Deciding Conditional Termination

Radu Iosif, Filip Konecny, Marius Bozga

Logical Methods in Computer Science
Vol. 10(3:8)2014, pp. 1–61
www.lmcs-online.org

Submitted Sep. 30, 2012
Published Aug. 21, 2014

DECIDING CONDITIONAL TERMINATION

MARIUS BOZGA[a], RADU IOSIF[b], AND FILIP KONEČNÝ[c]

[a,b] Univ. Grenoble Alpes/CNRS/VERIMAG, F-38000, Grenoble France
e-mail address: {bozga,iosif}@imag.fr

[c] EPFL IC IIF LARA, Station 14, 1015 Lausanne, Switzerland
e-mail address: filip.konecny@epfl.ch

Abstract. We address the problem of conditional termination, which is that of defining the set of initial configurations from which a given program always terminates. First we define the dual set, of initial configurations from which a non-terminating execution exists, as the greatest fixpoint of the function that maps a set of states into its pre-image with respect to the transition relation. This definition allows to compute the weakest non-termination precondition if at least one of the following holds: (i) the transition relation is deterministic, (ii) the descending Kleene sequence over-approximating the greatest fixpoint converges in finitely many steps, or (iii) the transition relation is well founded. We show that this is the case for two classes of relations, namely octagonal and finite monoid affine relations. Moreover, since the closed forms of these relations can be defined in Presburger arithmetic, we obtain the decidability of the termination problem for such loops.

We show that the weakest non-termination precondition for octagonal relations can be computed in time polynomial in the size of the binary representation of the relation. Furthermore, for every well-founded octagonal relation, we prove the existence of an effectively computable well-founded witness relation for which a linear ranking function exists. For the class of linear affine relations we show that the weakest non-termination precondition can be defined in Presburger arithmetic if the relation has the finite monoid property. Otherwise, for a more general subclass, called polynomially bounded affine relations, we give a method of under-approximating the termination preconditions.

Finally, we apply the method of computing weakest non-termination preconditions for conjunctive relations (octagonal or affine) to computing termination preconditions for programs with complex transition relations. We provide algorithms for computing transition invariants and termination preconditions, and define a class of programs, whose control structure has no nested loops, for which these algorithms provide precise results. Moreover, it is shown that, for programs with no nested control loops, and whose loops are labeled with octagonal constraints, the dual problem i.e. the existence of infinite runs, is NP-complete.

2012 ACM CCS: [**Software and its engineering**]: Software creation and management—Software verification and validation; Software organization and properties—Software functional properties—Formal methods—Model checking.

Key words and phrases: Integer Programs, Periodic Relations, Recurrent Sets, Termination Preconditions.

[a,b] Supported by the French National Research Agency (project ANR-09-SEGI-016 VERIDYC).
[b,c] Supported by the Rich Model Toolkit initiative (formally ESF COST action IC0901).
[c] Supported by the Czech Science Foundation (project P103/10/0306).

DOI:10.2168/LMCS-10(3:8)2014

1. Introduction

The termination problem asks whether every computation of a given program ends in a halting state. The universal termination problem asks whether a given program always terminates for every possible input configuration. Both problems are among the first ever to be shown undecidable, by A. Turing [43]. In many cases however, programs will terminate when started in certain configurations, and may[1] run forever, when started in other configurations. The problem of determining the set of configurations from which a program terminates on all paths is called *conditional termination.*

In this paper we focus on programs that handle integer variables, performing Presburger arithmetic tests and (possibly non-deterministic) updates. A first observation is that the set of configurations from which an infinite computation is possible is the greatest fixpoint of the pre-image pre_R of the program's transition relation[2] R. This set, called the *weakest recurrent set*, and denoted $\mathrm{wrs}(R)$ in our paper, is the limit of the descending sequence $\mathrm{pre}^0_R(\mathbf{true}), \mathrm{pre}^1_R(\mathbf{true}), \mathrm{pre}^2_R(\mathbf{true}), \ldots$, i.e. $\mathrm{wrs}(R) = \bigcap_{i=1}^{\infty} pre^n_R(\mathbf{true})$, if either (i) the pre-image of the transition relation is continuous (this is the case, for instance, when the transition relation is deterministic), (ii) the descending Kleene sequence that over-approximates the greatest fixpoint eventually stabilizes, or (iii) the relation is well founded, i.e. $\mathrm{wrs}(R) = \emptyset$. If, moreover, the closed form defining the infinite sequence of precondition sets $\{\mathrm{pre}^n_R(\mathbf{true})\}_{n\geq 1}$ can be defined using a decidable fragment of arithmetic, we obtain decidability proofs for the universal termination problem.

Contributions of this paper. The main novelty in this paper is of rather theoretical nature: we show that the non-termination preconditions for integer transition relations defined as either *octagons* or *linear affine loops with finite monoid property* are definable in quantifier-free Presburger arithmetic. Thus, the universal termination problem for such program loops is decidable. However, since quantifier elimination in Presburger arithmetic is a complex procedure, we have developed alternative ways of deriving the preconditions for non-termination, and in particular:

- for *octagonal relations*, we use a result from [10], namely that the sequence $\{R^i\}_{i\geq 0}$ is, in some sense, periodic. Based on this, we develop an algorithm that computes the weakest non-termination precondition of R in time polynomial in the size of the binary representation of R. Moreover, we investigate the existence of linear ranking functions and prove that for each well-founded octagonal relation, there exists an effectively computable witness relation for R, i.e. a relation that is well-founded if and only if the original relation is well-founded and, in this case, it also has a linear ranking function.
- for *linear affine relations*, weakest recurrent sets can be defined in Presburger arithmetic if we consider several restrictions concerning the transformation matrix. If the matrix A defining R has eigenvalues which are either zeros or roots of unity, all non-zero eigenvalues being of multiplicity one (these conditions are equivalent to the finite monoid property of [5, 21]), then $\mathrm{wrs}(R)$ is Presburger definable. Otherwise, if all non-zero eigenvalues of A are roots of unity, of multiplicities greater or equal to one, $\mathrm{wrs}(R)$ can be expressed

[1] If the program is non-deterministic, the existence of a single infinite run, among other finite runs, suffices to consider an initial configuration non-terminating.

[2] This definition is the dual of the *reachability set*, needed for checking safety properties: the reachability set is the least fixpoint of the post-image of the transition relation.

using polynomial terms. In this case, we can systematically issue Presburger termination preconditions, which are safe under-approximations of the complement of the $\mathrm{wrs}(R)$ set.

Unfortunately, in practice, the cases in which the closed form of the sequence of preconditions $\{\mathrm{pre}_R^n(\mathbf{true})\}_{n\geq 0}$ is definable in a decidable fragment of arithmetic, are fairly rare. All relations considered so far are conjunctive, meaning that they can represent only simple program loops of the form `while(condition){body}` where the loop body contains no further conditional constructs. Whereas in reality such simple programs are rare, our results can be used as building blocks of other termination proof methods [17], which discard *lasso-shaped* non-termination counterexamples one by one. Our method can be used for proving non-termination as well, by embedding it into general algorithms, such as [24].

In order to deal with more complicated program loops, we use the method of *transition invariants* [34] to compute safe under-approximations of the strongest termination preconditions. Concretely, we compute a *transition invariant*, which is an over-approximation of the transitive closure of the transition relation of the program, restricted to the states reachable from some set of initial configurations. If one can find a finite union $R_1^\# \cup \ldots \cup R_m^\#$ of octagonal relations that is a transition invariant, then we can compute an over-approximation of the weakest non-termination precondition as $\mathrm{wrs}(R_1^\#) \cup \ldots \cup \mathrm{wrs}(R_m^\#)$. The required termination precondition is the complement of this set.

This method can infer non-termination preconditions for programs without procedure calls. It is moreover shown to be complete, and to yield the precise result for a class of programs without nested loops, called *flat*. Moreover, we studied a restriction of flat programs in which all transitions within loops are labeled with octagonal constraints, and found that, for this restricted class, the problem of existence of infinite runs is NP-complete.

We have implemented the computation of transition invariants and procedure summaries in the FLATA tool for the analysis of integer programs. Several experiments on inferring non-termination preconditions have been performed, and reported.

Roadmap. The paper is organized as follows. Section 2 introduces the notation and some basic concepts needed throughout the paper. Section 3 defines weakest recurrent sets as greatest fixpoints of the pre-image of the transition relation. Sections 4 and 5 apply this definition to the computation of weakest recurrent sets for octagonal and linear affine relations. Section 6 extends the computation of weakest termination preconditions from simple conjunctive loops to integer programs, and Section 7 reports on the implementation and experiments performed on several integer programs. Finally, Section 8 concludes.

The core results presented in this paper have been reported in [11]. In addition to the work presented in [11], here we improve the time complexity upper bound for the computation of weakest non-termination preconditions for octagonal relations, and give a polynomial time algorithm. Moreover, we extend the results from [11] from simple conjunctive program loops to computing non-termination preconditions for full integer programs (whose transition rules are defined using quantifier-free Presburger arithmetic), by giving a decidability result to the universal termination problem, for a class of *flat* programs, i.e. without nested loops, and no branching within loops.

1.1. **Related Work.**

The literature on program termination is vast. Most work focuses however on universal termination, i.e. the question if a program will always terminate on all inputs, such as the techniques for synthesizing linear ranking functions of Sohn and Van Gelder [40] or Podelski and Rybalchenko [33], and the more sophisticated method of Bradley, Manna and Sipma [13], which synthesizes lexicographic polynomial ranking functions, suitable when dealing with disjunctive loops. However, not every terminating program (loop) has a linear (polynomial) ranking function. In this paper, we show that for an entire class of non-deterministic linear relations, defined using octagons, termination is always witnessed by a computable octagonal relation that has a linear ranking function.

