Symbolic Model Checking of Timed Automata using LTSmin

Sybe van Hijum

August 30, 2016

Contents

1 Introduction

Timed automata [2] is a widely used modelling formalism. A recent usage of this formalism is the modelling of biological signalling pathways [29]. ANIMO is a tool that generates these timed automata from biological signalling pathway models. Model checking techniques, like property checking are used on these timed automata. The technique however leads to large state spaces, and sometimes to models that are too large to handle by conventional methods. Therefore better model checking techniques for timed automata, that can handle larger state spaces are needed. We look into symbolic algorithms for timed automata.

BDDs (Binary Decision Diagrams) [1, 11] and variations like LDDs (List Decision Diagrams) [10] and MDDs (Multi-valued Decision Diagrams) [30] have proven their worth in model checking algorithms. Due to advances in this field, models with much larger state spaces can be explored on the same machine. This progress has not been translated directly to more efficient methods for timed automata, due to the real clock values that are used. Several methods have been proposed, like CDDs (Clock Difference Diagrams) [20], CMDs (Constraint Matrix Diagrams) [16], CRDs (Clock Restriction Diagrams) [32] and DDDs (Difference Decision Diagrams) [24, 27]. All of these methods show some extra difficulties or limitations over BDDs. Also after their introduction they have not been developed further.

LTSmin [9, 18] is a language-independent on-the-fly model checker with several algorithmic back-ends. Its symbolic back-end uses BDDs to both represent the state space and the transition relations of models. These BDDs are generated on-the-fly by the search algorithms. LTSmin has a language module for Uppaal [5] through the Opaal [13] lattice model checker. Through this module Uppaal models can be loaded into LTSmin. For this language currently, only the explicit-state multi-core back-end can be used [12]. This explicit-state approach showed efficient enough to compete with the latest version of the Uppaal model checker. It showed significant speedups on multi-core machines, at the cost of some memory increase however. To tackle the memory increase a combination of the opaal front-end and the symbolic back-end could be a solution.

The symbolic back-end of LTSmin provides both a memory reduction by using BDDs and a speedup by using multi-threaded search algorithms and the multi-threaded BDD package Sylvan [31]. Using this together with the Uppaal language front-end will hopefully result in a model checker that can compete both on time and memory consumption with the Uppaal model checker.

We will propose a symbolic reachability for timed automata that is capable of handling the models that are generated by the ANIMO tool.

2 Preliminaries

We will first define timed automata and zones, a method used to represent time in timed automata. Also a subsumption check over zones will be defined.

2.1 Timed Automata

Timed automata is a formalism that extends labelled transition systems with one or more clocks. Guards over these clocks, denoted as $G(C)$ can be used for transitions. Also reset actions for clock can be defined for transitions. All clocks in the system will increase at the same rate. As our work continues on [12] we use the same definition of timed automata.

Definition 1 (Timed Automata)**.** *An extended timed automaton is a 6-tuple* $A = \langle L, C, Act, l_0, \rightarrow, I_c \rangle$ *where*

- L *is a finite set of locations, typically denoted by* l
- C *is a finite set of clocks, typically denoted by* c
- Act *is a finite set of actions*
- $l_0 \in L$ *is the initial location*
- $\rightarrow \subseteq L \times G(C) \times Act \times 2^C \times L$ *is the (non-deterministic) transition relation. We normally write* $l \xrightarrow{g,a,r} l$*' for a transition., where* l *is the source location,* g *is the guard over the clocks,* a *is the action, and* r *is the set of clocks reset.*
- $I_C : L \rightarrow G(C)$ *is a function mapping locations to downwards closed clock invariants.*

With this definition we can combine a finite number of timed automata to a network of timed automata, which is a parallel composition, to define larger systems.

Definition 2 (Network of timed automata [12])**.** *Let* $Act = \{ch!, ch?|ch \in Chan\} \cup \{\tau\}$ *be a finite set of actions, and let* C *be a finite set of clocks. Then the parallel composition of extended timed automata* $A_i = \langle L_i, C, Act, L_0^i, \rightarrow_i, I_C^i \rangle$ *for all* $1 \leq i \leq n$*, where* $n \in \mathbb{N}$*, is a network of timed automata, denoted* $A = A_1||A_2||..||A_n$*.*

A network of timed automata is a parallel composition that synchronizes on a set of channels $Chan$ [5]. $ch!$ and $ch?$ represent the output and input action on the channel $ch \in Chan$.

$$\begin{array}{c|ccc} & \mathbf{O} & c_1 & c_2 \\ \hline \mathbf{O} & (0,\leq) & (0,\leq) & (0,\leq) \\ c_1 & (5,<) & (0,\leq) & (\infty,\leq) \\ c_2 & (4,\leq) & (\infty,\leq) & (0,\leq) \end{array}$$

Figure 1: DBM

2.2 Zones

For basic transition systems the state space can grow exponentially for the number of variables in the system. The state space of timed automata is by definition infinite, as clocks have real values. If a state is defined between two points in time, an infinite amount of moments in time can happen during that state. Even when some granularity is used, that defines that clocks will only increase with certain step size the automata can still have infinite state space if a clock is unbounded. To tackle this problem most model checkers use a notion of zones for the representation of time. A zone can be seen as a set of constraints over the clocks C of the form $c_i \sim x$ and $c_i - c_j \sim x$ where $\sim \in \{<, \leq, =, \geq, >\}$ and $x \in \mathbb{N}$. To represent these zones several data structures have been developed. One of the most common used structures are Difference Bound Matrices (DBMs) [6, 14].

These matrices use both a column and a row for each clock, and on each position (i, j) an upper bound on the difference between the clocks c_i and c_j is given in the form $c_i - c_j \preceq x$ where $\preceq \in \{<, \leq\}$ and $x \in \mathbb{Z}$. For the constraints over the single clocks an extra clock $\mathbf{O}$ with a constant value 0 is added. This way the upper and lower bound of a clock c_i can be given by $c_i - \mathbf{O} \preceq x$ and $\mathbf{O} - c_i \preceq y$. The addition of this $\mathbf{O}$ clock will give the matrix of a timed automaton always size $(|C| + 1)^2$. This way convex zones of clock variables can be represented. Each matrix can however only contain a single convex zone. Concave zones and multiple convex zones need multiple matrices to be represented. As a solution often a list of DBMs is used. In figure 1 we give an example of a DBM with two clocks: c_1 and c_2, representing the zone $0 \leq c_1 < 5 \wedge 0 \leq c_2 \leq 4$. The diagonal only contains $(0, \leq)$ values as these elements give the difference between a clock and itself, which is clearly always 0.

A number of operations on DBMs has been defined. We will introduce the operations we use. The same notation as [12] is used.

- $D \uparrow$ is called the delay operator. This lets time pass unlimitedly from the zone in D.
- $D \cap D'$ adds additional constraints from D' to D. This is used for transitions that have clock constraints. These constraints can be represented as a DBM.

- $D[r]$ with $r \subseteq C$, resets all clocks in r.
- D/B does a maximal bounds extrapolation. In section 4.13 we will go into more detail about this extrapolation.

2.3 Zone subsumption

In model checking an important function is to check if a certain state has been visited already earlier. For normal automata this can be done by comparing the newly found state to all states that have already been visited, and check if one of those states is equal to that new state. This is often done by more efficient methods, like hash functions, but the equality check remains. For states with zones this equality check does not suffice. Two zones do not need to be equal, but the newly discovered zone can also be a subset of the earlier discovered zones. In LTSmin this is done by a subsumption check [12] that is performed over the DBMs. This check is delegated to the Uppaal DBM library. The function checks if a new zone is a subset of the zone represented by a DBM.

2.4 Binary Decision Diagram

3 Related Work

In this related work section we will discuss a number of methods used for model checking timed automata. We will choose a method which we will use for the rest of this project.

3.1 Methods

Already several model checkers for timed automata exist such as Uppaal [5], KRONOS [33], RABBIT [8] and RED [32]. We focus mainly on the Uppaal tool as we use the same input format. Opaal [13], the language module for LTSmin, uses the XML format that is created by the Uppaal tools. This way we can use the Uppaal user interface to create and adapt models. We also use the Uppaal DBM library to represent zones.

The most established method to represent clock zones are DBMs. We gave an introduction to this structure in the preliminaries section. Several diagrams based on BDDs have been developed to represent zones. All of these are similar to DBMs in the sense that they use clock constraints to represent the zones. The structure of these diagrams is BDD-like to represent the zones more efficiently. Below we shortly describe four zone based methods. For each method we give an example, all examples represent $2 < c_1 - c_2 < 4 \vee 7 \leq c_1 - c_2 \leq 8$.

3.1.1 Clock Difference Diagram

CDDs [20] use single nodes for each variable and have multiple edges each containing a disjoint interval of that variable. This results in a node with a larger fanout. The upper and lower bound for each pair of clocks are represented in a single node, as the edges represent intervals. Requiring the disjointness of intervals can lead to a memory inefficient representation, as intervals need to be cut in more smaller parts. All algorithms on CDDs do not maintain disjointness, after every step it needs to be re-established. In Figure 2 we have an example of a CDD.

Definition 3 (Clock Difference Diagram [20])**.** *A clock difference diaram is defined as a directed, acyclic graph, which has*

- *a node called the start node from which all nodes of the graph are reachable*
- *inner nodes written as $((i, j), (I_1, , T_1, ..., (I_q, T_q))$ where (i, j) is the pair of clocks of the constraint, the I_n are intervals of the real numbers, and the T_n are CDDs again. We require completeness, i.e. $\bigcup_{n \in \{1,...,q\}} I_n = \mathbb{R}$*
- *end-nodes which are either TRUE or FALSE*

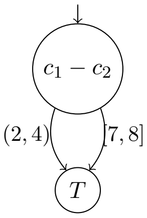


Figure 2: CDD representation

3.1.2 Difference Decision Diagram

DDDs [24, 27] use an upper-bound constraint for a variable pair on each node that can either be true or false. Each node thus has a fixed fanout of two. When a constraint is false, a next node will have another constraint on the same variable. This requires a fixed ordering based on the variables, values and operators. In Figure 3 an example of a DDD is shown.

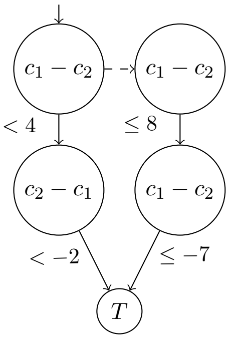


Figure 3: DDD representation

3.1.3 Clock Restriction Diagram

CRDs [32] differ mainly from CDDs by not using disjoint intervals but possibly overlapping upper bounds, for a pair of variables on their edges. This diagram will have a larger fanout per node, like CDDs. Several normal forms for this diagram are proposed, with different performance results. It is also shown that CRDs can be combined with BDDs into a single structure to fully symbolically represent the state space. In Figure 4 we give an example of a CRD.

Definition 4 (Clock Restriction Diagram [32])**.** *Given a set of variables* $V = \{x - x' | x, x' \in X \cup \{0\}\} \cup \{true\}$*, an evaluation index* Ω *over* V*,* *and a timing constant C_A, a CRD over V, Ω, and C_A is a tuple $D = (v, (\beta_1, D_1), ..., (\beta_n, D_n))$ with $n \geq 0$ and $v \in V$ such that*

- $v = true$ *iff* $n = 0$
- *if* $v \neq true$*, then for all* $1 \leq i \leq n, \beta_i \in B_{C_A}$ *and* D_i *is a CRD, say* $(v_i, (\beta_{i,1}, D_{i,1}), ..., (\beta_{i,m}, D_{i,m}))$*, over* V, Ω*, and* C_A *with* $v \prec_\Omega v_i$
- *if* $v \neq true$*, then for all* $1 \leq i < j \leq n$*,* $\beta_i \neq \beta_j$
- *if* $v \neq true$ *and* $n = 1$*, then* $\beta_1 \neq (<, \infty)$

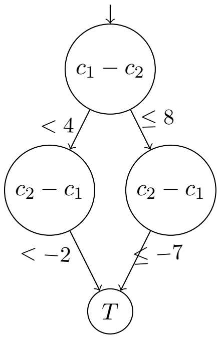


Figure 4: CRD representation

3.2 Constraint Matrix Diagram

CMDs [16] combine CDDs, CRDs and DBMs into a single structure. This diagram type differs from the others by having multiple constraints per edge, resulting in a diagram with few nodes. Upper- and lower-bounds of multiple clock pairs can be on a single edge. The diagram can also be used with only single constraints per edge, which gives a structure quite similar to CRDs. CMDs do not have a canonical form so only some reductions are proposed. An example of a CMD is given in Figure 5. This figure contains two examples, the first is a diagram of the constraint we use in this section. To show the difference with other diagrams we also give a diagram representing the same zone as the DBM in Figure 1.

Definition 5 (Constraint Matrix Diagram [16]). *A Constraint Matrix Diagram (CMD) over the set of constraint matrices* $\mathcal{M}$ *is a tuple* $M = (Q, q_0, q_\top, type, E)$ *where*

- Q *is a finite set of nodes*
- $q_0 \in Q$ *is the root node*

- $q_\top \in Q$ *is the sink*

- *type:* $Q \to I \cup \{I_{max}+1\}$ *is a total function that associates a constraint index to each node*

- $E \subseteq Q \times \mathcal{M} \times Q$ *is an edge relation*

Additionally, we require that (1) (Q, E) *is a directed acyclic graph with precisely one source node* q_0 *and one sink node* $q_\top$*; (2) type(*q_0*)* $= 0$ *and type(*$q_\top$*)* $= I_{max} + 1$*; (3) for each edge* $(q, m, q') \in E$*, minIdx(m)* $\geq$ *type(q) and maxIdx(m) ¡ type(*q'*).*

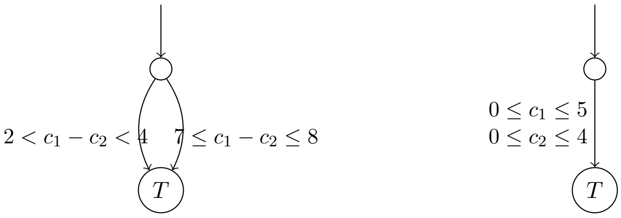


Figure 5: CMD representation

3.2.1 Zone BDD

In [15, 34] a method is proposed purely based on BDDs by translating the constraints directly into BDD nodes. We call this method BDD zones. This results in a unified structure for both the discrete variables and the clock constraints. The method is only a proof of concept and has not been implemented in a model checker and no performance results are known. Subsumption for this method may be difficult. On BDDs only equalities can be checked, and no inequalities. This way inclusion is not trivial to check by normal BDD algorithms.

3.2.2 Digitization

Digitization approximates the continuous values of clocks by using discrete values [7]. The method however only works for closed timed automata, meaning that no strict comparisons on clocks can be made in the model and that clocks only can be compared to integers. This approach is very sensitive to the granularity of the values used and the upper bound of the clock values. When fine granularity or large upper bounds are used, the memory usage will increase too much. An advantage of this approach is that basic model checking approaches can be used and no extra complexity due to zone calculations is added. This method results in a transition system with only discrete variables, so a normal BDD package can be used. In [28] a similar approach is proposed by using clock tick actions to represent time progress and removing clock variables altogether.

3.2.3 Orderings

A known difficulty in BDDs is the variable ordering. A bad ordering can lead to a BDD of exponential size, where a good ordering can sometimes lead to a significantly smaller diagram. Of the zone diagrams named above, only for CRDs experiments with different orderings have been conducted, the other researches assume a given ordering on the variables and the ordering of the values is fixed. The CRD case shows that full interleaving and having related variables close to each other in the ordering is preferable and gives the best results, both on speed and memory. This is the same result as expected with BDDs. This suggests that similar orderings should be used with these techniques. The techniques using normal BDDs can use standard BDD reorderings.

In Table 1 we compare the different types of diagrams we discussed above.

