Iterating Octagons

Marius Bozga[1], Codruţa Gîrlea[1], and Radu Iosif[1]

VERIMAG/CNRS, 2 Avenue de Vignate, 38610 Gières, France
{bozga,girlea,iosif}@imag.fr

Abstract. In this paper we prove that the transitive closure of a nondeterministic octagonal relation using integer counters can be expressed in Presburger arithmetic. The direct consequence of this fact is that the reachability problem is decidable for flat counter automata with octagonal transition relations. This result improves the previous results of Comon and Jurski [6] and Bozga, Iosif and Lakhnech [5] concerning the computation of transitive closures for difference bound relations. The importance of this result is justified by the wide use of octagons to computing sound abstractions of real-life systems [14]. We have implemented the octagonal transitive closure algorithm in a prototype system for the analysis of counter automata, called FLATA, and we have experimented with a number of test cases.

1 Introduction

Counter automata (register machines) are widely investigated models of computation. Since the result of Minsky [15] showing Turing-completeness of 2-counter machines, research on counter automata pursued in two directions. The first one is defining subclasses of counter automata for which various decision problems (e.g. reachability, emptiness, boundedness, disjointness, containment, equivalence) are found to be decidable. Examples include Reversal-bounded Counter Machines [12], Petri Nets and Vector Addition Systems [17] or Flat Counter Automata [13]. Often, decidability of various problems is achieved by defining the set of reachable configurations in a decidable logic, such as Presburger arithmetic [16]. Such definitions are precise, i.e. no information is lost by the use of over-approximation.

Another, orthogonal, direction of work is concerned with finding sound (but not necessarily complete) answers to the decision problems mentioned above, in a cost-effective way. Such approaches use abstract domains (Polyhedra [7], Octagons [14], Difference Constraints [1], etc.) and compute fixed points that are over-approximations of the set of reachable configurations.

Both approaches to the analysis of counter automata benefit, in some sense, from algorithms for computing transitive closures of arithmetic relations. If I is the initial set of configurations, and R is the transition relation of the counter automaton, then $R^*(I)$ (the image of I through R^*) is the set of reachable configurations, where $R^* = \bigcup_{n \geq 0} R^n$ is the transitive closure of R. The problem lies essentially in expressing the infinite disjunction from the definition of R^*, in a finite way.

In this paper we consider octagonal transition relations that are conjunctions of atoms of the form $\pm x \pm y \leq c$, where x and y are counter values, either at the current step, or at the next step (in which case they are denoted by primed variables), and $c \in \mathbb{Z}$ is an integer constant. For this class of relations, we prove that the transitive closure is expressible in Presburger arithmetic [16]. This improves the previous result of Comon and Jurski [6], showing that the transitive closure of a difference bound constraint (a conjunction of atoms of the form $x - y \leq c$, with x, y possible primed counters, and $c \in \mathbb{Z}$) is Presburger-definable.

We adopt the classical representation of octagonal constraints (or octagons) $\varphi(x_1, \ldots, x_n)$ as difference bound constraints $\varphi(y_1, \ldots, y_{2n})$, where y_{2i-1} stands for $+x_i$ and y_{2i} for $-x_i$, and the implicit condition $y_{2i-1} + y_{2i} = 0$, $1 \leq i \leq n$. With this convention, [2] provides an algorithm for computing the canonical form of an octagon, by first computing the strongest closure of the corresponding difference bound constraint (using the classical Floyd-Warshall cubic algorithm), and subsequently tightening the constraints of the form $y_{2i} - y_{2i-1} \leq c$ and $y_{2i-1} - y_{2i} \leq d$ by adjusting c to $2\lfloor c/2 \rfloor$ and d to $2\lfloor d/2 \rfloor$, respectively. We apply this idea to tightening octagonal relations of the form R^k, where R is an octagon and $k \geq 1$ is the arbitrary number of iterations, obtaining in this way a Presburger formula $\psi(k, x_1, ..., x_n, x'_1, ..., x'_n)$ equivalent to the k-th iteration of φ. The transitive closure of R is thus $R^* = \exists k.\psi$.

The main application of this result is that the following problems are decidable, for the class of counter automata with octagonal transition rules:

- *reachability*: the automaton has a run leading from a configuration in I to a configuration in S, where I and S are Presburger-definable sets of configurations.
- *emptiness*: the automaton has at least a run starting with all counters set to zero, and leading to a final control location.

In particular, decidability of the reachability problem is useful for the verification of safety properties (e.g. assertion checking) of integer programs, whereas the emptiness problem is a promising approach for the analysis of programs with integer arrays. Indeed, the works of [10, 4] reduce the satisfiability problem for two logics on integer arrays to the emptiness problem of a counter automaton. By enlarging the class of counter automata for which this problem is decidable, we enhance the expressiveness of (decidable) logics of integer arrays.

Finally, we have implemented our method in a tool for the analysis of counter automata, called FLATA [9]. We have experimented with a number of test cases and provided several experimental results.

1.1 Related Work

The domain of counter machines has been investigated starting with the seminal work of Minsky [15]. His result on Turing-completeness of 2-counter machines motivated research on subclasses of counter automata, for which some problems are decidable, such as: Reversal-bounded Counter Machines [12], Petri Nets and Vector Addition Systems [17] or Flat Counter Automata [13].

The class of Flat Counter Automata which is closest to our work is the one studied by Comon and Jurski in [6]. In this work, they prove that the transitive closure of a difference bound constraint is Presburger-definable. In [5] we showing how to effectively compute the transitive closure of a difference bound constraint directly as a finite set of linear inequation systems, opening thus the possibility of using SMT tools for the analysis of such models.

Octagonal constraints are investigated in the comprehensive paper of Miné [14]. Among other results, his paper presents a cubic time tightening algorithm for an octagonal constraint, which is an improvement of the classical algorithm of Harvey and Stuckey [11]. However, this algorithm is not suitable to tightening octagonal constraints of parametric size, as the ones we obtain by iteration. For this reason, we adapt the (newer) tightening algorithm of Bagnara, Hill and Zaffanella [2] to octagons obtained by arbitrary iteration, as they prove that it is sufficient to adjust the constants *after* the computation of minimal paths (by the Floyd-Warshall algorithm).

Our paper extends to octagons the class of non-deterministic relations for which the transitive closure can be effectively expressed in Presburger arithmetic. This result relies essentially on our method from [5] to computing minimal paths in constraint graphs obtained by iteration, and the idea of [2] for tightening (finite) octagonal relations.

On a different line of work, Boigelot [3], and Finkel and Leroux [8] have studied the computation of transitive closure for affine relations of the form $\mathbf{x}' = A\mathbf{x} + \mathbf{b}$. Their class of systems differs in nature from ours, in what their transition relations are functional (deterministic), whereas octagons are not. Because of this, their results seem incomparable to ours.

Roadmap The paper is organized as follows. Section 2 introduces difference bound constraints and difference bound relations, recalling a number of results on DBMs, Section 3 defines octagonal constraints, and gives a necessary quantifier elimination result on octagons, while Section 4 is dedicated to our main result, namely computing the transitive closure of an octagonal relation. Section 5 gives implementation results, and finally, Section 6 concludes.

2 Difference Bounds

In this section we recall several definitions and results on difference bound constraints, and the transitive closure of difference bound relations. In the rest of the paper, $\mathbb{Z}$ denotes the set of integer numbers, $n > 0$ is the number of variables and $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ is the tuple of variables. If $\varphi(\mathbf{x})$ is a logical formula in which $x_1, x_2, \ldots, x_n$ occur free, and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ is a tuple of values, $\varphi[\mathbf{v}/\mathbf{x}]$ denotes the formula in which each occurrence of x_i has been replaced by v_i. We denote by $\mathbf{v} \models \varphi$ the fact that $\varphi[\mathbf{v}/\mathbf{x}]$ is logically equivalent to true. We say that φ is *consistent* if there exists at least one $\mathbf{v} \in \mathbb{Z}^n$ such that $\mathbf{v} \models \varphi$, and *inconsistent* otherwise. If φ is a formula, let $AP(\varphi)$ denote the set of atomic propositions in φ. If m is a matrix, then $m_{i,j}$ denote the element of m situated at line i and column j.

2.1 Difference Bound Constraints

Definition 1. *Let $\mathbf{x} = (x_1, x_2, ..., x_n)$ be a set of variables ranging over $\mathbb{Z}$. Then a formula $\phi(\mathbf{x})$ is a* difference bound constraint *if it is equivalent to a finite conjunction of atomic propositions of the form $x_i - x_j \leq \alpha_{i,j},\ i \neq j,\ 1 \leq i, j \leq n$, where $\alpha_{i,j} \in \mathbb{Z}$.*

For instance, $x - y = 5$ is a difference bound constraint, as it is equivalent to $x - y \leq 5 \wedge y - x \leq -5$. In practice difference bound constraints are represented either as matrices or as graphs, each of these representations being suitable for particular procedures (e.g. closure, iteration). We define these representations and procedures below.

Definition 2. *Let $\mathbf{x} = (x_1, x_2, ..., x_n)$ be a set of variables ranging over $\mathbb{Z}$ and $\phi(\mathbf{x})$ be a difference bound constraint. Then a* difference bound matrix *(DBM) representing ϕ is an $n \times n$ matrix m such that:*

$$m_{i,j} = \begin{cases} \alpha_{i,j} & \textit{if } (x_i - x_j \leq \alpha_{i,j}) \in AP(\phi) \\ \infty & \textit{otherwise} \end{cases}$$

For a $n \times n$ DBM m we denote by $\gamma(m) = \{\mathbf{v} \in \mathbb{Z}^n \mid v_i - v_j \leq m_{i,j}, 1 \leq i, j \leq n\}$ the set of *concretizations* of m. Notice that this is exactly the set of models of the corresponding difference bound constraint φ, i.e. $\gamma(m) = \{\mathbf{v} \mid \mathbf{v} \models \varphi\}$. A DBM m is said to be consistent if $\gamma(m) \neq \emptyset$, and inconsistent otherwise.