A closely related work direction investigates the termination of programs abstracted using *size-change graphs*, i.e. graphs in which nodes are variables and edges indicate the decrease of values in a well-founded domain. In [3] the size-change termination problem is investigated for graphs annotated with difference bounds constraints. It is shown that, even if the general problem is undecidable, the restriction to size-change graphs with at most one incoming size-change arc per variable is PSPACE-complete. Our results are incomparable, since we consider multiple incoming size-change arcs, but restrict the control structure of the decidable class of programs to be *flat*, i.e. no nested loops are allowed. Moreover, we focus on the problem of computing the weakest non-termination precondition for simple loops labeled with octagonal relations, and solve it using a PTIME algorithm.

Another line of work considers the decidability of termination for simple (conjunctive) linear loops. Initially, Tiwari [42] showed decidability of termination for affine linear loops interpreted over *reals*, while Braverman [14] refined this result by showing decidability over *rationals* and over *integers*, for homogeneous relations of the form $C_1\mathbf{x} > 0 \ \wedge \ C_2\mathbf{x} \geq 0 \ \wedge \ \mathbf{x}' = A\mathbf{x}$. The non-homogeneous integer case seems to be much more difficult as it is closely related to the open *Skolem's Problem* (see, e.g. [31] for a discussion on this problem): given a linear recurrence $\{u_i\}_{i\geq 0}$, determine whether $u_i = 0$ for some $i \geq 0$. The related problem of existence of linear ranking functions for linear affine loops has been studied in [4]. This problem has been found to be in PTIME when the program variables range over mathematical reals, and coNP-complete when they range over integers.

To our knowledge, the first work on proving the existence of non-terminating computations is arguably [32], in the context of Constraint Logic Programming. Another important contribution, which considers simple imperative loops, is reported in [24]. The notion of *recurrent sets* occurs in this work, however, without the connection with fixpoint theory, which is introduced in the present work. Finding recurrent sets in [24] is complete with respect to a predefined set of templates, typically linear systems of rational inequalities.

The work which is closest to ours is probably that of Cook et al. [16]. In that paper, the authors develop an algorithm for deriving termination preconditions by first guessing a ranking function candidate (typically the linear term from the loop condition) and then inferring a supporting assertion which guarantees that the candidate function decreases with each iteration. The step of finding a supporting assertion requires a fixpoint iteration in order to find an invariant condition. Unlike our work, the authors of [16] do not address issues related to completeness: the method is not guaranteed to find the weakest precondition for termination, even in cases when this set can be computed. On the other hand, it is applicable to a large range of programs extracted from real-life software. To compare our method with theirs, we tried the examples available in [16]. For those which are polynomially bounded affine relations, we used our under-approximation method and have computed termination preconditions, which turn out to be slightly more general than the ones reported in [16].

2. Preliminary Definitions

We denote by $\mathbb{Z}$, $\mathbb{N}$ and $\mathbb{N}_+$ the sets of integers, positive (including zero) and strictly positive integers, respectively. We denote by $\mathbb{Z}_\infty$ and $\mathbb{Z}_{-\infty}$ the sets $\mathbb{Z} \cup \{\infty\}$ and $\mathbb{Z} \cup \{-\infty\}$, respectively. In this paper we use a set of variables $\mathbf{x} = \{x_1, x_2, \ldots, x_N\}$, for a given integer constant $N > 0$. The set of *primed* variables is $\mathbf{x}' = \{x'_1, x'_2, \ldots, x'_N\}$. These variables are assumed to be ranging over $\mathbb{Z}$. For a set $S \subseteq \mathbb{Z}$ of integers, we denote by $\min S$ the smallest integer $s \in S$, if one exists, and by $\inf S$ the largest element $m \in \mathbb{Z}_{-\infty}$ such that $m \leq s$, for all $s \in S$. If $S = \emptyset$, we convene that $\min S = \inf S = \infty$.

A *linear term* $t(\mathbf{x})$ over a set of variables in $\mathbf{x}$ is a linear combination of the form $a_0 + \sum_{i=1}^{N} a_i x_i$, where $a_0, a_1, \ldots, a_N \in \mathbb{Z}$. *Presburger arithmetic* is the first-order logic over *atomic propositions* of the form $t(\mathbf{x}) \leq 0$. Presburger arithmetic has quantifier elimination and is decidable [35]. Moreover, the satisfiability of its *quantifier-free fragment* is NP-complete in the size of the binary representation of the formula [44]. For simplicity, we consider only formulas in Presburger arithmetic in this paper.

For a first-order logical formula φ, let $FV(\varphi)$ denote the set of its free variables. By writing $\varphi(\mathbf{x})$ we imply that $FV(\varphi) \subseteq \mathbf{x}$. For a formula $\varphi(\mathbf{x})$, we denote by $\varphi[t_1/x_1, \ldots, t_N/x_N]$ the formula obtained from φ by syntactically replacing each free occurrence of $x_1, \ldots, x_N$ with the terms $t_1, \ldots, t_N$, respectively. For a first-order logical formula φ, let $Atom(\varphi)$ denote the set of atomic propositions in φ.

A *valuation* of $\mathbf{x}$ is a function $\nu : \mathbf{x} \to \mathbb{Z}$. The set of all such valuations is denoted by $\mathbb{Z}^{\mathbf{x}}$. If $\nu \in \mathbb{Z}^{\mathbf{x}}$, we denote by $\nu \models \varphi$ the fact that the formula obtained from φ by replacing each occurrence of x_i with $\nu(x_i)$ is valid. Similarly, an arithmetic formula $\phi_R(\mathbf{x}, \mathbf{x}')$ defining a relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is evaluated with respect to two valuations ν_1 and ν_2, by replacing each occurrence of x_i with $\nu_1(x_i)$ and each occurrence of x'_i with $\nu_2(x_i)$. The satisfaction relation is denoted $(\nu_1, \nu_2) \models \phi_R$. By $\models \varphi$ we denote the fact that φ is *valid*, i.e. logically equivalent to **true**. We say that an arithmetic formula $\varphi(\mathbf{x})$ is *consistent* if there exists a valuation ν such that $\nu \models \varphi$. We use the symbols $\Rightarrow, \Leftrightarrow$ to denote logical implication and equivalence, respectively. The consistency of a formula φ is usually denoted by writing $\varphi \not\Leftrightarrow \mathbf{false}$. In the following, we will sometimes abuse notation and use the same symbols for relations (sets) and their defining formulas.

The composition of two relations $R_1, R_2 \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is defined as $R_1 \circ R_2 = \{(\nu, \nu') \in \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}} \mid \exists \nu'' \in \mathbb{Z}^{\mathbf{x}} \,.\, (\nu, \nu'') \in R_1 \ \wedge \ (\nu'', \nu') \in R_2\}$. The *identity relation* on $\mathbf{x}$ is defined as $\mathcal{I}_{\mathbf{x}} = \{(\nu, \nu) \mid \nu \in \mathbb{Z}^{\mathbf{x}}\}$. For any relation $R \subseteq \mathbb{Z}^{\mathbf{x}}$, we define $R^0 = \mathcal{I}_{\mathbf{x}}$ and $R^{i+1} = R^i \circ R$, for all $i \geq 0$. The relation R^i is called the *i-th power* of R in the sequel. With these notations, $R^+ = \bigcup_{i=1}^{\infty} R^i$ denotes the *transitive closure* of R, and $R^* = R^+ \cup \mathcal{I}_{\mathbf{x}}$ denotes the *reflexive and transitive closure* of R. A relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is said to be *deterministic* if and only if $(\nu, \nu') \in R$ and $(\nu, \nu'') \in R$ implies $\nu' = \nu''$, for all $\nu, \nu', \nu'' \in \mathbb{Z}^{\mathbf{x}}$. Let $\mathrm{pre}_R : 2^{\mathbb{Z}^{\mathbf{x}}} \to 2^{\mathbb{Z}^{\mathbf{x}}}$ be the *pre-image* function defined as $\mathrm{pre}_R(S) = \{\nu \mid \exists \nu' \in S \,.\, (\nu, \nu') \in R\}$, for any $S \subseteq \mathbb{Z}^{\mathbf{x}}$.

A function $F : 2^{\mathbb{Z}^{\mathbf{x}}} \to 2^{\mathbb{Z}^{\mathbf{x}}}$ is said to be *monotonic* if and only if $S \subseteq T$ implies $F(S) \subseteq F(T)$, for any two sets $S, T \subseteq \mathbb{Z}^{\mathbf{x}}$, and $\cap$*-continuous* if and only if $F(\cap_{i=1}^{\infty} S_i) = \cap_{i=1}^{\infty} F(S_i)$, for any infinite sequence $\{S_i\}_{i=1}^{\infty}$ of valuation sets, where $S_i \subseteq \mathbb{Z}^{\mathbf{x}}$ for all $i \geq 1$. The *greatest fixpoint* F is the largest set S such that $F(S) = S$, and is denoted $\mathrm{gfp}(F)$.

3. Weakest Preconditions for Non-termination

This section is concerned with the definition of weakest preconditions for non-termination, and the characterization of such preconditions as greatest fixpoints of the pre-image function. We also give certain conditions under which these fixpoints are computable as limits of descending Kleene sequences, and finally, define them using first-order integer arithmetic.

In the rest of this section, let $\mathbf{x} = \{x_1, \ldots, x_N\}$ be a set of variables ranging over integers, for some constant $N > 0$. We start by proving several properties of the pre-image function.

