$
$$\texttt{(a[z1]=3) (z1<z2))}$$

- Node 128 at depth 11 generated by applying the sequence of transitions $(\tau_4(\texttt{z3}, \texttt{z1});\ \epsilon)^{-1}$

and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z3]=3) (}\neg\texttt{(z3=z1)) (}\neg\texttt{(a[z1]=1)}$$
$$\texttt{(w[z1]=}\bot\texttt{) (}\neg\texttt{(a[z1]=8))}$$
$$\texttt{(}\neg\texttt{(z3=z2)) (s[z2]=}\ \top\texttt{) (w[z2]=}\ \bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(a[z2]=8)) (a[z2]=2) (}\neg\texttt{(z2=z1)}$$
$$\texttt{(}\neg\texttt{(a[z1]=1)) (w[z1]=}\ \bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(a[z1]=8)) (}\neg\texttt{(z2=z3))}$$
$$\texttt{(w[z1]=}\ \bot\texttt{) (z1<z2) (s[z1]=}\ \bot\texttt{) (a[z1]=3)}$$
$$\texttt{(z1<z2))}$$

- Node 129 at depth 11 generated by applying the sequence of transitions $(\tau_2(\texttt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z3]=2) (}\neg\texttt{(z3=z1)) (}\neg\texttt{(a[z1]=1)}$$
$$\texttt{(w[z1]=}\bot\texttt{) (}\neg\texttt{(a[z1]=8))}$$
$$\texttt{(}\neg\texttt{(z3=z2)) (s[z2]=}\ \top\texttt{) (w[z2]=}\ \bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(a[z2]=8)) (a[z2]=3) (}\neg\texttt{(z2=z1)}$$
$$\texttt{(}\neg\texttt{(a[z1]=1)) (w[z1]=}\ \bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(a[z1]=8)) (}\neg\texttt{(z2=z3))}$$
$$\texttt{(w[z1]=}\ \bot\texttt{) (z1<z2) (s[z1]=}\ \bot\texttt{) (a[z1]=3)}$$
$$\texttt{(z1<z2))}$$

- Node 130 at depth 11 generated by applying the sequence of transitions $(\tau_2(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z2]=2) (}\neg\texttt{(z2=z3)) (}\neg\texttt{(a[z3]=1)}$$
$$\texttt{(w[z3]=}\bot\texttt{) (}\neg\texttt{(a[z3]=8))}$$
$$\texttt{(a[z1]=1) (}\neg\texttt{(z2=z1)) (s[z1]=}\ \top\texttt{)}$$
$$\texttt{(w[z1]=}\ \bot\texttt{) (w[z1]=}\ \bot\texttt{) (z1<z2) (z1<z2))}$$

- Node 131 at depth 11 generated by applying the sequence of transitions $(\tau_3(\texttt{z3});\ \epsilon)^{-1}$

and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z3]=3)(a[z1]=1)}\ \texttt{(}\neg\texttt{(a[z2]=1))}$$
$$\texttt{(w[z2]=}\top\texttt{)}\ \texttt{(a[z2]=3)}\ \texttt{(}\neg\texttt{(z2=z3))}$$
$$\texttt{(a[z1]=1)}\ \texttt{(}\neg\texttt{(z2=z1))}\ \texttt{(s[z1]=}\ \top\texttt{)}$$
$$\texttt{(w[z1]=}\ \bot\texttt{)}\ \texttt{(w[z1]=}\ \bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(z1<z2))}$$

- Node 132 at depth 11 generated by applying the sequence of transitions $(\tau_5(\texttt{z3}, \texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z3]=4)}\ \texttt{(}\neg\texttt{(z3=z1))}\ \texttt{(s[z1]=}\top\texttt{)}$$
$$\texttt{(w[z1]=}\bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z1]=8))}\ \texttt{(a[z2]=3)}$$
$$\texttt{(}\neg\texttt{(z2=z3))}\ \texttt{(a[z1]=1)}\ \texttt{(}\neg\texttt{(z2=z1)}$$
$$\texttt{(s[z1]=}\ \top\texttt{)}\ \texttt{(w[z1]=}\ \bot\texttt{)}\ \texttt{(w[z1]=}\ \bot\texttt{)}$$
$$\texttt{(z1<z2)}\ \texttt{(z1<z2))}$$

- Node 133 at depth 11 generated by applying the sequence of transitions $(\tau_1(\texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}. \quad \texttt{(}\wedge\ \texttt{(a[z1]=1)}\ \texttt{(s[z2]=}\bot\texttt{)}\ \texttt{(a[z2]=2)}\ \texttt{(}\neg\texttt{(z2=z1)}$$
$$\texttt{(}\neg\texttt{(= 2 1))}\ \texttt{(w[z1]=}\bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(z2=z1))}\ \texttt{(s[z1]=}\ \top\texttt{)}\ \texttt{(w[z1]=}\ \bot\texttt{)}$$
$$\texttt{(w[z1]=}\ \bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(z1<z2))}$$

- Node 134 at depth 11 generated by applying the sequence of transitions $(\tau_4(\texttt{z1}, \texttt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z1]=3)}\ \texttt{(}\neg\texttt{(z1=z3))}\ \texttt{(}\neg\texttt{(a[z3]=1)}$$
$$\texttt{(w[z3]=}\bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z3]=8))}$$
$$\texttt{(a[z2]=1)}\ \texttt{(s[z3]=}\ \bot\texttt{)}\ \texttt{(a[z3]=4)}\ \texttt{(}\neg\texttt{(z3=z2)}$$
$$\texttt{(s[z2]=}\ \top\texttt{)}\ \texttt{(w[z2]=}\ \bot\texttt{)}\ \texttt{(}\neg\texttt{(z2=z1)}$$
$$\texttt{(w[z1]=}\bot\texttt{)}\ \texttt{(}\neg\texttt{(z2=z3))}$$
$$\texttt{(w[z1]=}\ \bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(z1<z2))}$$

- Node 135 at depth 11 generated by applying the sequence of transitions $(\tau_4(\mathtt{z1}, \mathtt{z4});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}. \quad (\wedge\ (\mathtt{a[z1]=3})\ (\neg(\mathtt{z1=z4}))\ (\neg(\mathtt{a[z4]=1})\ (\mathtt{w[z4]=}\bot)\ (\neg(\mathtt{a[z4]=8}))\ (\mathtt{a[z2]=1})\ (\mathtt{s[z3]=}\ \bot)\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z2})\ (\mathtt{s[z2]=}\ \top)\ (\mathtt{w[z2]=}\ \bot)\ (\neg(\mathtt{z2=z1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 136 at depth 11 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z2]=1})(\mathtt{s[z1]=}\ \bot)\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\ \top)\ (\mathtt{w[z2]=}\ \bot)\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\ \bot)\ (\neg(\mathtt{a[z1]=8})\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\ \bot)\ (\mathtt{a[z1]=4})\ (\mathtt{z1<z2}))$$

- Node 137 at depth 11 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\ \top)\ (\mathtt{w[z2]=}\ \bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z1})\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\ \bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\ \bot)\ (\mathtt{a[z1]=4})\ (\mathtt{z1<z2}))$$