Definition 3. *Let $\mathbf{x} = (x_1, x_2, ..., x_n)$ be a set of variables ranging over $\mathbb{Z}$ and $\phi(\mathbf{x})$ be a difference bound constraint. Then ϕ can be represented as a weighted graph $\mathcal{G}$ with vertices $x_1, x_2, ..., x_n$ in which there is an arc with weight $\alpha_{i,j}$ between x_i and x_j in $\mathcal{G}$ if there is a constraint $x_i - x_j \leq \alpha_{i,j}$ in ϕ. This graph is also called a* constraint graph.

Whenever the graph $\mathcal{G}$ is obvious from the context, we will denote by $x \xrightarrow{\alpha} y$ the fact that there exists an edge with weight α from x to y in $\mathcal{G}$. Notice that the DBM m of a difference bound constraint is the incidence matrix of its corresponding constraint graph. This graph will be denoted as $\mathcal{G}(m)$ in the following. The three notions (constraint, matrix, graph) are related by the following theorem :

Theorem 1. *Let ϕ be a difference bound constraint, m the corresponding DBM and $\mathcal{G}(m)$ the corresponding graph. Then the following three statements are equivalent :*

1. *ϕ is inconsistent*

2. $\mathcal{G}(m)$ *contains at least one negative weight cycle*
3. $\gamma(m) = \emptyset$

On one hand, the DBM representation of a difference bound constraint is suitable for computing its normal form, i.e. the most "explicit" formula that has the same set of models.

Definition 4. *An $n \times n$ consistent DBM m is said to be* closed *if and only if the following hold:*

1. $m_{i,i} = 0 \ \forall 1 \leq i \leq n$
2. $m_{i,j} \leq m_{i,k} + m_{k,j} \ \forall 1 \leq i, j, k \leq n$

The *shortest path closure* of a consistent DBM m is a closed DBM m^* such that $\gamma(m) = \gamma(m^*)$. It is well-known that, if m is consistent then m^* is unique, and it can be computed from m in time $\mathcal{O}(n^3)$, by the classical Floyd-Warshall algorithm. Moreover, the following condition holds, for all $1 \leq i, j \leq n$:

$$m^*_{i,j} = \min \left\{ \sum_{l=0}^{k-1} m_{i_l, i_{l+1}} | x_i = x_{i_0} x_{i_1} ... x_{i_k} = x_j \text{ is a path in } \mathcal{G}(m) \right\}$$

On the other hand, the graph representation of a difference bound constraint is suitable for existential quantifier elimination[1]. Concretely, given a difference bound constraint $\phi(\mathbf{x})$, the formula $\exists x_k . \phi$ is a difference bound constraint as well, and its corresponding graph is effectively computable from the graph of ϕ, as shown by the following theorem :

Theorem 2. *Let $\mathbf{x} = (x_1, x_2, ..., x_n)$ be a set of variables ranging over $\mathbb{Z}$, $\phi(\mathbf{x})$ be a difference bound constraint and m be the corresponding $n \times n$ DBM. Then, for any $1 \leq k \leq n$ the formula $\exists x_k . \phi(\mathbf{x})$ is a difference bound constraint, and its corresponding constraint graph is obtained by erasing the vertex x_k together with the incident arcs from the graph $\mathcal{G}(m^*)$. Moreover, the DBM of the resulting graph is also closed.*

The importance of this result will be made clear in the next section, because it directly implies that the class of difference bound relations is closed under composition. This is the first ingredient of our transitive closure method.

2.2 Difference Bound Relations

Definition 5. *Let $\mathbf{x} = (x_1, x_2, ..., x_n)$, $\mathbf{x}' = (x'_1, x'_2, ..., x'_n)$ be sets of variables ranging over $\mathbb{Z}$. A relation $R(\mathbf{x}, \mathbf{x}')$ is a* difference bound relation *if it is equivalent to a finite conjunction of terms of the form $x_i - x_j \leq a_{i,j}$,$x'_i - x_j \leq b_{i,j}$, $x_i - x'_j \leq c_{i,j}$, or $x'_i - x'_j \leq d_{i,j}$, where $a_{i,j}, b_{i,j}, c_{i,j}, d_{i,j} \in \mathbb{Z}$, $1 \leq i, j \leq n$.*

[1] In general, difference bound constraints are not closed under universal quantification, however finite disjunctions of difference bound constraints are, since the negation of a difference bound constraint is always equivalent to a finite disjunction of difference constraints.

According to the previous section, a difference bound relation can be represented as a constraint graph with nodes in the set $\mathbf{x} \cup \mathbf{x}'$, such that $x \xrightarrow{\alpha} y$ if and only if $x - y \leq \alpha \in AP(R)$, for all $x, y \in \mathbf{x} \cup \mathbf{x}'$. Just like before, the incidence matrix of this graph is the DBM of the relation.

In the following, we denote $\mathbf{x}^{(l)} = (x_1^{(l)}, x_2^{(l)}, \ldots, x_n^{(l)})$, $\mathbf{x}^{(\geq l)} = \bigcup_{s \geq l} \mathbf{x}^{(s)}$ and $\mathbf{x}^{(\leq l)} = \bigcup_{s \leq l} \mathbf{x}^{(s)}$, for any $l \geq 0$. Given a difference bound relation $R(\mathbf{x}, \mathbf{x}')$, we define the k-th iteration of R:

$$R^k(\mathbf{x}^{(0)}, \mathbf{x}^{(k)}) = \exists \mathbf{x}^{(1)} \ldots \exists \mathbf{x}^{(k-1)}.R(\mathbf{x}^{(0)}, \mathbf{x}^{(1)}) \wedge \ldots \wedge R(\mathbf{x}^{(k-1)}, \mathbf{x}^{(k)})$$

for all $k \geq 1$. The transitive closure of R is defined as $R^* = \exists k.R^k$.

Notice that, since existential quantifiers can be eliminated from difference bound constraints (cf. Theorem 2), difference bound relations are closed under composition, and therefore R^k is a difference bound relation, for any $k \geq 0$.

We now recall a result from [5], namely that the k-th iteration R^k of a difference bound relation R is equivalent to a finite set of linear inequation systems. As a result, the R^* is directly definable in Presburger arithmetic.

The constraint graph $\mathcal{G}^k$, representing the matrix of R^k (i.e. $R(\mathbf{x}^{(0)}, \mathbf{x}^{(1)}) \wedge \ldots \wedge R(\mathbf{x}^{(k-1)}, \mathbf{x}^{(k)})$) is the graph composed of k connected copies of the constraint graph of R.

Definition 6. *Let $\mathbf{x} = (x_1, x_2, ..., x_n)$, $\mathbf{x}' = (x_1', x_2', ..., x_n')$ be sets of variables ranging over $\mathbb{Z}$ and $R(\mathbf{x}, \mathbf{x}')$ a DBM relation. The constraint graph of R^k has as set of vertices $\bigcup_{l=0}^{k} \mathbf{x}^{(l)}$ and, for all $1 \leq i, j \leq n$, for all $0 \leq l < k$:*

$$\begin{aligned}
x_i^{(l)} \xrightarrow{a} x_j^{(l)} &\iff x_i - x_j \leq a \in AP(R) \\
x_i^{(l)} \xrightarrow{a} x_j^{(l+1)} &\iff x_i - x_j' \leq a \in AP(R) \\
x_i^{(l+1)} \xrightarrow{a} x_j^{(l)} &\iff x_i' - x_j \leq a \in AP(R) \\
x_i^{(l+1)} \xrightarrow{a} x_j^{(l+1)} &\iff x_i' - x_j' \leq a \in AP(R)
\end{aligned}$$

In order to compute R^k, for a given $k \geq 1$, we must first compute the closure of the constraint graph from Definition 6, in order to remove the intermediary nodes $\mathbf{x}^{(l)}$, $0 < l < k$. According to Theorem 2, R^k is a difference bound constraint, and the graph obtained after eliminating the intermediary variables is the constraint graph of R^k. Therefore, R^k can be written as a conjunction of the form:

$$\bigwedge_{1 \leq i,j \leq n} x_i^{(0)} - x_j^{(0)} \leq \min_k \{x_i^{(0)} \rightsquigarrow x_j^{(0)}\} \wedge \bigwedge_{1 \leq i,j \leq n} x_i^{(0)} - x_j^{(k)} \leq \min_k \{x_i^{(0)} \rightsquigarrow x_j^{(k)}\} \wedge$$
$$\bigwedge_{1 \leq i,j \leq n} x_i^{(k)} - x_j^{(k)} \leq \min_k \{x_i^{(k)} \rightsquigarrow x_j^{(k)}\} \wedge \bigwedge_{1 \leq i,j \leq n} x_i^{(k)} - x_j^{(0)} \leq \min_k \{x_i^{(k)} \rightsquigarrow x_j^{(0)}\}$$

where $\min_k\{x \rightsquigarrow y\} \in \mathbb{Z} \cup \{\pm\infty\}$ denotes the value of the minimal path between nodes x and y in the constraint graph of R^k[2]. Notice that R^k is satisfiable if and only there are no cycles of negative cost within the constraint graph from Definition 6 (cf. Theorem 1). Since this graph is obtained by connecting k copies of R, if there is a negative cycle in the graph, there will also be a negative cycle that goes through $x_i^{(0)}$, for some $1 \leq i \leq n$.

The main result of [6,5] is that $\min_k\{x_i^{(0)} \rightsquigarrow x_j^{(0)}\}$, $\min_k\{x_i^{(0)} \rightsquigarrow x_j^{(k)}\}$, $\min_k\{x_i^{(k)} \rightsquigarrow x_j^{(k)}\}$ and $\min_k\{x_i^{(k)} \rightsquigarrow x_j^{(0)}\}$ are Presburger definable functions of k.