Proposition 3.1. *Let $R, R' \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be relations and $S, S' \subseteq \mathbb{Z}^{\mathbf{x}}$ be sets of valuations. The following hold:*

1. *If $R \subseteq R'$ and $S \subseteq S'$ then $\mathrm{pre}_R(S) \subseteq \mathrm{pre}_{R'}(S')$. Consequently, pre_R is monotonic.*
2. *If $1 \leq n \leq m$ then $\mathrm{pre}^n_R(S) \supseteq \mathrm{pre}^m_R(S)$. Consequently, the sequence $\{\mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}})\}_{n \geq 1}$ is descending.*

Proof. (1) Let $\nu \in \mathrm{pre}_R(S)$ be a valuation. Hence there exist $\nu' \in S \subseteq S'$ such that $(\nu, \nu') \in R \subseteq R'$. But then $\nu \in \mathrm{pre}_{R'}(S')$. Monotonicity of pre_R follows by taking $R' = R$.
(2) We have:

$$\begin{array}{rcll}
\mathbb{Z}^{\mathbf{x}} & \supseteq & \mathrm{pre}_R(\mathbb{Z}^{\mathbf{x}}) & \text{since } \mathbb{Z}^{\mathbf{x}} \text{ is the universal set} \\
\mathrm{pre}_R(\mathbb{Z}^{\mathbf{x}}) & \supseteq & \mathrm{pre}^2_R(\mathbb{Z}^{\mathbf{x}}) & \text{by the monotonicity of } \mathrm{pre}_R \text{ at point (1)} \\
& \ldots & & \\
\mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}}) & \supseteq & \mathrm{pre}^{n+1}_R(\mathbb{Z}^{\mathbf{x}}) &
\end{array}$$

Hence the sequence $\{\mathrm{pre}^n_R\}_{n \geq 1}$ is descending. □

We next define the notions of $*$-*consistent* and *well-founded* relation.

Definition 3.2. A relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is said to be $*$-*consistent* if and only if, for any $m \geq 0$, there exists a finite sequence of valuations $\{\nu_i\}_{i=1}^m$, where $\nu_i \in \mathbb{Z}^{\mathbf{x}}$ for all $i \geq 1$, such that $(\nu_i, \nu_{i+1}) \in R$, for all $i = 1, \ldots, m-1$. R is said to be *well founded* if and only if there is no infinite sequence of valuations $\{\nu_i\}_{i \geq 1}$, such that $\nu_i \in \mathbb{Z}^{\mathbf{x}}$ and $(\nu_i, \nu_{i+1}) \in R$, for all $i \geq 0$.

Notice that if a relation is not $*$-consistent, then it is also well founded. However the dual is not true. For instance, the relation $R = \{(n, n-1) \mid n > 0\}$ is both $*$-consistent and well founded. Also notice that a relation R is $*$-consistent if and only if R^i is consistent for all $i \geq 1$.

Definition 3.3. A set $S \subseteq \mathbb{Z}^{\mathbf{x}}$ is said to be a *non-termination precondition* for a relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ if and only if for each $\nu \in S$ there exists an infinite sequence of valuations $\{\nu_i\}_{i \geq 0}$ such that $\nu = \nu_0$ and $\nu_i \in \mathbb{Z}^{\mathbf{x}}$, $(\nu_i, \nu_{i+1}) \in R$, for all $i \geq 0$.

If $S_0, S_1, \ldots$ are all non-termination preconditions for R, then the (possibly infinite) union $\bigcup_{i=0,1,\ldots} S_i$ is a non-termination precondition for R as well. The set $\mathrm{wnt}(R) = \bigcup\{S \in \mathbb{Z}^{\mathbf{x}} \mid S \text{ is a non-termination precondition for } R\}$ is called the *weakest non-termination precondition* for R. A relation R is well founded if and only if $\mathrm{wnt}(R) = \emptyset$. A set S such that $S \cap \mathrm{wnt}(R) = \emptyset$ is called a *termination precondition*.

Definition 3.4. A set $S \subseteq \mathbb{Z}^{\mathbf{x}}$ is said to be *recurrent* for a relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ if and only if $S \subseteq \mathrm{pre}_R(S)$.

Notice that if S is a recurrent set for a relation R, then for each $\nu \in S$ there exists $\nu' \in S$ such that $(\nu, \nu') \in R$.

Proposition 3.5. *Let $S_0, S_1, \ldots \in \mathbb{Z}^{\mathbf{x}}$ be a (possibly infinite) sequence of sets, all of which are recurrent for a relation $R \in \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$. Then their union $\bigcup_{i=0,1,\ldots} S_i$ is recurrent for R as well.*

Proof. For each i we have $S_i \subseteq \mathrm{pre}_R(S_i) \subseteq \mathrm{pre}_R(\bigcup_{j=0,1,\ldots} S_j)$. The last inclusion is by the monotonicity of pre_R. Hence $\bigcup_{j=0,1,\ldots} S_j \subseteq \mathrm{pre}_R(\bigcup_{j=0,1,\ldots} S_j)$. □

The set $\mathrm{wrs}(R) = \bigcup\{S \in \mathbb{Z}^{\mathbf{x}} \mid S \text{ is a recurrent set for } R\}$ is called the *weakest recurrent set* for R. By Proposition 3.5, $\mathrm{wrs}(R)$ is recurrent for R. The following lemma shows that in fact, $\mathrm{wrs}(R)$ is exactly the set of valuations from which an infinite iteration of R is possible and, equivalently, the greatest fixpoint of the transition relation's pre-image.

Lemma 3.6. *For every relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$,*

$$\mathrm{wrs}(R) = \mathrm{wnt}(R) = \mathrm{gfp}(\mathrm{pre}_R).$$

Proof. "$\mathrm{wrs}(R) = \mathrm{gfp}(\mathrm{pre}_R)$" By the *Knaster-Tarski Fixpoint Theorem*[3],

$$\mathrm{gfp}(\mathrm{pre}_R) = \bigcup\{S \mid S \subseteq \mathrm{pre}_R(S)\} = \mathrm{wrs}(R).$$

"$\mathrm{wrs}(R) \subseteq \mathrm{wnt}(R)$" Let $\nu_0 \in \mathrm{wrs}(R)$ be a valuation. Then there exists $\nu_1 \in \mathrm{wrs}(R)$ such that $(\nu_0, \nu_1) \in R$. Applying this argument infinitely many times, one can construct an infinite sequence $\nu_0, \nu_1, \nu_2, \ldots$ such that $(\nu_i, \nu_{i+1}) \in R$, for all $i \geq 0$. Hence $\nu_0 \in \mathrm{wnt}(R)$.

"$\mathrm{wnt}(R) \subseteq \mathrm{wrs}(R)$" Let $\nu_0 \in \mathrm{wnt}(R)$ be a valuation and let $\nu_0, \nu_1, \nu_2, \ldots$ be an arbitrary infinite sequence such that $(\nu_i, \nu_{i+1}) \in R$, for all $i \geq 0$. Clearly, $\nu_1 \in \mathrm{wnt}(R)$ too. Consequently, $\nu_0 \in \mathrm{pre}_R(\mathrm{wnt}(R))$ for each state $\nu_0 \in \mathrm{wnt}(R)$ and hence, $\mathrm{wnt}(R) \subseteq \mathrm{pre}_R(\mathrm{wnt}(R))$. Thus, $\mathrm{wnt}(R)$ is a recurrent set and hence $\mathrm{wnt}(R) \subseteq \mathrm{wrs}(R)$. □

The following lemma gives sufficient conditions under which $\mathrm{wrs}(R)$ can be computed as the limit $\bigcap_{n \geq 1} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})$ of the infinite descending Kleene sequence:

$$\mathrm{pre}_R(\mathbb{Z}^{\mathbf{x}}) \supseteq \mathrm{pre}_R^2(\mathbb{Z}^{\mathbf{x}}) \supseteq \mathrm{pre}_R^3(\mathbb{Z}^{\mathbf{x}}) \ldots$$

Lemma 3.7. *Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a relation such that at least one of the following holds:*
(1) $\bigcap_{n \geq 1} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}}) = \emptyset$, *or*
(2) $\mathrm{pre}_R^{n_2}(\mathbb{Z}^{\mathbf{x}}) = \mathrm{pre}_R^{n_1}(\mathbb{Z}^{\mathbf{x}})$ *for some $n_2 > n_1 \geq 1$, or*
(3) pre_R *is $\cap$-continuous.*
Then, we have $\mathrm{wrs}(R) = \bigcap_{n \geq 1} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})$. *Moreover,* $\mathrm{wrs}(R) = \emptyset$ *if (1) holds and* $\mathrm{wrs}(R) = \mathrm{pre}_R^{n_1}(\mathbb{Z}^{\mathbf{x}})$ *if (2) holds.*

Proof. By Lemma 3.6, $\mathrm{wnt}(R) = \mathrm{wrs}(R) = \mathrm{gfp}(\mathrm{pre}_R)$. Since $\mathrm{gfp}(\mathrm{pre}_R)$ is a fixpoint, it follows that $\mathrm{gfp}(\mathrm{pre}_R) = \mathrm{pre}_R^n(\mathrm{gfp}(\mathrm{pre}_R))$ for each $n \geq 1$. Since $\mathrm{gfp}(\mathrm{pre}_R) \subseteq \mathbb{Z}^{\mathbf{x}}$, it follows that $\mathrm{pre}_R^n(\mathrm{gfp}(\mathrm{pre}_R)) \subseteq \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})$ for each $n \geq 1$, by monotonicity of pre_R (Proposition 3.1). Hence we obtain that $\mathrm{gfp}(\mathrm{pre}_R) \subseteq \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})$ for each $n \geq 1$ and consequently:

$$\mathrm{wnt}(R) = \mathrm{wrs}(R) = \mathrm{gfp}(\mathrm{pre}_R) \subseteq \bigcap_{n \geq 1} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})$$

We distinguish between the three cases from the hypothesis:

[3] We use the version given as Prop. A.10 in [30], pg. 400.

(1) We have $\emptyset \subseteq \mathrm{wrs}(R) \subseteq \bigcap_{n\geq 1} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}}) = \emptyset$. Hence, in this case we obtain $\mathrm{wrs}(R) = \bigcap_{n\geq 1} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}}) = \emptyset$.