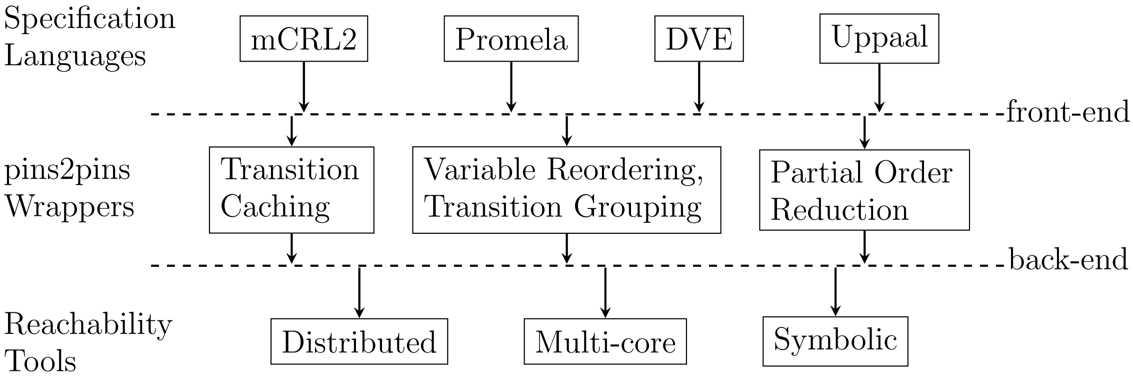


Figure 6: Modular structure of LTSmin

3.3 LTSmin

LTSmin [9, 18] is a language independent model checker. It is built in a modular way such that new languages can be added by a PINS (Partitioned Next-State Interface) without too much effort, and new algorithms can be added easily. LTSmin offers four different algorithmic back-ends for model analysis: symbolic, multi-core, sequential and distributed. All of these back-ends support different types of reduction and model checking. Several language modules have already been built for LTSmin such as mCRL2, Promela, DVE and Uppaal. The modular structure of LTSmin is

Table 1: Comparing Diagrams

Type	Pro	Con
DBM	Canonical form for convex zones Existing library Inclusion check	Concave zones need multiple DBMs Not memory efficient
DDD	Structure like LDD Re-ordering of variables possible Apply same efficiency as BDDs Discrete variables also in DDD	Canonicity hard to obtain No on the fly canonicity Expensive normal form computation Only time performance tested Only reduction algorithms
CDD	Structure like MDD Inclusion check (intersection of complement)	No algorithm to get normal form Only high level algorithms given Methods don't maintain disjointness Expensive normal form computation No implementation results available Disjointness memory inefficient
CRD	Combination with BDD possible Variable reordering shows advantage Library available Some benchmarks exp better than CDD Extensive benchmarks Good performance backwards reach	3 possible canonical forms No algorithms in paper Some benchmarks linear worse than CDD
CMD	Benchmarks against RED and Uppaal	Results differ per case Needs translation from vector to edges Two reduced forms
BDD discrete	Using existing BDD packages Good performance for small clock values	Performance decreases fast for large values Not possible with current Opaal PINS Introducing additional 'tick' actions Only for closed timed automata
BDD zones	Using existing BDD packages All variable reorderings possible Only need direct translation DBM to state vector Easy to implement	Losing zone containment No implementation results

shown in Figure 6. The PINS is the core of LTSmin. This interface abstracts as much as possible from the model without losing the structure. It represents states as fixed length integer arrays. The main function of the interface is a (partitioned) next-state function which returns the successor states. With these functions a state space can be generated on the fly. With the use of dependency matrices event locality can be determined statically [22]. With these matrices, more efficient symbolic algorithms can be used, the number of next-state calls can be reduced, efficient variable re-orderings can be used, and transition caching can be used. In the current Uppaal PINS the next-state function is not partitioned and therefore no meaningful dependency matrix is created, and none of these algorithms can be used. Also the DBM variable is only represented by a pointer, which is not a meaningful value for the transition system. LTSmin uses the pointer to a DBM to do the subsumption check as described in section 2.3.

3.4 Difference Decision Diagrams

We have discussed several symbolic approaches for representing zones. All of these approaches have benefits and downsides over each other. We chose to develop one of these approaches in LTSmin. We wanted a diagram that can store both discrete states and zones, this can either be done in the diagram, or in a combination of the diagram and BDD or LDD nodes. Also a subsumption check on the diagram should be possible. We chose from the four zone-representing diagrams discussed earlier. The CDD approach was not chosen due to the memory inefficient disjoint intervals and their algorithms not maintaining these disjointness. The CMD approach is too similar to DBMs, on which we already have an approach. The choice between CRD and DDD was between two quite similar diagrams. We have decided to continue on the DDD. It is a diagram form that is closely related to LDDs, for which we already have a library, so we can reuse parts of the LDD library, and it is also quite compatible to the current PINS structure and its next-state function, so no big changes are needed to that.

So DDDs are a diagram type that seems to fit well in the current structure we have, but there is still room for some more research. First we give the definition of a DDD.

Definition 6 (Difference Decision Diagram [27])**.** *A difference decision diagram (DDD) is a directed acyclic graph* (V, E)*. The vertex set* V *contains two terminals* 0 *and* 1 *with out-degree zero, and a set of non-terminal vertices with out-degree two and the following attributes.*

Attribute	*Type*	*Description*
pos(v), neg(v)	***Var***	*Positive variable x_i, and negative variable x_j.*
op(v)	$\{<, \leq\}$	*Operator $<$or $\leq$.*
const(v)	$\mathbb{D}$	*Constant c.*
high(v), low(v)	V	*High-branch h, and low-branch l.*

The set E contains the edges $(v, low(v))$ and $(v, high(v))$, where $v \in V$ is a non-terminal vertex.

Now we have the definition of the structure. We also give the semantics of this structure.

Definition 7 (DDD semantics)**.** *The semantics of a vertex is defined recursively by the function $\mathcal{V} : V \to \boldsymbol{Exp}$:*

- $\mathcal{V}[[0]] \overset{\text{def}}{=} \mathit{false},$
- $\mathcal{V}[[1]] \overset{\text{def}}{=} \mathit{true},$
- $\mathcal{V}[[v]] \overset{\text{def}}{=} \begin{cases} (pos(v) - neg(v) < const(v)) \to \mathcal{V}[[high(v)]], \mathcal{V}[[low(v)]] \mathit{if}\ op(v) =' <' \\ (pos(v) - neg(v) \leq const(v)) \to \mathcal{V}[[high(v)]], \mathcal{V}[[low(v)]] \mathit{if}\ op(v) =' \leq' \end{cases}$

In the semantics we only take the information on the high edges. The implicit information on the low edge is not used. A node can thus only represent an upper-bound which is either true or false, it can not implicitly represent a lower-bound on the same variable pair. This representation also makes it easier to work with the state-vectors of LTSmin.

In [27] a canonical form for DDDs is discussed, also called a fully reduced DDD. Only definitions are given here, no algorithms to reach this form. It is stated that it is difficult to reach this fully reduced form. It is not clear if they managed to make their apply function in such a way that it maintains canonicity, as the function for BDDs does. To reach canonicity, local reductions and ordering are a first step, but it is not enough due to dependencies among the constraints. For BDDs the local reductions and ordering are sufficient to reach a canonical form. First we give some notational shorthands and then we define an ordering and local reductions on DDDs.

$$\begin{array}{lcl} var(v) & = & (pos(v), neg(v)) \\ bound(v) & = & (const(v), op(v)) \\ cstr(v) & = & (var(v), bound(v)) \end{array}$$

To order DDD nodes we use the operator $\prec$. This orders variables and variable pairs in a predefined order. It orders bounds by increasing constants, and the $<$ operator before the $\leq$ operator. So a node v with $bound(v) = (0, <)$ comes before $bound(u) = (0, \leq)$ which comes before $bound(w) = (1, <)$.

Definition 8 (Ordered DDD [27])**.** *An ordered DDD (ODDD) is a DDD where each non-terminal vertex v satisfies:*

1. $neg(v) \prec pos(v)$,
2. $var(v) \prec var(high(v))$,
3. $var(v) \prec var(low(v))$ *or*
   $var(v) = var(low(v))$ *and* $bound(v) \prec bound(low(v))$.

After ordering a DDD some local reductions can be defined to reduce the size of a DDD.

Definition 9 (Locally Reduced DDD [27])**.** *A locally reduced DDD ($R_L DDD$) is an ODDD satisfying, for all non-terminals u and v:*

1. $\mathbb{D} = \mathbb{Z}$ *implies* $\forall v.op(v) =' \leq'$,
2. $(cstr(u), high(u), low(u)) = (cstr(v), high(v), low(v))$ *implies* $u = v$,
3. $low(v) \neq high(v)$,
4. $var(v) = var(low(v))$ *implies* $high(v) \neq high(low(v))$.

We give an example of the last point in figure 7. Here both diagrams represent the same zone: $2 < c_1 - c_2 \leq 8$. The node with < 4 on the high edge is redundant in this example and can thus be removed.

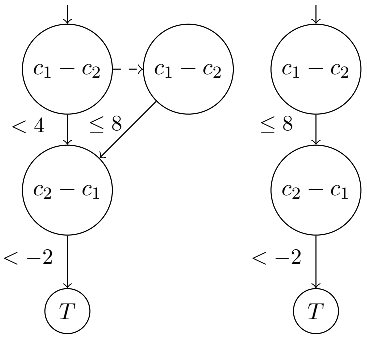


Figure 7: Local reduction

For BDDs these reductions would be enough to have a fully canonical structure. For DDDs this is not the case, due to dependencies between the bounds. In Figure 8 we give an example for this by giving two different locally reduced DDDs representing the same zone. The resulting zone of both these DDDs is drawn in Figure 9, which is the square in which both clock c_1 and c_2 are between 0 and 5.

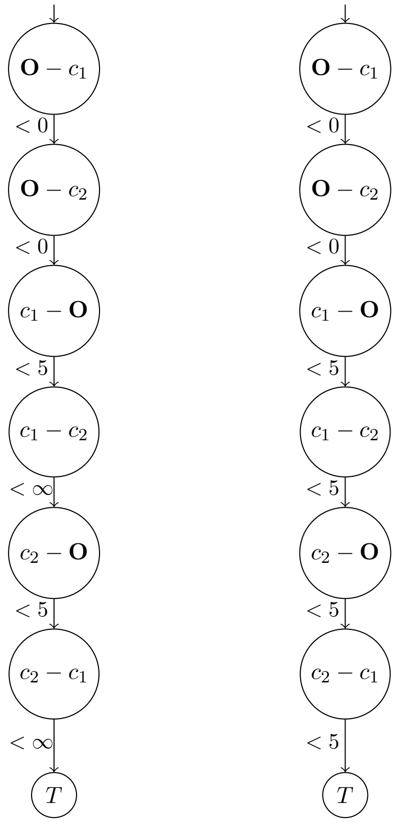


Figure 8: Two DDDs representing the same zone

The $R_L DDD$ is clearly not canonical. We first define a path in a DDD as the bound on all high edges that are traversed in a single walk from the top node to the true node. A path will only have one bound for each variable pair.

Definition 10 (Path-reduced DDD [27]). *A path-reduced DDD ($R_P DDD$) is a locally reduced DDD where all paths are feasible.*

This definition ensures that all paths in a DDD actually represent a zone, and that there are no redundant paths in the DDD that just represent an empty set. This usage of paths is compatible to the state vectors used in LTSmin. An $R_P DDD$ is still not canonical. We need to define tightness, saturation and disjunctive vertices. To define tightness we first need to define dominating constraints.

Definition 11 (Dominating constraint [27]). *A constraint $x_i - x_j \lesssim c$ is dominating in a path p if all other constraints $x_i - x_j \lesssim' c'$ on the same pair of variables in p are less restrictive.*

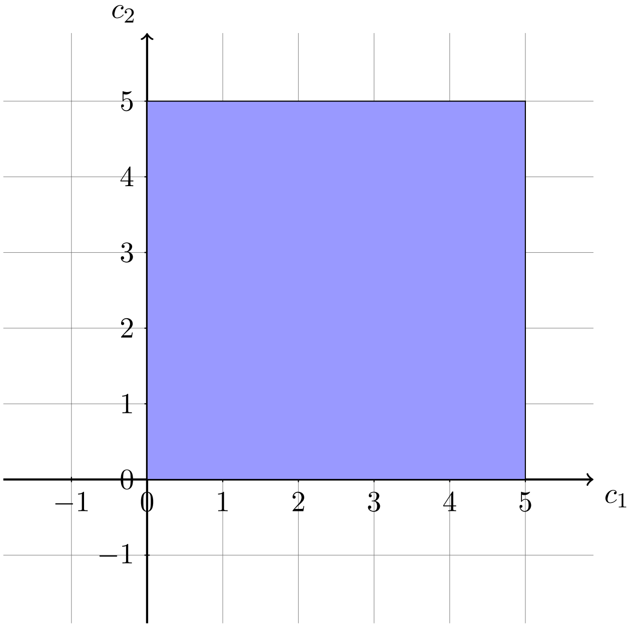


Figure 9: Resulting zone of DDDs in figure 8

Definition 12 (Tightness [27]). *A dominating constraint $\alpha = x_i - x_j \lesssim c$ is tight in a feasible path $[p] = [p_1] \wedge \alpha \wedge [p_2]$ if for all tighter constraints $(c', \lesssim') < (c, \lesssim)$, the systems $[p_1] \wedge (x_i - x_j \lesssim' c') \wedge [p_2]$ and $[p]$ have different solutions. A path p is tight if it is feasible and all dominating constraints on it are tight. An $R_L DDDu$ is tight if all paths from u are tight.*

Definition 13 (Saturation [27]). *A tight path p from an $R_P DDD$ is saturated if for all constraints α not on p, if α is added to p either (1) α is not dominating and tight, or (2) the constraint system $[p_1] \wedge \neg\alpha$ is infeasible when $[p]$ is written $[p] = [p_1] \wedge [p_2]$ with all constraints on p_1 smaller than α with respect to $\prec$ and all constraints on p_2 larger than α. An $R_P DDD$ u is saturated if all paths from u are saturated.*

Definition 14 (Disjunctive vertex [27]). *Let p be a path leading to the vertex u in a DDD, and assume $\alpha = cstr(u), h = high(u)$, and $l = low(u)$. Then u is disjunctive in p if $[p] \wedge (\alpha \rightarrow h, l)$ and $[p] \wedge (h \vee l)$ have the same set of solutions.*

All of these definitions together lead to the following definition of a fully reduced DDD.

Definition 15 (Fully reduced DDD [27]). *An $R_p DDD$ u is a fully-reduced DDD ($R_F DDD$) if it is tight, saturated and has no disjunctive vertices.*

We assume that this fully-reduced DDD is canonical and work from that. It is not ensured that this is actually the case, there is no proof for it.

Conjecture 1 (Canonical DDD [27])**.** *If u and v are R_FDDDs with the same set of solutions then $u = v$.*

DDDs can also be used to represent the discrete variables in automata. This is done by translating the variable into a difference constraint. For example $x_1 = 3$ will be translated into $x_1 - 0 \leq 3 \wedge 0 - x_1 \leq -3$, thus resulting into a DDD with two nodes. We will instead connect the DDD to an LDD to represent discrete variables to limit the number of nodes.

So far we only found the results of two benchmark tests of DDDs, Milner's scheduler and Fischer's protocol [25]. Here the DDD approach has been compared with KRONOS and Uppaal which were both slower than the DDD implementation. The results of these benchmarks show no memory usage or number of nodes needed.

3.5 List Decision Diagram

We will introduce the LDD structure here. An LDD is used to represent variables with integer values, not only binary values. In contrast to MDDs this is done for one value per node, resulting in nodes with equal size. We will first define the LDD structure.

Definition 16 (List Decision Diagram)**.** *A List Decision Diagram (LDD) is a directed acyclic graph (V, E). The vertex set V contains two terminals 0 and 1 with out-degree zero, and a set of non-terminal vertices with out-degree two and the following attributes.*

Attribute	*Type*	*Description*
var(v)	***Var***	*Variable x*
const(v)	$\mathbb{Z}$	*Constant c.*
high(v), low(v)	V	*High-branch h, and low-branch l.*

The set E contains the edges $(v, low(v))$ and $(v, high(v))$, where $v \in V$ is a non-terminal vertex.