Example 1. Let $R(\mathbf{x}, \mathbf{x}')$ be the following DBM relation, where $\mathbf{x} = \{x_1, x_2, x_3\}$:

$$R(\mathbf{x}, \mathbf{x}') = x_1 - x_1' \leq -1 \wedge x_1 - x_2 \leq 0 \wedge x_2 - x_3 \leq 7 \wedge x_2' - x_2 \leq -2 \wedge x_3 - x_3' \leq -3$$

Figure 1 shows the graph representation of R^k, for $k = 1, 2, 3 \ldots$. By computing the minimal weight paths in the constraint graph of R^k for $k = 1, 2, 3, \ldots$ we obtain, e.g. :

$$\begin{aligned} R^{(1)}(\mathbf{x}, \mathbf{x}') = {} & x_1 - x_2 \leq 0 \wedge x_1 - x_3 \leq 7 \wedge x_2 - x_3 \leq 7 \wedge x_1 - x_1' \leq -1 \wedge x_1 - x_3' \leq 4 \wedge \\ & \wedge x_2 - x_3' \leq 4 \wedge x_3 - x_3' \leq -3 \wedge x_2' - x_2 \leq -2 \wedge x_2' - x_3 \leq 5 \wedge x_2' - x_3' \leq 2 \end{aligned}$$

$$\begin{aligned} R^{(2)}(\mathbf{x}, \mathbf{x}') = {} & x_1 - x_2 \leq -3 \wedge x_1 - x_3 \leq 4 \wedge x_2 - x_3 \leq 7 \wedge x_1 - x_1' \leq -2 \wedge x_1 - x_3' \leq -2 \wedge \\ & \wedge x_2 - x_3' \leq 1 \wedge x_3 - x_3' \leq -6 \wedge x_2' - x_2 \leq -4 \wedge x_2' - x_3 \leq 3 \wedge x_2' - x_3' \leq -3 \end{aligned}$$

$$\begin{aligned} R^{(3)}(\mathbf{x}, \mathbf{x}') = {} & x_1 - x_2 \leq -6 \wedge x_1 - x_3 \leq 1 \wedge x_2 - x_3 \leq 7 \wedge x_1 - x_1' \leq -3 \wedge x_1 - x_3' \leq -8 \wedge \\ & \wedge x_2 - x_3' \leq -2 \wedge x_3 - x_3' \leq -9 \wedge x_2' - x_2 \leq -6 \wedge x_2' - x_3 \leq 1 \wedge x_2' - x_3' \leq -8 \end{aligned}$$

$$\begin{aligned} R^{(n \geq 4)}(\mathbf{x}, \mathbf{x}') = {} & x_1 - x_2 \leq -3 - 3(n-2) \wedge x_1 - x_3 \leq -2 - 3(n-4) \wedge x_2 - x_3 \leq 7 \wedge \\ & x_1 - x_1' \leq -n \wedge x_1 - x_3' \leq -14 - 6(n-4) \wedge x_2 - x_3' \leq 1 - 3(n-2) \wedge \\ & x_3 - x_3' \leq -3n \wedge x_2' - x_2 \leq -2n \wedge x_2' - x_3 \leq 3 - 2(n-2) \wedge \\ & x_2' - x_3' \leq -3 - 5(n-2) \end{aligned}$$

□

3 Octagonal Constraints

This section is dedicated to octagonal constraints. We provide preliminary results that are needed to define transitive closures of octagonal relations, in the next section.

[2] If $\min_k\{x \rightsquigarrow y\} = -\infty$ the constraint is logically equivalent to false, and if $\min\{x \rightsquigarrow y\} = \infty$ it is logically equivalent to true.

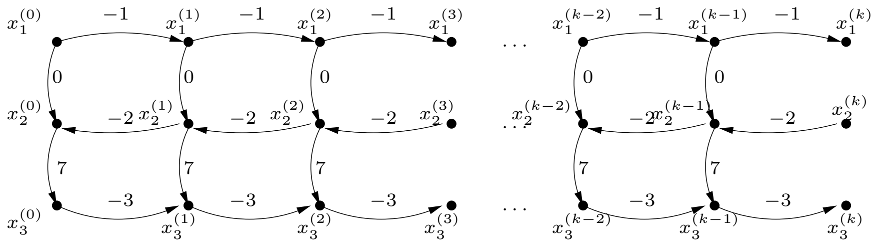

Fig. 1. Graph representation of $R^k,\ k = 1, 2, 3, \ldots$

Definition 7. *Let* $\mathbf{x} = (x_1, x_2, ..., x_n)$ *be a set of variables ranging over* $\mathbb{Z}$. *Then a formula* $\phi(\mathbf{x})$ *is an* octagonal constraint *if it is equivalent to a finite conjunction of terms of the form* $\pm x_i \pm x_j \leq \alpha_{i,j}$, $2x_i \leq \beta_i$, *or* $-2x_i \leq \gamma_i$, *where* $\alpha_{i,j}, \beta_i, \gamma_i \in \mathbb{Z}$ *and* $i \neq j,\ 1 \leq i, j \leq n$.

The name *octagon* comes from the fact that, in two dimensions, these constraints can be graphically represented by polyhedra with at most eight edges. We represent octagons using the set of variables $\mathbf{y} = (y_1, y_2, \ldots, y_{2n})$, with the convention that y_{2i-1} stands for x_i and y_{2i} for $-x_i$, respectively. For instance, the octagonal constraint $x_1 + x_2 = 3$ is represented as $y_1 - y_4 \leq 3 \wedge y_2 - y_3 \leq -3$.

If we denote by $\overline{\phi} = \phi[y_1/x_1, y_2/-x_1, \ldots, y_{2n-1}/x_n, y_{2n}/-x_n]$, we obtain the following valid entailment: $\phi(\mathbf{x}) \rightarrow (\exists y_2, y_4, \ldots, y_{2n}.\overline{\phi})[x_1/y_1, \ldots, x_n/y_{2n-1}]$. Moreover $\phi(\mathbf{x}) \leftrightarrow (\exists y_2, y_4, \ldots, y_{2n}.\overline{\phi} \wedge \bigwedge_{i=1}^{n} y_{2i-1} + y_{2i} = 0)[x_1/y_1, \ldots, x_n/y_{2n-1}]$.

To handle the $\mathbf{y}$ variables in the following, we define $\overline{i} = i - 1$, if i is even, and $\overline{i} = i + 1$ if i is odd. Obviously, we have $\overline{\overline{i}} = i$, for all $i \in \mathbb{Z},\ i \geq 0$. The following definition extends the matrix representation from difference bound constraints to octagons:

Definition 8. *Let* $\mathbf{x} = (x_1, x_2, ..., x_n)$ *be a set of variables ranging over* $\mathbb{Z}$ *and* $\phi(\mathbf{x})$ *be an octagonal constraint. Then an* octagonal difference bound matrix *or octagonal DBM representing* ϕ *is an* $2n \times 2n$ *matrix* m *such that:*

$$
\begin{array}{lll}
(x_i - x_j \leq \alpha_{i,j}) \in AP(\phi) & \iff & m_{2i-1,2j-1} = m_{2j,2i} = \alpha_{i,j} \\
(-x_i - x_j \leq \alpha_{i,j}) \in AP(\phi) & \iff & m_{2i,2j-1} = m_{2j,2i-1} = \alpha_{i,j} \\
(-x_i + x_j \leq \alpha_{i,j}) \in AP(\phi) & \iff & m_{2i,2j} = m_{2j-1,2i-1} = \alpha_{i,j} \\
(x_i + x_j \leq \alpha_{i,j}) \in AP(\phi) & \iff & m_{2i-1,2j} = m_{2j-1,2i} = \alpha_{i,j} \\
(2x_i \leq \beta_i) \in AP(\phi) & \iff & m_{2i-1,2i} = \beta_i \\
(-2x_i \leq \delta_i) \in AP(\phi) & \iff & m_{2i,2i-1} = \delta_i
\end{array}
$$

A $2n \times 2n$ octagonal DBM m is said to be *coherent* if and only if $m_{i,j} = m_{\bar{j},\bar{i}}$, for all $1 \leq i, j \leq 2n$. This property is needed since any constraint $x_i - x_j \leq \alpha$, $1 \leq i, j \leq n$ can be represented as both $y_{2i-1} - y_{2j-1} \leq \alpha$ and $y_{2j} - y_{2i} \leq \alpha$. If m is coherent, we denote by

$$\gamma^{Oct}(m) = \{(v_1, v_2, ..., v_n) \in \mathbb{Z}^n \mid (v_1, -v_1, v_2, -v_2, ..., v_n, -v_n) \in \gamma(m)\}$$

the set of concretizations, i.e. the set of models of the octagonal constraint represented by m. Also, m is said to be consistent if $\gamma^{Oct}(m) \neq \emptyset$, and inconsistent otherwise. The *octagonal graph* of an octagonal constraint $\phi(\mathbf{x})$, represented as a difference bound constraint $\overline{\phi}(\mathbf{y})$ with DBM m, has vertices $\mathbf{y}$, and an arc labeled by $m_{i,j}$ between y_i and y_j if and only if $m_{i,j} < \infty$, $1 \leq i, j \leq 2n$.

Definition 9. *A consistent coherent* $2n \times 2n$ *DBM* m *in* $\mathbb{Z}$ *is said to be* tightly closed *if and only if the following hold:*

1. $m_{i,i} = 0 \; \forall 1 \leq i \leq 2n$
2. $m_{i,\bar{i}}$ *is even* $\forall 1 \leq i \leq 2n$
3. $m_{i,j} \leq m_{i,k} + m_{k,j} \; \forall 1 \leq i, j, k \leq 2n$
4. $m_{i,j} \leq (m_{i,\bar{i}} + m_{\bar{j},j})/2 \; \forall 1 \leq i, j \leq 2n$

The intuition behind the last point is the following: since $y_i - y_{\bar{i}} \leq m_{i,\bar{i}}$ and $y_{\bar{j}} - y_j \leq m_{\bar{j},j}$ and $y_i = -y_{\bar{i}}$, $y_j = -y_{\bar{j}}$ if we interpret the DBM m as an octagonal constraint, we have that $y_i \leq \lfloor \frac{m_{i,\bar{i}}}{2} \rfloor$ and $-y_j \leq \lfloor \frac{m_{\bar{j},j}}{2} \rfloor$, hence $y_i - y_j \leq \lfloor \frac{m_{i,\bar{i}}}{2} \rfloor + \lfloor \frac{m_{\bar{j},j}}{2} \rfloor$. Therefore, the tightening of an octagonal DBM has to come up with values for $m_{i,j}$ that are smaller than $\lfloor \frac{m_{i,\bar{i}}}{2} \rfloor + \lfloor \frac{m_{\bar{j},j}}{2} \rfloor$, for all $1 \leq i, j \leq 2n$.

