EFFICIENT SYMBOLIC REPRESENTATIONS FOR ARITHMETIC CONSTRAINTS IN VERIFICATION*

CONSTANTINOS BARTZIS and TEVFİK BULTAN
Department of Computer Science, University of California, Santa Barbara CA 93106, USA

Received (received date)
Revised (revised date)
Communicated by Editor's name

ABSTRACT
In this paper we discuss efficient symbolic representations for infinite-state systems specified using linear arithmetic constraints. We give algorithms for constructing finite automata which represent integer sets that satisfy linear constraints. These automata can represent either signed or unsigned integers and have a lower number of states compared to other similar approaches. We present efficient storage techniques for the transition function of the automata and extend the construction algorithms to formulas on both boolean and integer variables. We also derive conditions which guarantee that the pre-condition computations used in symbolic verification algorithms do not cause an exponential increase in the automata size. We experimentally compare different symbolic representations by using them to verify non-trivial concurrent systems. Experimental results show that the symbolic representations based on our construction algorithms outperform the polyhedral representation used in Omega Library, and the automata representation used in LASH.

Keywords: automata, Presburger arithmetic, symbolic model checking

1. Introduction
Symbolic representations enable verification of systems with large state spaces which cannot be analyzed using enumerative approaches [1]. Recently, symbolic model checking has been applied to verification of infinite-state systems using symbolic representations that can encode infinite sets [2, 3, 4]. One class of infinite-state systems is systems that can be specified using linear arithmetic formulas on unbounded integer variables. Verification of such systems has many interesting applications such as monitor specifications [5], mutual exclusion protocols [3, 4], parameterized cache coherence protocols [6], and static analysis of access errors in dynamically allocated memory locations (buffer overflows) [7]. In this paper we present new symbolic representations for linear arithmetic formulas and experimental results on efficiency of different symbolic representations.

*This work is supported in part by NSF grant CCR-9970976 and NSF CAREER award CCR-9984822.
There are two basic approaches to symbolic representation of linear arithmetic constraints in verification: 1) Polyhedral representation: In this approach linear arithmetic formulas are represented in a disjunctive form where each disjunct corresponds to a convex polyhedron. Each polyhedron corresponds to a conjunction of linear constraints [8, 2, 4]. This approach can be extended to full Presburger arithmetic by including divisibility constraints (which can be represented as an equality constraint with an existentially quantified variable) [3, 9]. 2) Automata representation: An arithmetic constraint on $v$ integer variables can be represented by a $v$-track automaton that accepts a string if it corresponds to a $v$-dimensional integer vector (in binary representation) that satisfies the corresponding arithmetic constraint [10, 11, 12, 13]. For both of these symbolic representations one can implement algorithms for intersection, union, complement, existential quantifier elimination operations, and subsumption, emptiness and equivalence tests, and therefore use them in model checking.

In this paper we present construction algorithms for the automata representation of sets satisfying Presburger arithmetic formulas. We also experimentally compare two alternative automata representations and the polyhedra representation. Our construction algorithms are based on finite state transducers which compute linear functions (used in the arithmetic constraints that are being translated to FA) by processing the bits of the variables starting with the least significant bits. The input encoding is the same as the one used in [10] and the resulting FA are equivalent, however, our construction is also able to handle negative integers. Also we are able to prove tighter bounds on the sizes of the generated automata. The sizes of the generated automata and the input encoding in our construction are different than the construction given in [13]. We present automata construction for divisibility constraints which can be used as an alternative to projection operation required for Presburger formulas with quantification. We also show that the pre-condition computations required in symbolic verification algorithms do not cause an exponential increase in the automata representation if certain realistic conditions are satisfied.

We implemented our construction algorithm using the MONA tool [14] and integrated it to a set of tools for infinite-state model checking [15]. We experimented with a large set of examples. To compare the performance of our construction algorithm to other approaches we also integrated the LASH tool [16] which uses the automata construction given in [13], and Omega Library [17] which uses a polyhedral representation to the same set of tools and ran them on the same set of examples. Our experimental results show that our construction algorithm produces more compact representations than the construction algorithm given in [13]. Also automata representation is more efficient compared to the polyhedral representation used in [17].

The rest of the paper is organized as follows. In Sections 2 and 3 we give our automata construction algorithms for Presburger arithmetic formulas. In Section 4 we present an alternative encoding and discuss efficient storage techniques for the transition function of the FA and extend the construction algorithms to formulas on both boolean and integer variables. In Section 5 we summarize the complexity
results and discuss the related work. In Section 6 we derive conditions which guarantee that the pre-condition computations do not cause an exponential increase in the FA size. In Section 7 we discuss our implementation and experimental results. Finally, we state our conclusions in Section 8.

2. Finite Automata Representation for Linear Constraints on Natural Numbers

In this section we describe our algorithm for constructing a finite automaton that accepts the set of natural number tuples that satisfy a Presburger arithmetic formula on \( v \) variables. The same problem has been solved in [10]. Here we give a similar approach that enables us to prove a tighter bound on the size of the resulting automaton and can also be easily generalized to include negative integers as we will show in Section 3.

We encode numbers using their binary representation. A \( v \)-tuple of natural numbers \((n_1, n_2, ..., n_v)\) is encoded as a word over the alphabet \(\{0, 1\}^v\), where the \(i_{th}\) letter in the word is \((b_{i1}, b_{i2}, ..., b_{iv})\) and \(b_{ij}\) is the \(i_{th}\) least significant bit of number \(n_j\). Given a Presburger formula \(\phi\), we construct a finite automaton \(\text{FA}(\phi) = (K, \Sigma, \delta, e, F)\) that accepts the language \(L(\phi)\) over the alphabet \(\Sigma = \{0, 1\}^v\), which contains all the encodings of the natural number tuples that satisfy the formula. \(K\) is the set of automaton states, \(\Sigma\) is the input alphabet, \(\delta: K \times \Sigma \to K\) is the transition function, \(e \in K\) is the initial state, and \(F \subseteq K\) is the set of final or accepting states.

2.1. Addition of \( v \) variables \(\sum_{i=1}^{v} x_i\)

As a basis for all following construction algorithms we will use a state machine that performs linear arithmetic over natural numbers, which we will refer to as BSM (for basic state machine) from now on. Formally, the BSM is a Mealy machine or a finite state transducer \((K, \Sigma, \Lambda, \delta, e)\), where \(K\) is a set of states, \(\Sigma\) is the input alphabet, \(\Lambda\) is the output alphabet, \(e \in K\) is the initial state, and \(\delta: K \times \Sigma \to K \times \Lambda\) is the transition function from pairs of states and input symbols to pairs of states and output symbols.