- Node 138 at depth 11 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$

and labelled by

$\exists$z1, z2, z3. (∧ (a[z3]=2) (¬(z3=z2)) (¬(a[z2]=1)
(w[z2]=⊥) (¬(a[z2]=8))
(a[z1]=1) (s[z2]= ⊥) (¬(z3=z1))
(s[z1]= ⊤) (w[z1]= ⊥) (a[z2]=5)(w[z1]= ⊥)
(w[z2]= ⊥) (z1<z2) (z2<z3) (¬(z1=z3)
(w[z2]= ⊥) (z1<z2))

- Node 139 at depth 11 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$\exists$z1, z2, z3. (∧ (a[z3]=3) (¬(z3=z1)) (¬(a[z1]=1)
(w[z1]=⊥) (¬(a[z1]=8))
(a[z1]=3) (a[z2]=1) (w[z3]=⊤) (a[z2]=1)
(s[z1]= ⊥) (¬(z3=z2)) (s[z2]= ⊤)
(w[z2]= ⊥) (¬(z2=z1)) (¬(z2=z3)
(z1<z2) (s[z1]= ⊥) (z1<z2))

- Node 140 at depth 11 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z4});\ \epsilon)^{-1}$ and labelled by

$\exists$z1, z2, z3, z4. (∧ (a[z3]=3) (¬(z3=z4)) (¬(a[z4]=1)
(w[z4]=⊥) (¬(a[z4]=8))
(a[z1]=3) (a[z2]=1) (w[z3]=⊤) (a[z2]=1)
(s[z1]= ⊥) (¬(z3=z2)) (s[z2]= ⊤)
(w[z2]= ⊥) (¬(z2=z1)) (¬(z2=z3)
(z1<z2) (s[z1]= ⊥) (z1<z2))

- Node 141 at depth 11 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$

and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z3]=2) (}\neg\texttt{(z3=z1)) (}\neg\texttt{(a[z1]=1)}$$
$$\texttt{(w[z1]=}\bot\texttt{) (}\neg\texttt{(a[z1]=8))}$$
$$\texttt{(a[z2]=1)(s[z1]=}\ \bot\texttt{) (}\neg\texttt{(z3=z2))}$$
$$\texttt{(s[z2]=}\ \top\texttt{) (w[z2]=}\ \bot\texttt{) (}\neg\texttt{(z2=z1))}$$
$$\texttt{(}\neg\texttt{(a[z1]=1)) (w[z1]=}\ \bot\texttt{) (}\neg\texttt{(a[z1]=8)}$$
$$\texttt{(}\neg\texttt{(z2=z3)) (w[z1]=}\ \bot\texttt{)}$$
$$\texttt{(z1<z2) (s[z1]=}\ \bot\texttt{) (a[z1]=5) (z1<z2))}$$

- Node 142 at depth 11 generated by applying the sequence of transitions $(\tau_3(\texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z1]=3) (a[z2]=1) (}\neg\texttt{(a[z3]=1))}$$
$$\texttt{(w[z3]=}\top\texttt{) (a[z3]=3) (}\neg\texttt{(z3=z1))}$$
$$\texttt{(a[z2]=1)(s[z1]=}\ \bot\texttt{) (}\neg\texttt{(z3=z2))}$$
$$\texttt{(s[z2]=}\ \top\texttt{) (w[z2]=}\ \bot\texttt{) (}\neg\texttt{(z2=z1))}$$
$$\texttt{(}\neg\texttt{(z2=z3)) (z1<z2) (s[z1]=}\ \bot\texttt{)}$$
$$\texttt{(z1<z2))}$$

- Node 143 at depth 12 generated by applying the sequence of transitions $(\tau_1(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z2]=1)(s[z1]=}\bot\texttt{) (s[z3]=}\bot\texttt{) (a[z3]=4)}$$
$$\texttt{(}\neg\texttt{(z3=z2)) (s[z2]=}\top\texttt{) (w[z2]=}\bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(z2=z1)) (}\neg\texttt{(a[z1]=1))}$$
$$\texttt{(w[z1]=}\bot\texttt{) (}\neg\texttt{(a[z1]=8)) (}\neg\texttt{(z2=z3)}$$
$$\texttt{(w[z1]=}\ \bot\texttt{) (z1<z2) (s[z1]=}\ \bot\texttt{)}$$
$$\texttt{(a[z1]=2) (z1<z2))}$$

- Node 144 at depth 12 generated by applying the sequence of transitions $(\tau_4(\texttt{z3}, \texttt{z1});\ \epsilon)^{-1}$

and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z3]=3) (}\neg\texttt{(z3=z1)) (}\neg\texttt{(a[z1]=1)}$$
$$\texttt{(w[z1]=}\bot\texttt{) (}\neg\texttt{(a[z1]=8))}$$
$$\texttt{(}\neg\texttt{(z3=z2)) (s[z2]=}\ \top\texttt{) (w[z2]=}\ \bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(a[z2]=8)) (a[z2]=2) (}\neg\texttt{(z2=z1)}$$
$$\texttt{(}\neg\texttt{(a[z1]=1)) (w[z1]=}\ \bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(a[z1]=8)) (}\neg\texttt{(z2=z3))}$$
$$\texttt{(w[z1]=}\ \bot\texttt{) (z1<z2) (s[z1]=}\ \bot\texttt{) (a[z1]=2)}$$
$$\texttt{(z1<z2))}$$

- Node 145 at depth 12 generated by applying the sequence of transitions $(\tau_2(\texttt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z3]=2) (}\neg\texttt{(z3=z1)) (}\neg\texttt{(a[z1]=1)}$$
$$\texttt{(w[z1]=}\bot\texttt{) (}\neg\texttt{(a[z1]=8))}$$
$$\texttt{(}\neg\texttt{(z3=z2)) (s[z2]=}\ \top\texttt{) (w[z2]=}\ \bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(a[z2]=8)) (a[z2]=3) (}\neg\texttt{(z2=z1)}$$
$$\texttt{(}\neg\texttt{(a[z1]=1)) (w[z1]=}\ \bot\texttt{)}$$
$$\texttt{(}\neg\texttt{(a[z1]=8)) (}\neg\texttt{(z2=z3))}$$
$$\texttt{(w[z1]=}\ \bot\texttt{) (z1<z2) (s[z1]=}\ \bot\texttt{) (a[z1]=2)}$$
$$\texttt{(z1<z2))}$$