The definition is almost equal to DDDs, Definition 4. The difference is the operator that is not in LDDs. LDDs can be seen as a DDD with not a $<$ or $\leq$ as operator, but a $=$.

4 Implementation

This section will go more into detail about the implementation we made and the design choices that were needed.

4.1 Flattening DBM

In the LTSmin implementation that we already have the state vector consists of all discrete variables and an 64 bit pointer to a C++ class containing a DBM [12]. For a symbolic solution this pointer has no meaning, thus we take the actual values from the DBM and put these into the state vector. This increases the length of a state vector, but does not need to increase the memory footprint, as the DBM was already stored. In the DBM library we use a DBM is represented by a one-dimensional array of 32-bit integers. In the integers the complete bound is stored, so both the operator and the constant value. We flattened the DBMs to work with a symbolic solution. We only did this on the edges of the successor function. So this function reads a state with a flattened DBM as input and returns successor states, again with flattened DBMs, internally the original DBM representation is still used. This way the code had to be adapted the least. In this flattening step we removed the diagonal elements of each DBM. By the way DBMs are constructed this will always represent the difference between a clock and itself. This difference is by definition always 0, so it can be removed, and hard coded be set to $(0, \leq)$ internally. This reduces the number of state variables in the state vector by one for each clock. This flattening of DBMs results into a language module that can be connected to all LTSmin algorithmic back-ends for state-space generation.

4.2 Dependency Matrices

To get the best possible result of the regrouping algorithms, the dependency matrices had to be made as sparse as possible. This has been done for both the read matrix and may-write matrix. For even better results, also the must-write matrix is needed. This needs effort when analysing the code, this can be done, but is left out for this thesis. To generate the matrices we parse the Uppaal models. First of all, all C-like code is parsed. Here it is stored per function which variables are read and written, and which other functions are called. Next all transitions are parsed, here some variables are read and written directly. Transitions can also call functions, in such cases the variables that were found in the parsing of these functions are added to the read and may-write variables of the transition. In the third step we need to look at the time extrapolation. This extrapolation is based on the value of the location variable, so it results in a read dependency. In some cases, there is no difference between all possible location values for this extrapolation, so a location does not need to be read. A final step is that a location variable that can be urgent or committed always has to be read. If this location is in an urgent state, than no other transitions can happen, so all other transitions have to check that they are not in an urgent state. In which only an other transition can take place. The correct filling of the matrices is only for the discrete parts of the states. For the zone part, to optimizations have been created. The matrices for these parts will always be filled. The problem is that changing only one clock can have a much larger impact on a DBM when a normal form is used. The flattened DBMs and the sparser dependency matrices together enable the reordering algorithms in the symbolic back-end of LTSmin to be used.

4.3 DBM reduction

We work towards a fully reduced DDD solution. This is already started at the language module side. The next-state function will only return tight and saturated paths. In DBM terms this is a minimal constraint system [6]. As the length of a state-vector cannot be changed on the fly, all removed constraints are set to $(\infty, <)$. This means that there is no upper-bound on the variable pair of that position. In Algorithm 2 which uses Algorithm 1 we show the algorithm that determines all bounds that are not needed an can be set to $(\infty, <)$. The DBM library cannot use these minimal constraint systems. In the next-state function the incoming DBM is tightened, then all needed operations for the successor generation are conducted and if a successor is returned, its DBM is again turned into a minimal constraint system. This will give algorithmic overhead for each next-state call. The advantage of this procedure is that many bounds will be redundant and turned into $(\infty, <)$. In the symbolic back-end these bounds which are the same can be shared in a single node. Thus taking more time in the successor generator, it can also reduce the number of nodes in the algorithmic back-end. This reduction is used in the successor generator for the LDD symbolic back-end, and will also be used for the DDD solution.

Algorithm 1 Reduce

```
procedure REDUCE($dbm, dim$)
    for $i \in dim$ do
        for $j \in dim$ do
            for $k \in dim$ do
                if !($dbm[i,k] \vee dbm[k,j] \vee dbm[i,j]$ on diagonal) then
                    if $dbm[i,k] + dbm[k,j] \leq dbm[i,j]$ then
                        $dbm[i,j] := \infty$
```

Algorithm 2 Reduce

```
procedure ReduceZero($dbm, dim$)
    $placed[dim]$ all 0
    $red[dim, dim]$ all 0
    $eq[dim, dim]$ all 0
    $cl := 0$
    $newDBM[dim, dim]$ diagonal $\infty$ rest 0
    for $i \in dim$ do
        if $placed[i] = 0$ then
            for $j \in$ dim do
                if $dbm[i, j] + dbm[j, i] = 0$ then
                    $placed[j] := 1$
                    $eq[cl, j] := 1$
            $cl + +$
    $repr[cl]$
    for $i \in cl$ do
        for $j \in dim$ do
            if $eq[i, j] = 1$ then
                $repr[i] := j$
                break
    $clg[cl, cl]$
    for $i \in cl$ do
        for $j \in cl$ do
            $clg[i, j] := dbm[repr[i], repr[j]]$
    Reduce($clg, cl$)
    for $i \in cl$ do
        for $j \in dim$ do
            if $eq[i, j] = 1$ then
                for $k \in dim$ do
                    if $eq[i, k]$ then
                        $newDBM[j, k] = dbm[j, k]$
        for $j \in cl$ do
            $newDBM[repr[i], repr[j]] := clg[i, j]$
    return newDBM
```

4.4 Connecting LDD and DDD

To represent the discrete variables in states LDD nodes are used. The structure of these nodes is quite similar to DDD nodes. We decided to not mix the nodes, but to first have all the LDD nodes and then all DDD nodes in the tree. In the state vector the first part exists of all discrete variables, the last part are the DBM variables. The top of the diagram can be seen as a MTLDD(Multi-Terminal List Decision Diagram) with not values on the leaf nodes, but pointers to DDD nodes. The DDD part is not influenced by the LDD part, as a node is only influenced by the nodes below it, it has no information about the nodes above it in the diagram. This strict separation between LDD and DDD nodes makes that the reordering algorithms cannot be used, as this would mix the types of nodes. The lack of reordering makes it however possible to reconstruct the DBMs on the DDD side. This is used for the minus function which we discuss later.

4.5 DDD nodes

We used the basis of the LDD package in Sylvan to create our DDD nodes. The nodes are the same as the LDD nodes, only two previously unused bits are now used to store the operator and the type of the node. DDD nodes are stored in 128 bits, represented as a struct of two 64 bit integers. The hashtable that is already used by Sylvan is specifically for 128 bit entries, so the DDD nodes can use the same hashtable. A node is in C code represented as follows:

```
struct dddnode {
    uint64_t a, b;
} * dddnode_t;
```

In this struct the value (32 bits), the true edge (40 bits), the false edge (40 bits) and a type bit, operator bit and flag bit are stored. These values are not specifically named in the struct, all values are stored in the two integers a and b. Figure 10 shows how this is coded in memory. The type, operator and flag bit are stored in the black areas. We do not show them explicitly due to the scale. The type bit indicates if a node is a DDD or an LDD node, if it is set to 0 it should be treated as a normal LDD node. The operator bit shows if the operator is $<$ or $\leq$, this can only be used if the type bit is also set to 1 (DDD). The flag bit is used in some algorithms to indicate that a certain node has already been visited. All of this is stored compactly in the two 64 bit integers. The total information is 115 bits, so there are still 17 unused bits, all unused bits are set to 0. The depth of the node is not stored, this can be calculated by going down through the structure. This implies that no level can be skipped. Other DDD algorithms and reductions show that some levels are not needed. We solved this by indication a skipped level

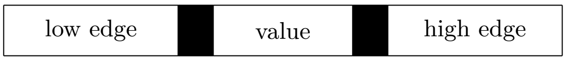


Figure 10: In memory representation of DDD node

by $(\infty, <)$, which is true for every upper bound. For such nodes the false edge will always directly lead to the false end node.

4.6 Creating Nodes

To create a node a special MK function is used. This function will ensure that a DDD is always locally reduced. This MK function is shown in algorithm **??**. This function ensures the correct total structure and puts newly created nodes in the hashtable. The actual creation of a node is done in the MakeNode function that is called inside the MK function. The code for the MakeNode function is not shown here as it is only technical coding, putting all the information in the struct.

Algorithm 3 MK

```
procedure MK($value, h, l, type, op$)
    if $h = 0 \wedge type = LDD$ then
        return $l$
    if $h = 1 \wedge l = 1$ then
        return 1
    if $h = 0 \wedge l = 0$ then
        return 0
    if $h = 0 \wedge l \neq 0$ then
        return 1
    if $h = high(l)$ then
        return $l$
    $node$ = MAKENODE($value, h, l, type, op$)
    if $node \notin table$ then
        PUT($node$)
    return $node$
```

4.7 Apply

One of the core operations on DDDs is the apply operation. This operation takes two DDDs and a binary operator and combines the two DDDs according to the operator. The apply function for DDDs is a generalisation of the function for BDDs. In [27] a general definition of the algorithm is given. We turned this more mathematical definition into an algorithm, we give pseudo-code in Algorithm 3. The algorithm will search down to the leaf nodes and use the operator on that level. We can optimize this a bit for cases where we see two equal nodes, or only one leaf node. In Algorithm 4 we give the pseudo-code for the apply function with the or operator, or the union function, this way we can increase performance by not going down the entire diagram if we already found a false leaf, or two equal nodes. The apply operator does not ensure path-reducedness, even when both inputs are path reduced.

Algorithm 4 Apply

```
procedure APPLY($v1, v2, op$)
    if $v1 \in \{0,1\} \wedge v2 \in \{0,1\}$ then
        $result \leftarrow (v1\ op\ v2)$
    else if $var(v1) \prec var(v2)$ then
        $high \leftarrow$ APPLY($high(v1), v2, op$)
        $low \leftarrow$ APPLY($low(v1), v2, op$)
        $result \leftarrow$ MK($cstr(v1), high, low$)
    else if $var(v2) \prec var(v1)$ then
        $high \leftarrow$ APPLY($high(v2), v1, op$)
        $low \leftarrow$ APPLY($low(v2), v1, op$)
        $result \leftarrow$ MK($cstr(v2), high, low$)
    else if $v1 \prec v2$ then
        $high \leftarrow$ APPLY($high(v1), high(v2), op$)
        $low \leftarrow$ APPLY($low(v1), v2, op$)
        $result \leftarrow$ MK($cstr(v1), high, low$)
    else if $v2 \prec v1$ then
        $high \leftarrow$ APPLY($high(v1), high(v2), op$)
        $low \leftarrow$ APPLY($v1, low(v2), op$)
        $result \leftarrow$ MK($cstr(v2), high, low$)
    else if $v1 = v2$ then
        $high(v1) \leftarrow$ APPLY($high(v1), high(v2), op$)
        $low(v1) \leftarrow$ APPLY($low(v1), low(v2), op$)
        $result \leftarrow$ MK($cstr(v1), high, low$)
    return $result$
```

4.8 Minus

The minus function, used for the reachability, has not been implemented as a DDD function. This function is different to other functions, as information has to be transferred over different levels. For simple cases, an upper bound in one of the operands of the minus, can become a lowerbound in the result, and vice-versa. A simple one-dimensional example is [0..8]/[0..4), this will result in [4..8]. In this case the 4 is the upper-bound of the subtrahend. It will however become the lower-bound of the difference. As lower- and

Algorithm 5 Union

```
procedure UNION($v1, v2$)
    if $v1 = v2$ then return $v1$
    else if $v1 =$ false then return $v2$
    else if $v2 =$ false then return $v1$
    else if $var(v1) \prec var(v2)$ then
        $high \leftarrow$ UNION($high(v1), v2$)
        $low \leftarrow$ UNION($low(v1), v2$)
        $result \leftarrow$ MK($cstr(v1), high, low$)
    else if $var(v2) \prec var(v1)$ then
        $high \leftarrow$ UNION($high(v2), v1$)
        $low \leftarrow$ UNION($low(v2), v1$)
        $result \leftarrow$ MK($cstr(v2), high, low$)
    else if $v1 \prec v2$ then
        $high \leftarrow$ UNION($high(v1), high(v2)$)
        $low \leftarrow$ UNION($low(v1), v2$)
        $result \leftarrow$ MK($cstr(v1), high, low$)
    else if $v2 \prec v1$ then
        $high \leftarrow$ UNION($high(v1), high(v2)$)
        $low \leftarrow$ UNION($v1, low(v2)$)
        $result \leftarrow$ MK($cstr(v2), high, low$)
    else if $v1 = v2$ then
        $high(v1) \leftarrow$ UNION($high(v1), high(v2)$)
        $low(v1) \leftarrow$ UNION($low(v1), low(v2)$)
        $result \leftarrow$ MK($cstr(v1), high, low$)
    return $result$
```

upper-bounds are saved on different levels in DDDs this makes the function different from all other functions, which only look at values on the same level.

In Figure 11 we have a two-dimensional example of how the minus function can become more complex for multiple-dimensions. In this case we make a hole in a larger zone. Both the minuend and the subtrahend are represented by a DDD with a single path, as shown in figure 12. For simplicity we removed the diagonals in this example, as they play no role. The difference however becomes a DDD with 4 paths and 10 nodes, Figure 13. Again a lot of upper- and lower-bounds are switched. Already for this example we could not find an algorithm that does this in general. For more dimensions, and DDDs with already multiple paths the problem will only get harder. That is why we returned to a DBM function for this.

The DBM function we use is defined in the Uppaal DBM library. The minus function is defined over a federation of DBMs. This federation is a C++ class containing multiple DBMs. This federation is needed as we can do a minus over a collection of zones, multiple paths in the DDD, and the result can contain multiple zones. As already shown in the example of Figure 11. For this function we first take the normal LDD minus function over the discrete part. At the first DDD level, representing the zones, the DBM function is called. From this level all possible paths are searched, and for each path a DBM is created and tightened. All these DBMs are put in a federation, on which the library function can be called. The result is again (a possibly empty) federation. If the federation is empty, simply a DDD-false node is returned. Otherwise each DBM is turned into a DDD path and these paths are made into a single structure using the union function.

4.9 Relation

The transition relation we use is stored in an LDD structure. Both bound values and operators are implicitly encoded in a single value, like in the DBM library. When creating new nodes, the nodes are matched against the state space. By checking the type of the node on the current level it can be checked if the relation node should be treated as a normal LDD node with a discrete variable, or as an LDD node which implicitly stores an upper-bound. The choice to not use the DDD type nodes in the relation has been made to have better support for possible future reordering options. If reorderings are used, it would need explicit information for which relation levels contain zone variables, with matching against the states this extra information is not needed.

4.10 BFS

The DBM minus function we use is quite expensive. As it is imported from a library we do not know the exact complexity. To overcome this problem we will use two different versions of the search algorithm. Our second version will not use the minus function. In Algorithm 5 we show the standard BFS algorithm, this will be the first algorithm we use. Algorithm 6 shows how we can edit this algorithm. The constraint of the loop is changed from an empty check of the current set, to a check that the total visited set has not been changed. This check is basically the same, the first checks if now new states are found, the second checks that the total state-space has not been changed. This change now shows that the minus is not necessary any more, as shown in Algorithm 7. This version uses the same check as the previous one, but now the minus of the current and the visited set has been removed. The implication is that the current set will in some cases be larger than in the previous algorithm. This will have some negative impact on the next-state calls, which will take more time. Not using the expensive minus function might compensate for that. We have implemented these two versions in the bfs-prev algorithm [22]. This is the default search algorithm that is used in LTSmin. In the results section we will show the outcome of both BFS algorithms.