(2) Since pre_R is a monotonic function, the sequence $\{\mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})\}_{n\geq 1}$ is descending:
$$\mathrm{pre}_R^{n_1}(\mathbb{Z}^{\mathbf{x}}) \supseteq \mathrm{pre}_R^{n_1+1}(\mathbb{Z}^{\mathbf{x}}) \supseteq \ldots \supseteq \mathrm{pre}_R^{n_2}(\mathbb{Z}^{\mathbf{x}}) = \mathrm{pre}_R^{n_1}(\mathbb{Z}^{\mathbf{x}})$$
Hence, $\mathrm{pre}_R^{n_1}(\mathbb{Z}^{\mathbf{x}}) = \mathrm{pre}_R^{n}(\mathbb{Z}^{\mathbf{x}})$, for all $n \geq n_1$, i.e. $\mathrm{pre}_R^{n_1}(\mathbb{Z}^{\mathbf{x}})$ is a fixpoint of pre_R, and thus we obtain:
$$\bigcap_{n\geq 0} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}}) = \mathrm{pre}_R^{n_1}(\mathbb{Z}^{\mathbf{x}}) \subseteq \mathrm{gfp}(\mathrm{pre}_R)$$
Since $\mathrm{gfp}(\mathrm{pre}_R) \subseteq \bigcap_{n\geq 1} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})$, we obtain:
$$\mathrm{wrs}(R) = \mathrm{gfp}(\mathrm{pre}_R) = \bigcap_{n\geq 1} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})$$
Since $\mathrm{pre}_R^{n_1}(\mathbb{Z}^{\mathbf{x}})$ is a fixpoint, then
$$\mathrm{wrs}(R) = \bigcap_{n\geq 1} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}}) = \bigcap_{1\leq n\leq n_1} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}}) = \mathrm{pre}_R^{n_1}(\mathbb{Z}^{\mathbf{x}})$$

(3) If pre_R is $\cap$-continuous, then $\mathrm{wrs}(R) = \mathrm{gfp}(\mathrm{pre}_R) = \bigcap_{n\geq 1} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})$, by Kleene Fixpoint Theorem [26]. □

In the next section, we show that Lemma 3.7 is applicable, for different reasons, to both octagonal (Definition 4.20) and finite-monoid affine (Definition 5.1) relations: octagonal relations are either well founded (1), or their descending Kleene sequences stabilize (2), and linear affine relations are $\cap$-continuous (3). Thus one can compute the weakest non-termination precondition for these classes as the limit of a descending Kleene sequence. Next, we show that, for relations satisfying one of the conditions of Lemma 3.7, one can also define the weakest non-termination precondition in first order arithmetic.

Definition 3.8. Let $\{S_i\}_{i\geq 1}$ be an infinite sequence of valuation sets, $S_i \subseteq \mathbb{Z}^{\mathbf{x}}$, for all $i \geq 1$. The *closed form* of $\{S_i\}_{i\geq 1}$ is a formula $\widehat{S}(k, \mathbf{x})$ such that, for all $n \geq 1$ and all $\nu \in \mathbb{Z}^{\mathbf{x}}$:
$$\nu \in S_n \Leftrightarrow \nu \models \widehat{S}[n/k]$$

In the rest of the paper, we shall define the weakest non-termination precondition $\mathrm{wnt}(R)$ for relations R that are octagonal or finite monoid affine. Assuming that at least one of the hypotheses of Lemma 3.7 holds and that $\widehat{\mathrm{pre}_R}(k, \mathbf{x})$ is a closed form of the sequence $\{\mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})\}_{n\geq 1}$, the weakest non-termination precondition of R is equivalent to the first-order arithmetic formula on the right hand side in the following equivalence:
$$(\mathrm{wnt}(R))(\mathbf{x}) \Leftrightarrow \forall k \geq 1 \ .\ \widehat{\mathrm{pre}_R}(k, \mathbf{x}) \tag{3.1}$$
In the upcoming developments, we will show that $\widehat{\mathrm{pre}_R}(k, \mathbf{x})$ is Presburger definable, for octagonal and finite monoid affine relations R. As a direct consequence of (3.1), the weakest non-termination precondition is definable in Presburger arithmetic. Since satisfiability is decidable for Presburger arithmetic [35], the universal termination problem for octagonal and finite-monoid affine relations is decidable as well.

Example 3.9. Consider the relation $R(x, x') \Leftrightarrow x \geq 0 \wedge x' = x - 1$. The closed form of the sequence $\{\mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})\}_{n\geq 1}$ is $\widehat{\mathrm{pre}_R}(k, x) \Leftrightarrow k \geq 1 \wedge x \geq k - 1$. Then, by (3.1), we have:
$$(\mathrm{wnt}(R))(\mathbf{x}) \Leftrightarrow \forall k \geq 1 \ .\ \widehat{\mathrm{pre}_R}(k, x) \Leftrightarrow \forall k \geq 1 \ .\ k \geq 1 \wedge x \geq k - 1 \Leftrightarrow \mathbf{false}$$
Hence the relation R is well founded. □

4. Octagonal Relations

Octagonal constraints (also known as Unit Two Variables Per Inequality or UTVPI, for short) appear in the context of abstract interpretation where they have been extensively studied as an abstract domain [29]. They are defined syntactically as conjunctions of atomic propositions of the form $\pm x \pm y \leq c$, where x and y are variables and $c \in \mathbb{Z}$ is an integer constant. They are a generalization of the simpler notion of *difference bounds constraints*. Since most results concerning octagons rely on notions related to difference bounds constraints, we introduce first the latter, for reasons of self-containment.

4.1. **Difference Bounds Relations.**

Difference bounds constraints are also known as *zones* in the context of timed automata verification [1] and abstract interpretation [29, 28]. They are defined syntactically as conjunctions of atomic propositions of the form $x - y \leq c$, where x and y are variables and $c \in \mathbb{Z}$ is an integer constant. Difference bounds constraints can be represented as matrices and graphs. These matrices (graphs) have a canonical form, which is used for efficient inclusion checks, and can be computed by the classical Floyd-Warshall shortest path algorithm [19].

Definition 4.1. A formula $\phi(\mathbf{x})$ is a *difference bounds constraint* if it is a finite conjunction of atomic propositions of the form $x_i - x_j \leq a_{ij},\ 1 \leq i, j \leq N$, where $a_{ij} \in \mathbb{Z}$.

For example, the equality constraint $x - y = 5$ is equivalent to the difference bounds constraint $x - y \leq 5 \wedge y - x \leq -5$. In practice, difference bounds constraints are represented either as matrices or as graphs:

Definition 4.2. Let $\mathbf{x} = \{x_1, x_2, \ldots, x_N\}$ be a set of variables ranging over $\mathbb{Z}$ and $\phi(\mathbf{x})$ be a difference bounds constraint. Then the *difference bounds matrix* (DBM) representing ϕ is the matrix $M_\phi \in \mathbb{Z}_\infty^{N \times N}$ such that:

$$(M_\phi)_{ij} = \begin{cases} a_{ij} & \text{if } (x_i - x_j \leq a_{ij}) \in \mathit{Atom}(\phi) \\ \infty & \text{otherwise} \end{cases}$$

We denote by $\mu(\phi) \overset{def}{=} \max\{|c| \mid (x_i - x_j \leq c) \in \mathit{Atom}(\phi)\}$ the maximal absolute value over all constants that appear in $\phi(\mathbf{x})$.

Weighted graphs are central to the upcoming developments. An *integer weighted digraph* is a tuple $G = \langle V, E \rangle$, where V is a set of vertices, $E \subseteq V \times \mathbb{Z} \times V$ is a set of integer-labeled edges. When G is clear from the context, we denote by $u \xrightarrow{\alpha} v$ the fact that $(u, \alpha, v) \in E$. A *path* in G is a sequence of the form $\pi : v_0 \xrightarrow{\alpha_1} v_1 \ \cdots \ v_{p-1} \xrightarrow{\alpha_p} v_p$ such that $(v_{i-1}, \alpha_i, v_i) \in E$ for all $1 \leq i \leq p$. A path is *elementary* if $v_i = v_j$ only if $i = 1$ and $j = p$. A *cycle* is a path of length greater than zero, whose source and destination vertices are the same. An *elementary cycle* is a cycle who is elementary.

Definition 4.3. Let $\mathbf{x} = \{x_1, x_2, \ldots, x_N\}$ be a set of variables ranging over $\mathbb{Z}$ and $\phi(\mathbf{x})$ be a difference bounds constraint. Then ϕ can be represented as the weighted graph $\mathcal{G}_\phi = (\mathbf{x}, \rightarrow)$, where each vertex corresponds to a variable, and there is an edge $x_i \xrightarrow{a_{ij}} x_j$ in $\mathcal{G}_\phi$ if and only if there exists a constraint $x_i - x_j \leq a_{ij}$ in ϕ, called the *constraint graph* of ϕ.

Clearly, M_ϕ is the incidence matrix of $\mathcal{G}_\phi$. If $M \in \mathbb{Z}_\infty^{N\times N}$ is a DBM, the corresponding difference bounds constraint is defined as:

$$\Delta[M] \equiv \bigwedge_{\substack{1\leq i,j\leq N \\ M_{ij}<\infty}} x_i - x_j \leq M_{ij} \tag{4.1}$$

For two difference bounds matrices $M_1, M_2 \in \mathbb{Z}_\infty^{N\times N}$, let $\min(M_1,M_2) \in \mathbb{Z}_\infty^{N\times N}$ be the matrix defined as $(\min(M_1,M_2))_{ij} = \min((M_1)_{ij},(M_2)_{ij})$, for all $1 \leq i,j \leq N$. We write $M_1 = M_2$ if and only if $(M_1)_{ij} = (M_2)_{ij}$ for all $1 \leq i,j \leq N$ and $M_1 \leq M_2$ if and only if $(M_1)_{ij} \leq (M_2)_{ij}$ for all $1 \leq i,j \leq N$. We write $M_1 < M_2$ if and only if $M_1 \leq M_2$ and $M_1 \neq M_2$. A DBM M is said to be *consistent* if and only if its corresponding constraint $\Delta[M]$ is consistent (4.1). We denote in the following by $\perp\!\!\!\perp^N$ any inconsistent DBM of size $N \times N$. The next definition gives a canonical form for consistent DBMs.

Definition 4.4. A consistent DBM $M \in \mathbb{Z}_\infty^{N\times N}$ is said to be *closed* if and only if $M_{ii} = 0$ and $M_{ij} \leq M_{ik} + M_{kj}$, for all $1 \leq i,j,k \leq N$.