The tight closure of a $2n \times 2n$ octagonal DBM m is an octagonal DBM m^*_t such that $\gamma^{Oct}(m) = \gamma^{Oct}(m^*_t)$, and m^*_t is tightly closed. By Theorem 7 in [14], we know that the tight closure of a consistent octagonal DBM exists and is unique.

We now characterize the consistency of octagonal constraints using their DBM representations. The following result, proved in [2], is crucial for the developments of the next section, therefore we cite (a slightly modified version of) it here:

Theorem 3 ([2]). *Let* m *be a* $2n \times 2n$ *octagonal DBM such that* $\gamma(m) \neq \emptyset$, *and* m^* *be its closure. Suppose that* $\left\lfloor \frac{m^*_{i,\bar{i}}}{2} \right\rfloor + \left\lfloor \frac{m^*_{\bar{i},i}}{2} \right\rfloor \geq 0$, *for all* $1 \leq i \leq 2n$. *Then* $\gamma^{Oct}(m) \neq \emptyset$ *and the DBM* m^T *defined as:*

$$m^T_{i,j} = min \left\{ m^*_{i,j}, \left\lfloor \frac{m^*_{i,\bar{i}}}{2} \right\rfloor + \left\lfloor \frac{m^*_{\bar{j},j}}{2} \right\rfloor \right\}$$

for all $1 \leq i, j \leq 2n$, *is the tight closure of* m.

It follows immediately that an octagonal constraint is consistent if and only if (1) its constraint graph representation does not contain negative weight cycles and moreover, (2) if the sum between the halved weights of the minimal paths from any node x_i to $x_{\bar{i}}$, and from $x_{\bar{i}}$ and x_i is positive. Notice that the lack of negative weight cycles alone is not enough, as shown by the following example.

Example 2. Let $\phi(x, y, z, x', y', z') = (x - y' \leq 1) \wedge (y' + x \leq -2) \wedge (-x + z' \leq 1) \wedge (-z' - x \leq 0)$ be an octagonal constraint on integer variables x, y, z and x', y', z'. The constraint is inconsistent since it implies $(1 \leq 2x \leq 1)$ and thus has no integer solution. However, its corresponding octagonal DBM does not contain negative weight cycles. The tightening step, i.e. replacing each element $m_{i\bar{i}}$ with $2\left\lfloor \frac{m_{i\bar{i}}}{2} \right\rfloor$, exhibits two negative weight cycles, between $+x$ and $-x$, and between $+z'$ and $-z'$. $\square$

We are now ready to give the result of existential quantification over variables occurring within octagons. Namely, we prove that, if $\phi(x_1, \ldots, x_n)$ is an octagonal constraint, the formula $\exists x_k.\phi$, for some $1 \leq k \leq n$ is again an octagonal constraint, and its representation is effectively computable from the constraint graph of ϕ.

In the following, we assume w.l.o.g. that $k = n$ (if this is not the case, we proceed to reindexing variables). From now on assume that $\phi(x_1, \ldots, x_n)$ is consistent, and let m be its $2n \times 2n$ tightly closed coherent octagonal DBM. We denote by $\beta(m)$ the $2n-2 \times 2n-2$ matrix from which the $2n-1$ and $2n$ lines and columns have been eliminated. Notice that these correspond to the x_n and $-x_n$ terms, respectively.

Lemma 1. *Let $m \in \mathbb{Z}_{2n \times 2n}$ be the coherent and tightly closed difference bound matrix for $\phi(x_1, \ldots, x_n)$. Then $\beta(m)$ is also coherent and tightly closed.*

The following theorem proves that octagons are closed under existential quantification.

Theorem 4. *Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ be a set of variables ranging over $\mathbb{Z}$, $\phi(\mathbf{x})$ a consistent octagonal constraint and m the corresponding $2n \times 2n$ octagonal DBM. Then formula $\exists x_k.\phi(\mathbf{x})$ is equivalent to erasing vertices y_{2k} and y_{2k-1} together with the incident arcs from the graph $\mathcal{G}(m_t^*)$. Moreover, the resulting graph is also coherent and tightly closed.*

4 Octagonal Relations

This section is dedicated to our main result, the definition of the transitive closure of an octagonal relation in Presburger arithmetic. An octagonal relation is defined in a similar way to a difference bound relation.

Definition 10. *Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{x}' = (x'_1, x'_2, \ldots, x'_n)$ be sets of variables ranging over $\mathbb{Z}$. Then an octagonal relation $R(\mathbf{x}, \mathbf{x}')$ is a relation that can be written as a finite conjunction of terms of the form $\pm x_i \pm x_j \leq a_{i,j}$,$\pm x'_i \pm x_j \leq b_{i,j}$, $\pm x_i \pm x'_j \leq c_{i,j}$, $\pm x'_i \pm x'_j \leq d_{i,j}$, $\pm 2x_i \leq e_{i,j}$ or $\pm 2x'_i \leq f_{i,j}$, where $a_{i,j}, b_{i,j}, c_{i,j}, d_{i,j}, e_{i,j}, f_{i,j} \in \mathbb{Z}$ and $1 \leq i, j \leq n$, $i \neq j$.*

The DBM and graph representation of an octagonal relation are defined as in the previous case of difference bound relations. For the rest of this section, let $R(\mathbf{x}, \mathbf{x}')$ be an octagonal relation and $\overline{R}(\mathbf{y}, \mathbf{y}')$ be its difference bound representation. Let $\mathcal{G}$ be the graph of $\overline{R}$, $\overline{R}^k$ be the k-th iteration of $\overline{R}$, m_k be its DBM, and $\mathcal{G}^k$ be the graph corresponding to $\overline{R}^k$, obtained by connecting k copies of $\mathcal{G}$. The formal definition of $\mathcal{G}^k$ is similar to Definition 6.

In order to compute R^k, we need two ingredients. First, we need to check for consistency of the unfolded relation, that is we need to check that $\gamma^{Oct}(m_k) \neq \emptyset$. Second, we need to obtain the strongest octagonal constraints between $\mathbf{y^{(0)}}$ and $\mathbf{y^{(k)}}$ in $\mathcal{G}^k$. By Theorem 4, all intermediate vertices $\mathbf{y^{(l)}}$, $0 < l < k$ can be eliminated from $\mathcal{G}^k$, and the result is a tightly closed octagonal graph, whose interpretation is equivalent to R^k.

By Theorem 3, both points require the computation of the values $(m_k{}^*)_{i^{(l)},\overline{i^{(l)}}}$ and $(m_k{}^*)_{\overline{i^{(l)}},i^{(l)}}$, for all $1 \leq i \leq 2n$ and $0 \leq l \leq k$, where the index $i^{(l)}$ refers to the variable $y_i^{(l)}$ in the DBM representation of $\overline{R}(\mathbf{y}, \mathbf{y'})$. But these values can now be defined by Presburger formulae, using the results from [6, 5]. To understand this point, consider the situation depicted in Figure 4.

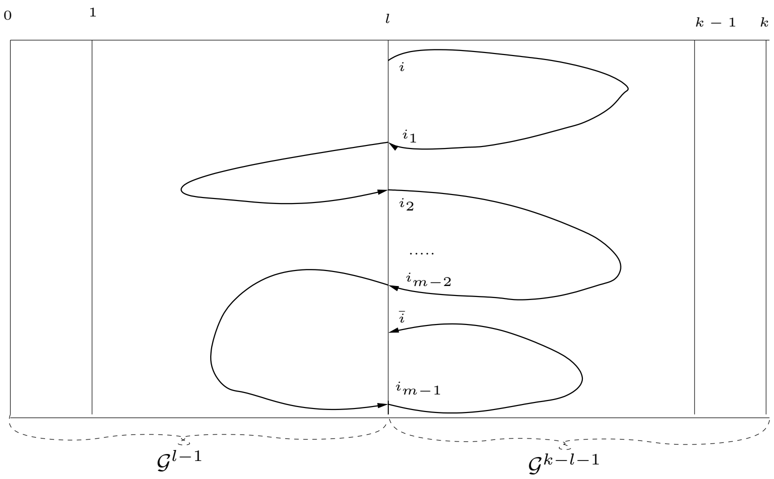

Fig. 2. Computing paths of weight $(m_k{}^*)_{i^{(l)},\overline{i^{(l)}}}$

Assume in the following that $\mathcal{G}^k$ has no cycles of negative weight. The absence of negative cycles can be checked a-priori using e.g. the method in [5]. Since we are aiming at computing minimal weight paths, it is sufficient to consider acyclic paths only[3]. For a fixed $0 < l < k$, an acyclic path between the nodes $y_i{}^{(l)}$ and $y_{\bar{i}}{}^{(l)}$, for some $1 \leq i \leq 2n$, can be decomposed in at most $2n-1$ segments starting and ending in $\mathbf{y}^{(l)}$, but not intersecting with $\mathbf{y}^{(l)}$, other than in the beginning and in the end. Moreover, if the path considered is of minimal weight, these segments are of minimal weight as well.

[3] If a path has a cycle of a positive weight, it cannot be minimal.

Let $1 \leq i = i_0, i_1, \ldots, i_m = \bar{i} \leq 2n$, be a set of pairwise distinct indices, such that

$$(m_k^*)_{i^{(l)},\overline{i^{(l)}}} = \sum_{j=0}^{m-1} (m_k^*)_{i_j^{(l)},i_{j+1}^{(l)}}$$

As in Figure 4, several of the paths $y_i^{(l)} \leadsto y_{i_1}^{(l)}, y_{i_1}^{(l)} \leadsto y_{i_2}^{(l)}, \ldots, y_{i_{m-1}}^{(l)} \leadsto y_{\bar{i}}^{(l)}$ will contain only nodes $\mathbf{y}^{(\leq l)}$, whereas the rest will contain only nodes from $\mathbf{y}^{(\geq l)}$. Notice that, the $\mathbf{y}^{(\leq l)}$ paths are paths between the terminal nodes of $\mathcal{G}^{l-1}$, whereas the $\mathbf{y}^{(\geq l)}$ paths are paths between the initial nodes of $\mathcal{G}^{k-l-1}$. Therefore, we have:

- $(m_k^*)_{i_j^{(l)},i_{j+1}^{(l)}} = \min_{l-1}\{y_{i_j}^{(l)} \leadsto y_{i_{j+1}}^{(l)}\}$, if $y_{i_j}^{(l)} \leadsto y_{i_{j+1}}^{(l)}$ belongs to $\mathbf{y}^{(\leq l)}$, and
- $(m_k^*)_{i_j^{(l)},i_{j+1}^{(l)}} = \min_{k-l-1}\{y_{i_j}^{(0)} \leadsto y_{i_{j+1}}^{(0)}\}$, if $y_{i_j}^{(l)} \leadsto y_{i_{j+1}}^{(l)}$ belongs to $\mathbf{y}^{(\geq l)}$.