Algorithm 6 BFS

```
procedure BFS($initial$)
    $vis := cur := initial$
    while $cur \neq \emptyset$ do
        $cur := next(cur)$
        $vis := vis \cup cur$
        $cur := cur \setminus vis$
```

Algorithm 7 BFS

```
procedure BFS($initial$)
    $vis := cur := initial$
    $vis_{prev} := \emptyset$
    while $vis \neq vis_{prev}$ do
        $vis_{prev} := vis$
        $cur := next(cur)$
        $vis := vis \cup cur$
        $cur := cur \setminus vis$
```

Algorithm 8 BFS

```
1: procedure BFS($initial$)
2:     $vis := cur := initial$
3:     $vis_{prev} := \emptyset$
4:     while $vis \neq vis_{prev}$ do
5:         $vis_{prev} := vis$
6:         $cur := next(cur)$
7:         $vis := vis \cup cur$
```

4.11 State-space count

One of the basic outputs that LTSmin gives when calculating a state-space, is the number of states. For timed automata this is not trivial, as a state is not well defined. Systems with digitization will have other states than systems which use zones for representing time. Even for zones no clear definition of a state exists, as DBMs give no canonical representation of zones, when they are not convex. Now our representation with DDDs will again give another result. We decided to take as the state count only the number of discrete states. This number should be equal for each method for analysing timed automata.

4.12 Successor Generator

The language module uses the opaal successor generator for Uppaal models. This generator is written in Python and reads Uppaal XML files. A C++ file is generated from this. These files are compiled to object files which can be dynamically linked to LTSmin. The structure of the next-state function is slightly different from [12]. The new structure can be found in algorithm 8. At line 6, the function iterates over all outgoing transitions from the current location. If it is an internal transition the successor will be generated on lines 9-18. If it is a sending transition, receivers will be searched for on lines 20-32. In the generated C++ code the loops on lines 5 and 21 are unrolled. The algorithm contains several empty checks, on lines 8, 13, 23 and 27. After each addition of constraints the DBM can possibly be empty. If the DBM is at one of these points empty, no point in time exists where the new state can exist, so further exploration of the transition is not needed. After the empty checks on lines 13 and 27 the extrapolation and the reduction are done. These operations can not empty the DBM, the extrapolation can make the zone larger, not smaller. The reduction will not change the zone at all, only its representation. If the DBM is not empty before these operations it can safely be put into the output.

Algorithm 9 Next-State

```
procedure Next-State($s_{in} = \{l_1, ...l_n, l_{n+1}, ..., l_m\}$)
    $out\_states := \emptyset$
    $D$ :=CreateDBM($\{l_{n+1}, ..., l_m\}$)
    TightenDBM($D$)
    for $l_i \in l_1, ..., l_n$ do
        for all $l_i \xrightarrow{g,a,r} l'_i$ do
            $D' := D \cap g$
            if $D' \neq \emptyset$ then
                if $a = \tau$ then
                    $D' := D'[r]$
                    $D' := D' \uparrow$
                    $D' := D' \cap I^i_C(l'_i) \cap \bigcap_{k \neq i} I^k_C(l_k)$
                    if $D' \neq \emptyset$ then
                        $D' := D'/B(l_1, ..., l'_i, ..., l_n)$
                        ReduceZero($D'$)
                        $\{l'_{n+1}, ..., l'_m\}$ :=FlattenDBM($D'$)
                        $s_{out} := \{l_1, ..., l'_i, ..., l_n, l'_{n+1}, ..., l'_m\}$
                        $out\_states := out\_states \cup s_{out}$
                else
                    if $a = ch!$ then
                        for $l_j \in l_1, ..., l_n, j \neq i$ do
                            for all $l_j \xrightarrow{g_j, ch?, r_j} l'_j$ do
                                if $D''$” $= D' \cap g_j \neq \emptyset$ then
                                    $D'' := D''[r][r_j]$
                                    $D'' := D'' \uparrow$
                                    $D'' := D'' \cap I^i_C(l'_i) \cap I^j_C(l'_j) \cap \bigcap_{k \neq \{i,j\}} I^k_C(l_k)$
                                    if $D'' \neq \emptyset$ then
                                        $D'' := D''/B(l_1, ..., l'_i, ..., l'_j, ..., l_n)$
                                        ReduceZero($D''$)
                                        $\{l'_{n+1}, ..., l'_m\}$ :=FlattenDBM($D'$)
                                        $s_{out} := \{l_1, ..., l'_i, ..., l'_j, ..., l_n, l'_{n+1}, ..., l'_m\}$
                                        $out\_states := out\_states \cup s_{out}$
    return $out\_states$
```

4.13 Time Extrapolation

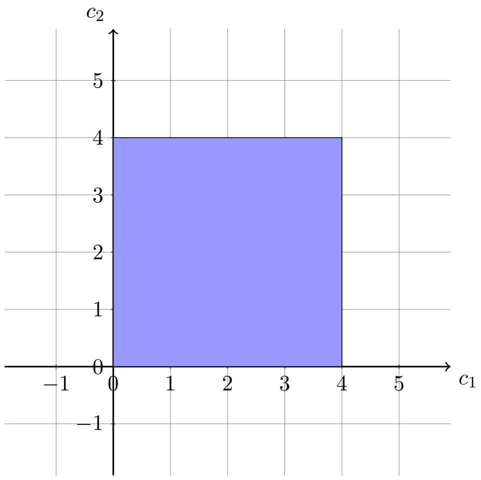
In the successor generator step a time extrapolation is used. This extrapolation step reduces the number of DBMs created and makes sure that this number is finite. The most coarse abstraction as described in [4] is used. This extrapolation reduces the number of zones that are explored significantly. It also makes that less improvements can be made on the representation of the zones, for some models all states are extrapolated to the same zone, so nothing interesting happens at the timed side of the model any more. In opaal this algorithm is implemented in such a way that all Uppaal locations are always read. The maximum extrapolation is based on the values of these locations. Only if there is no difference between all values for a certain location, it is not needed to read this. This results into an densely populated dependency matrix for the location variables.

4.14 Animo Models

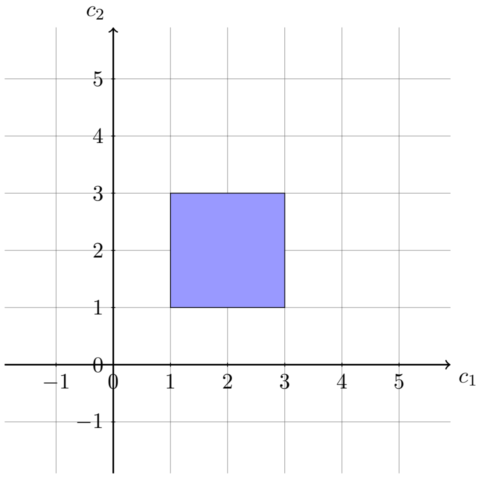
We started the project with ANIMO models that were not compatible with opaal, as opaal does only support a subset of all options of Uppaal. First of all we changed the model, such that it does not use global variables in in the system declaration. Also some smaller changes to the use of structs had to be made. This resulted in a basic ANIMO model that is compatible. Larger models are still not compatible due to clock guards on input synchronization channels. This is a feature only recently implemented by Uppaal (version 4.1.3). Opaal does not support this feature, and its semantics are not completely clear, as it is not described in the manual. Adding this to opaal can be done, but is not trivial. This improvement of the language module is out of scope of this thesis.

4.15 Correctness

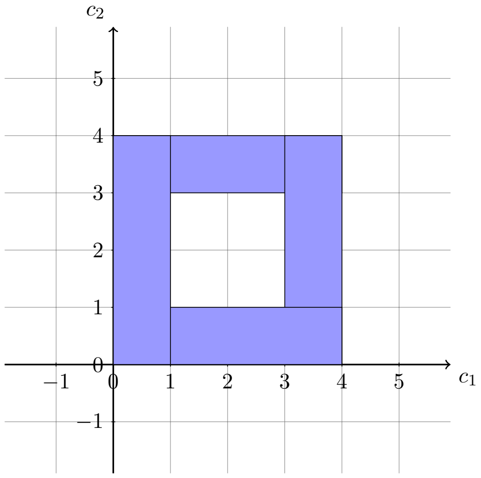
The DDD state space generator needs to be checked for correctness to say anything about the results. We only checked for partial correctness by comparing discrete states. Counting the discrete state-space can be done by counting the number of paths until the first DDD level in the diagram. These numbers were compared to the discrete state space in the LDD solution without reordering, here the discrete state-space can also be determined by counting paths until the first level representing zones. We can not directly compare state-spaces to Uppaal, different representations of the timing part of the state-space can give different numbers.



(a) Minuend



(b) Subtrahend



(c) Difference

Figure 11: Minus complexity example

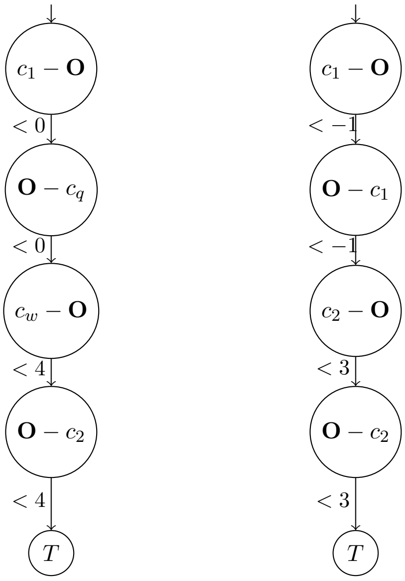


Figure 12: DDD representation of the minuend and subtrahend of figure 11

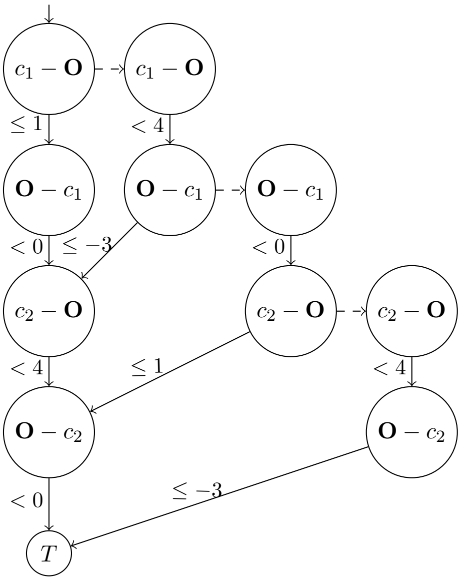


Figure 13: DDD representation of the difference of figure 11

5 Experiments

Below we describe the different models we used to run the benchmarks. We tried to find models that scale up for a number of nodes or processes, so that we can also check the behaviour of our approaches for different sizes of the same model. In this section we use the terminology 'locations' and other 'discrete variables'. The definition of timed automata does not have this difference, but we use it to describe models, because the time extrapolation is dependent on locations, and not on the other discrete variables. This dependency fills a large part of the dependency matrices. In this section, a location is a location in the Uppaal transition system editor, the other discrete variables are declared in the C-like syntax that Uppaal uses.

5.1 Viking

The set of Viking tests, models the classical Viking and bridge problem. It models 4 Vikings at a dark bridge, they only carry one torch. The torch is only strong enough to give light for 2 Vikings. All Vikings have different walking speeds, a faster Viking will have to adapt to a slower one, when crossing the bridge together. The walking speed of the Vikings is modelled by time constraints on the action of letting go of the torch. The model has a low number of discrete variables, one per Viking, one for the torch and an indicator for the side of the bridge on which the torch is. It has a global clock and a clock per Viking. The standard version of this problem has 4 Vikings. This can however be generalized to n Vikings.

The model results in a densely filled dependency matrix. The torch and all Viking variables are always read for the time extrapolation. Only the side indicator is not always read. The write matrix is sparser.

The difference between the LDD representation with flattened DBMs and the DDD representation is quite small for this model. In the extrapolation step all clock zones are set to $[0..\infty]$ for all states, so in both diagrams the zones are represented by a single path. So the interesting things are only happening in the discrete parts.

5.2 Fischer

Fischer's mutual exclusion protocol [19] is modelled for a number of processes. There is no synchronization between processes, only blocking of actions can occur. This model has a slightly higher number of discrete variables compared to the Viking tests. Each process has a location and an id. The model also has 2 global discrete variables. Each process has a local clock, no global clock is used.

The dependency matrix of this model has some sparse rows, as each model has an id, which is a constant and can only be read. Again all the location variables are always read due to the time extrapolation.

5.3 CSMA-CD

The Carrier Sense Multiple Access/Collision Detection [33] is modelled for a number of senders. The model has a few discrete variables, it only has locations and one global counter. The system is modelled with a single bus and n senders. Each sender and the bus have a local clock, no global clock is used. The model uses a lot of synchronizations between the senders and the bus.

5.4 Animo

We could not use the ANIMO models, only the smallest model with no synchronizations was possible. As we started the project to work on ANIMO models, we still included that single model in the benchmark set. It is a model with only one node, so only one location variable. The model has two clocks, a global clock and a clock for the node. Further it does have quite a large number of discrete variables. Both the global declaration and the node have a portion of C-like code with a number of global variables.

This results in a model with a quite sparse dependency matrix, as only the single location is used for the time extrapolation. We expected this model to have good performance for the LDD method with variable reordering.

5.5 Lynch-Shavit

The Lynch-Shavit mutual exclusion protcol [21] is modelled for different number of processes. The structure of the model is quite like the Fischer model. It only uses one global variable more than Fischer.

5.6 Milner

Milners scheduler [23] is modelled for a number of nodes. The structure is like that of the CSMA-CD model, except that it does not use a bus. The model has a lot of synchronizations between the nodes, and between the node and a global process. Each node has two clocks, so the zone representation blows up quickly.

5.7 Other models

We also used some models that we could not scale up enough due to memory/time limitations, or that could not scale up due to the nature of the model. We will not describe those models into detail. These models were the critRegion, Critical, bocdp(-fixed) [17], bando and timelock model.

5.8 Benchmark Runs

We ran benchmarks with the different solutions we described to compare them to each other. The DDD solution has been ran with the two BFS-prev algorithms as explained in section 4.10, we also used the bfs algorithm from LTSmin. For the LDD solution we only used the original BFS-prev algorithm. We ran this without reordering and with some of the reordering algorithms that LTSmin provides. We used the options gsa, rb4w, cw, rs,rn, rs,ru. These results are compared to the explicit-state multi-core LTSmin and the original Uppaal. All experiments have been done with and without the DBM reduction. All solutions are ran with one thread. The LDD and explicit-state multi-core solutions can be ran with multiple treads. The DDD solution does not support this, so for comparison reasons all methods are used in single-core mode. We also used the new language module with flattened DBMs in combination with the explicit-state multi-core tool.

6 Results

In this section we will only give an overview of all experiment results. The complete tables with all results are added in appendix A. In table 2 and table 3 we have summarized the results for some of the most interesting models. For the DDD, LDD and mc-flattened column, we give the best result that was found in the different experiment setups.

6.1 Time

The timed results show that our symbolic solutions are slower for almost all models, compared to both Uppaal and the explicit state multi-core tool. Only for the small bocdp models we have a symbolic solution that is faster than Uppaal.

One of the reasons we found was the high number of next-state calls. This is much higher than for the explicit-state tool as we partitioned the next-state function. For symbolic solutions this should be and advantage, as locality of transitions can be used. This same advantage should hold for the LDD solution we have, but the dependency matrices are too densely filled to give a real advantage. For the DDD solution we do not even make use of these localities, so there all advantages are lost. To confirm this hypothesis we also ran experiments without the partitioned next-state function. This gave for almost all models much better results. The results differ from a small loss in speed to a speedup of a factor 10. This is still not enough to compete with Uppaal, but makes it possible to explore larger models within a given time-bound.

Another problem seems to be the flattening of the DBM. This is an extra action that has to be executed in each next-state call, compared to the multi-core tool. This flattening is not a really expensive operation, it is only copying values, but it has to be executed a lot of times. For the DDD approach it is also necessary to close each DBM, as the DDD structure does not guarantee this. This is a more expensive operation and will also be executed in each next-state call. We implemented this in the language module, this closing is used for all experiments, so also for the experiments where it is not explicitly needed. This will also explain why the explicit state tool with subsumption is in most cases faster than the explicit state tool with flattened DBMs and without subsumption, even for models where subsumption will not have a real role, like the Viking models.