When adding \( v \) variables, all the BSM has to remember is all the possible values for the carry, which in particular are all the integers between 0 and \( v - 1 \). Thus a BSM with \( v \) states is sufficient. At any point, the BSM adds up all the bits of the current letter plus the carry value of the current state, writes the resulting bit to the output, and moves to a new state according to the value of the new carry. The initial state is the one with carry value zero. Formally, \(K = \{0, 1, ..., v - 1\}\), \(\Sigma = \{0, 1\}^v\), \(\Lambda = \{0, 1\}\), \(e = 0\), and \(\delta(k, (b_1, ..., b_v)) = ((k + \sum_{i=1}^{v} b_i)/2, (k + \sum_{i=1}^{v} b_i) \mod 2)\), where \(a \mod b\) is the remainder of the division of \(a\) by \(b\).

2.2. Linear functions \(\sum_{i=1}^{v} a_i \cdot x_i\)

Now each variable is multiplied with a positive (negative) coefficient. The only change to the above addition process is that now the bit of the \(i_{th}\) variable is added
(subtracted) $|a_i|$ times. For the moment, we assume that there is no constant term. Obviously the number of possible values of the carry (and thus the number of states) is now equal to $\sum_{i=1}^{v} |a_i|$. This is true if the GCD of all the coefficients is 1. If this is not the case, we can divide all the coefficients with their GCD.

Formally, $\Sigma$, $\Lambda$ and $e$ are the same as before, $K = \{ k | \sum_{a_i<0} a_i \leq k \leq \sum_{a_i>0} a_i \}$ and $\delta(k, (b_1, ..., b_v)) = (\lfloor (k + \sum_{i=1}^{v} a_i \cdot b_i)/2 \rfloor, (k + \sum_{i=1}^{v} a_i \cdot b_i) \text{ mod } 2)$.

An example BSM for calculating $x + 2y$ is shown in Figure 1. The transitions are labeled with the current bits of $x$ and $y$ and also the bit written to the output.

2.3. Checking for equality with zero $\sum_{i=1}^{v} a_i \cdot x_i = 0$

From now on we describe Finite Automata (FA) based on the BSM. This means that we now characterize the states as accepting and rejecting and there is no output. This FA operates similarly to the BSM, except that after computing every bit, instead of printing it to the output, it compares it against zero. While the comparison is successful (the resulting bit is indeed zero), the FA continues its normal operation. Otherwise it jumps to an extra sink state. The size of this FA is at most one more than the size of the BSM. The accepting state is the initial state (carry is zero) and all the others are rejecting. If we are checking for non-equality, all we need to do is make the accepting states non-accepting and vice-versa. Formally, $\text{FA}(\sum_{i=1}^{v} a_i \cdot x_i = 0) = (K, \Sigma, \delta, e, F)$, where $K = \{ k | \sum_{a_i<0} a_i \leq k \leq \sum_{a_i>0} a_i \} \cup \{ \text{sink} \}$, $\Sigma = \{0,1\}^v$, $e = 0$, $F = \{0\}$, and the transition function $\delta$ is defined as:

$$\delta(k, (b_1, ..., b_v)) = \begin{cases} 
(k + \sum_{i=1}^{v} a_i \cdot b_i)/2 & \text{if } k + \sum_{i=1}^{v} a_i \cdot b_i \text{ is even and } k \neq \text{sink} \\
\text{sink} & \text{otherwise}
\end{cases}$$

2.4. Checking inequalities

The situation now is simpler. If we are checking for $< 0$, the FA is identical to the BSM, except that it does not produce any output. The accepting states are all the states representing negative carries. All the other states are rejecting. If we are checking for $\geq 0$, we take the complement of the above described FA, by making
the accepting states rejecting and vice versa. For the rest of the cases \((> 0, \leq 0)\), we change the signs of all coefficients and then we construct the FA like before. Formally, \(FA(\sum_{i=1}^{n} a_i \cdot x_i < 0) = (K, \Sigma, \delta, e, F)\), where \(K = \{k \mid \sum_{a_i > 0} a_i \leq k \leq \sum_{a_i < 0} a_i\}\) is the set of states, \(\Sigma = \{0, 1\}^v\) is the alphabet, \(e = 0\) is the initial state, \(F = \{k \mid k \in K \land k < 0\}\) is the set of accepting states, and the transition function is \(\delta(k, (b_1, \ldots, b_n)) = (k + \sum_{i=1}^{n} a_i \cdot b_i)/2\).

2.5. Constant term

So far we assumed no constant term in the equations and inequations or, in other words, the constant term was zero. Now suppose that the linear combination of the variables is compared against a non-zero integer constant term \(c\), i.e. we are constructing a FA for a constraint of the form \(\sum_{i=1}^{n} a_i \cdot x_i \sim c\), where \(-c \in \{=, \neq, >, \geq, \leq, <\}\). All we have to do is make the state corresponding to a carry value of \(-c\) the initial state of the FA \((e = -c)\), that is, we begin with a carry of \(-c\) and by gradually adding the linear combination of the variables, we compare the result against zero, as we did before. If no such state exists, we introduce one. Of
course we need to introduce more states corresponding to values between $-c$ and the carry value closest to $-c$. Specifically, for inequalities, the set of states becomes

$$K = \{ k \mid \sum_{a_i < 0} a_i \leq k \leq \sum_{a_i > 0} a_i \lor 0 \leq k \leq -c \lor -c \leq k \leq 0 \}.$$ 

Thus the number of states now becomes $|K| = S = \min(-c, \sum_{a_i < 0} a_i) + \max(-c, \sum_{a_i > 0} a_i)$. For equalities, there is one extra sink state. Note that this upper bound on the number of states is tighter than the one given in [10], even though the construction algorithms are similar. The algorithms for constructing FA from equations and inequations are given in Figures 2 and 3, respectively.

There is an alternative way to cope with the constant term. If $l = \log_2 c$ is the length of the binary representation of the constant $c$, we can stack $l + 1$ BSMs in $l + 1$ layers. For equations, any transition from layer $1 \leq i \leq l$, whose output is the same as the $i_{th}$ bit of $c$ goes to the appropriate state of layer $i + 1$, if the output is different, it goes to the sink state. Initial state is the initial state of the first BSM. Accepting states are the accepting states of the final BSM. For inequations ($< c$), all transitions from any layer except the last go to the appropriate state of the next layer and accepting states are those representing a negative carry. The total number of states is at most $(l + 1) \cdot \sum_{i=1}^n |a_i|$, i.e. $|K| \leq (\log_2 c + 1) \cdot \sum_{i=1}^n |a_i|$. Note that the two approaches described will result in the same automaton, when minimized. We can choose which one to use depending on the expected upper bound on the number of states.