Intuitively, the closure of a consistent DBM contains all information induced by the triangle inequality $M_{ij} \leq M_{ik} + M_{kj}$. It is well known that, M is consistent if and only if it does not contain a negative weight circuit, i.e. there is no sequence of indices $1 \leq i_1, \ldots, i_p \leq N$ such that $M_{i_1i_2} + \ldots + M_{i_{p-1}i_p} + M_{i_pi_1} < 0$. If M is consistent, then its closure is unique[4]. Given a consistent DBM $M \in \mathbb{Z}_\infty^{N\times N}$, we denote by M^* the (unique) closed DBM such that $\Delta[M] \Leftrightarrow \Delta[M^*]$. The consistency of a DBM can be decided in PTIME by the classical Floyd-Warshall shortest path algorithm (Algorithm 1), which computes also the closure of consistent DBMs:

Proposition 4.5. *Let $M \in \mathbb{Z}_\infty^{N\times N}$ be a DBM representing a difference bounds constraint ϕ. If M is consistent, the output of Algorithm 1 is its closure M^*. Otherwise, if M is inconsistent, Algorithm 1 will report this fact. The running time of the algorithm is of the order $\mathcal{O}(N^3 \cdot (N + \log_2 \mu(\phi)))$.*

Proof. The correctness proof of the Floyd-Warshall algorithm is standard, e.g. Theorem 3.3.5 in [28] proves that

- eventually $M_{ii} < 0$ for some $1 \leq i \leq N$, if M is inconsistent
- the algorithm returns M^*, if M is consistent

Note that inconsistency of M is detected either on line 2 or on line 8.

For each $1 \leq i,j,k \leq N$, let M^0_{ij} be the value of M_{ij} after the loop on line 1 terminates and let M^k_{ij} be the value of M_{ij} after the k-th iteration of the outermost loop on line 4 terminates. For each $0 \leq k \leq N$, we define $\mu_k \overset{def}{=} \max\{|M^k_{ij}| \mid M^k_{ij} < \infty\}$. For each $1 \leq k \leq N$, we partition the set $\{(i,j) \mid 1 \leq i,j \leq N\}$ as follows:

$$\begin{array}{rcl} A_k & = & \{(i,j) \mid i \neq k \wedge j \neq k\} \\ B_k & = & \{(i,j) \mid (i \neq k \wedge j = k) \vee (i = k \wedge j \neq k)\} \\ C_k & = & \{(k,k)\} \end{array}$$

We next analyze how the updated of matrix entries depend on one another during the k-th iteration of the outermost loop and analyze how the changes are propagated. Clearly, each $(i,j) \in A_k$ depends on itself and on 2 entries $(i,k),(k,j) \in B_k$, each $(i,j) \in B_k$ depends

[4] See, e.g. [29], Section 3.2

on itself and on $(k,k) \in C_k$, and the entry $(k,k) \in C_k$ depends only on itself. It is easy to see, due to the test on line 8, that before executing the update on line 7, $M_{\ell\ell} = 0$ for each $1 \leq \ell \leq N$. Thus, the following holds for each $1 \leq k \leq N$:

$$\begin{array}{lclcl}
\forall(k,k) \in C_k \,.\, M^k_{kk} & = & \min(M^{k-1}_{kk}, M^{k-1}_{kk} + M^{k-1}_{kk}) & = & 0 \\
\forall(i,k) \in B_k \,.\, M^k_{ik} & = & \min(M^{k-1}_{ik}, M^{k-1}_{ik} + M^{k-1}_{kk}) & = & M^{k-1}_{ik} \leq \mu_{k-1} \\
\forall(k,j) \in B_k \,.\, M^k_{kj} & = & \min(M^{k-1}_{kj}, M^{k-1}_{kk} + M^{k-1}_{kj}) & = & M^{k-1}_{kj} \leq \mu_{k-1} \\
\forall(i,j) \in A_k \,.\, M^k_{ij} & = & \min(M^{k-1}_{ij}, M^{k-1}_{ik} + M^{k-1}_{kj}) & \leq & 2 \cdot \mu_{k-1}
\end{array}$$

Hence, $\mu_k \leq 2 \cdot \mu_{k-1}$ for each $1 \leq k \leq N$ and consequently, $\mu_N \leq 2^N \cdot \mu_0 = 2^N \cdot \mu(\phi)$. Thus, the min and sum operations at line 7 can be executed in time at most $\log_2 \mu_N$ which is of the order $\mathcal{O}(N + \log_2 \mu(\phi))$. Since line 7 is iterated N^3 times, the complexity of the nested loops at lines 4–8 is $\mathcal{O}(N^3 \cdot (N + \log_2 \mu(\phi)))$. The loop at lines 1–3 does not add to this factor. □

Algorithm 1 The Floyd-Warshall shortest path algorithm

```
   input a difference bounds matrix $M \in \mathbb{Z}_\infty^{N \times N}$
   output $M^*$ if $M$ is consistent, and report "inconsistent" otherwise
1: for all $i = 1, \ldots, N$ do
2:     if $M_{ii} < 0$ then report "inconsistent"
3:     else $M_{ii} \leftarrow 0$
4: for all $k = 1, \ldots, N$ do
5:     for all $i = 1, \ldots, N$ do
6:         for all $j = 1, \ldots, N$ do
7:             $M_{ij} \leftarrow \min(M_{ij}, M_{ik} + M_{kj})$
8:             if $i = j$ and $M_{ii} < 0$ then report "inconsistent"
```

The closure of DBMs is needed to check the equivalence and entailment of two difference bounds constraints. Moreover, it is used for quantifier elimination.

Proposition 4.6. *Let $\phi(\mathbf{x})$, $\phi_1(\mathbf{x})$ and $\phi_2(\mathbf{x})$, where $\mathbf{x} = \{x_1, \ldots, x_N\}$, be consistent difference bounds constraints. Then the following hold:*

(1) *$\phi_1 \Leftrightarrow \phi_2$ if and only if $M^*_{\phi_1} = M^*_{\phi_2}$,*
(2) *$\phi_1 \Rightarrow \phi_2$ if and only if $M^*_{\phi_1} \leq M^*_{\phi_2}$.*
(3) *for any $1 \leq k \leq N$, there exists a difference bounds constraint $\psi(\mathbf{x} \setminus \{x_k\})$, such that $\psi \Leftrightarrow \exists x_k \,.\, \phi$, and $M^*_\psi \in \mathbb{Z}_\infty^{N-1 \times N-1}$ is obtained by eliminating the k-th line and column from M^*_ϕ.*

Proof. The points (1), (2) and (3), are equivalent to the Theorems 3.4.1, 3.4.2 and 3.6.1 (second point) in [28], respectively. □

Difference bounds relations are relations defined by difference bounds constraints over primed and unprimed variables (e.g. $x - x' \leq 0$). Difference bounds relations have been studied by Comon and Jurski who showed, in [15], that their transitive closure is Presburger definable. In the rest of this paper, for each difference bounds relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$, we denote by $R(\mathbf{x}, \mathbf{x}')$ any difference bounds constraint that defines R. Each DBM $M_{R(\mathbf{x},\mathbf{x}')} \in \mathbb{Z}_\infty^{2N \times 2N}$ corresponding to $R(\mathbf{x}, \mathbf{x}')$ is a matrix of dimension $2N \times 2N$, that can be split into four matrices of dimension $N \times N$, corresponding to the top-left, bottom-left, top-right and bottom-right corners, denoted as ${}^{\blacksquare}M_{R(\mathbf{x},\mathbf{x}')}, {}_{\blacksquare}M_{R(\mathbf{x},\mathbf{x}')}, M^{\blacksquare}{}_{R(\mathbf{x},\mathbf{x}')}, M_{\blacksquare R(\mathbf{x},\mathbf{x}')} \in \mathbb{Z}_{\infty}^{N\times N}$. Notice the equivalence $\Delta[{}^{\blacksquare}M^{*}{}_{R(\mathbf{x},\mathbf{x}')}] \Leftrightarrow \exists \mathbf{x}' \, . \, R(\mathbf{x},\mathbf{x}')$ for every consistent constraint $R(\mathbf{x},\mathbf{x}')$, by Proposition 4.6 (third point). In the rest of this section, we will often write M_R instead of $M_{R(\mathbf{x},\mathbf{x}')}$, whenever the defining constraint $R(\mathbf{x},\mathbf{x}')$ is clear from the context. In the following, the projection operators are assumed to have lower priority than closure operators, e.g. ${}^{\blacksquare}M_R^{*}$ stands for ${}^{\blacksquare}(M_R^{*})$.

Example 4.7. Figure 1(a) shows the constraint graph $\mathcal{G}_R$ for the difference bounds relation defined as $R(\mathbf{x},\mathbf{x}') \equiv x_2 - x_1' \le -1 \wedge x_3 - x_2' \le 0 \wedge x_1 - x_3' \le 0 \wedge x_4' - x_4 \le 0 \wedge x_3' - x_4 \le 0$. Figure 1(b) shows the closed DBM representation of R.

We show next that the composition of two difference bounds relations encoded as DBMs can be computed in PTIME using Algorithm 1. Let $R_1, R_2 \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be two difference bounds relations. We write M_1 and M_2 for $M_{R_1(\mathbf{x},\mathbf{x}')}$ and $M_{R_2(\mathbf{x},\mathbf{x}')}$, i.e. the DBMs corresponding to the difference bounds constraints $R_1(\mathbf{x},\mathbf{x}')$ and $R_2(\mathbf{x},\mathbf{x}')$, respectively. Let $\mathcal{M}_{12} \in \mathbb{Z}^{3N\times 3N}$ be the following matrix:

$$\mathcal{M}_{12} = \begin{pmatrix} {}^{\blacksquare}M_1 & M_1{}^{\blacksquare} & \infty \\ {}_{\blacksquare}M_1 & \min(M_{1\blacksquare}, {}^{\blacksquare}M_2) & M_2{}^{\blacksquare} \\ \infty & {}_{\blacksquare}M_2 & M_{2\blacksquare} \end{pmatrix} \tag{4.2}$$

and let $M_1 \odot M_2 \in \mathbb{Z}^{2N\times 2N}$ be the matrix obtained by erasing the lines and columns $N+1, \ldots, 2N$ from the closure $\mathcal{M}_{12}^{*}$, if $\mathcal{M}_{12}$ is consistent, and $\perp\!\!\!\perp^{2N}$, otherwise.