But since the $\min_j\{x \leadsto y\}$ functions are definable in Presburger arithmetic [6, 5], we obtain that $(m_k^*)_{i,\bar{i}}$ are Presburger definable as well. Since moreover, integer division can be defined in Presburger as

$$\left\lfloor \frac{u}{2} \right\rfloor = v \iff 2v \leq u \leq 2v+1$$

it is possible to encode the consistency check of Theorem 3 by a Presburger formula, and effectively perform the check required by Theorem 3:

$$\bigwedge_{\substack{1 \leq i \leq 2n \\ 0 \leq l \leq k}} \left\lfloor \frac{m^*_{i^{(l)},\overline{i^{(l)}}}}{2} \right\rfloor + \left\lfloor \frac{m^*_{\overline{i^{(l)}},i^{(l)}}}{2} \right\rfloor \geq 0$$

After quantifier elimination, the strongest octagonal relations are obtained by taking the restriction of the tight closure of m_k to $\mathbf{y}^{(0)}$ and $\mathbf{y}^{(k)}$, according to Theorem 3:

$$y_i{}^{(0)} - y_j{}^{(k)} \leq (m_{kt}^*)_{i^{(0)},j^{(k)}} = min\left\{(m_{kt}^*)_{i^{(0)},j^{(k)}},\ \left\lfloor \frac{(m_{kt}^*)_{i^{(0)},\overline{i^{(0)}}}}{2} \right\rfloor + \left\lfloor \frac{(m_{kt}^*)_{\overline{j^{(k)}},j^{(k)}}}{2} \right\rfloor\right\}$$
$$y_i{}^{(k)} - y_j{}^{(0)} \leq (m_{kt}^*)_{i^{(k)},j^{(0)}} = min\left\{(m_{kt}^*)_{i^{(k)},j^{(0)}},\ \left\lfloor \frac{(m_{kt}^*)_{i^{(k)},\overline{i^{(k)}}}}{2} \right\rfloor + \left\lfloor \frac{(m_{kt}^*)_{\overline{j^{(0)}},j^{(0)}}}{2} \right\rfloor\right\}$$
$$y_i{}^{(0)} - y_j{}^{(0)} \leq (m_{kt}^*)_{i^{(0)},j^{(0)}} = min\left\{(m_{kt}^*)_{i^{(0)},j^{(0)}},\ \left\lfloor \frac{(m_{kt}^*)_{i^{(0)},\overline{i^{(0)}}}}{2} \right\rfloor + \left\lfloor \frac{(m_{kt}^*)_{\overline{j^{(0)}},j^{(0)}}}{2} \right\rfloor\right\}$$
$$y_i{}^{(k)} - y_j{}^{(k)} \leq (m_{kt}^*)_{i^{(k)},j^{(k)}} = min\left\{(m_{kt}^*)_{i^{(k)},j^{(k)}},\ \left\lfloor \frac{(m_{kt}^*)_{i^{(k)},\overline{i^{(k)}}}}{2} \right\rfloor + \left\lfloor \frac{(m_{kt}^*)_{\overline{j^{(k)}},j^{(k)}}}{2} \right\rfloor\right\}$$

Since we showed that all weights of the form $m^*_{i^{(l)},\overline{i^{(l)}}}$ are definable in Presburger arithmetic, it follows that R^k is also Presburger definable. Consequently, the transitive closure of R is the Presburger formula $\exists k.R^k$, leading to the following theorem:

Theorem 5. *The transitive closure of an integer octagonal relation is Presburger definable.*

Notice however, that paths of the forms $y_i^{(0)} \rightsquigarrow y_j^{(0)}$ or $y_i^{(k)} \rightsquigarrow y_j^{(k)}$ reside on one side only, therefore we do not need to split them into left- and right-segments, as we did with in the general case. This simplifies the computation of the transitive closure, assuming that R^k is consistent, for all $k \geq 1$[4].

Example 3. Let $R(\mathbf{x}, \mathbf{x}')$ be the following octagonal relation, where $\mathbf{x} = \{x_1, x_2\}$

$$R(\mathbf{x}, \mathbf{x}') = x_1 + x_2 \leq 5 \wedge x'_1 - x_1 \leq -2 \wedge x'_2 - x_2 \leq -3$$

Figure 3 shows the graph representation of R^k for $k = 1, 2, 3, \ldots$. The n step closure is

$$\begin{aligned} R^n(\mathbf{x}, \mathbf{x}') = {} & x_1 + x_2 \leq 5 \wedge x'_1 - x_1 \leq -2n \wedge x'_2 - x_2 \leq -3n \wedge \\ & x_1 + x'_2 \leq 5 - 3n \wedge x_2 + x'_1 \leq 5 - 2n \wedge x'_1 + x'_2 \leq 5 - 5n \end{aligned}$$

□

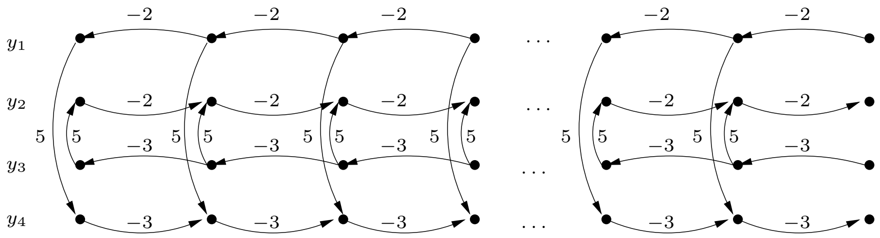

Fig. 3. Graph representation of $\overline{R}^k$, $k = 1, 2, 3, \ldots$

5 Implementation and Experience

We have implemented the method for computing transitive closures of octagonal relations in a tool for the analysis of counter automata, that we are currently developing. Table 1 shows several octagonal relations (first column), the closed

[4] The formula used to check consistency of $R(\mathbf{x}, \mathbf{x}')^k$, $k \geq 0$ is of size $\mathcal{O}(2^{2n \log 2n})$, where n is the number of variables in $\mathbf{x}$

form of their iteration (second column), the execution times (in milliseconds) needed to compute the closed forms without consistency checks (third column), and with consistency checks (fourth column). Notice that the first relation is the difference bound relation example from Section 2, for which no consistency check is needed.

R	R^n	*time (ms)*	
		−check	*+check*
$x_1 - x_2 \leq 0$ $x_2 - x_3 \leq 7$ $x_1 - x_1' \leq -1$ $x_3 - x_3' \leq -3$ $x_2' - x_2 \leq -2$	$x_1 - x_2 \leq 3 - 3n$ $x_1 - x_3 \leq 10 - 3n$ $x_2 - x_3 \leq 7$ $x_1 - x_1' \leq -n$ $x_1 - x_3' \leq 10 - 6n$ $x_2 - x_3' \leq 7 - 3n$ $x_3 - x_3' \leq -3n$ $x_2' - x_2 \leq -2n$ $x_2' - x_3 \leq 7 - 2n$ $x_2' - x_3' \leq 7 - 5n$	383	
$+x_1 + x_2' \leq -1$ $-x_2 - x_1' \leq -2$	$n \equiv_2 0 \Rightarrow +x_1 - x_1' \leq -3n/2$ $n \equiv_2 0 \Rightarrow +x_2' - x_2 \leq -3n/2$ $n \equiv_2 1 \Rightarrow +x_1 + x_2' \leq -1 - 3(n-1)/2$ $n \equiv_2 1 \Rightarrow -x_2 - x_1' \leq -2 - 3(n-1)/2$	75	116
$+x_1 - x_1' \leq 0$ $+x_1 + x_2' \leq -1$ $-x_2 - x_1' \leq -2$	$n \equiv_2 0 \Rightarrow +x_1 - x_1' \leq -3n/2$ $n \equiv_2 1 \Rightarrow +x_1 - x_1' \leq -3(n-1)/2$ $n \equiv_2 0 \Rightarrow +x_2' - x_2 \leq -3n/2$ $n \equiv_2 1 \wedge n \geq 3 \Rightarrow +x_2' - x_2 \leq -3 - 3(n-3)/2$ $n \equiv_2 0 \wedge n \geq 2 \Rightarrow +x_1 + x_2' \leq -1 - 3(n-2)/2$ $n \equiv_2 1 \Rightarrow +x_1 + x_2' \leq -1 - 3(n-1)/2$ $n \equiv_2 0 \wedge n \geq 2 \Rightarrow -x_2 - x_1' \leq -2 - 3(n-2)/2$ $n \equiv_2 1 \Rightarrow -x_2 - x_1' \leq -2 - 3(n-1)/2$	81	124
$+x_1 + x_2 \leq 5$ $+x_1' - x_1 \leq -2$ $+x_2' - x_2 \leq -3$	$+x_1 + x_2 \leq 5$ $+x_1' - x_1 \leq -2n$ $+x_2' - x_2 \leq -3n$ $+x_1 + x_2' \leq 5 - 3n$ $+x_2 + x_1' \leq 5 - 2n$ $+x_1' + x_2' \leq 5 - 5n$	11686	38729

Table 1. Experimental results

The tool, called FLATA, is implemented in Java(TM), and it is currently available at [9]. The execution times from Table 1 are relative to a Intel(R) Xeon(TM) CPU 3.00GHz equipped with 1 Gb of RAM. As an approximate upper bound, we can in principle handle difference bound relations on ten counters, and/or octagons on five counters, within reasonable execution times ($\approx$ 10 min).