2.6. Presburger formulas

Presburger formulas contain Boolean connectives between atomic linear constraints (equations and inequations) and quantifiers. Given two linear constraints $\phi_1$ and $\phi_2$ and the automata $\text{FA}(\phi_1)$ and $\text{FA}(\phi_2)$ representing them (with sizes $|\text{FA}(\phi_1)|$ and $|\text{FA}(\phi_2)|$ respectively), we can easily construct a new FA that accepts the Boolean AND (OR) between them by computing the intersection (union) of the two FA. It is known that such a FA contains at most $|\text{FA}(\phi_1)| \cdot |\text{FA}(\phi_2)|$ states. Similarly we can deal with NOT, by FA complementation. Given a formula $\phi$ containing $l$ atomic linear constraints of the form $\phi_j : \sum_{i=1}^n a_{i,j} \cdot x_i \sim c_j, 1 \leq j \leq l$, where $\sim \in \{=, \neq, >, \geq, \leq, <\}$, and Boolean connectives, one would expect the size of $\text{FA}(\phi)$ to be $\prod_{j=1}^l |\text{FA}(\phi_j)|$. Fortunately, $|\text{FA}(\phi)|$ can be much less. Suppose $\phi$ contains $m$ atomic linear constraints $\psi_1, ..., \psi_m$ with distinct coefficients and $\text{FA}(\psi_j) = (K_j, \Sigma, \delta_j, c_j, F_j)$ is defined as described earlier. Now $\text{FA}(\phi) = (K, \Sigma, \delta, c, F)$ can be constructed as follows. Each state of $\text{FA}(\phi)$ will correspond to a carry value for each of the distinct constraints (or sink for equalities). Transitions are defined in a similar way to those for single constraints. Finally, any state can be characterized as accepting iff $\phi$ evaluates to true according to the carries stored in that state. Formally, $\Sigma = \{0, 1\}^v$, $K = \prod_{j=1}^m K_j$, $\delta((k_1, ..., k_m), \sigma) = (\delta(k_1, \sigma), ..., \delta(k_m, \sigma))$, where $\delta = (e_1, e_2, ..., e_m)$. Clearly the size of $\text{FA}(\phi)$ is $O(|\prod_{j=1}^m \sum_{i=0}^v |a_{i,j}| \cdot \prod_{i=1}^v |d_{i,j}|)$. Hence, the size of the $\text{FA}(\phi)$ depends on the number of distinct atomic constraints in $\phi$, i.e., repetition of an atomic constraint does not increase the size of the $\text{FA}(\phi)$.

If some variable is existentially quantified, we can compute a non-deterministic
FA accepting the projection of the initial FA on the remaining variables and then
determinize it. The size of the resulting deterministic FA can be exponential on the
size of the initial FA, i.e. \( |FA(\exists x_i, \phi)| = 2^{|FA(\phi)|} \) in the worst case. The resulting FA
may not accept all satisfying encodings (with any number of leading zeros). We can
overcome this by identifying all rejecting states \( k \) such that \( \delta(k, (0, 0, ..., 0)) \in F \),
and make them accepting. Clearly, this modification does not increase the size of
the FA. Universal quantification can be similarly implemented by the use of the FA
complementation.

It is known that any Presburger formula can be expressed in a disjunctive form,
where each disjunct is a conjunction of equality, inequality and divisibility con-
straints [18]. Divisibility constraints are of the form \( \sum_{i=1}^{n} a_i x_i + c \equiv_d 0 \), where \( d \) is
a positive integer constant, and \( \equiv_d \) means equivalent modulo \( d \). Given a Presburger
arithmetic formula in the form \( \exists x_i, \phi \) where \( \phi \) is a conjunction of atomic equality
and inequality constraints, one can construct a formula \( \phi' \) which is equivalent to
\( \exists x_i, \phi \) and \( \phi' \) consists of atomic equality, inequality, and divisibility constraints and
\( x_i \) does not appear in \( \phi' \) [18]. Hence, if we can construct FA for arithmetic formulas
with divisibility constraints we would have an alternative approach to constructing
FA for quantified formulas. Having shown how to construct FA for equations and
inequations, here we describe the construction of FA for divisibility constraints.

First we describe a FA \((K, \Sigma, \delta, \epsilon, F)\) that accepts an integer if it is divisible by \( d \),
by reading its bits in most-significant to least-significant bit order, i.e. \( \Sigma = \{0, 1\} \).
There are \( d \) states, each representing the remainder of the division of the input with
\( d \), i.e., \( K = \{0, 1, ..., d-1\} \). State 0 is the entry state and also the only accepting
state. Finally, \( \delta(k, 0) = (2 \cdot k) \mod d \) and \( \delta(k, 1) = (2 \cdot k + 1) \mod d \). In order
to make this FA “compatible” with those for equations and inequations described
earlier, we need to reverse the bit order. That is easy when \( d \) is odd. We just reverse
all the transitions. One can easily verify that the resulting FA is deterministic. This
is because in the initial FA the entry state is the same with the unique accepting
state and also there are no same-labeled transitions originating in distinct states
and going to the same state. If \( d \) is even, then it can be written as \( 2^n \cdot m \) where
\( m \) is odd and \( n > 0 \). We can build a FA for divisibility with \( m \) as described above
and add \( n + 1 \) states to check if the first \( n \) least significant bits of the input are
zero. The resulting FA will have at most \( d \) states. Now we can define \( FA(\sum_{i=1}^{n} a_i x_i + c \equiv_d 0) = (K, \Sigma, \delta, \epsilon, F) \), based on
\( FA(y \equiv_d 0) = (K_{d_{\forall}}, \{0, 1\}, \delta_{d_{\forall}}, 0, \{0\}) \) and
\( BSM(\sum_{i=1}^{n} a_i x_i + c) = (K_{BSM}, \Sigma_{BSM}, \delta_{BSM}, \epsilon_{BSM}) \). In particular, \( K = K_{BSM} \times K_{d_{\forall}}, \Sigma = \Sigma_{BSM}, \epsilon = (e_{BSM}, 0), F = F_{BSM} \times \{0\} \) and finally \( \delta((k_1, k_2), (k_1, b) \land \delta_{d_{\forall}}(k_2, b) = k_2' \). The size of this FA is \( S \cdot d \), where
\( S \) was defined in Section 2.5.