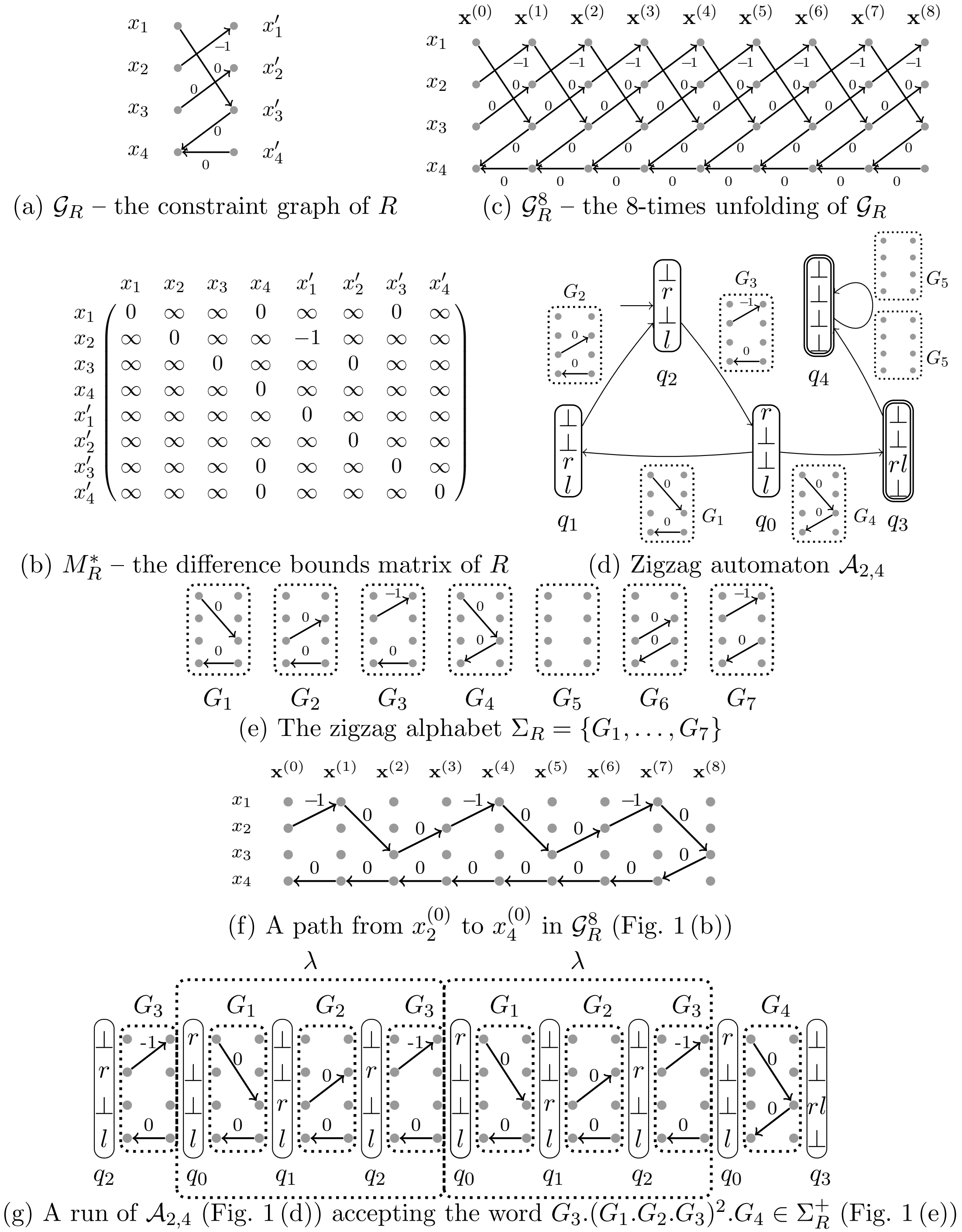
Proposition 4.8. *Let $R_1, R_2 \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be two relations defined by the difference bounds constraints $R_1(\mathbf{x},\mathbf{x}')$ and $R_2(\mathbf{x},\mathbf{x}')$, respectively. Then $\Delta[M_{R_1(\mathbf{x},\mathbf{x}')} \odot M_{R_2(\mathbf{x},\mathbf{x}')}]$ defines the composition $R_1 \circ R_2 \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$. Moreover, $M_{R_1(\mathbf{x},\mathbf{x}')} \odot M_{R_2(\mathbf{x},\mathbf{x}')}$ can be computed in time $\mathcal{O}(N^3 \cdot (N + \log_2(\max(\mu(R_1), \mu(R_2)))))$.*

Proof. The composition $R_1 \circ R_2$ is defined by the formula $\exists \mathbf{y} \, . \, R_1(\mathbf{x},\mathbf{y}) \wedge R_2(\mathbf{y},\mathbf{x}')$. It is easy to see that $\mathcal{M}_{12}$ is the DBM corresponding to the conjunction $R_1(\mathbf{x},\mathbf{y}) \wedge R_2(\mathbf{y},\mathbf{x}')$, after the elimination of the redundant constraints on $\mathbf{y}$, i.e. the replacement of any conjunction of the form $x_i - x_j \le c \wedge x_i - x_j \le d$ by $x_i - x_j \le \min(c,d)$. The existential quantifiers are eliminated by checking the consistency of $\mathcal{M}_{12}$, computing its closure, and erasing the lines and columns $N+1, \ldots, 2N$ (by Proposition 4.6, third point). The time complexity upper bound is a direct consequence of the complexity of Algorithm 1 (Proposition 4.5) used to compute $\mathcal{M}_{12}^{*}$. □

In general, for a DBM $M \in \mathbb{Z}_{\infty}^{2N\times 2N}$, we define $M^{\odot^1} = M$ and $M^{\odot^n} = M^{\odot^{n-1}} \odot M$, for any $n > 1$. An inductive argument shows that the difference bounds constraint $\Delta[M^{\odot^n}_{R(\mathbf{x},\mathbf{x}')}]$ defines R^n, for any difference bounds relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ and $n > 0$. In the following, we write $R^n(\mathbf{x},\mathbf{x}')$ for $\Delta[M^{\odot^n}_{R(\mathbf{x},\mathbf{x}')}]$.

4.2. Zigzag Automata.

In this section we introduce an automata-theoretic model for reasoning about the powers of a difference bounds relation. Since a difference bounds relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is represented by a difference constraint formula $R(\mathbf{x},\mathbf{x}')$, which, in turn, can be seen as a constraint graph $\mathcal{G}_R$ (Definition 4.3), the m-th power of R can be seen as a constraint graph consisting of m copies of $\mathcal{G}_R$:


x_1
x_2
x_3
x_4
x'_1
x'_2
x'_3
x'_4
−1
0
$\mathbf{x}^{(0)}$ $\mathbf{x}^{(1)}$ $\mathbf{x}^{(2)}$ $\mathbf{x}^{(3)}$ $\mathbf{x}^{(4)}$ $\mathbf{x}^{(5)}$ $\mathbf{x}^{(6)}$ $\mathbf{x}^{(7)}$ $\mathbf{x}^{(8)}$
G_1
G_2
G_3
G_4
G_5
G_6
G_7
q_0
q_1
q_2
q_3
q_4
r
l
rl
$\perp$
λ
-1

(a) $\mathcal{G}_R$ – the constraint graph of R

(c) $\mathcal{G}_R^8$ – the 8-times unfolding of $\mathcal{G}_R$

$$\begin{array}{c|cccccccc}
 & x_1 & x_2 & x_3 & x_4 & x'_1 & x'_2 & x'_3 & x'_4 \\
\hline
x_1 & 0 & \infty & \infty & 0 & \infty & \infty & 0 & \infty \\
x_2 & \infty & 0 & \infty & \infty & -1 & \infty & \infty & \infty \\
x_3 & \infty & \infty & 0 & \infty & \infty & 0 & \infty & \infty \\
x_4 & \infty & \infty & \infty & 0 & \infty & \infty & \infty & \infty \\
x'_1 & \infty & \infty & \infty & \infty & 0 & \infty & \infty & \infty \\
x'_2 & \infty & \infty & \infty & \infty & \infty & 0 & \infty & \infty \\
x'_3 & \infty & \infty & \infty & 0 & \infty & \infty & 0 & \infty \\
x'_4 & \infty & \infty & \infty & 0 & \infty & \infty & \infty & 0
\end{array}$$

(b) M_R^* – the difference bounds matrix of R

(d) Zigzag automaton $\mathcal{A}_{2,4}$

(e) The zigzag alphabet $\Sigma_R = \{G_1, \ldots, G_7\}$

(f) A path from $x_2^{(0)}$ to $x_4^{(0)}$ in $\mathcal{G}_R^8$ (Fig. 1 (b))

(g) A run of $\mathcal{A}_{2,4}$ (Fig. 1 (d)) accepting the word $G_3.(G_1.G_2.G_3)^2.G_4 \in \Sigma_R^+$ (Fig. 1 (e)) which encodes the path from Fig. 1 (f)

FIGURE 1. Illustration of various notions for a difference bounds relation $R \Leftrightarrow x_2 - x'_1 \leq -1 \wedge x_3 - x'_2 \leq 0 \wedge x_1 - x'_3 \leq 0 \wedge x'_4 - x_4 \leq 0 \wedge x'_3 - x_4 \leq 0$.