- Node 146 at depth 12 generated by applying the sequence of transitions $(\tau_4(\texttt{z3}, \texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}. \quad \texttt{(}\wedge\ \texttt{(a[z3]=3) (}\neg\texttt{(z3=z1)) (}\neg\texttt{(a[z1]=1)}$$
$$\texttt{(w[z1]=}\bot\texttt{) (}\neg\texttt{(a[z1]=8))}$$
$$\texttt{(a[z2]=1)(s[z1]=}\ \bot\texttt{) (}\neg\texttt{(z3=z2))}$$
$$\texttt{(s[z2]=}\ \top\texttt{) (w[z2]=}\ \bot\texttt{) (}\neg\texttt{(z2=z1))}$$
$$\texttt{(}\neg\texttt{(a[z1]=1)) (w[z1]=}\ \bot\texttt{) (}\neg\texttt{(a[z1]=8)}$$
$$\texttt{(}\neg\texttt{(z2=z3)) (w[z1]=}\ \bot\texttt{)}$$
$$\texttt{(z1<z2) (s[z1]=}\ \bot\texttt{) (a[z1]=3) (z1<z2))}$$

- Node 147 at depth 12 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z1})\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=3})\ (\mathtt{z1<z2}))$$

- Node 148 at depth 12 generated by applying the sequence of transitions $(\tau_3(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=3})(\mathtt{a[z1]=1})\ (\neg(\mathtt{a[z2]=1}))\ (\mathtt{w[z2]=}\top)\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z3}))\ (\mathtt{a[z1]=1})\ (\neg(\mathtt{z2=z1}))\ (\mathtt{s[z1]=}\top)\ (\mathtt{w[z1]=}\bot)\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 149 at depth 12 generated by applying the sequence of transitions $(\tau_5(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z1}))\ (\mathtt{s[z1]=}\top)\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z3}))\ (\mathtt{a[z1]=1})\ (\neg(\mathtt{z2=z1})\ (\mathtt{s[z1]=}\top)\ (\mathtt{w[z1]=}\bot)\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 150 at depth 12 generated by applying the sequence of transitions $(\tau_2(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z2]=2})\ (\mathtt{a[z3]=3})(\mathtt{a[z1]=1})\ (\neg(\mathtt{z2=z3})\ (\mathtt{a[z1]=1})\ (\neg(\mathtt{z2=z1}))\ (\mathtt{s[z1]=}\top)\ (\mathtt{w[z1]=}\bot)\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 151 at depth 12 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=2})\ (\mathtt{a[z1]=1})\ (\neg(\mathtt{a[z2]=1}))\ (\mathtt{w[z2]=}\top)\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z3}))\ (\mathtt{a[z1]=1})\ (\neg(\mathtt{z2=z1}))\ (\mathtt{s[z1]=}\ \top)\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 152 at depth 12 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z2}))\ (\neg(\mathtt{a[z2]=1})\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\neg(\mathtt{z3=z1}))\ (\mathtt{s[z1]=}\ \top)\ (\mathtt{w[z1]=}\ \bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z3})\ (\mathtt{a[z1]=1})\ (\neg(\mathtt{z2=z1}))\ (\mathtt{s[z1]=}\ \top)\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 153 at depth 12 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z1]=3})\ (\neg(\mathtt{z1=z3}))\ (\mathtt{w[z3]=}\bot)\ (\mathtt{a[z2]=1})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\ \top)\ (\mathtt{w[z2]=}\ \bot)\ (\neg(\mathtt{z2=z1}))\ (\mathtt{w[z1]=}\ \bot)\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 154 at depth 12 generated by applying the sequence of transitions $(\tau_4(\mathtt{z3}, \mathtt{z1});\ \epsilon)^{-1}$

and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}.\ \ (\wedge\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z1]=3})\ (\neg(\mathtt{z1=z4}))\ (\neg(\mathtt{a[z4]=1})\ (\mathtt{w[z4]=}\bot)\ (\neg(\mathtt{a[z4]=8}))\ (\mathtt{a[z2]=1})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{z2=z1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 155 at depth 12 generated by applying the sequence of transitions $(\tau_5(\mathtt{z4}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}.\ \ (\wedge\ (\mathtt{a[z4]=4})\ (\neg(\mathtt{z4=z1}))\ (\mathtt{s[z1]=}\top)\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z1]=3})\ (\neg(\mathtt{z1=z4}))\ (\mathtt{a[z2]=1})\ (\mathtt{s[z3]=}\bot)\ (\mathtt{a[z3]=4})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{z2=z1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 156 at depth 12 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z2]=1})(\mathtt{s[z1]=}\bot)\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8})\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=4})\ (\mathtt{z1<z2}))$$

- Node 157 at depth 12 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$

and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})$$
$$(\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))$$
$$(\mathtt{a[z1]=3})\ (\mathtt{a[z2]=1})\ (\mathtt{a[z2]=1})(\mathtt{s[z1]=}\ \bot)$$
$$(\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\ \top)\ (\mathtt{w[z2]=}\ \bot)$$
$$(\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{z2=z3}))$$
$$(\mathtt{z1<z2})\ (\mathtt{s[z1]=}\ \bot)\ (\mathtt{z1<z2}))$$

- Node 158 at depth 12 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}. \quad (\wedge\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z4}))\ (\neg(\mathtt{a[z4]=1})$$
$$(\mathtt{w[z4]=}\bot)\ (\neg(\mathtt{a[z4]=8}))$$
$$(\mathtt{a[z1]=3})\ (\mathtt{a[z2]=1})\ (\mathtt{a[z2]=1})(\mathtt{s[z1]=}\ \bot)$$
$$(\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\ \top)\ (\mathtt{w[z2]=}\ \bot)$$
$$(\neg(\mathtt{z2=z1}))\ (\neg(\mathtt{z2=z3}))$$
$$(\mathtt{z1<z2})\ (\mathtt{s[z1]=}\ \bot)\ (\mathtt{z1<z2}))$$

- Node 159 at depth 12 generated by applying the sequence of transitions $(\tau_3(\mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z1]=3})\ (\mathtt{a[z2]=1})\ (\neg(\mathtt{a[z3]=1}))$$
$$(\mathtt{w[z3]=}\top)\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))$$
$$(\mathtt{a[z2]=1})(\mathtt{s[z1]=}\ \bot)\ (\neg(\mathtt{z3=z2}))$$
$$(\mathtt{s[z2]=}\ \top)\ (\mathtt{w[z2]=}\ \bot)\ (\neg(\mathtt{z2=z1}))$$
$$(\neg(\mathtt{z2=z3}))\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\ \bot)$$
$$(\mathtt{z1<z2}))$$

- Node 160 at depth 12 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$

and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ \texttt{(a[z3]=2)}\ \texttt{(a[z1]=3)}\ \texttt{(a[z2]=1)}\ (\neg\texttt{(z3=z1)}$$
$$\texttt{(a[z2]=1)(s[z1]=}\ \bot)\ (\neg\texttt{(z3=z2)}$$
$$\texttt{(s[z2]=}\ \top)\ \texttt{(w[z2]=}\ \bot)\ (\neg\texttt{(z2=z1)}$$
$$\texttt{(}\neg\texttt{(z2=z3))}\ \texttt{(z1<z2)}$$
$$\texttt{(s[z1]=}\ \bot)\ \texttt{(z1<z2))}$$