The last problem we see are the large state-vectors. This is mostly due to the quadratic size of the DBMs. For each of these variables a DDD level is created. As we have shown earlier, in some cases a lot of these levels will not have any impact on the zone represented. We can exploit this a little by setting these nodes to $(\infty, <)$, but the time-expensive function that does this has too much of an impact on the timing results. The diagram

	DDD	LDD	mc-flattened	mc-original	uppaal
fischer6	481.9	48.3	19.2	0.4	0.0
critRegion4	56.3	39.5	24.3	0.5	0.1
Critical_04-25-50	TO	TO	1.1	0.9	0.6
CSMACD_08	1.9	7.3	6.9	0.5	0.1
viking12	17.6	18.7	10.4	0.7	1.0
Lynch5-16	34.2	120.0	50.0	0.3	0.0
bocdp	0.1	0.2	0.2	0.0	0.2
bocdpFIXED	0.2	0.2	0.1	0.0	0.3
bando	0.2	0.2	0.1	0.0	0.3
Milner-8Nodes-flat	0.4	1.2	1.4	0.1	0.0
hddi_input_10	TO	93.3	43.1	0.0	0.0

Table 2: Time Results

	DDD	LDD
fischer6	15156	85041
critRegion4	55890	100006
Critical_03-25-50	3291	17505
CSMACD_08	36098	321001
viking12	342	342
Lynch5-16	49430	112397
bocdp	487	355
bocdpFIXED	488	427
bando	488	425
Milner-8Nodes-flat	11012	30883
hddi_input_10	TO	454246

Table 3: Node Results

could make much more use of this by skipping levels. This is not possible in our implementation as we only implicitly store the level of each node by its depth.

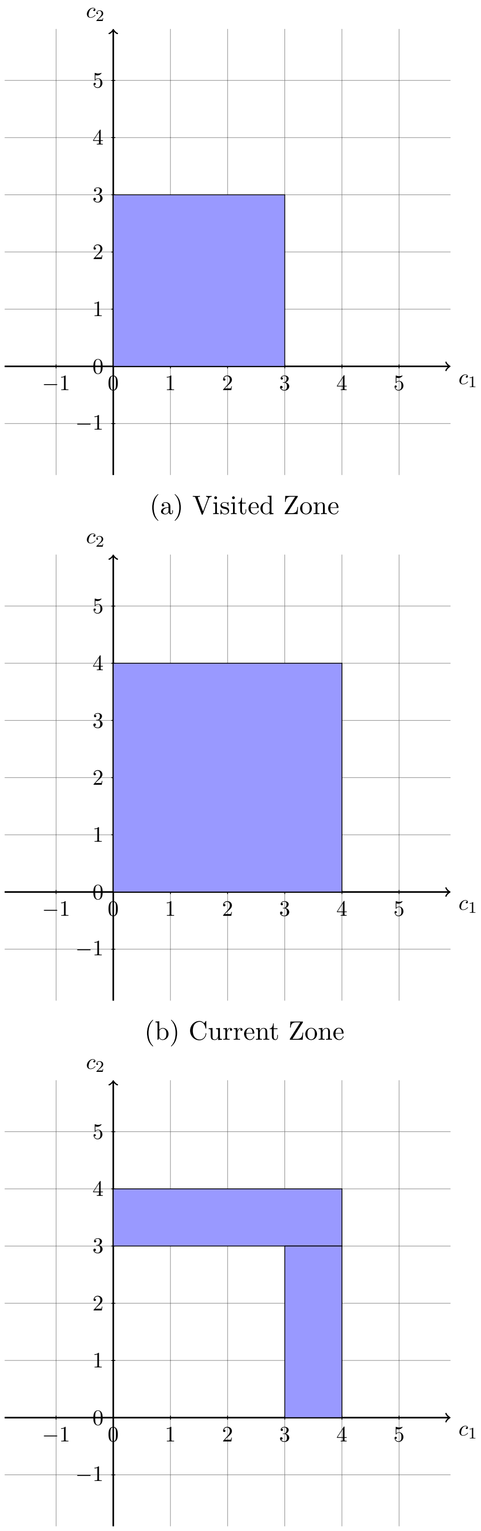
6.2 Memory

We have not measured memory usage. A good symbolic solution will use a lot of memory for caching when it is available. Comparing this to other solutions which use less caching will not be representative. We do compare the number of nodes between the different solutions.

For most models the best DDD solutions uses less nodes than the best LDD solution. This is what we expected as local reductions on clocks can be made. For the smallest models the LDD sometimes gives less nodes for some reorderings. These models have such low number of clocks that no reductions can be made yet. The bocdp and bando models are the largest models which have a lower LDD than DDD representation. These models have quite a high number of discrete variables with a low number of clocks. For most larger models the LDD solution without reordering is smaller than with reordering. This is probably due to the densely filled matrices, so no good reorderings can be created from them.

There is a difference between the number of nodes for the normal BFS and the BFS without minus. This is possible because we do not use a canonical form of DDDs. Most results show a higher number of nodes for the runs with the minus. In figure 14 we show an example of how this can happen. We assume all zones in the figures belong to the same set of locations. In figure 14a we have the zone that is already visited. Now a new state with the zone in figure 14b is discovered. If the minus is not used, successors of this state are directly generated from the set of locations and this zone. If the minus is used the first zone will first be subtracted before successors are generated. The result of the subtraction is shown in figure 14c. This is not a convex zone, so a DDD with multiple paths is needed. From this state also other successors can be generated, possibly needing more nodes to be represented. If the newly generated states are then unioned with the visited set the result can again have more nodes than the version without minus. The less fractionated zones in the current set can also have implications on the time results, as less work in the next-state function is needed. On the other hand the next-state function can also need extra time, as some states would otherwise have completely been removed from the current set, and no work for that states would need to be done.

The DBM reduction does not give the results we aimed for. For most models exploration is faster without the reduction. This is due to the expensive algorithm that the reduction is. Also the reduction of the number of nodes is not what we hoped for. Most models get more nodes when the reduction is turned on. The reduction can however still become usefull if we go to a canonical DDD representation.



(a) Visited Zone

(b) Current Zone

(c) After Minus

Figure 14: Minus fragmentation

7 Different Semantics

We chose in our implementation to take no information from the low edges of nodes. A node only represents an upper-bound, a false edge does not implicitly represent a lower bound. This is a design choice we made to be able to switch efficiently from the DBM representation in the language module to the DDD representation. We could however also have used a semantics where the low edges do represent a lower-bound. We did not implement this, but this section will discuss this other semantics.

Definition 17. *The semantics of a vertex is defined recursively by the function $\mathcal{V} : V \rightarrow \boldsymbol{Exp}$:*

- $\mathcal{V}[[0]] \overset{\text{def}}{=} \mathit{false},$
- $\mathcal{V}[[1]] \overset{\text{def}}{=} \mathit{true},$
- $\mathcal{V}[[v]] \overset{\text{def}}{=} \begin{cases} (pos(v) - neg(v) < const(v)) \rightarrow \mathcal{V}[[high(v)]], \mathcal{V}[[low(v)]] \mathit{if}\ op(v) =' <' \\ (pos(v) - neg(v) \leq const(v)) \rightarrow \mathcal{V}[[high(v)]], \mathcal{V}[[low(v)]] \mathit{if}\ op(v) =' \leq' \end{cases}$

The semantics are almost equal to the one in definition 5, the difference is in the interpretation of the low edge. In this semantics the low edge does not just represent that the upper-bound is higher than the bound of the node, but the actual value of the variable is higher than the bound of the node.

7.1 DBM Translation

The translation from a single DBM to a DDD will not change. The translation from multiple DBMs will change neither, as that can be done as a union of DBMs which are individually translated to a DDD. The other way around, from a DDD back to a DBM becomes more complicated. For a DDD with a single path to true nothing will change. For paths that go down some low edges the translation will change. The falsification of an upper-bound, leading to a lower-bound, or a upper-bound of the inverse pair, can overrule the upper-bound of an other node. We give an example in figure 15. In this example all nodes that are not in the path we consider are hidden. The DDD will have more nodes to reach this representation. In figure 16 we have a DBM for both interpretations. In figure 16a we have the DBM as we use the interpretation from our implementation. In figure 16b the DBM of the other interpretation is shown. The difference between the two DBMs is on the position $c_2 - O$). The information from the low edge of the $O - c_2$ node has overruled the information of the high edge of the $c_2 - O$ node. Using a canonical form of a DDD can also overcome this problem.

To make the translation from DDD to DBM correctly the relative positions of the upper- and lower-bound of each pair of variables need to be

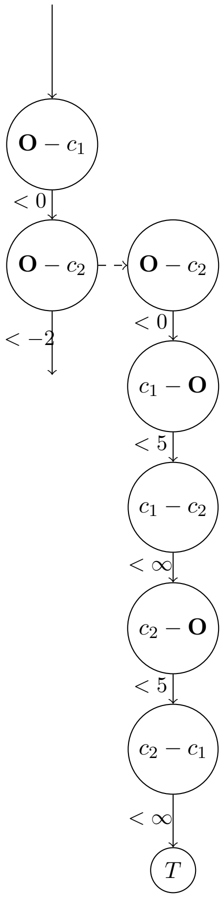


Figure 15: Implicit bound DDD

known. Also a function to determine the stronger bound of a pair needs to be created. Lastly the bounds need to be changed correctly. A $<$ sign changes into a $\leq$ and vice versa, the constant is multiplied by -1. We give an example of this change:

$$c_1 - c_2 \not< 3$$
$$\Updownarrow$$
$$c_1 - c_2 \geq 3$$
$$\Updownarrow$$
$$c_2 - c_1 \leq -3$$

A similar translation will have to be conducted in the relprod function. This function does not explicitly need the DBMs. The relations that are used are however created in the language module which uses DBMs. In the current implementation, a path in the state space needs to be found that

$$\begin{array}{cccc} & \mathbf{O} & c_1 & c_2 \\ \mathbf{O} & (0,\leq) & (0,<) & (0,<) \\ c_1 & (5,<) & (0,\leq) & (\infty,<) \\ c_2 & (5,<) & (\infty,<) & (0,\leq) \end{array}$$

(a) Original semantics

$$\begin{array}{cccc} & \mathbf{O} & c_1 & c_2 \\ \mathbf{O} & (0,\leq) & (0,<) & (0,<) \\ c_1 & (5,<) & (0,\leq) & (\infty,<) \\ c_2 & (2,\leq) & (\infty,<) & (0,\leq) \end{array}$$

(b) New semantics

Figure 16: DBM's of two different DDD interpretations

has on each level the same high edges as the relation. Which low edges are traversed on the way is not important. Now this information is taken into account some changes will have to be made. A simple path in the relation, might need some false edges in the state-space to get all the correct bounds.

7.2 Minus

Implementation of the minus function will become easier in DDDs, no coupling to the DBM library will be needed any more. First of all we will give the complement function. We give the pseudocode for this function in algorithm 9. The algorithm switches all 0 and 1 nodes. This will have a running time of $O(n)$ where n is the number of nodes in the tree. Our current implementation does not skip levels in the DDD towards a 1 node. This can happen in this complement function. This can be solved by filling the gap that is created with nodes with $(\infty, <)$ as bound. Another solution would be to allow this behaviour, this would need some extra work when creating state-vectors out of a diagram.

Algorithm 10 Complement

```
procedure COMPLEMENT($a$)
    if $a = 0$ then
        return 1
    if $a = 1$ then
        return 0
    $h :=$ COMPLEMENT($high(a)$)
    $l :=$ COMPLEMENT($low(a)$)
    return MK($bound(a), h, l$)
```

With this function we can create a minus function, as for set theory, minus can be defined as $A \backslash B = A \cap \overline{B}$. Now we can build the minus function from the complement and intersection function as shown in algorithm 10. This algorithm is probably less complex than the DBM minus we currently use. We do not know the exact complexity of the DBM minus algorithm, so we cannot call this certain.

Algorithm 11 Minus

```
procedure MINUS($a, b$)
    if $a = 0$ then
        return 0
    if $b = 0$ then
        return 1
    $notB$ =COMPLEMENT($b$)
    $result$ = INTERSECTION($a, notB$)
    return $result$
```

8 Future Work

In this section we discuss improvements that can be made for better results. In the previous section we already discussed the possibility of different semantics. This is also future work, but is written in a separate section.

8.1 Canonization

The DDD package does not use any canonical form. This means that some operations like equality and emptiness become less trivial. They can however still be done. The diagrams are ordered and locally reduced. The resulting state-vectors that the language module produces are also path-reduced. Most operators do not preserve this path-reducedness, so most diagrams will not be path-reduced.

We can implement two types of reduced DDDs. A DDD that is only path-reduced can be called semi-canonical [27]. This means that a tautology and a unsatisfiable expression can only be represented by a true or false node. This will make the checking for an empty DDD trivial, the DDD is only empty if the top node is a false node. We also defined full reducedness as a DDD that is tight and saturated, and has no disjunctive vertices. This fully reduced version is assumed to be canonical. A canonical DDD will change the equality test in a simple pointer comparison of the top nodes. Several algorithms to reach a reduced form are known [26].

The canonical forms are not needed at all times, only for some functions that need the specific form. Therefore we can choose to not have a canonical form at all times. One can choose to canonize the DDD after each operation, or to do this only before operations that actually need this form. The first option will have much canonization calls, where the second option will have less. The first option however, might have a DDD that is in all cases closer to the canonical form, so canonization might take less time, especially when caching is used. The semi-canonical form can also be used for emptiness checks, as the fully reduced diagram is not needed there. To get optimal results we need to find out what is the best option.

8.2 Reordering

The current DDD implementation is not compatible with the reordering algorithms. All algorithms will probably have to be changed somehow. In the current implementation it is assumed that on the top there is a set of LDD nodes, and from a certain level only DDD nodes exist. With reordering this could be mixed, so algorithms can not rely on this any more. A special case will again be the minus function. It is now done by recreating DBMs from the DDD. This can be done, as the nodes are ordered in the same way as the DBM. When reorderings are used this is not trivial any more. It will need to be explicitly stored which variable is on which level. For the different semantics that we introduced in section 7, a similar problem will occur. We suggested a minus function using the complement. For zones the complement is well defined, as there is a ∞ value representing the most upper- and lower-bounds of possible values. For discrete variables this is not directly clear.

Another option for reordering, which will probably solve some of the problems with the minus function would be reordering, but keeping the discrete and the zone parts separated. The discrete part could use the normal reordering algorithms. As the matrices for the zone variables are completely filled, the reordering algorithms can not do something useful on that level. Here experiments with manual reorderings can be tried. Now the standard ordering of the DBMs is used. It might be that having both bounds on a pair of clocks together gives better results, or maybe even other orderings.

8.3 Sparser Dependency Matrix

The dependency matrices are densely filled. We already discussed the problems in section 4.2. There are some solutions that can improve this. Smaller transition groups can be created, maybe even splitting the discrete part and the timed part of a transition. Another option that needs more work, is also filling the may-write matrices. The current code parsing that generates the matrices is not powerful enough to make a difference between may- and must-write variables. On this level also improvements can be made. The parts of the matrices for the zone variables are always filled, as the change of a single clock can have an impact on much of the DBM. We did not check however if an analysis can be done that finds fields which are not changed, or do not need to be read in a transition. A better analysis of the changes in DBMs can lead to sparser matrices on the zone variable side. The final improvement can be made for arrays. If the current implementation sees that a field from an array is read or written, then all fields in the array get a read or write dependency. It should be possible to only have dependencies for the fields that are actually read or written.

Splitting the discrete and timed part of a transition can also result in sparser dependency matrices. This would result in a set of discrete transition groups which only need access to the clock variables on which a bound is calculated. A single transition group will be created to model the continuation of time. This group will also do the time extrapolation. This group will probably need access to all variables as time extrapolation will still be dependent on the locations. Still also some location upperbounds can be present. It will however lead to a matrix that is less densely filled, such that the reordering algorithms and short next-state calls can result in much better performances.

8.4 Multi-Core

The DDD library is built in the Sylvan framework which allows for multi-threaded decision diagrams. The DDD library is not suited for multi-threading however. Most operations are already suited for multi-threading. The biggest problem is in the minus operation. This uses the DBM library. This part is not completely thread-safe. We expect this problem to be in the coupling between the DDD and the DBM library, in the DBM part no objects can be shared between threads. We expect that making the DDD part suitable for multi-threading will give much better time results.