Definition 4.9. Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a difference bounds relation, where $\mathbf{x} = \{x_1, \ldots, x_N\}$, and $\mathcal{G}_R$ be the constraint graph of a difference bounds constraint $R(\mathbf{x}, \mathbf{x}')$ defining R. The *n-times unfolding* of $\mathcal{G}_R$ is defined for every $n > 0$ as:

$$\mathcal{G}_R^n = (\bigcup_{k=0}^{n} \mathbf{x}^{(k)}, \rightarrow)$$

where $\rightarrow \subseteq (\bigcup_{k=0}^{n} \mathbf{x}^{(k)}) \times \mathbb{Z} \times (\bigcup_{k=0}^{n} \mathbf{x}^{(k)})$, $\mathbf{x}^{(k)} = \{x_i^{(k)} \mid 1 \leq i \leq N\}$ and for all $0 \leq k < n$, there is an edge:

- $x_i^{(k)} \xrightarrow{c} x_j^{(k)}$ if and only if $(x_i - x_j \leq c) \in \mathit{Atom}(R(\mathbf{x}, \mathbf{x}'))$
- $x_i^{(k)} \xrightarrow{c} x_j^{(k+1)}$ if and only if $(x_i - x_j' \leq c) \in \mathit{Atom}(R(\mathbf{x}, \mathbf{x}'))$
- $x_i^{(k+1)} \xrightarrow{c} x_j^{(k)}$ if and only if $(x_i' - x_j \leq c) \in \mathit{Atom}(R(\mathbf{x}, \mathbf{x}'))$
- $x_i^{(k+1)} \xrightarrow{c} x_j^{(k+1)}$ if and only if $(x_i' - x_j' \leq c) \in \mathit{Atom}(R(\mathbf{x}, \mathbf{x}'))$

where $x_i^{(k)} \xrightarrow{c} x_j^{(\ell)}$ stands for $(x_i^{(k)}, c, x_j^{(\ell)}) \in \rightarrow$.

Each constraint in $R^n(\mathbf{x}, \mathbf{x}')$ corresponds to a path between extremal[5] vertices in $\mathcal{G}_R^n$. Notice that, since difference bounds relations are closed under composition (Proposition 4.8), then R^n is a difference bounds relation, for any $n > 0$. For any given integer $n > 0$, assuming that R^n is consistent, R^n is defined by the following difference constraint:

$$\begin{array}{ll} \bigwedge_{1 \leq i,j \leq N} & x_i - x_j \leq \min_{[\mathcal{G}_R^n]}\{x_i^{(0)} \rightarrow x_j^{(0)}\} \wedge x_i' - x_j' \leq \min_{[\mathcal{G}_R^n]}\{x_i^{(n)} \rightarrow x_j^{(n)}\} \wedge \\ & x_i - x_j' \leq \min_{[\mathcal{G}_R^n]}\{x_i^{(0)} \rightarrow x_j^{(n)}\} \wedge x_i' - x_j \leq \min_{[\mathcal{G}_R^n]}\{x_i^{(n)} \rightarrow x_j^{(0)}\} \end{array} \tag{4.3}$$

where $\min_{[\mathcal{G}_R^n]}\{x_i^{(p)} \rightarrow x_j^{(q)}\}$ stands for the minimal weight between all paths among the extremal vertices $x_i^{(p)}$ and $x_j^{(q)}$ in $\mathcal{G}_R^n$, for $p, q \in \{0, n\}$.

Example 4.10. Figure 1(c) depicts the 8-times unfolding of $\mathcal{G}_R$ for the relation $R(\mathbf{x}, \mathbf{x}') \equiv x_2 - x_1' \leq -1 \wedge x_3 - x_2' \leq 0 \wedge x_1 - x_3' \leq 0 \wedge x_4' - x_4 \leq 0 \wedge x_3' - x_4 \leq 0$ from Example 4.7.

The set of paths between any two extremal vertices in the unfolding graph $\mathcal{G}_R^n$ of a difference bounds relation R, for some $n > 0$, can be seen as words over the finite alphabet of subgraphs of $\mathcal{G}_R$ that are accepted by a finite weighted automaton called *zigzag automaton* [12]. Intuitively, a zigzag automaton reads, at step i in the computation, all edges between $\mathbf{x}^{(i)}$ and $\mathbf{x}^{(i+1)}$ simultaneously. The weight of a transition fired by the zigzag automaton at step i is the sum of the weights of these edges. A run of a zigzag automaton of length $n > 0$ will thus encode a path between the extremal vertices in $\mathcal{G}_R^n$. Since we are interested in the minimal weight paths (4.3), we aim at computing the minimal weight among all runs of length n, as a function of n. One of the results of [12] is that the minimal weight functions are definable in Presburger arithmetic, hence the transitive closures of difference bounds relations are Presburger definable as well. Moreover, one of the results of [10] is that these functions generate *periodic* sequences. In this paper we use zigzag automata to define the closed form of the sequence $\{\mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})\}_{n \geq 1}$ of sets (preconditions) from which larger and larger executions, of length $n = 1, 2, \ldots$ are possible. This section is concerned with the formal definition of zigzag automata.

[5] A vertex v is said to be *extremal* in $\mathcal{G}_R^n$ if $v \in (\mathbf{x}^{(0)} \cup \mathbf{x}^{(n)})$.

4.2.1. *The Zigzag Alphabet.* Without losing generality, we work with a simplified, yet equivalent, form of difference bounds relations. Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a difference bounds relation, and $R(\mathbf{x}, \mathbf{x}')$ be a difference bounds constraint defining R. We can replace all atomic propositions of the form $x - y \leq c$ in $R(\mathbf{x}, \mathbf{x}')$ by conjunctions $x - z' \leq c \ \wedge \ z' - y \leq 0$, and all atomic propositions of the form $x' - y' \leq c$ by conjunctions $x' - z \leq c \ \wedge \ z - y' \leq 0$, for some variables $z \in \mathbf{x} \setminus FV(R(\mathbf{x}, \mathbf{x}'))$, one for each replaced atomic proposition, not occurring initially in $R(\mathbf{x}, \mathbf{x}')$. We assume further on that any given difference bounds constraint $R(\mathbf{x}, \mathbf{x}')$ does not contain atomic propositions of the form $x - y \leq c$ or $x' - y' \leq c$, and that its constraint graph $\mathcal{G}_R$ is *bipartite*, i.e. it does only contain edges from $\mathbf{x}$ to $\mathbf{x}'$ or vice versa.

We define the zigzag automaton that is used to define the closed form of precondition sequences $\{\mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})\}_{n \geq 0}$, where $\mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}}) \subseteq \mathbb{Z}^{\mathbf{x}}$ are sets defined only by constraints between unprimed variables. Since $\mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}}) = \mathrm{pre}_{R^n}(\mathbb{Z}^{\mathbf{x}})$, and taking into account the definition of the n-th powers of R (4.3), these constraints correspond to minimal weight paths of the form $x_i^{(0)} \to x_j^{(0)}$ in $\mathcal{G}_R^n$. These paths are represented by words $w = w_1 \ldots w_n$, as follows: the symbol w_i represents *simultaneously* all edges of π that involve only nodes from $\mathbf{x}^{(i)} \cup \mathbf{x}^{(i+1)}$, for all $0 \leq i < n$. With these considerations, the alphabet Σ_R is the set of graphs G satisfying the following conditions:

(1) the set of nodes of G is $\mathbf{x} \cup \mathbf{x}'$
(2) for any $x, y \in \mathbf{x} \cup \mathbf{x}'$, there is an edge labeled with $c \in \mathbb{Z}$ from x to y only if $(x - y \leq c) \in \mathit{Atom}(\phi)$
(3) the in-degree and out-degree of each node are at most one
(4) the number of edges from $\mathbf{x}$ to $\mathbf{x}'$ equals the number of edges from $\mathbf{x}'$ to $\mathbf{x}$

We denote by Σ_R^+ the set of all non-empty words using symbols from Σ_R. The weight of any symbol $G \in \Sigma_R$, denoted $\omega(G)$, is the sum of the weights that occur on its edges. For a word $w = w_1 w_2 \ldots w_n \in \Sigma_R^+$, we define its weight as $\omega(w) = \sum_{i=1}^n \omega(w_i)$.

Example 4.11. Figure 1(e) shows the zigzag alphabet Σ_R for the difference bounds relation $R \Leftrightarrow x_2 - x_1' \leq -1 \wedge x_3 - x_2' \leq 0 \wedge x_1 - x_3' \leq 0 \wedge x_4' - x_4 \leq 0 \wedge x_3' - x_4 \leq 0$ from Example 4.7.

4.2.2. *The Transition Table of Zigzag Automata.* For each pair of variables $x_i, x_j \in \mathbf{x} = \{x_1, \ldots, x_N\}$, we define an automaton $\mathcal{A}_{ij}$ that encodes all paths from $\mathcal{G}_R^n$, starting in $x_i^{(0)}$ and ending in $x_j^{(0)}$, for some $n > 0$. These automata share the same alphabet and transition table, and differ only by the choice of the sets of initial and final states. The common transition table is defined as $T_R = \langle Q, \delta \rangle$, where the set of states Q is the set of N-tuples $\mathbf{q} = \langle \mathbf{q}_1, \ldots, \mathbf{q}_N \rangle$ of symbols $\mathbf{q}_i \in \{\ell, r, \ell r, r\ell, \perp\}$ capturing the direction of the incoming and outgoing edges of the alphabet symbols: ℓ for a path traversing from right to left, r for a path traversing from left to right, ℓr for a right incoming and right outgoing path, $r\ell$ for a left incoming and left outgoing path, and $\perp$ when there are no incoming nor outgoing edges from that node (see Figure 1(g) for an example of the use of states in a zigzag automaton). The set of transitions δ is the set of transitions of the form $\mathbf{q} \xrightarrow{G} \mathbf{q}'$ such that for every $1 \leq i \leq N$:

- $\mathbf{q}_i = \ell$ iff G has one edge whose destination is x_i, and no other edge involving x_i,
- $\mathbf{q}'_i = \ell$ iff G has one edge whose source is x_i', and no other edge involving x_i',
- $\mathbf{q}_i = r$ iff G has one edge whose source is x_i, and no other edge involving x_i,
- $\mathbf{q}'_i = r$ iff G has one edge whose destination is x_i', and no other edge involving x_i',

- $\mathbf{q}_i = \ell r$ iff G has exactly two edges involving x_i, one having x_i as source, and another as destination,
- $\mathbf{q'}_i = r\ell$ iff G has exactly two edges involving x'_i, one having x'_i as source, and another as destination,
- $\mathbf{q'}_i \in \{\ell r, \bot\}$ iff G has no edge involving x'_i,
- $\mathbf{q}_i \in \{r\ell, \bot\}$ iff G has no edge involving x_i.