- Node 161 at depth 13 generated by applying the sequence of transitions $(\tau_4(\texttt{z3}, \texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ \texttt{(a[z3]=3)}\ (\neg\texttt{(z3=z1))}\ (\neg\texttt{(a[z1]=1)}$$
$$\texttt{(w[z1]=}\bot)\ (\neg\texttt{(a[z1]=8))}$$
$$\texttt{(a[z2]=1)(s[z1]=}\ \bot)\ (\neg\texttt{(z3=z2))}$$
$$\texttt{(s[z2]=}\ \top)\ \texttt{(w[z2]=}\ \bot)\ (\neg\texttt{(z2=z1))}$$
$$(\neg\texttt{(a[z1]=1))}\ \texttt{(w[z1]=}\ \bot)\ (\neg\texttt{(a[z1]=8)}$$
$$\texttt{(}\neg\texttt{(z2=z3))}\ \texttt{(w[z1]=}\ \bot)$$
$$\texttt{(z1<z2)}\ \texttt{(s[z1]=}\ \bot)\ \texttt{(a[z1]=2)}\ \texttt{(z1<z2))}$$

- Node 162 at depth 13 generated by applying the sequence of transitions $(\tau_2(\texttt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ \texttt{(a[z3]=2)}\ (\neg\texttt{(z3=z1))}\ (\neg\texttt{(a[z1]=1)}$$
$$\texttt{(w[z1]=}\bot)\ (\neg\texttt{(a[z1]=8))}$$
$$\texttt{(}\neg\texttt{(z3=z2))}\ \texttt{(s[z2]=}\ \top)\ \texttt{(w[z2]=}\ \bot)$$
$$\texttt{(}\neg\texttt{(a[z2]=8))}\ \texttt{(a[z2]=2)}\ (\neg\texttt{(z2=z1)}$$
$$\texttt{(}\neg\texttt{(a[z1]=1))}\ \texttt{(w[z1]=}\ \bot)$$
$$\texttt{(}\neg\texttt{(a[z1]=8))}\ \texttt{(}\neg\texttt{(z2=z3))}$$
$$\texttt{(w[z1]=}\ \bot)\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\ \bot)\ \texttt{(a[z1]=2)}$$
$$\texttt{(z1<z2))}$$

- Node 163 at depth 13 generated by applying the sequence of transitions $(\tau_2(\texttt{z3});\ \epsilon)^{-1}$

and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=2})\ (\mathtt{a[z1]=1})\ (\neg(\mathtt{a[z2]=1}))\ (\mathtt{w[z2]=}\top)\ (\mathtt{a[z2]=2})\ (\neg(\mathtt{z2=z3}))\ (\mathtt{a[z1]=1})\ (\neg(\mathtt{z2=z1}))\ (\mathtt{s[z1]=}\ \top)\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 164 at depth 13 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=2})\ (\mathtt{a[z2]=2})\ (\mathtt{a[z1]=1})\ (\neg(\mathtt{z2=z3})\ (\mathtt{a[z1]=1})\ (\neg(\mathtt{z2=z1}))\ (\mathtt{s[z1]=}\ \top)\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 165 at depth 13 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}. \quad (\wedge\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z2}))\ (\neg(\mathtt{a[z2]=1})\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\neg(\mathtt{z3=z1}))\ (\mathtt{s[z1]=}\ \top)\ (\mathtt{w[z1]=}\ \bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z2]=3})\ (\neg(\mathtt{z2=z3})\ (\mathtt{a[z1]=1})\ (\neg(\mathtt{z2=z1}))\ (\mathtt{s[z1]=}\ \top)\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 166 at depth 13 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}. \quad (\wedge\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z1]=3})\ (\neg(\mathtt{z1=z4}))\ (\neg(\mathtt{a[z4]=1})\ (\mathtt{w[z4]=}\ \bot)\ (\neg(\mathtt{a[z4]=8}))\ (\mathtt{a[z2]=1})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\ \top)\ (\mathtt{w[z2]=}\ \bot)\ (\neg(\mathtt{z2=z1}))\ (\mathtt{w[z1]=}\ \bot)\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\ \bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 167 at depth 13 generated by applying the sequence of transitions $(\tau_5(\mathtt{z4}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}.\ \ (\wedge\ (\mathtt{a[z4]=4})\ (\neg(\mathtt{z4=z1}))\ (\mathtt{s[z1]=}\top)$$
$$(\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z3]=3})$$
$$(\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1}))$$
$$(\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z1]=3})$$
$$(\neg(\mathtt{z1=z4}))\ (\mathtt{a[z2]=1})\ (\neg(\mathtt{z3=z2})$$
$$(\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{z2=z1})$$
$$(\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{z2=z3}))$$
$$(\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 168 at depth 13 generated by applying the sequence of transitions $(\tau_4(\mathtt{z1}, \mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z1]=3})\ (\neg(\mathtt{z1=z3}))\ (\neg(\mathtt{a[z3]=1})$$
$$(\mathtt{w[z3]=}\bot)\ (\neg(\mathtt{a[z3]=8}))$$
$$(\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))\ (\mathtt{w[z1]=}\bot)$$
$$(\mathtt{a[z2]=1})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)$$
$$(\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{z2=z1}))\ (\mathtt{w[z1]=}\bot)$$
$$(\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})$$
$$(\mathtt{z1<z2}))$$

- Node 169 at depth 14 generated by applying the sequence of transitions $(\tau_2(\mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ \ (\wedge\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1})$$
$$(\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))$$
$$(\mathtt{a[z2]=1})(\mathtt{s[z1]=}\bot)\ (\neg(\mathtt{z3=z2}))$$
$$(\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{z2=z1}))$$
$$(\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8})$$
$$(\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)$$
$$(\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=2}))$$

- Node 170 at depth 14 generated by applying the sequence of transitions $(\tau_5(\mathtt{z4}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}.\ \ (\wedge\ (\mathtt{a[z4]=4})\ (\neg(\mathtt{z4=z1}))\ (\mathtt{s[z1]=}\top)\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1}))\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z1]=3})\ (\neg(\mathtt{z1=z4}))\ (\mathtt{a[z2]=1})\ (\neg(\mathtt{z3=z2})\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{z2=z1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 171 at depth 14 generated by applying the sequence of transitions $(\tau_4(\mathtt{z4}, \mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}.\ \ (\wedge\ (\mathtt{a[z4]=3})\ (\neg(\mathtt{z4=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z4=z1}))\ (\mathtt{s[z1]=}\top)\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z3]=3})\ (\neg(\mathtt{z3=z1})\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z1]=3})\ (\neg(\mathtt{z1=z4})\ (\mathtt{a[z2]=1})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{z2=z1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 172 at depth 15 generated by applying the sequence of transitions $(\tau_4(\mathtt{z4}, \mathtt{z1});\ \epsilon)^{-1}$

and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}.\ \ (\wedge\ (\mathtt{a[z4]=3})\ (\neg(\mathtt{z4=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z4=z1}))\ (\mathtt{s[z1]=}\top)\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1})\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z1]=3})\ (\neg(\mathtt{z1=z4})\ (\mathtt{a[z2]=1})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{z2=z1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