8.5 Animo Model Compatibility

The project started to find a solution to model-check ANIMO models. This part has not succeeded. ANIMO models use a Uppaal feature that is not supported by opaal, using clock bounds on input channels. The problem why this can not be fixed directly is in the unrolling of the transitions in the next-state function. Adding the clock constraints on any of the input channels can lead to an empty DBM, in such cases the transition would not be returned. The semantics would however create the transitions, but not synchronize with the location leading to the empty DBM. To ensure that in such cases all possible transitions that can happen will be returned, a unroll of all possible combinations of synchronizing transitions would be needed. This will need a redesign of that part of the successor generator. If this functionality is added to opaal, all ANIMO models should be compatible with opaal, and thus with our symbolic solution.

8.6 Subsumption

The subsumption check that is included in the multi-core explicit-state backend in LTSmin is not implemented in the DDD library. This can be implemented as a DDD operation, with the implication operator and the apply function. A check $a \subseteq b$ will result in true if $b \implies a$ returns true. If a canonical form is used as well, the result will be only a true node, or a single path of $(\infty, <)$ nodes, depending on the possibility of skipping levels. This can limit the number of states added to the current set in the state algorithm, thus reducing the number of next-state calls needed. The most obvious subsumption check would be the check that a newly discovered zone is subsumed by the already visited state-space. It can however also be turned around, check if the visited state-space is subsumed by the newly discovered zone. In such a case the zone in the state space can be replaced by this new zone, such that the union function is not needed, this will not reduce the next-state calls however.

8.7 Checking Properties

The model-checker that we have created is only suited for state-space generation. It is not suited for property checking. One extra function is needed to use the LTSmin mu-calculus checker, which can also check CTL* formulas. The DDD library needs to be extended with a relprev function, which returns the predecessors given a set of states and a relation. This will only result in a discrete model-checker. LTSmin is not suited for timing properties. Some timing properties can be checked by extending the model with an extra automaton.

8.8 Skipping Levels

In the original DDD structure it is possible to skip levels. In our implementation this is not possible as the depth of the nodes is only stored explicitly. Skipping levels can be a good option however. In our DBM reduction we already set all unused bounds to $(\infty, <)$. In a structure where levels can be skipped, each node containing this value can be removed. This would need a change in the DDD nodes. Two choices can be made here. Nodes can be made of variable size, such that each possible value of depth can be added. One can also choose for a fixed depth field, and thus node-size. This would give a maximum bound to the depth of a diagram. The hashtable that is currently used to store all nodes would also need some changes. The current table is built specifically for nodes of 128 bits.

We ran some small experiments to see on what scale improvements can be achieved. The number of infinity nodes in the final state-spaces of some of our larger models were counted. This was done using the bfs-prev search strategy and with DBM reduction turned on. This showed that 25% to 90% of all nodes were nodes with infinity as bound. In theory all of these can be removed. This will not only reduce the number of nodes, but can also reduce the depth of recursive calls in the DDD. This can result in significant speedups.

9 Conclusions

The first goal of this project was to build a symbolic model-checker for timed automata in LTSmin. This has succeeded, we have a model-checker which uses the opaal language front-end for Uppaal models, and the symbolic back-end of LTSmin, using either the LDD or the new DDD package. This has all been achieved without changing the PINS structure. We only added one call to it which returns the number of discrete variables a model has.

The experiment results were not what we hoped for. The results are slower than both Uppaal, and the explicit-state tool that was already implemented in LTSmin. We were not able to replicate the results that were achieved earlier [27]. This can be explained by either the different structure of our model-checker or by the improvements that have been made by Uppaal since then [3].

One of the most fundamental problems we see are the densely filled dependency matrices. This makes it much harder to find good reorderings for symbolic structures. From our perspective this is also one of the key factors why partial order reduction for timed automata is a real challenge. Only when sparser dependency matrices can be achieved, the partial order reduction in LTSmin can be used effectively.

We have proposed a number of improvements that can be made to the DDD structure. Or even a complete overhaul of the DDDs by changing the semantics of the diagram. All of these improvements can be built upon the structure we created. With these improvements we hope that a symbolic model-checker can be built that can really compete with Uppaal and other model-checkers for timed automata.

We sticked as much as possible to the LDD design of Sylvan. This to use all of the optimizations that have already been created. On some points we expect better results when we step away from this design. Especially the skipping of levels in a diagram seems to be a serious issue, as this can reduce the size of the diagram significantly. Doing this will require some extra effort, as important parts of Sylvan, as the hashtable storing all nodes, cannot be used directly.

References

[1] S. B. Akers. Binary decision diagrams. *IEEE Trans. Comput.*, 27(6):509–516, June 1978.

[2] Rajeev Alur and David L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183 – 235, 1994.

[3] Gerd Behrmann, Johan Bengtsson, Alexandre David, Kim G. Larsen, Paul Pettersson, and Wang Yi. UPPAAL implementation secrets. In *Proc. of 7*th *International Symposium on Formal Techniques in Real-Time and Fault Tolerant Systems*, 2002.

[4] Gerd Behrmann, Patricia Bouyer, Kim G. Larsen, and Radek Pelánek. *Lower and Upper Bounds in Zone Based Abstractions of Timed Automata*, pages 312–326. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.

[5] Gerd Behrmann, Alexandre David, and Kim G. Larsen. A tutorial on Uppaal. In Marco Bernardo and Flavio Corradini, editors, *Formal Methods for the Design of Real-Time Systems*, volume 3185 of *Lecture Notes in Computer Science*, pages 200–236. Springer Berlin Heidelberg, 2004.

[6] Johan Bengtsson. *Clocks, DBMS and States in Timed Systems (Uppsala Dissertations from the Faculty of Science Technology, 39).* Uppsala Universitet, 7 2002.

[7] Dirk Beyer. Efficient reachability analysis and refinement checking of timed automata using BDDs. In T. Margaria and T. F. Melham, editors, *Proceedings of the 11th IFIP Advanced Research Working Conference on Correct Hardware Design and Verification Methods (CHARME 2001, Livingston, September 4-7)*, LNCS 2144, pages 86–91. Springer-Verlag, Heidelberg, 2001.

[8] Dirk Beyer, Claus Lewerentz, and Andreas Noack. Rabbit: A tool for BDD-based verification of real-time systems. In W. A. Hunt and F. Somenzi, editors, *Proceedings of the 15th International Conference on Computer Aided Verification (CAV 2003, Boulder, CO, July 8-12)*, LNCS 2725, pages 122–125. Springer-Verlag, Heidelberg, 2003.

[9] S. C. C. Blom, J. C. van de Pol, and M. Weber. LTSmin: Distributed and symbolic reachability. In T. Touili, B. Cook, and P. Jackson, editors, *Computer Aided Verification, Edinburgh*, volume 6174 of *Lecture Notes in Computer Science*, pages 354–359, Berlin, July 2010. Springer Verlag.

[10] Stefan Blom and Jaco van de Pol. Symbolic reachability for process algebras with recursive data types. In J.S. Fitzgerald, A.E. Haxthausen, and H. Yenigun, editors, *Theoretical Aspects of Computing*, volume 5160 of *Lecture Notes in Computer Science*, pages 81–95, Berlin, Germany, August 2008. Springer Verlag.

[11] R.E. Bryant. Graph-based algorithms for boolean function manipulation. *Computers, IEEE Transactions on*, C-35(8):677–691, Aug 1986.

[12] A. E. Dalsgaard, A. W. Laarman, K. G. Larsen, M. C. Olesen, and J. C. van de Pol. Multi-core reachability for timed automata. In M. Jurdzinski and D. Nickovic, editors, *10th International Conference on Formal Modeling and Analysis of Timed Systems, FORMATS 2012, London, UK*, volume 7595 of *Lecture Notes in Computer Science*, pages 91–106, London, September 2012. Springer Verlag.

[13] Andreas Engelbredt Dalsgaard, Ren Rydhof Hansen, Kenneth Yrke Jørgensen, Kim Gulstrand Larsen, Mads Chr. Olesen, Petur Olsen, and Ji Srba. opaal: A lattice model checker. In Mihaela Bobaru, Klaus Havelund, GerardJ. Holzmann, and Rajeev Joshi, editors, *NASA Formal Methods*, volume 6617 of *Lecture Notes in Computer Science*, pages 487–493. Springer Berlin Heidelberg, 2011.

[14] David L. Dill. Timing assumptions and verification of finite-state concurrent systems. In Joseph Sifakis, editor, *Automatic Verification Methods for Finite State Systems*, volume 407 of *Lecture Notes in Computer Science*, pages 197–212. Springer Berlin Heidelberg, 1990.

[15] Junwei Du, Huiping Zhang, Gang Yu, and Xi Wang. A full symbolic compositional reachability analysis of timed automata based on BDD. In *Advanced Computational Intelligence (ICACI), 2015 Seventh International Conference on*, pages 218–222, March 2015.

[16] R. Ehlers, D. Fass, M. Gerke, and H.-J. Peter. Fully symbolic timed model checking using constraint matrix diagrams. In *Real-Time Systems Symposium (RTSS), 2010 IEEE 31st*, pages 360–371, Nov 2010.

[17] K. Havelund, A. Skou, K. G. Larsen, and K. Lund. Formal modeling and analysis of an audio/video protocol: an industrial case study using UPPAAL. In *Real-Time Systems Symposium, 1997. Proceedings., The 18th IEEE*, pages 2–13, Dec 1997.

[18] A. W. Laarman, J. C. van de Pol, and M. Weber. Multi-Core LTSmin: Marrying Modularity and Scalability. In M. Bobaru, K. Havelund, G. Holzmann, and R. Joshi, editors, *Proceedings of the Third International Symposium on NASA Formal Methods, NFM 2011, Pasadena,*

CA, USA, volume 6617 of *Lecture Notes in Computer Science*, pages 506–511, Berlin, July 2011. Springer Verlag.

[19] Leslie Lamport. A fast mutual exclusion algorithm. *ACM Trans. Comput. Syst.*, 5(1):1–11, January 1987.

[20] Kim Larsen, Carsten Weise, Wang Yi, and Justin Pearson. Clock difference diagrams. *BRICS Report Series*, 5(46), 1998.

[21] N. Lynch and N. Shavit. Timing based mutual exclusion. In *Proc. of the Annual Real-Time Symposium (RTSS)*, pages 2–11, 1992.

[22] Jeroen Meijer, Gijs Kant, Stefan Blom, and Jaco van de Pol. Read, write and copy dependencies for symbolic model checking. In Eran Yahav, editor, *Hardware and Software: Verification and Testing*, volume 8855 of *Lecture Notes in Computer Science*, pages 204–219. Springer International Publishing, 2014.

[23] R. Milner. *Communication and Concurrency.* Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1989.

[24] J. Møller, J. Lichtenberg, H. R. Andersen, and H. Hulgaard. Difference decision diagrams. Technical Report IT-TR-1999-023, Department of Information Technology, Technical University of Denmark, Building 344, DK-2800 Lyngby, Denmark, February 1999.

[25] Jesper Møller, Henrik Hulgaard, and Henrik Reif Andersen. Symbolic model checking of timed guarded commands using difference decision diagrams. *The Journal of Logic and Algebraic Programming*, 5253:53 – 77, 2002.

[26] Jesper Møller and Jakob Lichtenberg. Difference decision diagrams. Master's thesis, Department of Information Technology, Technical University of Denmark, Building 344, DK-2800 Lyngby, Denmark, aug 1998.

[27] Jesper Møller, Jakob Lichtenberg, HenrikReif Andersen, and Henrik Hulgaard. Difference decision diagrams. In Jörg Flum and Mario Rodriguez-Artalejo, editors, *Computer Science Logic*, volume 1683 of *Lecture Notes in Computer Science*, pages 111–125. Springer Berlin Heidelberg, 1999.

[28] TruongKhanh Nguyen, Jun Sun, Yang Liu, JinSong Dong, and Yan Liu. Improved BDD-based discrete analysis of timed systems. In Dimitra Giannakopoulou and Dominique Méry, editors, *FM 2012: Formal Methods*, volume 7436 of *Lecture Notes in Computer Science*, pages 326–340. Springer Berlin Heidelberg, 2012.

[29] Stefano Schivo, Jetse Scholma, Brend Wanders, Ricardo A. Urquidi Camacho, Paul E. van der Vet, Marcel Karperien, Rom Langerak, Jaco van de Pol, and Janine N. Post. Modelling biological pathway dynamics with timed automata. In *12th IEEE International Conference on Bioinformatics & Bioengineering, BIBE 2012, Larnaca, Cyprus, November 11-13, 2012*, pages 447–453, 2012.

[30] A. Srinivasan, T. Ham, S. Malik, and R.K. Brayton. Algorithms for discrete function manipulation. In *Computer-Aided Design, 1990. ICCAD-90. Digest of Technical Papers., 1990 IEEE International Conference on*, pages 92–95, Nov 1990.

[31] Tom van Dijk and Jaco van de Pol. Sylvan: Multi-core decision diagrams. In Christel Baier and Cesare Tinelli, editors, *Tools and Algorithms for the Construction and Analysis of Systems*, volume 9035 of *Lecture Notes in Computer Science*, pages 677–691. Springer Berlin Heidelberg, 2015.

[32] Farn Wang. Efficient verification of timed automata with BDD-like data-structures. In LenoreD. Zuck, PaulC. Attie, Agostino Cortesi, and Supratik Mukhopadhyay, editors, *Verification, Model Checking, and Abstract Interpretation*, volume 2575 of *Lecture Notes in Computer Science*, pages 189–205. Springer Berlin Heidelberg, 2003.

[33] Sergio Yovine. Kronos: a verification tool for real-time systems. *International Journal on Software Tools for Technology Transfer*, 1(1-2):123–133, 1997.

[34] Huiping Zhang, Junwei Du, Ling Cao, and Guixin Zhu. A full symbolic reachability analysis algorithm of timed automata based on BDD. In *Autonomous Decentralized Systems (ISADS), 2015 IEEE Twelfth International Symposium on*, pages 301–304, March 2015.

A Experiment Results

This appendix contains all experimental results. The tables were too large to fit on a single page, so they have been cut in three parts. The first three tables show the timing results in seconds. The last three tables show the number of nodes in the final state-space for all the symbolic tools. The first five rows show the different options that have been used. The first row gives the state-store, this can be DDD, LDD or explicit-state. The second row gives the search-order, this can be either bfs-prev, bfs or, no-minus which is the altered bfs-prev we created as mentioned in section 4.10. The third row indicates if a partitioned-next state function is used or not. The fourth row indicates which reordering option, if any, is used. The fifth row indicates if the DBM-reduction, as mentioned in section 4.3, is used. The third table also contains a sixth row indicating the representation of the DBM. All options use a flattened DBM, only the explicit-state multi-core tool can use a pointer to the DBM, as this is the only point where this is used, the row is not included in the other tables. A "TO" in any of the tables means that a time-out has occurred. For all experiments this time-out has been set to 600 seconds.