6 Conclusions

We have considered the problem of computing transitive closures of octagonal relations, which are finite conjunctions of atomic formulae of the form $\pm x \pm y \leq c$, where x and y are possibly primed integer variables. We show that the k-th iteration of such a relation has a Presburger definable closed form. As a consequence, the transitive closure is also Presburger definable. This result enlarges the class of non-deterministic counter automata for which the reachability problem is decidable, to counter automata with octagonal transition relations. This result is expected to have an impact in the fields of software verification, as abstract models of software systems are described using octagons. We have implemented our method in a tool for the analysis of counter automata, and report on a number of experiments.

References

1. R. Bagnara. *Data-Flow Analysis for Constraint Logic-Based Languages*. Ph. D. Thesis, Dipartimento di Informatica, Università di Pisa, 1997.
2. Roberto Bagnara, Patricia M. Hill, and Enea Zaffanella. An improved tight closure algorithm for integer octagonal constraints. In *In Proc. Verification, Model Checking and Abstract Interpretation*, 2008.
3. B. Boigelot. On iterating linear transformations over recognizable sets of integers. *TCS*, 309(2):413–468, 2003.
4. Marius Bozga, Peter Habermehl, Radu Iosif, and Tomas Vojnar. A logic of singly indexed arrays. In *Intl. Conference on Logic Programming, Artificial Intellingence and Reasoning*, 2008.
5. Marius Bozga, Radu Iosif, and Yassine Lakhnech. Flat parametric counter automata. In *Proc. Intl. Conference on Automata, Languages and Programming (ICALP 2006)*, volume 4052, pages 577–588. LNCS, Springer-Verlag, 2006.
6. Hubert Comon and Yan Jurski. Multiple counters automata, safety analysis and presburger arithmetic. In *Proceedings of the 10th International Conference on Computer Aided Verification*, volume LNCS 1427, pages 268 – 279, 1998.
7. Patrick Cousot and Nicolas Halbwachs. Automatic discovery of linear restraints among variables of a program. In *Fifth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 84–97. ACM Press, 1978.
8. A. Finkel and J. Leroux. How to compose presburger-accelerations: Applications to broadcast protocols. In *Proc. FST&TCS*, volume 2556 of *LNCS*, pages 145–156. Springer, 2002.
9. http://www-verimag.imag.fr/~async/flata/flata.html.
10. Peter Habermehl, Radu Iosif, and Tomas Vojnar. What else is decidable about integer arrays? In *Proc. of Eleventh International Conference on Foundations of Software Science and Computation Structures*, 2008.
11. Warwick Harvey and Peter Stuckey. A unit two variable per inequality integer constraint solver for constraint logic programming. In *Australian Computer Science Conference*, pages 102–111, 1997.
12. O. H. Ibarra. Reversal-bounded multicounter machines and their decision problems. *Journal of the Association for Computing Machinery*, 25(1):116 – 133, January 1978.

13. J. Leroux and G. Sutre. Flat counter automata almost everywhere! In *Proc. ATVA*, volume 3707 of *LNCS*, pages 489–503. Springer, 2005.
14. A. Miné. The octagon abstract domain. *Higher-Order and Symbolic Computation*, 19(1):31–100, 2006.
15. M. Minsky. *Computation: Finite and Infinite Machines*. Prentice-Hall, 1967.
16. M. Presburger. Über die Vollstandigkeit eines gewissen Systems der Arithmetik. *Comptes rendus du I Congrés des Pays Slaves*, Warsaw 1929.
17. C. Reutenauer. *Aspects Mathématiques des Réseaux de Petri*. Collection Études et Recherches en Informatique. Masson, 1989.

A Proofs

Proof of Theorem 1:

Proof. (1) and (3) are equivalent, since $\gamma(m) = \{\mathbf{v} \mid \mathbf{v} \models \varphi\}$. The equivalence of (2) and (3) is Theorem 1 in [14]. □

Proof of Theorem 2:

Proof. W.l.o.g. we assume that $k = n$, and let $\mathbf{v}' = (v_1, v_2, \ldots, v_{n-1})$. Let $\mathcal{G}'$ be the restriction of $\mathcal{G}(m^*)$ to $(x_1, x_2, \ldots, x_{n-1})$, and m' be its $n-1 \times n-1$ incidence matrix. It is sufficient to show that:

$$\gamma(m') = \{(v_1, v_2, \ldots, v_{n-1}) \mid (v_1, v_2, \ldots, v_{n-1}, v) \in \gamma(m^*) \text{ for some } v \in \mathbb{Z}\}$$

The "$\supseteq$" direction is obvious, since m' is the restriction of m^* to $(x_1, x_2, \ldots, x_{n-1})$. For the "$\subseteq$" direction, we must show that there exists $v \in \mathbb{Z}$ such that $v_i - v \leq {m^*}_{i,n}$ and $v - v_j \leq {m^*}_{n,j}$, for all $1 \leq i, j \leq n$. But this amounts to $v_i - {m^*}_{i,n} \leq {m^*}_{n,j} + v_j$, for all $1 \leq i, j \leq n$. Since $(v_1, v_2, \ldots, v_{n-1}) \in \gamma(m')$ we have $v_i - v_j \leq {m^*}_{i,j}$, for all $1 \leq i, j \leq n$. Since m^* is closed, ${m^*}_{i,j} \leq {m^*}_{i,n} + {m^*}_{n,j}$, which leads to the conclusion. The DBM m' is closed as a direct consequence of the fact that m^* is closed. □

Proof of Lemma 1:

Proof. Coherence. By definition, $\beta(m)_{\bar{j},\bar{i}} = m_{\bar{j},\bar{i}}$ and $\beta(m)_{i,j} = m_{i,j}$. Since m is coherent, $m_{i,j} = m_{\bar{j}\bar{i}}\ \forall 1 \leq i, j < 2n-1$ and this implies that $\beta(m)_{i,j} = \beta(m)_{\bar{j},\bar{i}}\ \forall 1 \leq i, j < 2n-1$, therefore $\beta(m)$ is coherent.

Tight closure. The following conditions must hold:

1. $\beta(m)_{i,j} \leq \beta(m)_{i,l} + \beta(m)_{l,j}\ \forall 1 \leq i, j, l < 2n-1$. By the above definition, $\beta(m)_{i,j} = m_{i,j}$. Since m is tightly closed, $m_{i,j} \leq m_{i,l} + m_{l,j}\ \forall 1 \leq l < 2n-1$, and since all the nodes l of $\beta(m)$ are also nodes of m, this implies $\beta(m)_{ij} \leq \beta(m)_{il} + \beta(m)_{lj}\ \forall 1 \leq i, j, l < 2n-1$
2. $\beta(m)_{i,\bar{i}}$ is even $\forall 1 \leq i < 2n-1$. By definition, $\beta(m)_{i,\bar{i}} = m_{i,\bar{i}}$. Since m is tightly closed, $m_{i,\bar{i}}$ is even, therefore so is $\beta(m)_{i,\bar{i}}$

3. $\beta(m)_{i,i} = 0\ \forall 1 \leq i < 2n-1$. By definition, $\beta(m)_{i,i} = m_{i,i} = 0\ \forall 1 \leq i < 2n-1$, since m is tightly closed.
4. $\beta(m)_{i,j} \leq \frac{\beta(m)_{i,\bar{\imath}}+\beta(m)_{\bar{\jmath},j}}{2}\ \forall 1 \leq i,j < 2n-1$. Given the definition of β, we get, analogously, that this reduces to $m_{i,j} \leq \frac{m_{i,\bar{\imath}}+m_{\bar{\jmath},j}}{2}\ \forall 1 \leq i,j < 2n-1$ This is true since m is tightly closed, and this implies $\beta(m)_{i,j} \leq \frac{\beta(m)_{i,\bar{\imath}}+\beta(m)_{\bar{\jmath},j}}{2}\ \forall 1 \leq i,j < 2n-1$.

□

Proof of Theorem 4:

Proof. As stated before, we take x_k as x_n without loss of generality.

Let us find formula $\exists x_n.\phi(\mathbf{x})$, by means of the Fourier - Motzkin procedure.

$\phi(\mathbf{x}) = (\wedge \pm x_i \pm x_j \leq \alpha_{i,j}) \wedge (\wedge 2x_i \leq \beta_i) \wedge (\wedge -2x_i \leq \delta_i)$

Let

- $R_+(x_n) = \{(x_n + x_i \leq \alpha_{n,i}) \in AP(\phi)\} \cup \{(2x_n \leq \beta_n) \in AP(\phi)\} \cup \{(x_n - x_j \leq \alpha_{n,j}) \in AP(\phi)\}$,
- $R_-(x_n) = \{(x_l - x_n \leq \alpha_{l,n}) \in AP(\phi)\} \cup \{(-2x_n \leq \delta_n) \in AP(\phi)\}$ and
- $\psi(\mathbf{x}_{(-)}) = (\wedge \pm x_i \pm x_j \leq \alpha_{i,j}) \wedge (\wedge 2x_i \leq \beta_i) \wedge (\wedge -2x_i \leq \delta_i)$, where $\mathbf{x}_{(-)} = (x_1, x_2, ..., x_{n-1}) = \mathbf{x} \backslash x_n$, such that x_n does not occur in ψ.

Then $\phi(\mathbf{x}) = (\bigwedge_{\gamma_+ \in R_+(x_n)} \gamma_+) \wedge (\bigwedge_{\gamma_- \in R_-(x_n)} \gamma_-) \wedge \psi(\mathbf{x}_{(-)})$.