- Node 173 at depth 16 generated by applying the sequence of transitions $(\tau_2(\mathtt{z4});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}, \mathtt{z4}.\ \ (\wedge\ (\mathtt{a[z4]=2})\ (\neg(\mathtt{z4=z1}))\ (\neg(\mathtt{a[z1]=1})\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\neg(\mathtt{z4=z1}))\ (\mathtt{s[z1]=}\top)\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z3]=2})\ (\neg(\mathtt{z3=z1})\ (\neg(\mathtt{a[z1]=1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{a[z1]=8}))\ (\mathtt{a[z1]=3})\ (\neg(\mathtt{z1=z4})\ (\mathtt{a[z2]=1})\ (\neg(\mathtt{z3=z2}))\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{z2=z1}))\ (\mathtt{w[z1]=}\bot)\ (\neg(\mathtt{z2=z3}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{z1<z2}))$$

C.3 Szymanski with invariants

Synthesized invariants

An implication $p \Rightarrow q$ is written as $(\Rightarrow\ p\ \ q)$.

$$
\begin{aligned}
Inv_1(\mathtt{a},\mathtt{s},\mathtt{w}) &:= \forall \mathtt{z1}.(\Rightarrow\ (\mathtt{a[z1]=7})\ (\mathtt{s[z1]=}\top)) \\
Inv_2(\mathtt{a},\mathtt{s},\mathtt{w}) &:= \forall \mathtt{z1}.(\Rightarrow\ (\mathtt{a[z1]=6})\ (\mathtt{s[z1]=}\top)) \\
Inv_3(\mathtt{a},\mathtt{s},\mathtt{w}) &:= \forall \mathtt{z1}.(\Rightarrow\ (\mathtt{a[z1]=5})\ (\mathtt{s[z1]=}\top)) \\
Inv_4(\mathtt{a},\mathtt{s},\mathtt{w}) &:= \forall \mathtt{z1}.(\Rightarrow\ (\mathtt{a[z1]=3})\ (\mathtt{s[z1]=}\top)) \\
Inv_5(\mathtt{a},\mathtt{s},\mathtt{w}) &:= \forall \mathtt{z1}.(\Rightarrow\ (\mathtt{a[z1]=3})\ (\mathtt{w[z1]=}\top)) \\
Inv_6(\mathtt{a},\mathtt{s},\mathtt{w}) &:= \forall \mathtt{z1}.(\Rightarrow\ (\mathtt{a[z1]=4})\ (\neg\ (\wedge\ (\mathtt{s[z1]=}\bot)\ (\mathtt{w[z1]=}\top)))) \\
Inv_7(\mathtt{a},\mathtt{s},\mathtt{w}) &:= \forall \mathtt{z1}.(\Rightarrow\ (\mathtt{a[z1]=2})\ (\neg\ (\wedge\ (\mathtt{s[z1]=}\bot)\ (\mathtt{w[z1]=}\top)))) \\
Inv_8(\mathtt{a},\mathtt{s},\mathtt{w}) &:= \forall \mathtt{z1}.(\Rightarrow\ (\mathtt{a[z1]=1})\ (\neg\ (\wedge\ (\mathtt{s[z1]=}\bot)\ (\mathtt{w[z1]=}\top))))
\end{aligned}
$$

Interestingly, the invariants synthesized by our tool formally state relationships between the control location stored in the program counter `a` *and the values stored in the flags* `s` *and* `w`*. For example,* Inv_1 *tells us that if a process is at control location* `7`*, then the value of the flag* `s` *must be set to true.*

Indeed, the effects of such invariants is to make redundant all those transitions which are enabled in a certain state which sets the value of the auxiliary flags to a value which is incompatible with that prescribed by the invariants. See Section C.4 below for more on how to synthesize invariants and how they prune the search space.

List of reachable nodes

The formula labelling node i *in Figure 3 may be different from that labelling node* i *in Figure 2. However, modulo renaming of nodes, it is possible to show that the graph in Figure 2 is a sub-graph of that in Figure 3 (this can be seen in Figure 4). The renaming* ρ *is defined as follows (mapping nodes in Figure 3 to those in Figure 2):*

$$
\begin{aligned}
0 \mapsto 0,\ \ 1 \mapsto 1,\ \ 2 \mapsto 2,\ \ 3 \mapsto 3,\ \ 4 \mapsto 6, \\
5 \mapsto 11,\ \ 6 \mapsto 12,\ \ 7 \mapsto 18,\ \ 8 \mapsto 20,\ \ 9 \mapsto 21, \\
10 \mapsto 30,\ \ 11 \mapsto 32,\ \ 12 \mapsto 33,\ \ 13 \mapsto 34,\ \ 14 \mapsto 44, \\
15 \mapsto 46,\ \ 16 \mapsto 48,\ \ 17 \mapsto 49,\ \ 18 \mapsto 62,\ \ 19 \mapsto 65, \\
20 \mapsto 67,\ \ 21 \mapsto 84,\ \ 22 \mapsto 105.
\end{aligned}
$$

It is not difficult to see that any $\exists^I$*-formula labelling node* i *in Figure 3 is logically* A_I^E*-equivalent to that labelling node* $\rho(i)$ *in Figure 2. Furthermore, it is also true that for any pair* (i, j) *of nodes in Figure 3, the label of the edge* (i, j) *is identical to that of the edge* $(\rho(i), \rho(j))$ *in Figure 2.*

- Node 0 at depth 0 generated by applying the sequence of transitions ϵ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z1]=7)}\ \texttt{(z1<z2)}\ \texttt{(a[z2]=7))}$$

- Node 1 at depth 1 generated by applying the sequence of transitions $(\tau_7(\texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z1]=6)}\ \texttt{(z1<z2)}\ \texttt{(a[z2]=7))}$$

- Node 2 at depth 1 generated by applying the sequence of transitions $(\tau_7(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z2]=6)(z1<z2)}\ \texttt{(s[z1]=}\bot\texttt{)}\ \texttt{(a[z1]=7)}\ \texttt{(z1<z2))}$$

- Node 3 at depth 2 generated by applying the sequence of transitions $(\tau_6(\texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z1]=5)}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(a[z2]=7))}$$

- Node 4 at depth 3 generated by applying the sequence of transitions $(\tau_5(\texttt{z1}, \texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z1]=4)}\ \texttt{(s[z2]=}\top\texttt{)}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z2]=8))}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(a[z2]=7))}$$

- Node 5 at depth 4 generated by applying the sequence of transitions $(\tau_4(\texttt{z1}, \texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z1]=3)}\ \texttt{(}\neg\texttt{(a[z2]=1))}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z2]=8))}\ \texttt{(s[z2]=}\ \top\texttt{)}\ \texttt{(w[z2]=}\ \bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z2]=8))}\ \texttt{(w[z2]=}\ \bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(a[z2]=7))}$$

- Node 6 at depth 4 generated by applying the sequence of transitions $(\tau_7(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z2]=6)}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\bot\texttt{)}\ \texttt{(a[z1]=4)}\ \texttt{(s[z2]=}\top\texttt{)}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(z1<z2))}$$