Statestore	DDD	DDD	DDD	DDD	DDD	DDD	DDD	DDD	DDD	DDD	DDD	DDD
Search-order	bfs-prev	bfs-prev	bfs-prev	bfs-prev	bfs	bfs	bfs	bfs	no-minus	no-minus	no-minus	no-minus
Partitioned	+	-	+	-	+	-	+	-	+	-	+	-
Reorder	-	-	-	-	-	-	-	-	-	-	-	-
DBM-reduction	+	+	-	-	+	+	-	-	+	+	-	-
fischer1	0.2	0.1	0.1	0.1	0.2	0.1	0.1	0.1	0.1	0.1	0.1	0.1
fischer2	0.2	0.2	0.1	0.1	0.2	0.1	0.2	0.2	0.1	0.2	0.1	0.1
fischer3	0.3	0.2	0.2	0.2	0.3	0.2	0.2	0.2	0.2	0.2	0.2	0.2
fischer4	0.5	0.3	0.3	0.2	0.4	0.2	0.3	0.2	0.3	0.2	0.3	0.2
fischer5	10.7	3.9	7.3	2.8	7.6	2.8	5.7	2.5	6.2	2.9	5.7	2.5
fischer6	TO	TO	TO	TO	TO	TO	TO	TO	TO	481.9	TO	532.6
critRegion1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
critRegion2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
critRegion3	1.9	1.2	0.4	0.3	1.9	1.2	0.4	0.3	1.8	1.2	0.4	0.3
critRegion4	TO	TO	68.4	56.3	TO	TO	462.9	TO	TO	TO	471.7	TO
Critical_01-25-50	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Critical_02-25-50	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
Critical_03-25-50	9.5	5.9	0.9	0.6	8.8	5.5	0.9	0.6	8.5	5.9	0.9	0.6
Critical_04-25-50	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO
CSMACD_01	0.2	0.1	0.1	0.1	0.2	0.1	0.1	0.1	0.1	0.1	0.1	0.1
CSMACD_02	0.2	0.1	0.1	0.1	0.2	0.1	0.1	0.1	0.1	0.1	0.1	0.1
CSMACD_03	0.2	0.2	0.2	0.2	0.2	0.1	0.2	0.1	0.2	0.1	0.1	0.1
CSMACD_04	0.3	0.2	0.2	0.2	0.3	0.2	0.2	0.2	0.2	0.2	0.2	0.2
CSMACD_05	0.7	0.3	0.3	0.2	0.4	0.2	0.2	0.2	0.3	0.2	0.2	0.2
CSMACD_06	3.2	1.1	1.0	0.5	0.8	0.4	0.5	0.3	0.6	0.4	0.5	0.3
CSMACD_07	13.4	4.8	3.6	1.6	1.9	0.9	1.1	0.7	1.5	0.9	1.1	0.7
CSMACD_08	53.1	22.3	14.6	6.2	5.3	2.5	3.2	1.9	4.2	2.5	3.2	1.9
viking1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
viking2	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
viking3	0.2	0.2	0.2	0.2	0.2	0.1	0.2	0.2	0.2	0.1	0.1	0.1
viking4	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
viking5	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
viking6	0.5	0.3	0.4	0.2	0.5	0.3	0.5	0.2	0.6	0.3	0.5	0.2
viking7	0.8	0.4	0.7	0.3	0.8	0.4	0.7	0.3	0.8	0.4	0.7	0.3
viking8	2.3	0.9	1.8	0.5	2.4	0.9	1.8	0.5	2.2	0.9	1.8	0.5
viking9	6.6	2.5	5.2	1.2	6.6	2.5	5.1	1.2	6.5	2.5	5.2	1.2
viking10	20.3	7.2	15.1	3.2	20.5	7.2	15.1	3.2	19.0	7.2	15.1	3.2
viking11	62.4	20.4	43.4	8.5	60.6	20.5	43.3	8.5	54.9	20.5	43.4	8.6
viking12	114.6	40.2	109.4	17.7	114.6	40.2	108.9	17.6	115.1	40.2	109.8	17.7
Lynch1-16	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Lynch2-16	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
Lynch3-16	0.4	0.2	0.3	0.2	0.4	0.2	0.3	0.2	0.3	0.2	0.3	0.2
Lynch4-16	5.8	2.6	3.6	1.6	5.2	2.6	3.2	1.5	4.6	2.8	3.4	1.6
Lynch5-16	251.3	110.9	114.8	48.2	143.4	67.4	71.8	34.2	130.9	74.1	75.6	36.7
bocdp	0.2	0.2	0.2	0.2	0.2	0.1	0.2	0.2	0.2	0.2	0.2	0.2
bocdpFIXED	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
bando	0.3	0.2	0.2	0.2	0.3	0.2	0.2	0.2	0.2	0.2	0.2	0.2
timelock	0.2	0.1	0.0	0.0	0.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Milner-2Nodes-flat	0.3	0.2	0.2	0.2	0.2	0.1	0.1	0.2	0.2	0.2	0.1	0.2
Milner-3Nodes-flat	0.3	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
Milner-4Nodes-flat	0.4	0.2	0.2	0.2	0.3	0.2	0.2	0.2	0.2	0.2	0.2	0.2
Milner-5Nodes-flat	0.4	0.3	0.3	0.2	0.4	0.2	0.2	0.2	0.3	0.2	0.2	0.2
Milner-6Nodes-flat	0.6	0.3	0.3	0.3	0.6	0.3	0.3	0.3	0.4	0.3	0.3	0.3
Milner-7Nodes-flat	0.8	0.5	0.5	0.3	0.8	0.4	0.5	0.3	0.5	0.4	0.4	0.3
Milner-8Nodes-flat	1.2	0.7	0.7	0.5	1.2	0.6	0.7	0.4	0.8	0.5	0.6	0.4
hddi_input_1	0.2	0.2	0.2	0.2	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
hddi_input_2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.1	0.2	0.1	0.2
hddi_input_3	104.2	104.2	18.2	17.9	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
hddi_input_4	TO	TO	TO	TO	0.3	0.2	0.3	0.2	0.3	0.2	0.3	0.2
hddi_input_5	TO	TO	TO	TO	1.1	0.5	0.3	0.2	1.1	0.5	0.3	0.2
hddi_input_6	TO	TO	TO	TO	307.2	22.3	305.2	18.3	308.2	22.2	304.8	18.3
hddi_input_7	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO
hddi_input_8	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO
hddi_input_9	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO
hddi_input_10	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO
ANIMO_small	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2

Statestore	LDD	LDD	LDD	LDD	LDD	LDD	LDD	LDD	LDD	LDD
Search-order	bfs-prev	bfs-prev	bfs-prev	bfs-prev	bfs-prev	bfs-prev	bfs-prev	bfs-prev	bfs-prev	bfs-prev
Partitioned	+	-	+	-	+	-	+	-	+	-
Reorder	gsa	gsa	rb4w	rb4w	cw	cw	rs,rn	rs,rn	rs,ru	rs,ru
DBM-reduction	+	-	+	-	+	-	+	-	+	-
fischer1	0.4	0.3	0.2	0.1	0.2	0.1	0.2	0.1	0.2	0.1
fischer2	0.8	0.6	0.2	0.1	0.2	0.1	0.2	0.1	0.2	0.1
fischer3	1.3	1.0	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
fischer4	2.0	1.5	0.5	0.3	0.5	0.3	0.4	0.3	0.4	0.3
fischer5	6.3	4.8	4.6	3.5	4.0	3.0	3.7	2.7	3.5	2.6
fischer6	82.2	66.0	91.4	68.0	78.9	64.9	67.4	57.3	63.4	55.9
critRegion1	0.4	0.4	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
critRegion2	0.6	0.6	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
critRegion3	1.3	1.8	0.8	1.2	0.7	1.1	0.6	1.0	0.9	1.5
critRegion4	46.5	131.3	49.6	143.6	43.7	123.7	39.5	114.3	73.5	201.7
Critical_01-25-50	0.4	0.4	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Critical_02-25-50	0.6	0.6	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
Critical_03-25-50	6.3	5.4	6.0	5.1	4.6	3.8	3.9	3.5	7.1	6.3
Critical_04-25-50	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO
CSMACD_01	0.3	0.2	0.2	0.1	0.2	0.1	0.2	0.1	0.1	0.1
CSMACD_02	0.6	0.4	0.2	0.1	0.2	0.1	0.3	0.1	0.3	0.1
CSMACD_03	0.8	0.5	0.3	0.1	0.2	0.1	0.3	0.1	0.2	0.1
CSMACD_04	0.7	0.6	0.3	0.2	0.3	0.2	0.3	0.2	0.3	0.2
CSMACD_05	1.1	0.8	0.4	0.3	0.4	0.3	0.4	0.3	0.4	0.3
CSMACD_06	1.8	1.4	1.4	0.9	1.2	0.9	1.1	0.8	1.2	0.8
CSMACD_07	4.6	3.7	4.4	3.4	4.8	3.4	4.0	2.9	3.8	2.8
CSMACD_08	16.2	13.4	16.2	14.7	16.0	14.7	13.0	12.4	12.3	11.9
viking1	0.3	0.3	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
viking2	0.4	0.4	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
viking3	0.5	0.5	0.1	0.1	0.2	0.1	0.1	0.1	0.1	0.1
viking4	0.7	0.7	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
viking5	0.8	0.8	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
viking6	1.4	1.3	0.7	0.6	0.7	0.6	0.6	0.5	0.5	0.4
viking7	1.7	1.6	1.0	0.8	1.0	0.8	0.8	0.7	0.7	0.6
viking8	3.5	2.9	2.9	2.4	3.0	2.4	2.4	1.8	2.0	1.5
viking9	8.3	6.7	9.1	7.5	9.3	7.5	7.2	5.4	6.1	4.4
viking10	23.3	17.7	29.8	22.9	29.5	22.9	22.8	16.2	18.2	12.8
viking11	69.9	49.3	90.4	68.7	85.7	68.8	63.6	47.7	49.6	37.1
viking12	124.1	100.9	164.1	141.5	164.1	141.8	122.2	100.1	100.7	78.5
Lynch1-16	0.5	0.5	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Lynch2-16	1.0	1.1	0.2	0.2	0.1	0.1	0.2	0.1	0.2	0.2
Lynch3-16	2.2	1.8	0.5	0.3	0.5	0.3	0.4	0.3	0.4	0.3
Lynch4-16	7.9	6.2	6.6	5.1	5.6	4.2	5.2	3.9	4.9	3.7
Lynch5-16	149.8	134.1	191.8	162.6	162.5	137.9	147.5	126.3	142.8	123.1
bocdp	9.9	9.9	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
bocdpFIXED	9.8	9.7	0.2	0.2	0.2	0.2	0.3	0.2	0.3	0.2
bando	11.6	9.8	0.3	0.2	0.3	0.2	0.2	0.2	0.2	0.2
timelock	0.2	0.1	0.2	0.1	0.1	0.1	0.1	0.0	0.1	0.0
Milner-2Nodes-flat	0.5	0.4	0.3	0.2	0.2	0.2	0.2	0.2	0.2	0.2
Milner-3Nodes-flat	0.8	0.6	0.3	0.2	0.3	0.2	0.3	0.2	0.3	0.2
Milner-4Nodes-flat	1.5	0.9	0.7	0.4	0.7	0.4	0.7	0.4	0.7	0.4
Milner-5Nodes-flat	1.8	1.2	1.1	0.7	1.1	0.7	1.0	0.6	1.0	0.6
Milner-6Nodes-flat	2.6	1.7	1.7	1.1	1.6	1.1	1.5	0.9	1.5	0.9
Milner-7Nodes-flat	3.6	2.4	2.6	1.7	2.7	1.7	2.4	1.5	2.2	1.3
Milner-8Nodes-flat	5.1	3.4	4.1	2.8	4.1	2.8	3.5	2.2	3.4	1.9
hddi_input_1	0.2	0.3	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
hddi_input_2	0.3	0.3	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
hddi_input_3	0.4	0.4	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
hddi_input_4	0.7	0.8	0.6	0.6	0.6	0.6	0.5	0.5	0.5	0.5
hddi_input_5	1.7	1.8	1.5	1.6	1.6	1.6	1.3	1.3	1.2	1.3
hddi_input_6	5.9	6.8	7.4	8.4	7.5	8.5	5.5	6.4	5.5	6.3
hddi_input_7	18.9	22.7	27.5	32.1	27.6	32.3	18.9	22.6	18.9	22.6
hddi_input_8	64.1	78.9	95.2	113.7	95.1	114.2	64.1	78.9	64.1	79.0
hddi_input_9	144.6	172.3	206.6	240.5	207.0	241.5	146.1	171.7	144.0	172.8
hddi_input_10	429.6	521.4	TO	TO	TO	TO	428.4	519.9	429.5	520.3
ANIMO_small	0.7	0.7	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2

Statestore	LDD	LDD	LDD	LDD	Explicit	Explicit	Explicit	Uppaal
Search-order	bfs-prev	bfs-prev	bfs-prev	bfs-prev	bfs	bfs	bfs	
Partitioned	+	-	+	-	-	-	-	
Reorder	-	-	-	-	-	-	-	
DBM-reduction	+	-	+	-	-	-	+	
DBM	flat	flat	flat	flat	pointer	flat	flat	
fischer1	0.2	0.1	0.1	0.1	0.2	0.1	0.0	0.0
fischer2	0.2	0.1	0.1	0.1	0.3	0.1	0.0	0.0
fischer3	0.2	0.2	0.2	0.2	0.0	0.3	0.2	0.0
fischer4	0.5	0.3	0.3	0.2	0.1	0.9	0.9	0.0
fischer5	3.7	2.4	2.7	2.0	0.2	2.9	3.2	0.0
fischer6	66.4	57.4	57.4	48.3	0.4	19.2	26.2	0.0
critRegion1	0.1	0.1	0.1	0.1	0.0	0.0	0.0	0.0
critRegion2	0.2	0.2	0.2	0.2	0.1	0.2	0.2	0.0
critRegion3	0.7	0.6	1.1	1.0	0.2	2.4	2.1	0.0
critRegion4	45.0	44.5	122.5	136.3	0.5	58.5	24.3	0.1
Critical_01-25-50	0.1	0.1	0.1	0.1	0.0	0.0	0.0	0.0
Critical_02-25-50	0.2	0.2	0.2	0.2	0.1	0.4	0.4	0.0
Critical_03-25-50	4.1	4.8	3.7	4.5	0.3	1.0	1.7	0.0
Critical_04-25-50	TO	TO	TO	TO	0.9	1.1	1.7	0.6
CSMACD_01	0.2	0.1	0.1	0.1	0.0	0.0	0.0	0.0
CSMACD_02	0.2	0.1	0.1	0.1	0.0	0.0	0.0	0.0
CSMACD_03	0.3	0.2	0.1	0.1	0.0	0.1	0.1	0.0
CSMACD_04	0.3	0.2	0.2	0.2	0.1	0.4	0.4	0.0
CSMACD_05	0.5	0.2	0.3	0.2	0.2	0.8	0.8	0.0
CSMACD_06	1.3	0.6	0.9	0.5	0.3	1.6	1.6	0.0
CSMACD_07	4.6	1.9	3.3	1.7	0.3	3.0	3.4	0.0
CSMACD_08	15.1	7.9	14.3	7.3	0.5	6.9	8.1	0.1
viking1	0.1	0.1	0.1	0.1	0.0	0.0	0.0	0.0
viking2	0.1	0.1	0.1	0.1	0.0	0.0	0.0	0.0
viking3	0.2	0.1	0.1	0.1	0.0	0.1	0.1	0.0
viking4	0.2	0.2	0.2	0.2	0.1	0.2	0.3	0.0
viking5	0.2	0.2	0.2	0.2	0.2	0.5	0.5	0.0
viking6	0.7	0.3	0.6	0.2	0.3	0.9	1.0	0.0
viking7	1.0	0.4	0.8	0.3	0.3	1.4	1.5	0.0
viking8	3.0	0.9	2.4	0.5	0.4	2.1	2.4	0.0
viking9	9.7	2.6	7.4	1.3	0.5	2.6	3.8	0.1
viking10	30.3	7.4	22.6	3.3	0.7	3.5	7.6	0.2
viking11	86.6	20.9	67.7	9.0	1.0	6.0	18.0	0.5
viking12	162.9	41.2	140.7	18.7	0.7	10.4	32.9	1.0
Lynch1-16	0.1	0.1	0.1	0.1	0.0	0.0	0.0	0.0
Lynch2-16	0.2	0.1	0.2	0.2	0.0	0.2	0.2	0.0
Lynch3-16	0.5	0.3	0.3	0.3	0.1	1.2	1.2	0.0
Lynch4-16	5.3	3.8	4.0	3.5	0.2	3.4	3.8	0.0
Lynch5-16	164.4	138.0	129.6	120.0	0.3	50.0	68.4	0.0
bocdp	0.2	0.2	0.2	0.2	0.0	0.2	0.2	0.2
bocdpFIXED	0.3	0.2	0.2	0.2	0.0	0.1	0.2	0.3
bando	0.3	0.2	0.2	0.2	0.0	0.1	0.2	0.3
timelock	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Milner-2Nodes-flat	0.2	0.2	0.2	0.2	0.0	0.1	0.1	0.0
Milner-3Nodes-flat	0.3	0.2	0.2	0.2	0.0	0.4	0.4	0.0
Milner-4Nodes-flat	0.7	0.4	0.4	0.3	0.1	0.8	0.8	0.0
Milner-5Nodes-flat	1.0	0.6	0.7	0.5	0.1	0.9	1.0	0.0
Milner-6Nodes-flat	1.6	0.9	1.1	0.6	0.1	1.1	1.3	0.0
Milner-7Nodes-flat	2.6	1.3	1.7	0.9	0.1	1.2	1.6	0.0
Milner-8Nodes-flat	4.1	1.9	2.7	1.2	0.1	1.4	2.1	0.0
hddi_input_1	0.1	0.1	0.1	0.2	0.0	0.0	0.0	0.0
hddi_input_2	0.2	0.2	0.2	0.2	0.0	0.2	0.1	0.0
hddi_input_3	0.2	0.2	0.2	0.2	0.0	0.4	0.3	0.0
hddi_input_4	0.5	0.3	0.6	0.3	0.0	0.6	0.6	0.0
hddi_input_5	1.5	0.6	1.6	0.5	0.0	0.8	0.8	0.0
hddi_input_6	7.4	1.9	8.4	1.6	0.0	1.7	2.1	0.0
hddi_input_7	27.4	5.8	32.1	5.1	0.2	3.5	4.9	0.0
hddi_input_8	94.6	17.2	114.0	15.1	0.2	8.1	12.5	0.1
hddi_input_9	206.9	38.8	240.7	34.4	0.1	17.1	25.7	0.0
hddi_input_10	TO	104.6	TO	93.3	0.0	43.1	68.0	0.0
ANIMO_small	0.2	0.2	0.2	0.2	0.2	0.4	0.5	0.0