3. Finite Automata for Linear Constraints on Integers

So far we have described the construction of automata for linear constraints on
natural variables. Here we show how to build finite automata which accept linear
constraints on all integers, including negative, using 2's complement arithmetic.
These new FA are only twice as large as the former ones. The construction, again,
Input equation: \( \sum_{i=1}^{v} a_i \cdot x_i = c \)  Output FA: \((\Sigma, K, \delta, e, F)\)

\[\Sigma := \{0, 1\}^v \]
\[K := \{(-c, a), (-c, r), \text{sink}\} \]
\[e := (-c, a)\]

FOR ALL \(\sigma \in \Sigma\) \(\delta(\text{sink}, \sigma) := \text{sink}\) 

WHILE \(\exists (k, a) \in K, \sigma \in \Sigma\) s.t. \(\delta((k, a), \sigma) = \text{null}\) DO 

FOR ALL \(\sigma = (b_1, ..., b_i) \in \Sigma\) DO 

IF \(k' := (\sum_{i=1}^{v} a_i \cdot b_i + k)/2 \in \mathbb{Z}\) THEN 

IF \(k' = k\) THEN 

\(\delta((k, a), \sigma) := (k, a)\) 

ELSE 

\(K := K \cup \{(k', a), (k', r)\}\) 

\(\delta((k, a), \sigma) := (k', r)\) 

ELSE 

\(\delta((k, a), \sigma) := \text{sink}\) 

\(\delta((k, r), \sigma) := \delta((k, a), \sigma)\) 

\(F := \emptyset\) 

FOR ALL \((k, a) \in K\) DO 

\(F := F \cup \{(k, a)\}\)

the FA Algorithm for equations on integers

is based on the basic state machine which calculates linear formulas. As an example we use the constraint \(x + 2y = 0\), the BSM of which is shown in Figure 1. Again we describe automata for constraints with no constant terms. The addition of such terms is done in exactly the same way as in the previous section.

3.1. Finite automata for equality with zero

The procedure is based on the fact that in order for the FA to accept the encoding of a tuple of numbers, it must also accept the encoding of the same numbers with arbitrarily many sign bits (i.e. the most significant bit of each number repeated arbitrarily many times). This means that the according BSM must write only 0s when reading such an arbitrarily long word. The only way for the BSM to continue writing 0s by repeatedly receiving the same combination of bits is by following a looping transition. The FA contains two loops \((k, a)\) and \((k, r)\) of each state.
Input inequation: $\sum_{i=1}^{v} a_i \cdot x_i < c$  
Output FA: $(\Sigma, K, \delta, e, F)$

\[
\begin{align*}
\Sigma & := \{0, 1\}^{v} \\
K & := \{(-c, a), (-c, r)\} \\
e & := (-c, a) \\
\text{WHILE } \exists (k, a) \in K, \sigma \in \Sigma \text{ s.t. } \delta((k, a), \sigma) = \text{null DO} \\
& \quad \text{FOR ALL } \sigma = (b_1, ..., b_k) \in \Sigma \text{ DO} \\
& \quad \quad k' := \lfloor \sum_{i=1}^{v} a_i \cdot b_i + k \rfloor/2 \\
& \quad \quad \text{temp1} := k \\
& \quad \quad \text{temp2} := k' \\
& \quad \quad \text{WHILE temp1} \neq \text{temp2 DO} \\
& \quad \quad \quad \text{temp1} := \text{temp2} \\
& \quad \quad \quad \text{temp2} := \lfloor \sum_{i=1}^{v} a_i \cdot b_i + \text{temp1} \rfloor/2 \\
& \quad \quad \quad \text{IF } \lfloor \sum_{i=1}^{v} a_i \cdot b_i + \text{temp1} \rfloor/2 \in \mathbb{Z} \text{ THEN} \\
& \quad \quad \quad \quad \delta((k, a), \sigma) := \langle k', r \rangle \\
& \quad \quad \quad \text{ELSE} \\
& \quad \quad \quad \quad \delta((k, a), \sigma) := \langle k', a \rangle \\
& \quad \quad \quad \delta((k, r), \sigma) := \delta((k, a), \sigma) \\
F & := \emptyset \\
\text{FOR ALL } \langle k, a \rangle \in K \text{ DO} \\
F & := F \cup \{\langle k, a \rangle\}
\end{align*}
\]

Fig. 6. FA Algorithm for inequalities on integers

$k$ of the BSM, one accepting and one rejecting respectively. It also contains a rejecting sink state. Looping transitions in the BSM that write 0 go to the according accepting clone. All other transitions that write 0 go to the rejecting clone. All transitions that write 1 in the BSM go to the sink state. Formally, one can define the FA$(\sum_{i=1}^{v} a_i \cdot x_i = 0) = (K_{FA}, \Sigma, \delta_{FA}, e_{FA}, F)$ based on the BSM$(\sum_{i=1}^{v} a_i \cdot x_i)$=(K_{BSM}, \Sigma, \Lambda, \delta_{BSM}, e_{BSM}). In particular, $K_{FA} = \{(k, a), (k, r) | k \in K_{BSM}\} \cup \{\text{sink}\}, e_{FA} = (e_{BSM}, a), F = \{(k, a) | k \in K_{BSM}\}$ and

\[
\delta_{FA}((k, a), \sigma) = \delta_{FA}((k, r), \sigma) = \begin{cases} 
(k, a) & \text{iff } \delta_{BSM}(k, \sigma) = (k, 0) \\
(k', r) & \text{iff } \delta_{BSM}(k, \sigma) = (k', 0) \land k' \neq k \\
\text{sink} & \text{iff } \delta_{BSM}(k, \sigma) = (k', 1)
\end{cases}
\]

Obviously such an automaton has twice as many states and transitions as the BSM, thus its size is at most $2S + 1$, where $S$ was defined in Section 2.5. One can easily verify that this is the minimum possible. The algorithm for constructing FA for equations on integers is shown in Figure 4. The example automaton for $x + 2y = 0$ is shown in Figure 5. The sink state and all transitions to it have been omitted.