Sets $R_+(x_n)$ and $R_-(x_n)$ can be rewritten as:

$$\begin{cases} R_+(x_n) = \{(x_n \leq \alpha_{n,i} - x_i)\} \cup \{(x_n \leq [\frac{\beta_n}{2}])\} \cup \{(x_n \leq \alpha_{n,j} + x_j)\} \\ R_-(x_n) = \{(x_n \geq x_l - \alpha_{l,n})\} \cup \{(x_n \geq -[\frac{\delta_n}{2}])\} \end{cases} \quad (1)$$

and let

$$\begin{cases} V_+(x_n) = \{\alpha_+(\mathbf{x}_{(-)}) | (x_n \leq \alpha_+(\mathbf{x}_{(-)})) \in R_+(x_n)\} \\ V_-(x_n) = \{\alpha_-(\mathbf{x}_{(-)}) | (x_n \geq \alpha_-(\mathbf{x}_{(-)})) \in R_-(x_n)\} \end{cases} \quad (2)$$

Then $\exists x_n.\phi(\mathbf{x})$ is equivalent to $\psi(\mathbf{x}_{(-)}) \wedge (max(V_-(x_n)) \leq min(V_+(x_n)))$, which is in turn equivalent to

$\psi(\mathbf{x}_{(-)}) \wedge (\bigwedge_{\substack{\alpha_- \in V_-(x_n) \\ \alpha_+ \in V_+(x_n)}} \alpha_- \leq \alpha_+))$

Considering the definitions (1) and (2), $\exists x_n.\phi(\mathbf{x})$ can be rewritten as:

$$\psi(\mathbf{x}_{(-)}) \wedge \{x_l - \alpha_{l,n} \leq \alpha_{n,i} - x_i\} \wedge \{x_l - \alpha_{l,n} \leq \left[\frac{\beta_n}{2}\right]\} \wedge \{x_l - \alpha_{l,n} \leq \alpha_{n,j} + x_j\} \wedge$$

$$\wedge \{-\left[\frac{\delta_n}{2}\right] \leq \alpha_{n,i} - x_i\} \wedge \{-\left[\frac{\delta_n}{2}\right] \leq \left[\frac{\beta_n}{2}\right]\} \wedge \{-\left[\frac{\delta_n}{2}\right] \leq \alpha_{n,j} + x_j\}$$

and consequently as

$$\psi(\mathbf{x}_{(-)}) \wedge \{x_l + x_i \leq \alpha_{l,n} + \alpha_{n,i}\} \wedge \{x_l \leq \alpha_{l,n} + \left[\frac{\beta_n}{2}\right]\} \wedge \{x_l - x_j \leq \alpha_{l,n} + \alpha_{n,j}\} \wedge$$

$$\wedge\{x_i \leq \left\lceil\frac{\delta_n}{2}\right\rceil + \alpha_{n,i}\} \wedge \{0 \leq \left\lceil\frac{\delta_n}{2}\right\rceil + \left\lceil\frac{\beta_n}{2}\right\rceil\} \wedge \{-x_j \leq \left\lceil\frac{\delta_n}{2}\right\rceil + \alpha_{n,j}\} \quad (3)$$

Let m be the octagonal DBM of ϕ and m_t^* the tight closure of m. What we want to show is that:

$$\gamma^{Oct}(\beta(m_t^*)) = \{\mathbf{v}|(\exists x_n.\phi(\mathbf{x}))_{[\mathbf{v}/\mathbf{x}_{(-)}]} = T\} \quad (4)$$

or in other words

$$\gamma^{Oct}(\beta(m_t^*)) = \{(v_1, v_2, ..., v_{n-1})|(v_1, v_2, ..., v_{n-1}, v_n) \models \phi(\mathbf{x}), v_n \in \mathbb{Z}\} \quad (5)$$

1. $\gamma^{Oct}(\beta(m_t^*)) \subseteq \{(v_1, v_2, ..., v_{n-1})|(v_1, v_2, ..., v_{n-1}, v_n) \models \phi(\mathbf{x}), v_n \in \mathbb{Z}\}$
   Let $\mathbf{v} \in \gamma^{Oct}(\beta(m_t^*))$. We want to prove that $\mathbf{v}$ satisfies (3), and for that it must satisfy each term in (3):
   - *term* $\psi(\mathbf{x}_{(-)})$
     Since $\mathbf{v} \in \gamma^{Oct}(\beta(m_t^*))$ and by definition of β, it means that $\mathbf{v}$ satisfies all the constraints in m_t^* that do not imply x_n. Since $\gamma^{Oct}(m_t^*) = \gamma^{Oct}(m) \subseteq \{\mathbf{v}|(\phi(\mathbf{x}))_{[\mathbf{v}/\mathbf{x}]} = T\}$, this means that $\mathbf{v}$ also satisfies the part of ϕ not concerning x_n. But by definition of ψ, this part of ϕ is exactly ψ, therefore $\mathbf{v}$ satisfies $\psi(\mathbf{x}_{(-)})$.
   - *terms* $x_l + x_i \leq \alpha_{l,n} + \alpha_{n,i}$, *for* $(x_n + x_i \leq \alpha_{n,i}) \in \phi$ *and* $(x_l - x_n \leq \alpha_{l,n}) \in \phi$
     Since $(x_n + x_i \leq \alpha_{n,i}) \in \phi$ and $(x_l - x_n \leq \alpha_{l,n}) \in \phi$, there are in m_t^* arcs:
     $$\begin{cases} m^*_{t\ 2n-1,2i} & \leq \alpha_{n,i} \\ m^*_{t\ 2l-1,2n-1} & \leq \alpha_{l,n} \end{cases}$$
     Since m_t^* is tightly closed,
     $$m^*_{t\ 2l-1,2i} \leq m^*_{t\ 2l-1,2n-1} + m^*_{t\ 2n-1,2i} \leq \alpha_{l,n} + \alpha_{n,i}$$
     Since $l \neq n$ and $i \neq n$, it means that $l < n$ and $i < n$ and also $2l-1 < 2n-1$ and $2i < 2n-1$ therefore, by definition of β, $\beta(m_t^*)_{2l-1,2i} = m^*_{t\ 2l-1,2i}$:
     $$\beta(m_t^*)_{2l-1,2i} \leq \alpha_{l,n} + \alpha_{n,i}$$
     But $\mathbf{v} \in \gamma^{Oct}(\beta(m_t^*))$ therefore
     $$v_l - (-v_i) \leq \beta(m)_{2l-1,2i}$$
     which by the previous equation leads to
     $$v_l + v_i \leq \alpha_{l,n} + \alpha_{n,i}$$
     Therefore $\mathbf{v}$ satisfies this type of constraint.
   - *terms* $x_l \leq \alpha_{l,n} + \left\lceil\frac{\beta_n}{2}\right\rceil$, *for* $(x_l - x_n \leq \alpha_{l,n}) \in \phi$ *and* $(2x_n \leq \beta_n) \in \phi$
     Since $(x_l - x_n \leq \alpha_{l,n}) \in \phi$ and $(2x_n \leq \beta_n) \in \phi$, there are in m_t^* arcs:
     $$\begin{cases} m^*_{t\ 2n-1,2n} & \leq \beta_n \\ m^*_{t\ 2l-1,2n-1} & \leq \alpha_{l,n} \\ m^*_{t\ 2n,2l} & \leq \alpha_{l,n} \end{cases}$$

Since m_t^* is tightly closed,

$$m^*_{t\ 2l-1,2l} \leq m^*_{t\ 2l-1,2n-1} + m^*_{t\ 2n-1,2n} + m^*_{t\ 2n,2l} \leq \alpha_{l,n} + \beta_n + \alpha_{l,n}$$

Since $l \neq n$, it means that $l < n$ and also $2l-1 < 2n-1$ and $2l < 2n-1$ therefore, by definition of β, $\beta(m_t^*)_{2l-1,2l} = m^*_{t\ 2l-1,2l}$:

$$\beta(m_t^*)_{2l-1,2l} \leq 2\alpha_{l,n} + \beta_n$$

Furthermore, by Lemma 1, $\beta(m_t^*)$ is tightly closed, therefore $\beta(m_t^*)_{2l-1,2l}$ is even, so

$$\beta(m_t^*)_{2l-1,2l} \leq 2\alpha_{l,n} + 2\left[\frac{\beta_n}{2}\right]$$

But $\mathbf{v} \in \gamma^{Oct}(\beta(m_t^*))$ therefore

$$2\ v_l \leq \beta(m_t^*)_{2l-1,2l}$$

which by the previous equation leads to

$$v_l \leq \alpha_{l,n} + \left[\frac{\beta_n}{2}\right]$$

Therefore $\mathbf{v}$ satisfies this type of constraint.

– *terms* $x_l - x_j \leq \alpha_{l,n} + \alpha_{n,j}$, *for* $(x_l - x_n \leq \alpha_{l,n}) \in \phi$ *and* $(x_n - x_j \leq \alpha_{n,j}) \in \phi$

Since $(x_n - x_j \leq \alpha_{n,j}) \in \phi$ and $(x_l - x_n \leq \alpha_{l,n}) \in \phi$, there are in m_t^* arcs:

$$\begin{cases} m^*_{t\ 2n-1,2j-1} \leq \alpha_{n,j} \\ m^*_{t\ 2l-1,2n-1} \leq \alpha_{l,n} \end{cases}$$

Since m_t^* is tightly closed,

$$m^*_{t\ 2l-1,2j-1} \leq m^*_{t\ 2l-1,2n-1} + m^*_{t\ 2n-1,2j-1} \leq \alpha_{l,n} + \alpha_{n,j}$$

Since $l \neq n$ and $j \neq n$, it means that $l < n$ and $j < n$ and also $2l-1 < 2n-1$ and $2j-1 < 2n-1$ therefore, by definition of β, $\beta(m_t^*)_{2l-1,2j-1} = m^*_{t\ 2l-1,2j-1}$:

$$\beta(m_t^*)_{2l-1,2j-1} \leq \alpha_{l,n} + \alpha_{n,j}$$

But $\mathbf{v} \in \gamma^{Oct}(\beta(m_t^*))$ therefore

$$v_l - v_j \leq \beta(m_t^*)_{2l-1,2j-1}$$

which by the previous equation leads to

$$v_l - v_j \leq \alpha_{l,n} + \alpha_{n,j}$$

Therefore $\mathbf{v}$ satisfies this type of constraint.