Statestore	DDD	DDD	DDD	DDD	DDD	DDD	DDD	DDD
Search-order	bfs-prev	bfs-prev	bfs-prev	bfs-prev	bfs	bfs	bfs	bfs
Partitioned	+	-	+	-	+	-	+	-
Reorder	-	-	-	-	-	-	-	-
DBM-reduction	+	+	-	-	+	+	-	-
fischer1	14	14	14	14	14	14	14	14
fischer2	66	66	66	66	66	66	66	66
fischer3	509	509	468	468	288	288	250	250
fischer4	5025	5025	4631	4631	1300	1300	987	987
fischer5	49634	49634	46879	46879	5535	5535	3920	3920
fischer6	TO	TO	TO	444745	TO	TO	TO	TO
critRegion1	24	24	24	24	24	24	24	24
critRegion2	251	251	227	227	190	190	140	140
critRegion3	4643	4643	3042	3042	3836	3836	1683	1683
critRegion4	TO	TO	83145	83145	TO	TO	56222	TO
Critical_01-25-50	25	25	25	25	25	25	25	25
Critical_02-25-50	313	313	253	253	262	262	158	158
Critical_03-25-50	12322	12322	5265	5265	10898	10898	3291	3291
Critical_04-25-50	TO	TO	TO	TO	TO	TO	TO	TO
CSMACD_01	17	17	17	17	17	17	17	17
CSMACD_02	112	112	107	107	108	108	108	108
CSMACD_03	686	686	525	525	458	458	435	435
CSMACD_04	3305	3305	2210	2210	1356	1356	1357	1357
CSMACD_05	13867	13867	8320	8320	3478	3478	3790	3790
CSMACD_06	51633	51633	28838	28838	7925	7925	10099	10099
CSMACD_07	176965	176965	93717	93717	17069	17069	26381	26381
CSMACD_08	569760	569760	289252	289252	36098	36098	68197	68197
viking1	12	12	12	12	15	15	15	15
viking2	37	37	37	37	37	37	37	37
viking3	86	86	86	86	86	86	86	86
viking4	105	105	105	105	105	105	105	105
viking5	124	124	124	124	124	124	124	124
viking6	233	233	233	233	233	233	233	233
viking7	190	190	190	190	190	190	190	190
viking8	224	224	224	224	224	224	224	224
viking9	263	263	263	263	263	263	263	263
viking10	304	304	304	304	304	304	304	304
viking11	347	347	347	347	347	347	347	347
viking12	342	342	342	342	342	342	342	342
Lynch1-16	24	24	24	24	24	24	24	24
Lynch2-16	162	162	149	149	162	162	149	149
Lynch3-16	1175	1175	915	915	922	922	721	721
Lynch4-16	14280	14280	9795	9795	8246	8246	5750	5750
Lynch5-16	210433	210433	107391	107391	95362	95362	49430	49430
bocdp	541	541	487	487	541	541	487	487
bocdpFIXED	542	542	488	488	542	542	488	488
bando	542	542	488	488	542	542	488	488
timelock	4	4	4	4	4	4	4	4
Milner-2Nodes-flat	442	442	432	432	245	245	133	133
Milner-3Nodes-flat	2709	2709	2671	2671	918	918	528	528
Milner-4Nodes-flat	4999	4999	4809	4809	2968	2968	1776	1776
Milner-5Nodes-flat	9106	9106	8856	8856	5293	5293	3146	3146
Milner-6Nodes-flat	17008	17008	16030	16030	7755	7755	5078	5078
Milner-7Nodes-flat	25493	25493	24347	24347	12188	12188	7668	7668
Milner-8Nodes-flat	39887	39887	37433	37433	16324	16324	11012	11012
hddi_input_1	221	221	217	217	119	119	136	136
hddi_input_2	2735	2735	2457	2457	693	693	710	710
hddi_input_3	20485	20485	18508	18508	2013	2013	2338	2338
hddi_input_4	TO	TO	TO	TO	4495	4495	5377	5377
hddi_input_5	TO	TO	TO	TO	13824	13824	10331	10331
hddi_input_6	TO	TO	TO	TO	14175	14175	18682	18682
hddi_input_7	TO	TO	TO	TO	TO	TO	TO	TO
hddi_input_8	TO	TO	TO	TO	TO	TO	TO	TO
hddi_input_9	TO	TO	TO	TO	TO	TO	TO	TO
hddi_input_10	TO	TO	TO	TO	TO	TO	TO	TO
ANIMO_small	235	235	237	237	235	235	237	237

Statestore	DDD	DDD	DDD	DDD	LDD	LDD	LDD	LDD
Search-order	no-minus	no-minus	no-minus	no-minus	bfs-prev	bfs-prev	bfs-prev	bfs-prev
Partitioned	+	-	+	-	+	-	+	-
Reorder	-	-	-	-	gsa	gsa	rb4w	rb4w
DBM-reduction	+	+	-	-	+	-	+	-
fischer1	14	14	14	14	13	13	14	14
fischer2	66	66	66	66	65	64	63	61
fischer3	288	288	250	250	505	502	433	413
fischer4	1300	1300	987	987	3905	3757	3190	2877
fischer5	5535	5535	3920	3920	30665	26533	26004	20436
fischer6	TO	22060	TO	15156	240846	177329	215066	140947
critRegion1	24	24	24	24	24	24	20	20
critRegion2	190	190	140	140	358	399	296	362
critRegion3	3825	3825	1701	1701	5798	11387	5506	11296
critRegion4	TO	TO	55890	146808	146808	451815	140144	459489
Critical_01-25-50	25	25	25	25	24	24	23	23
Critical_02-25-50	262	262	158	158	499	542	427	489
Critical_03-25-50	11183	11183	3375	3375	29517	34331	28443	34754
Critical_04-25-50	TO	TO	TO	TO	TO	TO	TO	TO
CSMACD_01	17	17	17	17	17	17	17	17
CSMACD_02	108	108	108	108	101	111	101	111
CSMACD_03	458	458	435	435	553	578	551	619
CSMACD_04	1356	1356	1357	1357	2528	2737	2520	2729
CSMACD_05	3478	3478	3790	3790	8819	9422	10127	10473
CSMACD_06	7925	7925	10099	10099	37022	36646	36938	36562
CSMACD_07	17069	17069	26381	26381	104287	119267	125019	119022
CSMACD_08	36098	36098	68197	68197	399577	325031	398899	367047
viking1	15	15	15	15	15	15	24	24
viking2	37	37	37	37	37	37	66	66
viking3	86	86	86	86	91	91	176	176
viking4	105	105	105	105	111	111	196	196
viking5	124	124	124	124	131	131	216	216
viking6	233	233	233	233	241	239	504	504
viking7	190	190	190	190	197	200	342	342
viking8	224	224	224	224	235	234	415	415
viking9	263	263	263	263	275	274	495	495
viking10	304	304	304	304	317	317	581	581
viking11	347	347	347	347	359	359	671	671
viking12	342	342	342	342	356	356	621	621
Lynch1-16	24	24	24	24	22	22	27	27
Lynch2-16	162	162	149	149	185	173	217	210
Lynch3-16	922	922	721	721	1757	1738	2600	2531
Lynch4-16	8246	8246	6131	6131	22033	23182	32144	31516
Lynch5-16	95782	95782	51698	51698	236029	265223	406904	400277
bocdp	541	541	487	487	355	379	435	434
bocdpFIXED	542	542	488	488	427	487	448	457
bando	542	542	488	488	425	491	448	457
timelock	4	4	4	4	4	4	4	4
Milner-2Nodes-flat	245	245	133	133	327	532	394	586
Milner-3Nodes-flat	918	918	528	528	1571	2591	1702	2732
Milner-4Nodes-flat	2968	2968	1776	1776	4789	14916	4997	15423
Milner-5Nodes-flat	5293	5293	3146	3146	8596	27351	8946	28078
Milner-6Nodes-flat	7755	7755	5078	5078	14026	45279	14551	46271
Milner-7Nodes-flat	12188	12188	7668	7668	21348	69708	22098	71000
Milner-8Nodes-flat	16324	16324	11012	11012	30883	101633	31874	103272
hddi_input_1	119	119	136	136	134	142	134	148
hddi_input_2	693	693	710	710	1025	999	1090	1051
hddi_input_3	2013	2013	2338	2338	3675	4815	3971	5033
hddi_input_4	4495	4495	5377	5377	11493	16680	12572	17468
hddi_input_5	13824	13824	10331	10331	19470	40262	21584	43436
hddi_input_6	14175	14175	18682	18682	57930	112878	64959	118653
hddi_input_7	TO	TO	TO	TO	122999	255603	122999	255603
hddi_input_8	TO	TO	TO	TO	218050	503802	218050	503802
hddi_input_9	TO	TO	TO	TO	307943	911847	307943	911847
hddi_input_10	TO	TO	TO	TO	508598	1621272	TO	TO
ANIMO_small	235	235	237	237	283	180	405	405

Statestore	LDD	LDD	LDD	LDD	LDD	LDD	LDD	LDD	LDD	LDD
Search-order	bfs-prev	bfs-prev	bfs-prev	bfs-prev	bfs-prev	bfs-prev	bfs-prev	bfs-prev	bfs-prev	bfs-prev
Partitioned	+	-	+	-	+	-	+	-	+	-
Reorder	cw	cw	rs,rn	rs,rn	rs,ru	rs,ru	-	-	-	-
DBM-reduction	+	-	+	-	+	-	+	-	+	-
fischer1	13	13	14	14	14	14	14	14	14	14
fischer2	66	66	66	66	66	66	66	66	66	66
fischer3	532	552	409	420	409	420	409	409	420	420
fischer4	4184	4112	2541	2486	2541	2486	2541	2541	2486	2486
fischer5	32446	27909	17131	14526	17131	14526	17131	17131	14526	14526
fischer6	247845	179025	121944	85041	121944	85041	121944	121944	85041	85041
critRegion1	26	26	24	24	24	24	24	24	24	24
critRegion2	242	321	243	326	243	326	243	243	326	326
critRegion3	4627	11234	3743	9385	3743	9385	3743	3743	9385	9385
critRegion4	116312	428689	100006	369121	100006	369121	100006	100006	369121	369121
Critical_01-25-50	29	29	25	25	25	25	25	25	25	25
Critical_02-25-50	370	404	316	345	316	345	316	316	345	345
Critical_03-25-50	20293	27533	17505	23083	17505	23083	17505	17505	23083	23083
Critical_04-25-50	TO	TO	TO	TO	TO	TO	TO	TO	TO	TO
CSMACD_01	17	17	17	17	17	17	17	17	17	17
CSMACD_02	101	111	99	109	99	109	99	99	109	109
CSMACD_03	551	619	500	558	500	558	500	500	558	558
CSMACD_04	2520	2729	2205	2401	2205	2401	2205	2205	2401	2401
CSMACD_05	10127	10473	8634	9158	8634	9158	8634	8634	9158	9158
CSMACD_06	36938	36562	30862	31948	30862	31948	30862	30862	31948	31948
CSMACD_07	125019	119022	102821	104048	102821	104048	102821	102821	104048	104048
CSMACD_08	398899	367047	324047	321001	324047	321001	324047	324047	321001	321001
viking1	24	24	15	15	15	15	15	15	15	15
viking2	66	66	37	37	37	37	37	37	37	37
viking3	176	176	86	86	86	86	86	86	86	86
viking4	196	196	105	105	105	105	105	105	105	105
viking5	216	216	124	124	124	124	124	124	124	124
viking6	504	504	233	233	233	233	233	233	233	233
viking7	342	342	190	190	190	190	190	190	190	190
viking8	415	415	224	224	224	224	224	224	224	224
viking9	495	495	263	263	263	263	263	263	263	263
viking10	581	581	304	304	304	304	304	304	304	304
viking11	671	671	347	347	347	347	347	347	347	347
viking12	621	621	342	342	342	342	342	342	342	342
Lynch1-16	21	21	24	24	24	24	24	24	24	24
Lynch2-16	187	185	173	180	173	180	173	173	180	180
Lynch3-16	1649	1924	1277	1485	1277	1485	1277	1277	1485	1485
Lynch4-16	17146	22181	11113	14968	11113	14968	11113	11113	14968	14968
Lynch5-16	177187	231890	112397	159146	112397	159146	112397	112397	159146	159146
bocdp	517	532	572	587	572	587	572	572	587	587
bocdpFIXED	514	529	572	587	572	587	572	572	587	587
bando	514	529	572	587	572	587	572	572	587	587
timelock	4	4	4	4	4	4	4	4	4	4
Milner-2Nodes-flat	338	543	338	543	338	543	338	338	543	543
Milner-3Nodes-flat	1602	2622	1602	2622	1602	2622	1602	1602	2622	2622
Milner-4Nodes-flat	4834	14965	4834	14965	4834	14965	4834	4834	14965	14965
Milner-5Nodes-flat	8653	27410	8653	27410	8653	27410	8653	8653	27410	27410
Milner-6Nodes-flat	14100	45357	14100	45357	14100	45357	14100	14100	45357	45357
Milner-7Nodes-flat	21455	69806	21455	69806	21455	69806	21455	21455	69806	69806
Milner-8Nodes-flat	31008	101767	31008	101767	31008	101767	31008	31008	101767	101767
hddi_input_1	134	142	130	138	130	138	130	130	138	138
hddi_input_2	1023	997	1021	995	1021	995	1021	1021	995	995
hddi_input_3	3675	4815	3675	4815	3675	4815	3675	3675	4815	4815
hddi_input_4	11499	16686	11501	16688	11501	16688	11501	11501	16688	16688
hddi_input_5	19473	40265	19477	40269	19477	40269	19477	19477	40269	40269
hddi_input_6	57960	112908	57966	112914	57966	112914	57966	57966	112914	112914
hddi_input_7	108366	243123	108374	243131	108374	243131	108374	108374	243131	243131
hddi_input_8	189156	479334	189166	479344	189166	479344	189166	189166	479344	479344
hddi_input_9	275980	802694	275992	802706	275992	802706	275992	275992	802706	802706
hddi_input_10	TO	TO	454246	1412675	454246	1412675	TO	454246	TO	1412675
ANIMO_small	185	187	197	199	197	199	197	235	199	237