3.2. Finite automata for inequalities

Like before we will only describe the $< 0$ case. All other types of inequalities can be effectively derived from it. Now we want the result of the addition to be negative, thus having an 1 as a sign bit. Unfortunately, the bit most recently written by the BSM is not always the sign bit of the result, due to possible overflow. Thus, a tuple of integers renders a negative result iff by repeating their most significant bits an adequate number of times, the BSM will eventually enter a looping transition that
writes 1. Any number of repetitions greater or equal to the binary logarithm of
the sum of the absolute values of the coefficients is adequate. That is how many
extra bits of the result one would need to compute in order to avoid an overflow.
Again we create one accepting and one rejecting clone of each state of the BSM and
there is no sink state. Looping transitions that write 1 go to the accepting clone
and those which write 0 go to the rejecting clone. Any other transition goes to
the appropriate accepting clone, iff by repeatedly receiving the same combination
of bits the BSM will eventually enter a loop which writes 1. Otherwise it goes to
the rejecting clone. This condition is checked in the second WHILE loop in Figure
6. As explained earlier the loop will finish in at most $\log_2(\sum_{i=1}^{n} |a_i|)$ steps. Again,
one can formally define the $\text{FA}(\sum_{i=1}^{n} a_i \cdot x_i < 0)$ based on the $\text{BSM}(\sum_{i=1}^{n} a_i \cdot x_i)$.
Obviously this FA has $2S$ states. The algorithm for constructing FA for inequalities
on integers is shown in Figure 6. The example automaton for $x + 2y < 0$ is shown
in Figure 7.

Note that for both equations and inequations, the automata resulting from our
construction are deterministic, unlike those described in [13] which require (linear
time) determinization. Secondly, once a state has been created, all transitions
originating from it can be computed immediately (as opposed to [13]), which is
more convenient when transitions are stored using BDDs. Moreover, even though
we can prove an upper bound on the number of states different (and in many cases
better) than the one given in [13], if we follow the BSM stacking method for dealing
with the constant term, described in Section 2.5 we can achieve the same bound of
$O(\log_2 c \cdot \sum_{i=1}^{n} |a_i|)$. Finally, our construction and the one in [13] result in different
automata, because the accepted languages are different (one is the reverse of the
other).

4. Practical issues and extensions

In all FA construction algorithms given so far, $\nu$-tuples of integers have been
encoded as words over the alphabet $\{0,1\}^\nu$. While this encoding is convenient for
describing the algorithms and proving their complexity, it is inefficient in practice.
The reason is that the size of the transition function is proportional to the size of the alphabet. Thus, an alphabet with size exponential in the number of variables \( v \) is problematic. In this section we discuss two ways of dealing with this problem: 1) changing the encoding and 2) storing the transition function more efficiently. Finally, we use these ideas to construct FA for combined Presburger and Boolean formulas.

4.1. Alternative FA

Here we will describe an alternative FA construction. Alternative FA accepts the same values for the variables as before, but the encoding is different. There is only one track containing the bits of all the variables interleaved. Particularly, a \( v \)-tuple of natural numbers \((n_1, n_2, \ldots, n_v)\) is encoded as a word over the alphabet \(\{0, 1\}\), where the \(i_{th}\) least significant bit of number \(n_j\) appears in position \((i - 1) \cdot v + j\) of the word.

The construction procedure is similar but now we have to keep all the intermediate results of the addition of the \(i_{th}\) bit of the variables, thus we need the appropriate states to represent these results and to tell which variable’s bit is coming next. States will be labeled with a variable’s name and a value for an intermediate result. For the first variable there are as many states as the different possible values of the carry which are at most \(2S\). For the next variable there are at most \(|a_1|\) more states and so on. The total number of states in the automaton is \(2vS + \sum_{i=1}^{v} (v - i)|a_i|\) which is less than \(3vS\). Interestingly this leads us to the conclusion that the size of the automaton is minimized if the variables are ordered in increasing order of the absolute values of their coefficients.

4.2. Storing the transition function \(\delta\)

A problem with the FA representation for arithmetic constraints is the size of the transition function, since the number of transitions from each state is exponential on \(v\), the number of integer variables. Hence, it is impractical to store the transition function as a table. Actual implementations use different solutions to this problem. LASH [16] follows a technique similar to the Alternative FA described earlier. The input is serialized by interleaving the bits of each integer variable in some fixed order. This way there are (linearly) more states but only two transitions from each state. The weakness of this approach is that the number of states in the FA is proportional to the total number of variables and not only those with non-zero coefficients. On the other hand, MONA is an automata package [14] that uses BDDs [19] to store the transition function. In particular, for each FA state \(n\), there is a BDD representing the function \(\delta(n, (b_1, \ldots, b_v))\). The terminal nodes are also FA states and internal nodes can be shared. Since BDDs are a canonical representation for Boolean functions, given a fixed variable ordering, the size of the transition relation can be kept minimal, e.g., variables with zero coefficients do not appear in the BDD representing the transition function. Note that this BDD is isomorphic to the transition graph of the Alternative FA of the previous paragraph, thus its size
is linear on the number of integer variables $v$.

4.3. Adding Boolean formulas

Clearly, a Boolean formula $\phi$ with $n$ boolean variables can be represented by a FA that accepts the valuations of the Boolean variables that satisfy the formula. Using the alphabet $\{0, 1\}$, any word encoding a satisfying valuation has a fixed length $n$, hence the according language $L(\phi)$ is regular. Now suppose that $\phi$ is a general formula containing both Boolean subformulas ($B_1, ..., B_m$) and Presburger subformulas ($P_1, ..., P_n$) combined with Boolean connectives ($\land, \lor, \neg$, etc). Obviously one can construct a FA for $\phi$, with size $\prod_{i=1}^{m} |FA(B_i)| \cdot \prod_{i=1}^{n} |FA(P_i)|$. Fortunately, one can take advantage of the BDD representation for the transition function described in the previous paragraph to reduce the size of the FA for general formulas. The idea is to put the Boolean variables first in the total variable ordering. This way, the Boolean variables appear only in the first BDD representing the transition function from the initial state of $FA(\phi)$. If one can find a good variable ordering for the Boolean variables, this BDD can be kept small. In the worst case the size of this BDD is at most $\prod_{i=1}^{m} |FA(B_i)|$. The rest of the BDDs that represent the transitions in the FA($P_i$) for $1 \leq i \leq m$ are independent of the Boolean variables and thus their total size is at most $\prod_{i=1}^{n} |FA(P_i)|$. Finally the total size of the BDD representing the transition function of $FA(\phi)$ is $\prod_{i=1}^{m} |FA(B_i)| + \prod_{i=1}^{n} |FA(P_i)|$.