- Node 7 at depth 5 generated by applying the sequence of transitions $(\tau_2(\texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z1]=2)}\ \texttt{(}\neg\texttt{(a[z2]=1))}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z2]=8))}\ \texttt{(s[z2]=}\ \top\texttt{)}\ \texttt{(w[z2]=}\ \bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z2]=8))}\ \texttt{(w[z2]=}\ \bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(a[z2]=7))}$$

- Node 8 at depth 5 generated by applying the sequence of transitions $(\tau_4(\mathtt{z1}, \mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\quad (\wedge\ (\mathtt{a[z1]=3})\ (\neg(\mathtt{a[z2]=1}))\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=6})\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 9 at depth 5 generated by applying the sequence of transitions $(\tau_6(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\ (\wedge\ (\mathtt{a[z2]=5})\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=4})\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 10 at depth 6 generated by applying the sequence of transitions $(\tau_7(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\ (\wedge\ (\mathtt{a[z2]=6})\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=2})\ (\mathtt{w[z2]=}\bot)\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 11 at depth 6 generated by applying the sequence of transitions $(\tau_2(\mathtt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\ (\wedge\ (\mathtt{a[z1]=2})\ (\neg(\mathtt{a[z2]=1}))\ (\mathtt{w[z2]=}\bot)\ (\neg(\mathtt{a[z2]=8}))\ (\mathtt{a[z2]=6})\ (\mathtt{z1<z2})\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 12 at depth 6 generated by applying the sequence of transitions $(\tau_6(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\ (\wedge\ (\mathtt{a[z2]=5})\ (\mathtt{w[z1]=}\bot)\ (\mathtt{a[z1]=3})\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 13 at depth 6 generated by applying the sequence of transitions $(\tau_5(\mathtt{z2}, \mathtt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}, \mathtt{z3}.\ (\wedge\ (\mathtt{a[z2]=4})\ (\neg(\mathtt{z2=z3}))\ (\mathtt{s[z3]=}\top)\ (\mathtt{w[z3]=}\bot)\ (\neg(\mathtt{a[z3]=8}))\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=4})\ (\mathtt{z1<z2}))$$

- Node 14 at depth 7 generated by applying the sequence of transitions $(\tau_6(\mathtt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \mathtt{z1}, \mathtt{z2}.\quad (\wedge\ (\mathtt{a[z2]=5})\ (\mathtt{w[z1]=}\bot)\ (\mathtt{z1<z2})\ (\mathtt{s[z1]=}\bot)\ (\mathtt{a[z1]=2})\ (\mathtt{w[z2]=}\bot)\ (\mathtt{s[z2]=}\top)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{w[z2]=}\bot)\ (\mathtt{z1<z2}))$$

- Node 15 at depth 7 generated by applying the sequence of transitions $(\tau_6(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z2]=5)}\ \texttt{(w[z1]=}\bot\texttt{)}\ \texttt{(a[z1]=2)}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(s[z2]=}\ \top\texttt{)}\ \texttt{(w[z2]=}\ \bot\texttt{)}\ \texttt{(w[z2]=}\ \bot\texttt{)}\ \texttt{(z1<z2))}$$

- Node 16 at depth 7 generated by applying the sequence of transitions $(\tau_4(\texttt{z2}, \texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ \texttt{(a[z2]=3)}\ \texttt{(}\neg\texttt{(z2=z1))}\ \texttt{(}\neg\texttt{(a[z1]=1))}\ \texttt{(w[z1]=}\bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z1]=8))}\ \texttt{(}\neg\texttt{(z2=z3))}\ \texttt{(s[z3]=}\ \top\texttt{)}\ \texttt{(w[z3]=}\ \bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z3]=8))}\ \texttt{(w[z1]=}\ \bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\ \bot\texttt{)}\ \texttt{(a[z1]=4)}\ \texttt{(z1<z2))}$$

- Node 17 at depth 7 generated by applying the sequence of transitions $(\tau_5(\texttt{z3}, \texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ \texttt{(a[z3]=4)}\ \texttt{(}\neg\texttt{(z3=z2))}\ \texttt{(s[z2]=}\top\texttt{)}\ \texttt{(w[z2]=}\bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z2]=8))}\ \texttt{(a[z2]=4)}\ \texttt{(}\neg\texttt{(z2=z3))}\ \texttt{(w[z1]=}\bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\bot\texttt{)}\ \texttt{(a[z1]=4)}\ \texttt{(z1<z2))}$$

- Node 18 at depth 8 generated by applying the sequence of transitions $(\tau_5(\texttt{z2}, \texttt{z3});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ \texttt{(a[z2]=4)}\ \texttt{(}\neg\texttt{(z2=z3))}\ \texttt{(s[z3]=}\top\texttt{)}\ \texttt{(w[z3]=}\bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z3]=8))}\ \texttt{(w[z1]=}\bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\bot\texttt{)}\ \texttt{(a[z1]=2)}\ \texttt{(z1<z2))}$$

- Node 19 at depth 8 generated by applying the sequence of transitions $(\tau_5(\texttt{z2}, \texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}.\ \ (\wedge\ \texttt{(a[z2]=4)}\ \texttt{(}\neg\texttt{(z2=z1))}\ \texttt{(s[z1]=}\top\texttt{)}\ \texttt{(w[z1]=}\bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z1]=8))}\ \texttt{(w[z1]=}\bot\texttt{)}\ \texttt{(a[z1]=2)}\ \texttt{(z1<z2)}\ \texttt{(z1<z2))}$$

- Node 20 at depth 8 generated by applying the sequence of transitions $(\tau_2(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1}, \texttt{z2}, \texttt{z3}.\ \ (\wedge\ \texttt{(a[z2]=2)}\ \texttt{(}\neg\texttt{(z2=z1))}\ \texttt{(}\neg\texttt{(a[z1]=1))}\ \texttt{(w[z1]=}\bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z1]=8))}\ \texttt{(}\neg\texttt{(z2=z3))}\ \texttt{(s[z3]=}\ \top\texttt{)}\ \texttt{(w[z3]=}\ \bot\texttt{)}\ \texttt{(}\neg\texttt{(a[z3]=8))}\ \texttt{(w[z1]=}\ \bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\ \bot\texttt{)}\ \texttt{(a[z1]=4)}\ \texttt{(z1<z2))}$$

- Node 21 at depth 9 generated by applying the sequence of transitions $(\tau_4(\texttt{z2},\texttt{z1});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1},\texttt{z2},\texttt{z3}.\ \ (\wedge\ \texttt{(a[z2]=3)}\ (\neg\texttt{(a[z1]=1)})\ \texttt{(w[z1]=}\bot\texttt{)}\ (\neg\texttt{(a[z1]=8)})\ (\neg\texttt{(z2=z3)})\ \texttt{(s[z3]=}\top\texttt{)}\ \texttt{(w[z3]=}\bot\texttt{)}\ (\neg\texttt{(a[z3]=8)})\ \texttt{(w[z1]=}\bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\bot\texttt{)}\ \texttt{(a[z1]=2)}\ \texttt{(z1<z2)})$$