– *terms* $x_i \leq \left[\frac{\delta_n}{2}\right] + \alpha_{n,i}$, *for* $(x_n + x_i \leq \alpha_{n,i}) \in \phi$ *and* $(-2x_n \leq \delta_n) \in \phi$
Since $(x_n + x_i \leq \alpha_{n,i}) \in \phi$ and $(-2x_n \leq \delta_n) \in \phi$, there are in m_t^* arcs:

$$\begin{cases} m^*_{t\ 2n-1,2i} \leq \alpha_{n,i} \\ m^*_{t\ 2i-1,2n} \leq \alpha_{n,i} \\ m^*_{t\ 2n,2n-1} \leq \delta_n \end{cases}$$

Since m_t^* is tightly closed,

$$m^*_{t\ 2i-1,2i} \leq m^*_{t\ 2i-1,2n} + m^*_{t\ 2n,2n-1} + m^*_{t\ 2n-1,2i} \leq 2\ \alpha_{n,i} + \delta_n$$

Since $i \neq n$, it means that $i < n$ and also $2i-1 < 2n-1$ and $2i < 2n-1$ therefore, by definition of β, $\beta(m_t^*)_{2i-1,2i} = m^*_{t\ 2i-1,2i}$:

$$\beta(m_t^*)_{2i-1,2i} \leq 2\ \alpha_{n,i} + \delta_n$$

Furthermore, by Lemma 1, $\beta(m_t^*)$ is tightly closed, therefore $\beta(m_t^*)_{2i-1,2i}$ is even, so

$$\beta(m_t^*)_{2i-1,2i} \leq 2\alpha_{n,i} + 2\left[\frac{\delta_n}{2}\right]$$

But $\mathbf{v} \in \gamma^{Oct}(\beta(m_t^*))$ therefore

$$2\ v_i \leq \beta(m_t^*)_{2i-1,2i}$$

which by the previous equation leads to

$$v_i \leq \alpha_{n,i} + \left[\frac{\delta_n}{2}\right]$$

Therefore $\mathbf{v}$ satisfies this type of constraint.

– *terms* $-x_j \leq \left[\frac{\delta_n}{2}\right] + \alpha_{n,j}$, *for* $(x_n - x_j \leq \alpha_{n,j}) \in \phi$ *and* $(-2x_n \leq \delta_n) \in \phi$
Since $(x_n - x_j \leq \alpha_{n,j}) \in \phi$ and $(-2x_n \leq \delta_n) \in \phi$, there are in m_t^* arcs:

$$\begin{cases} m^*_{t\ 2n-1,2j-1} \leq \alpha_{n,j} \\ m^*_{t\ 2j,2n} \leq \alpha_{n,j} \\ m^*_{t\ 2n,2n-1} \leq \delta_n \end{cases}$$

Since m_t^* is tightly closed,

$$m^*_{t\ 2j,2j-1} \leq m^*_{t\ 2j,2n} + m^*_{t\ 2n,2n-1} + m^*_{t\ 2n-1,2j-1} \leq 2\ \alpha_{n,j} + \delta_n$$

Since $j \neq n$, it means that $j < n$ and also $2j-1 < 2n-1$ and $2j < 2n-1$ therefore, by definition of β, $\beta(m_t^*)_{2j,2j-1} = m^*_{t\ 2j,2j-1}$:

$$\beta(m)_{2j,2j-1} \leq 2\ \alpha_{n,j} + \delta_n$$

Furthermore, by Lemma 1, $\beta(m_t^*)$ is tightly closed, therefore $\beta(m_t^*)_{2j,2j-1}$ is even, so

$$\beta(m_t^*)_{2j,2j-1} \leq 2\alpha_{n,j} + 2\left[\frac{\delta_n}{2}\right]$$

But $\mathbf{v} \in \gamma^{Oct}(\beta(m_t^*))$ therefore

$$-2\ v_j \leq \beta(m_t^*)_{2j,2j-1}$$

which by the previous equation leads to

$$-v_j \leq \alpha_{n,j} + \left\lceil \frac{\delta_n}{2} \right\rceil$$

Therefore $\mathbf{v}$ satisfies this type of constraint.

– *terms* $0 \leq \left\lceil \frac{\delta_n}{2} \right\rceil + \left\lceil \frac{\beta_n}{2} \right\rceil$, *for* $(2x_n \leq \beta_n) \in \phi$ *and* $(-2x_n \leq \delta_n) \in \phi$
Since $(2x_n \leq \beta_n) \in \phi$ and $(-2x_n \leq \delta_n) \in \phi$, there are in m_t^* arcs:

$$\begin{cases} m^*_{t\ 2n,2n-1} \leq \delta_n \\ m^*_{t\ 2n-1,2n} \leq \beta_n \end{cases}$$

Since m_t^* is tightly closed, $m^*_{t\ 2n,2n-1}$ and $m^*_{t\ 2n-1,2n}$ are even and then the following hold:

$$\begin{cases} m^*_{t\ 2n,2n-1} \leq 2\ \left\lceil \frac{\delta_n}{2} \right\rceil \\ m^*_{t\ 2n-1,2n} \leq 2\ \left\lceil \frac{\beta_n}{2} \right\rceil \end{cases}$$

Since m is by hypothesis *consistent*, therefore there are no negative weight cycles, m_t^* is also consistent and tightly closed, and therefore

$$m^*_{t\ 2n,2n} = 0 \leq m^*_{t\ 2n,2n-1} + m^*_{t\ 2n-1,2n} \leq 2\left\lceil \frac{\delta_n}{2} \right\rceil + 2\left\lceil \frac{\beta_n}{2} \right\rceil$$

and equivalently

$$0 \leq \left\lceil \frac{\delta_n}{2} \right\rceil + \left\lceil \frac{\beta_n}{2} \right\rceil$$

Therefore this constraint is already satisfied, given ϕ is consistent.

2. $\gamma^{Oct}(\beta(m_t^*)) \supseteq \{(v_1, v_2, ..., v_{n-1}) | (v_1, v_2, ..., v_{n-1}, v_n) \models \phi(\mathbf{x}), v_n \in \mathbb{Z}\}$
By definition of the tight closure (Definition 9),

$$\{\mathbf{v} | (\phi(\mathbf{x}))_{[\mathbf{v}/\mathbf{x}]} = T\} = \gamma^{Oct}(m) = \gamma^{Oct}(m_t^*) = \{\mathbf{v} | (\phi_t^*(\mathbf{x}))_{[\mathbf{v}/\mathbf{x}]} = T\} \quad (6)$$

where

$$\begin{aligned} \phi_t^*(\mathbf{x}) = (&\bigwedge_{i\ odd, j\ odd} x_{(i+1)/2} - x_{(j+1)/2} \leq (m_t^*)\ _{i,j}) \wedge (\bigwedge_{i\ even, j\ odd} -x_{i/2} - x_{(j+1)/2} \leq (m_t^*)\ _{i,j}) \wedge \\ &\wedge (\bigwedge_{i\ odd, j\ even} x_{(i+1)/2} + x_{j/2} \leq (m_t^*)\ _{i,j}) \wedge (\bigwedge_{i\ even, j\ even} -x_{i/2} + x_{j/2} \leq (m_t^*)\ _{i,j}) \wedge \\ &\wedge (\bigwedge_{i\ even} 2\ x_{(i+1)/2} \leq (m_t^*)\ _{i,i+1}) \wedge (\bigwedge_{i\ odd} -2\ x_{i/2} \leq (m_t^*)\ _{i,i-1}) \end{aligned} \quad (7)$$

Let $\mathbf{v} \in \{(v_1, v_2, ..., v_{n-1}) | (v_1, v_2, ..., v_{n-1}, v_n) \models \phi(\mathbf{x})\}$ and let i, j be indices in $\beta(m_t^*)$. We want to prove that for any $1 \leq i, j < 2n-1$, $\mathbf{v}$ satisfies the constraint encoded by $\beta(m_t^*)_{i,j}$, namely $x_i - x_j \leq \beta(m_t^*)_{i,j}$. Note that i and j are less than $2n-1$ by definition of β and therefore the constraint is equivalent to $x_i - x_j \leq m^*_{t\ i,j}$. There are six cases that must be proven for $\mathbf{v}$:

– i and j are odd: $v_{(i+1)/2} - v_{(j+1)/2} \leq (m_t^*)_{\ i,j}$
– i is odd and j is even: $v_{(i+1)/2} + v_{j/2} \leq (m_t^*)_{\ i,j}$
– i is even and j is odd: $-v_{i/2} - v_{(j+1)/2} \leq (m_t^*)_{\ i,j}$
– i and j are even: $-v_{i/2} + v_{j/2} \leq (m_t^*)_{\ i,j}$
– i is odd and $j = i+1$ and is therefore even: $2\ v_{(i+1)/2} \leq (m_t^*)_{\ i,i+1}$
– i is even and $j = i-1$ and is therefore odd: $-2\ v_{i/2} \leq (m_t^*)_{\ i,i-1}$

Now, since $\mathbf{v} \in \{(v_1, v_2, ..., v_{n-1}) | (v_1, v_2, ..., v_{n-1}, v_n) \models \phi(\mathbf{x})\}$ it also means that $\mathbf{v} \in \{\mathbf{v} | (\psi(\mathbf{x}_{(-)})_{[\mathbf{x}/\mathbf{v}]} = T\}$ and by (6) ψ is also equivalent to the part of ϕ_t^* not containing constraints on x_n, therefore $\mathbf{v}$ satisfies all the constraints in (7) not concerning x_n. But this also means it satisfies the constraints of all the six cases given above, since x_n does not occur in $\beta(m_t^*)$.

Since the arc $\beta(m_t^*)_{ij}$ has been taken at random, we can infer that all the arcs of $\beta(m_t^*)$ are satisfied by $\mathbf{v}$, therefore, since again $\mathbf{v}$ has been taken at random from $\{(v_1, v_2, ..., v_{n-1}) | (v_1, v_2, ..., v_{n-1}, v_n) \models \phi(\mathbf{x}), v_n \in \mathbb{Z}\}$,

$$\gamma^{Oct}(\beta(m_t^*)) \supseteq \{(v_1, v_2, ..., v_{n-1}) | (v_1, v_2, ..., v_{n-1}, v_n) \models \phi(\mathbf{x}), v_n \in \mathbb{Z}\}$$

This concludes the proof of equivalence. The closure of $\beta(m_t^*)$ follows from Lemma 1. □