5. Complexity Outline

The following table summarizes the time complexity of the construction algorithms for linear integer arithmetic constraints, as well as the sizes of the resulting structures. The entries of the tables are worst-case asymptotic estimations. The size of a FA is the number of its states. Like before, $v$ denotes the number of integer variables, $a_i$ are the coefficients, $c$ is the constant term and $S = \min(-c, \sum_{a_i < 0} a_i) + \max(-c, \sum_{a_i > 0} a_i)$.

<table>
<thead>
<tr>
<th></th>
<th>FA for non-negative integers</th>
<th>FA for all integers</th>
<th>LASH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Construction Time</td>
<td>$2^v S$</td>
<td>$2^{v+1} S \log_2 S$</td>
<td>$2^{v+1} \log(</td>
</tr>
<tr>
<td>Construction Size</td>
<td>$S$</td>
<td>$2S$</td>
<td>$2\log(</td>
</tr>
</tbody>
</table>

The reader can find similarities between our FA construction algorithms and those proposed in [10] and [13]. Here we briefly explain the advantages of our approach. In [10] only constraints over non-negative integers are considered. We describe FA for constraints over all integers as well, by only doubling the complexity.

On the other hand, in [13] the complexity of $O(2 \cdot \log_2 |c| \cdot \sum_{i=1}^{v} |a_i|)$, where $c$ is the constant term and $|a_i|$ are the absolute values of the coefficients, is worse than ours for most practical cases. Note that by slightly modifying our construction we can also achieve that complexity, whenever needed. Moreover in [13] no algorithm
is given for constraints on non-negative integers. There are cases where all variables range over the non-negative integers, and adding extra constraints to denote that, would be wasteful. Also, in Section 4.1 we give a detailed complexity analysis for an alternative automaton that is equivalent to the “sequentialized” FA described in [13].

Finally, our transducer-based FA can be composed with FA for constraints beyond Presburger arithmetic, such as “$x$ is a power of two”.

6. Pre-condition computations

One of the fundamental operations in symbolic verification algorithms is computing the pre-condition of a set of states (configurations) of a system. One interesting issue is investigating the sizes of the FA that would be generated by the pre-condition operation if one uses the FA encoding described in the previous sections as a symbolic representation.

Given a set of states $S \subseteq \mathbb{Z}^n$ of a system as a relation on the state variables $x_1,\ldots,x_n$ and the transition relation $R \subseteq \mathbb{Z}^{2n}$ of the system as a relation on the current state and next state variables $x_1,\ldots,x_n,x'_1,\ldots,x'_n$, we would like to compute the pre-condition of $S$ with respect to $R$, $\text{pre}(S,R) \subseteq \mathbb{Z}^n$. We consider systems where $S$ and $R$ can be represented as Presburger arithmetic formulas, i.e., $S = \{(x_1,\ldots,x_n) \mid \phi_S(x_1,\ldots,x_n)\}$ and $R = \{(x_1,\ldots,x_n,x'_1,\ldots,x'_n) \mid \phi_R(x_1,\ldots,x_n,x'_1,\ldots,x'_n)\}$, where $\phi_S$ and $\phi_R$ are Presburger arithmetic formulas. For example, consider a system with three integer variables $x_1, x_2$ and $x_3$. Let the current set of states be $S = \{(x_1,x_2,x_3) \mid x_1 + x_2 = x_3\}$ and the transition relation be $R = \{(x_1,x_2,x_3,x'_1,x'_2,x'_3) \mid x_1 > 0 \land x'_1 = x_1 - 1 \land x'_2 = x_2 \land x'_3 = x_3\}$. Then the pre-condition of $S$ with respect to $R$ is $\text{pre}(S,R) = \{(x_1,x_2,x_3) \mid x_1 > 0 \land x_1 + x_2 = x_3 + 1\}$.

One can compute $\text{pre}(S,R)$ by first renaming the variables in $\phi_S$, then conjoint it with $\phi_R$, and then existentially eliminating the next state variables, i.e., $\phi_{\text{pre}(S,R)}$ is equivalent to $\exists x'_1\ldots\exists x'_n.(\phi_S|x'_1\leftarrow x_1,\ldots,x'_n\leftarrow x_n \land \phi_R)$ where $\psi_{|y-z|}$ is the formula generated by substituting $z$ for $y$ in $\psi$. Hence, to compute $\text{pre}(S,R)$ we need three operations: conjunction, existential variable elimination and renaming. As stated in Section 2.6, given FA($\phi$) representing the set of solutions of $\phi$, FA($\exists x_1,\ldots,\exists x_n,\phi$) can be computed using projection, and the size of the resulting FA is at most $O(2^{\text{FA($\phi$)}})$. Note that, existential quantification of more than one variable does not increase the worst case complexity since the determinization can be done once at the end, after all the projections are done. As discussed earlier, conjunction operation can be computed by generating the product automaton, and the renaming operation can be implemented as a linear time transformation of the transition function. Hence, given formulas $\phi_S$ and $\phi_R$ representing $S$ and $R$, and corresponding FA, FA($\phi_S$) and FA($\phi_R$), the size of the automaton FA($\phi_{\text{pre}(S,R)}$) is $O(2^{\text{FA($\phi_S$)}}\cdot\text{FA($\phi_R$)})$ in the worst case. Below, we show that under some realistic assumptions, the size of the automaton resulting from the pre-condition computation can be much better.

We assume that the formula $\phi_R$ defining the transition relation $R$ is a guarded-update of the form $\text{guard}(R) \land \text{update}(R)$, where $\text{guard}(R)$ is a Presburger formula
on current state variables \(x_1, \ldots, x_v\) and update\((R)\) is of the form \(x_i' = f(x_1, \ldots, x_v) \land \bigwedge_{j \neq i} x_j' = x_j\) for some \(1 \leq i \leq v\), where \(f : Z^v \to Z\) is a linear function. This is a realistic assumption, since in asynchronous concurrent systems, the transition relation is usually defined as a disjunction of such guarded-updates. This holds for all the concurrent systems we experimented with in Section 7. Also, note that, the pre-condition of a transition relation which is a disjunction of guarded-updates is the union of the pre-conditions of individual guarded-updates, and can be computed by computing pre-condition of one guarded-update at a time.

First, we consider two kinds of updates: \(x_i' = c\) and \(x_i' = x_i + c\), where \(c\) is an integer constant. Given \(\phi_S\) and \(\phi_R\), the formulas defining \(S\) and \(R\), respectively, we can show that for these two cases the size of \(FA(\phi_{\text{pre}(S,R)})\) can be less than or equal to the size of the \(FA(\phi_S \land \text{guard}(R))\) in certain cases, and in the worst case it is exponential in the number of distinct atomic constraints in \(\phi_S\), which is a significant improvement over the upper bound of \(O(2^{FA(\phi_S) + |FA(\phi_R)|})\) given above.