- Node 22 at depth 10 generated by applying the sequence of transitions $(\tau_2(\texttt{z2});\ \epsilon)^{-1}$ and labelled by

$$\exists \texttt{z1},\texttt{z2},\texttt{z3}.\ \ (\wedge\ \texttt{(a[z2]=2)}\ (\neg\texttt{(z2=z1)})\ (\neg\texttt{(a[z1]=1)})\ \texttt{(w[z1]=}\bot\texttt{)}\ (\neg\texttt{(a[z1]=8)})\ (\neg\texttt{(z2=z3)})\ \texttt{(s[z3]=}\top\texttt{)}\ \texttt{(w[z3]=}\bot\texttt{)}\ (\neg\texttt{(a[z3]=8)})\ \texttt{(w[z1]=}\bot\texttt{)}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\bot\texttt{)}\ \texttt{(a[z1]=2)})$$

C.4 Synthesized invariants and their effects

Consider node 2 *in Figure 4 (or, equivalently, in Figure 3 or 2). Without invariants (cf. Fig. 2), the fix-point test fails and transition* τ_6 *becomes applicable (on variable* z2*). Fortunately, it is possible to synthesize and invariant which makes node* 2 *redundant. Let us see how this done.*

Recall the $\exists^I$*-formula labelling node* 2*:*

$$\exists \texttt{z1},\texttt{z2}.\ \ (\wedge\ \texttt{(a[z2]=6)}\ \texttt{(z1<z2)}\ \texttt{(s[z1]=}\bot\texttt{)}\ \texttt{(a[z1]=7)}\ \texttt{(z1<z2)}). \tag{18}$$

By traversing (18)*, our heuristics forms two sets of literals each containing either variable* z1 *or variable* z2 *only, i.e.*

$$S_{\texttt{z1}} \ := \ \{\texttt{(s[z1]=}\bot\texttt{)},\texttt{(a[z1]=7)}\} \text{ and}$$
$$S_{\texttt{z2}} \ := \ \{\texttt{(a[z2]=6)}\}.$$

The literals in these two sets are used to guess the following two candidate invariants:

$$\forall \texttt{z1}.\neg(\wedge\ \texttt{(a[z1]=7)}\ \texttt{(s[z1]=}\bot\texttt{)}) \tag{19}$$
$$\forall \texttt{z1}.\neg\texttt{(a[z2]=6)}. \tag{20}$$

The negation of (19) *is passed to the backward reachable analysis algorithm in Figure 1 which returns* safe*; while it returns* unsafe *on the negation of* (20)*. As a consequence,* (19) *is a true safety invariant and it is recorded as* $Inv_1(\texttt{a},\texttt{s},\texttt{w})$*, which is shown logically equivalent to* (19) *by standard manipulations.*

Now, it is not difficult to see that the formula

$$\forall \texttt{x}.(\Rightarrow \texttt{(a[x]=7) (s[x]=}\top\texttt{))} \ \wedge$$
$$\exists \texttt{z1, z2}.(\wedge \texttt{ (a[z2]=6)(z1<z2) (s[z1]=}\bot\texttt{) (a[z1]=7) (z1<z2))}.$$

is A_I^E*-unsatisfiable (consider the existentially quantified variables* z1 *and* z2 *of* (18) *as (Skolem) constants and instantiate the universally quantified variable of* $Inv_1(\texttt{a}, \texttt{s}, \texttt{w})$ *to* z1*). So, by definition of invariant, we can avoid to further expand the sub-tree rooted at node* 2 *(the nodes of this sub-tree are boxed and shaded in Figure 4). Similar observations hold for nodes* $3, 48, 49, \ldots$ *in Figure 2.*

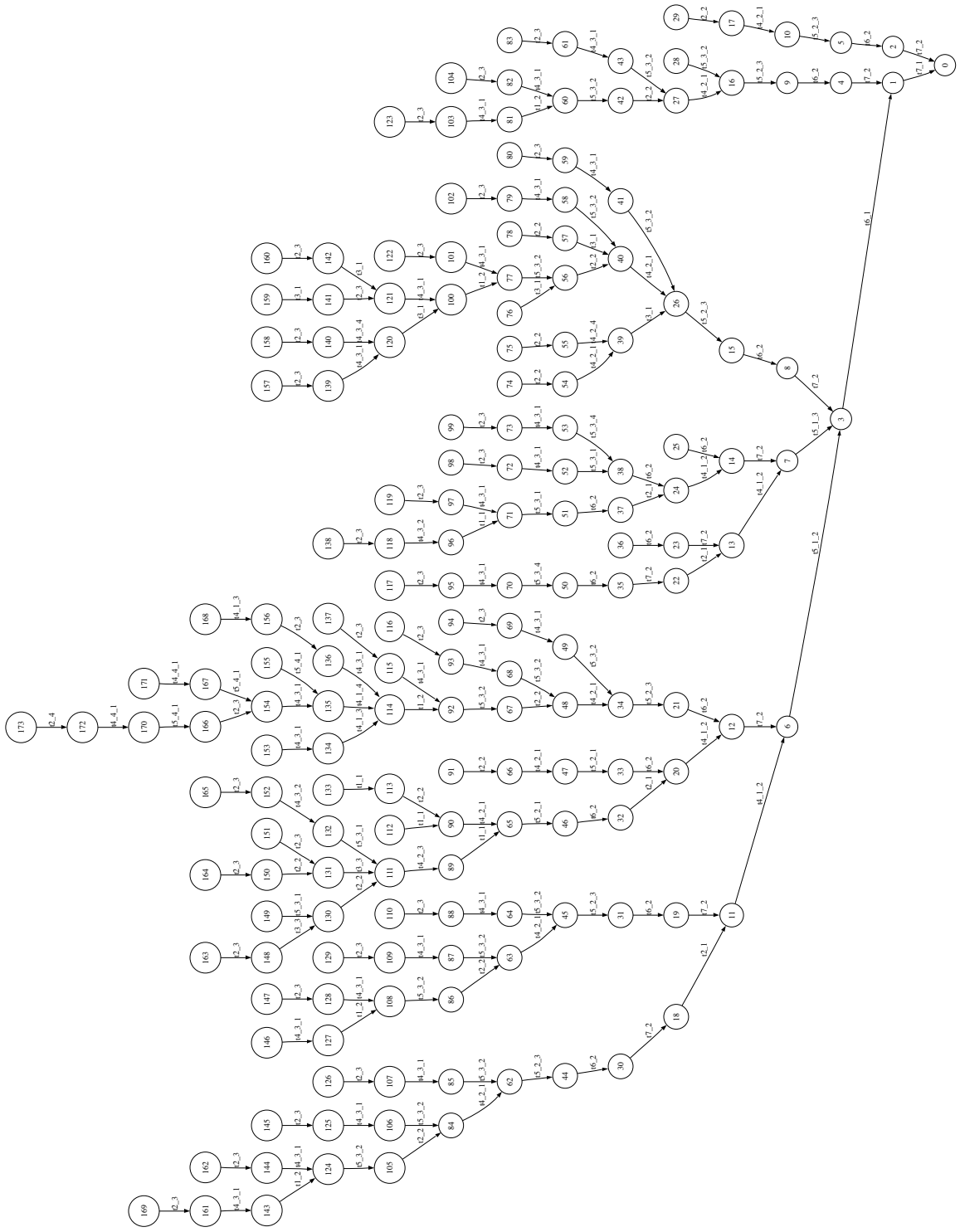


Figure 2: The graph of backward reachable nodes (**without** invariants)

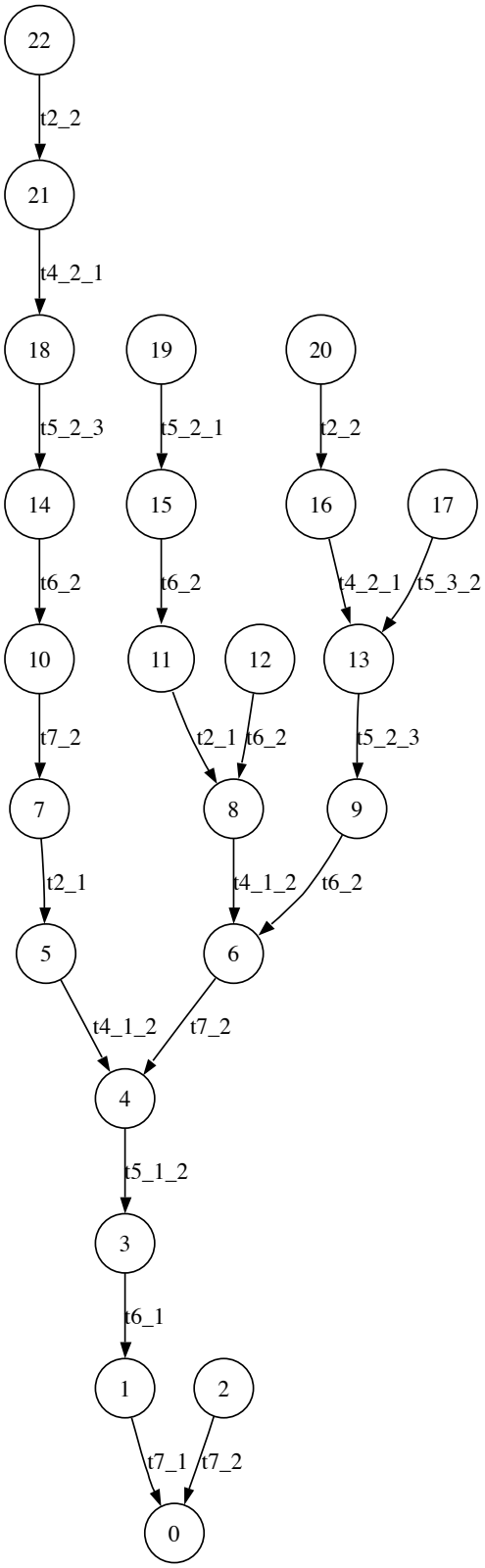


Figure 3: The graph of backward reachable nodes (**with** invariants)

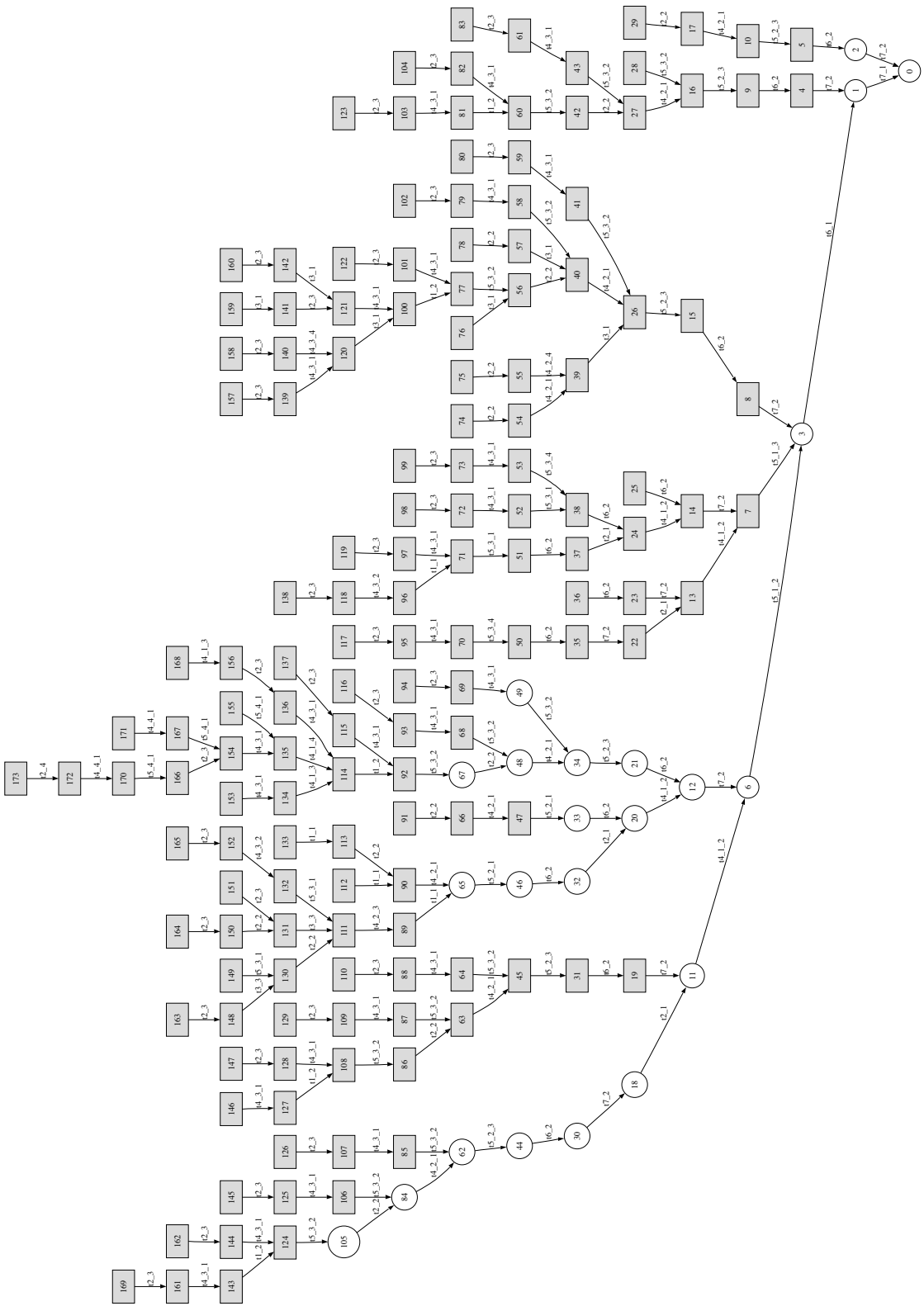


Figure 4: The graph showing the effect of invariants (**shaded boxes are pruned away** by using the synthesized invariants)