Suppose \(\phi_S\) consists of \(l\) atomic linear constraints of the form \(\phi_j : \sum_{i=1}^{v} a_{i,j} \cdot x_i \sim c_j, 1 \leq j \leq l\), where \(-c \in \{\leq, \neq, >, \geq, \leq, <\}\), and Boolean connectives. If \(x_k\) is updated by \(x_k' = c\), then \(\phi_{\text{pre}(S,R)}\) is equivalent to \(\phi_S[x_k \leftarrow c] \land \text{guard}(R)\). The \(FA(\phi_j)\) can be constructed by the BSM stacking method described in Section 2.5 where the resulting FA will have \(\log_2 c_j\) layers. The \(FA(\phi_j[x_k \leftarrow c])\) can be constructed based on the BSM stacking method for \(FA(\phi_j)\). The alphabet of \(FA(\phi_j)\) includes a bit for variable \(x_k\) whereas the alphabet of \(FA(\phi_j[x_k \leftarrow c])\) does not. Each layer in \(FA(\phi_j[x_k \leftarrow c])\) has the same states as in \(FA(\phi_j)\). Each transition in \(FA(\phi_j[x_k \leftarrow c])\) corresponds to a transition in \(FA(\phi_j)\) where the bit of \(x_k\) for that layer is equal to the corresponding bit of \(c\). The number of layers now becomes \(\max(\log_2 c_j, \log_2 |c|) + 1\). If \(|c| \leq |c_j|\), then \(|FA(\phi_j[x_k \leftarrow c])| = |FA(\phi_j)|\). If this holds for all \(j\), the size of the \(FA(\phi_{\text{pre}(S,R)})\) is equal to the size of the \(FA(\phi_S \land \text{guard}(R))\). Otherwise, it may increase exponentially on the number of \(|c_j|\)s that are less than \(|c|\).

If \(x_k\) is updated by \(x_k' = x_k + c\), then \(\phi_{\text{pre}(S,R)}\) can be derived from \(\phi_S\) by replacing each atomic constraint \(\sum_{i=1}^{v} a_{i,j} \cdot x_i \sim c_j\) with \(\sum_{i=1}^{v} a_{i,j} \cdot x_i \sim c_j - a_{k,j} \cdot c\) and then conjuncting the result with \(\text{guard}(R)\). The \(FA\) for both of these constraints can be constructed by the algorithms described in Section 2. If \(\min_{a_{i,j} < 0} (\sum_{a_i > 0} a_i) \leq -c_j - a_{k,j} \cdot c\), then \(FA(\sum_{a_i > 0} a_i \cdot x_i \sim c_j - a_{k,j} \cdot c)\) is less than or equal to the \(FA(\phi_{\text{pre}(S,R)})\). Again, if this condition holds for all \(j\), the size of the \(FA(\phi_{\text{pre}(S,R)})\) is less than or equal to the size of the \(FA(\phi_S \land \text{guard}(R))\). Otherwise, it may increase exponentially on the number of atomic constraints, for which the condition is violated.

In the most general case, an update can be in the form \(x_i' = \sum_{j=1}^{v} a_j \cdot x_j + c\). Even for such updates the number of atomic constraints in \(\phi_{\text{pre}(S,R)}\) will be at most the number of atomic constraints in \(\phi_S\) plus the number of atomic constraints in \(\text{guard}(R)\). An update in the above form may change all the coefficients on all atomic constraints \(\phi_j\) in \(\phi_S\). However, the size of the \(FA(\phi_{\text{pre}(S,R)})\) will not be more than the size of the \(FA(\phi_S \land \text{guard}(R))\) if the constant term and the sum of the absolute values of the coefficients in each individual atomic constraint \(\phi_j\) do not increase.
7. Implementation and Experiments

In this section we discuss the implementation of the presented algorithms and experimentally compare two alternative automata representations and the polyhedral representation for arithmetic constraints. Earlier results from our experiments were reported in [20].

In [21] polyhedral and automata representation for arithmetic constraints are compared experimentally for reachability analysis of several concurrent systems. The results show no clear winner. On some problem instances the polyhedral representation is superior, on some others automata representation is. Our experimental setup is more reliable compared to [21]. In [21] Boolean variables are mapped to integer variables when polyhedral representation is used. This is an inefficient encoding which gives an unfair advantage to the automata representation. In our experiments Boolean variables are not mapped to integers in any representation. Also, our tools perform full CTL model checking including liveness properties instead of just reachability analysis discussed in [21].

7.1. Implementation

Before we explain our implementation and experiments we would like to explain the tools we used. Omega Library is a symbolic manipulator for Presburger arithmetic formulas [17]. Omega Library uses a disjunctive normal form to represent Presburger arithmetic formulas where each disjunct corresponds to a conjunction of a set of equality, inequality or divisibility constraints.

MONA is an automata manipulation tool which also implements decision procedures for the Weak Second-order Theory of One or Two successors [22]. We used MONA’s automata package to implement our construction procedures and symbolic operations. We chose this specific package because its internal representation of state transitions using BDDs makes most of the operations time efficient. Of course we had to make various modifications to meet our needs and also implement functions not included in MONA such as checking for automata equivalence and emptiness.

LASH is a toolset for representing infinite sets and exploring infinite state spaces based on finite-state automata [16]. It includes a C library that provides FA construction functions for linear constraints as well as FA manipulation functions. In our experiments we examine their efficiency.

We integrated our construction algorithms to an infinite state CTL model checker called Action Language Verifier [23] built on top of the Composite Symbolic Library [15]. The Composite Symbolic Library uses an object-oriented design to combine different symbolic representations [15]. An abstract interface defines the operations used in symbolic verification: Boolean operations, equivalence and subsumption tests, and pre- and post-condition computations. To integrate a new symbolic representation to the Composite Symbolic Library one simply has to implement the abstract interface with specialized operations. Composite Symbolic Library supports a disjunctive composite representation for formulas on integer and Boolean
variables. A disjunctive composite representation is in the form $\bigvee_{i=1}^{n} \bigwedge_{t \in T} p_{it}$ where $p_{it}$ denotes the formula of type $t$ (which could be integer or Boolean) in the $i$th disjunct, and $n$ and $T$ denote the number of disjuncts and the set of variable types ($T = \{\text{integer, boolean}\}$), respectively. The methods such as intersection, union, complement, satisfiability check, subsumption test, which manipulate composite representations in the above form are implemented in the Composite Symbolic Library by calling the operations on integer and Boolean formula representations [15].

We integrated five different symbolic representations to the Composite Symbolic Library. The first three use the disjunctive composite representation used in Composite Symbolic Library to combine formulas on integer and Boolean variables. We used the BDD representation for Boolean formulas. We implemented three different integer formula representations using LASH [16] (version V3), Omega [17] (version V2), and our automata construction algorithms (version V1) which uses MONA automata package [14] as an automata manipulator. We also implemented two automata based representations using LASH (version V5) and our construction algorithms (version V4) again built on top of MONA automata package, for both Boolean and integer variables without using the disjunctive composite representation. The states of both Boolean and integer variables can be represented in an automaton, hence one can avoid using the disjunctive composite representation.

7.2. Experiments

We experimented with a large set of examples which are describe below. Each instance is labeled using NAME(number of processes)-(property number). Action Language specifications of these examples and properties are available at: http://www.cs.ucsb.edu/~bultan/composite/

First set of examples are monitor specifications for the sleeping barber problem. We verified three properties for systems with 2, 3, and 4 customer processes and one barber process (BARBERP-(1,2,3)). We also verified the three properties (BARBERP-(1,2,3)) on the parameterized system for arbitrary number of customer processes. BAKERY(2,3,4) and TICKET(2,3,4) are mutual exclusion protocols (for (2,3,4) processes, respectively). We verified both mutual exclusion (BAKERY(2,3,4)-1, TICKET(2,3,4)-1) and starvation-freedom properties for these protocols (BAKERY(2,3,4)-2, TICKET(2,3,4)-2). We analyzed a parameterized cache coherence protocol specification given in [6]. We verified three properties given in [6]. RW(4,16,64) is a monitor specification for readers-writers problem for various number of processes [24]. AIRPORT(2,4,8,16) is a monitor specification from [25] for airport ground traffic control simulation with various number of processes.

The results of our experimental evaluation of different representations are shown in Tables 1 and 2. We obtained the experimental results on a SUN ULTRA 10 work station with 768 Mbytes of memory, running SunOs 5.7. In Table 2, we show the types and the number of fixpoint iterations (F denotes the forward fixpoint computation, EG and EF denote the fixpoint computations for corresponding CTL operators), and the number of integer and boolean variables for each problem instance. For each version of the verifier we recorded the following statistics: 1) Time
elapsed during the construction of the symbolic representation of the transition system, shown in the table as CT. 2) Time elapsed during the verification process, shown as VT. It includes the time needed for forward or backward fixpoint computations, however, it excludes the construction time (CT). 3) For V1, V3, V4 and V5 that use automata as a symbolic representation we recorded the size (number of states) of the automaton representing the transition system, shown as TRS, and the size of the largest automaton computed during the fixpoint computation, shown as MS. As discussed above our automata construction algorithm used in versions V1 and V4 uses MONA automata package. MONA automata package uses BDDs to store the transition relation of the automata. Therefore, to make the comparison with LASH fair, for versions V1 and V4, we also give the total number of BDD nodes used in the MONA representation in parentheses. For V2 which uses a polyhedral representation we give the number of total atomic arithmetic constraints in the transition relation (TR AC) and the largest fixpoint iterate (MAX AC). For the instances marked with symbol †, the verification tool did not converge in an hour.

By inspecting the Tables 1 and 2 one can make the following observations. The number of states of the automata used in V1 is about an order of magnitude less that the number of states of the automata used in V3. This is due to the different encodings used in V1 and V3. Note that the transition function in V3 requires a constant amount of memory per state of the automata whereas in V1 the transitions from each state are encoded using BDDs. Hence, a better comparison would be to compare the number of states of the automata in V3 to the number of
Table 2. Experimental results for performance of different automata-based encodings of integer arithmetic constraints and boolean formulas. Time measurements appear in seconds.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Computed F_{syn}</th>
<th>V4 - Automata</th>
<th>V4 - LAXM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>int</td>
<td>bool</td>
</tr>
<tr>
<td>I2TA1</td>
<td>EF(1)</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>I2TA2</td>
<td>EF(11)</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>I2TA3</td>
<td>EF(5)</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>I2TA4</td>
<td>EF(10)</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>I2TA5</td>
<td>EF(11)</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>I2TA6</td>
<td>EF(13)</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>I2TA7</td>
<td>F(7)</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>I2TA8</td>
<td>F(7)</td>
<td>6</td>
<td>2</td>
</tr>
</tbody>
</table>

BDD nodes used to encode the transition function of the automata in V1 (shown in parenthesis under TRS and MS). We see that these numbers are comparable for each problem instance. However, V1 is much faster than V3. Hence, although the BDD encoding requires same amount of space as the encoding used in V3, it improves the verification time significantly. The amount of memory required for the polyhedra based approach used in V2 is proportional to the number of atomic constraints in the polyhedra which is shown under TR AC and MAX AC columns under V2. The increase in the memory requirement of V2 with the increasing problem size seems to be similar to the one observed for the automata based approaches V1 and V3. The verification time for V2 is between the verification time required for V1 and V3.

In general the memory requirement for version V4 seems to be less than that of V5. Also verification times for V4 are significantly faster than those of V5. V4 and V5 are both able to verify the problem instance BAKERY 4-2 whereas V1, V2, and V3 were not able to verify this property in an hour. However, for the AIRPORT example, V1, V2, and V3 scale better than V4 and V5. Both for V3 and V5 the symbolic representation construction time takes a significant amount of time for problem instances with large number of boolean variables. Based on these results we conclude that the versions based on our automata construction algorithms for linear integer arithmetic formulas and implemented using MONA automata package (V1 and V4) are the most time efficient of all.

8. Conclusions
In this work we have presented algorithms for constructing Finite Automata (FA) which represent integer sets that satisfy linear constraints. These automata can represent either signed or unsigned integers and have a lower number of states compared to other similar approaches. We discussed efficient storage techniques for the transition function of the FA and extended the construction algorithms to formulas on both boolean and integer variables. We also derived conditions which guarantee that the pre-condition computations used in symbolic verification algorithms do not cause an exponential increase in the FA size. Finally, we have tested the presented representations by using them to verify non-trivial systems and showed that in many cases they perform better than the polyhedral representation used in Omega Library, or the automata representation used in LASH.

References


12. Bernard Boigelot, Stéphane Rassart, and Pierre Wolper. On the expressiveness of