The weight of each transition $\mathbf{q} \xrightarrow{G} \mathbf{q'}$ from δ is the weight of its symbol $\omega(G)$. The weight of a run $\pi : q_1 \xrightarrow{a_1} q_2 \xrightarrow{a_2} \ldots \xrightarrow{a_n} q_{n+1}$, $n \geq 1$, is defined as $\omega(\pi) \overset{def}{=} \sum_{i=1}^{n} \omega(a_i)$.

The zigzag automaton recognizing paths from $x_i^{(0)}$ to $x_j^{(0)}$, for two distinct indices $1 \leq i, j \leq N$, $i \neq j$, is defined as $\mathcal{A}_{ij} = \langle T_R, I_{ij}, F \rangle$, where $I_{ij}, F \subseteq \{\ell, r, \ell r, r\ell, \bot\}^N$ are the sets of initial and final states, respectively:

$$\begin{array}{rcl} I_{ij} & = & \{\mathbf{q} \mid \mathbf{q}_i = r,\ \mathbf{q}_j = \ell,\ \mathbf{q}_h \in \{\ell r, \bot\},\ \forall h \in \{1, \ldots, N\} \setminus \{i, j\}\} \\ F & = & \{r\ell, \bot\}^N \end{array}$$

The zigzag automaton recognizing elementary cycles that traverse $x_i^{(0)}$ for some $1 \leq i \leq N$, is defined as $\mathcal{A}_{ii} = \langle T_R, I_{ii}, F \rangle$ where T_R and F are as defined previously and

$$I_{ii} = \{\mathbf{q} \mid \mathbf{q}_i = \ell r,\ \mathbf{q}_h \in \{\ell r, \bot\},\ \forall h \in \{1, \ldots, N\} \setminus \{i\}\}$$

Since the set of states of a zigzag automaton is the set of tuples $\{\ell, r, \ell r, r\ell, \bot\}^N$, then the number of states reachable from an initial state, and co-reachable from a final state is bounded by 5^N. In the following, we denote runs of the form $q_1 \xrightarrow{a_1} q_2 \xrightarrow{a_2} \ldots \xrightarrow{a_n} q_{n+1}$ in the zigzag automata by $q_1 \xrightarrow{a_1 \ldots a_n} q_{n+1}$. Given words $w_1, w_2 \in \Sigma_R^*$ and runs $\pi_1 = q_1 \xrightarrow{w_1} q_2$ and $\pi_2 = q_2 \xrightarrow{w_2} q_3$ of some zigzag automaton $\mathcal{A}_{ij}$, we write $\pi = \pi_1.\pi_2$ to denote their concatenation $q_1 \xrightarrow{w_1} q_2 \xrightarrow{w_2} q_3$.

Example 4.12. Figure 1(d) shows the zigzag automaton $\mathcal{A}_{24}$ of the difference bounds relation $R \Leftrightarrow x_2 - x'_1 \leq -1 \ \wedge\ x_3 - x'_2 \leq 0 \ \wedge\ x_1 - x'_3 \leq 0 \ \wedge\ x'_4 - x_4 \leq 0 \ \wedge\ x'_3 - x_4 \leq 0$ from Example 4.7 and Example 4.11. Note that useless[6] control states are not shown and hence the alphabet symbols G_6 and G_7 are not used. Figure 1(f) shows a path $x_2^{(0)} \to \ldots \to x_4^{(0)}$ from $\mathcal{G}_R^8$ which is encoded by the word $\gamma = G_3.(G_1.G_2.G_3)^2.G_4$. Figure 1(g) shows a run of $\mathcal{A}_{24}$ that accepts γ. The weights of the symbols in the word are $\omega(G_1) = \omega(G_2) = \omega(G_4) = 0$, $\omega(G_3) = -1$, hence $\omega(\gamma) = -3$.

4.2.3. *Language and Periodicity of Zigzag Automata.* We recall that $\mathcal{G}_R^n$ denotes the constraint graph obtained by concatenating the constraint graph of R to itself $n > 0$ times. A run of the zigzag automaton $\mathcal{A}_{ij} = \langle T_R, I_{ij}, F \rangle$, for some $1 \leq i, j \leq N$ is said to be *accepting* if it starts with a state from I_{ij} and it ends with a state from F. The following lemma relates certain paths in $\mathcal{G}_R^n$ to runs in zigzag automata.

Lemma 4.13 ([12]). *Let $R(\mathbf{x}, \mathbf{x'})$ be a difference bounds constraint defining a relation and let $\mathcal{G}_R$ be its constraint graph. Then for any $n \geq 1$ such that $R^n(\mathbf{x}, \mathbf{x'})$ is consistent and any $1 \leq i, j \leq N$, $i \neq j$, $\mathcal{A}_{ij}$ has an accepting run of length n if and only if there exists a path in $\mathcal{G}_R^n$, from $x_i^{(0)}$ to $x_j^{(0)}$. Moreover,*

$$(M^*_{R^n})_{ij} \ = \ \min\{\omega(\pi) \mid \pi \text{ is an accepting run in } \mathcal{A}_{ij} \text{ of length } n\}$$

[6] A control state is *useless* if it is not reachable from an initial state or no final state is reachable from it.

Furthermore, for any $n \geq 1$, $R^n(\mathbf{x}, \mathbf{x}')$ is inconsistent if and only if A_{ii} has an accepting run π such that $|\pi| = n$ and $\omega(\pi) < 0$ for some $1 \leq i \leq N$.

Proof. See [12], Lemma 4.3. □

The formula (4.3) defining the powers of a difference bounds relation R says that, if R^n is consistent, for a given $n > 0$, then R^n is definable by a closed DBM[7] $M_{R^n} \in \mathbb{Z}^{2N \times 2N}$. It follows that the set $\mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})$ is defined by ${}^{\blacksquare}M_n$, for any $n > 0$. Moreover, by (4.3), $({}^{\blacksquare}M_n)_{ij}$ is the minimum weight among all accepting runs of length n of $\mathcal{A}_{ij}$. In the following, we show that the sequence of matrices $\{{}^{\blacksquare}M_{R^n}\}_{n \geq 1}$ is *periodic* in the following sense:

Definition 4.14. An infinite sequence of integers $\{m_k\}_{k=1}^{\infty} \in \mathbb{Z}$ is said to be *periodic* if and only if:

$$\exists b \geq 1 \; \exists c \geq 1 \; \exists \lambda_0, \lambda_1, \ldots, \lambda_{c-1} \in \mathbb{Z} \; . \; m_{b+(k+1)c+i} = \lambda_i + m_{b+kc+i}$$

for all $k \geq 1$ and $i = 0, 1, \ldots, c-1$. An infinite sequence of matrices $\{M_k\}_{k=1}^{\infty} \in \mathbb{Z}_{\infty}^{N \times N}$ is said to be *periodic* if and only if:

$$\exists b \geq 1 \; \exists c \geq 1 \; \exists \Lambda_0, \Lambda_1, \ldots, \Lambda_{c-1} \in \mathbb{Z}_{\infty}^{N \times N} \; . \; M_{b+(k+1)c+i} = \Lambda_i + M_{b+kc+i}$$

for all $k \geq 1$ and $i = 0, 1, \ldots, c-1$. The smallest b, c for which the above holds are called the *prefix* and *period* of the periodic sequence, respectively. $\Lambda_0, \Lambda_1, \ldots, \Lambda_{c-1}$ are called the *rates* of the periodic sequence.

Intuitively, the elements situated at equal distances ($c \geq 1$) beyond a certain threshold ($b \geq 1$) in a periodic sequence, differ by equal quantities. The following proposition establishes the equivalence between periodic sequences of integers and matrices:

Proposition 4.15. *An infinite sequence of matrices $\{M_k\}_{k=1}^{\infty} \in \mathbb{Z}_{\infty}^{N \times N}$ is periodic if and only if the sequences $\{(M_k)_{ij}\}_{k=1}^{\infty} \in \mathbb{Z}_{\infty}$ are periodic, for all $1 \leq i, j \leq N$. Moreover, the prefix, period and rates of the $\{M_k\}_{k=1}^{\infty}$ sequence are effectively computable given the prefix, period and rates of the $\{(M_k)_{ij}\}_{k=1}^{\infty}$ sequences, respectively.*

Proof. See Lemma 1 in [10]. □

Periodicity of integer sequences is preserved by several arithmetic operations, as shown by the following lemma:

Lemma 4.16. *Let $\{s_k\}_{k=1}^{\infty} \in \mathbb{Z}_{\infty}$ and $\{t_k\}_{k=1}^{\infty}$ be two periodic sequences of integers, of given prefix, period and rates. Then the sequences $\{\min(s_k, t_k)\}_{k=1}^{\infty}$, $\{s_k + t_k\}_{k=1}^{\infty}$ and $\{\lfloor \frac{s_k}{2} \rfloor\}_{k=1}^{\infty}$ are periodic, and moreover, their prefix, period and rates are effectively computable, respectively.*

Proof. See Lemma 6 in [10]. □

Formally, a *weighted digraph* is a tuple $G = \langle V, E, \omega \rangle$, where V is a set of vertices, $E \subseteq V \times V$ is a set of edges, and $\omega : E \to \mathbb{Z}$ is a weight function. The following theorem shows that the matrices giving the weights of the minimal weight paths of a given length in a weighted graph form a periodic sequence of matrices.

Theorem 4.17. *Let $G = \langle V, E, \omega \rangle$ be a weighted graph, $V = \{v_1, \ldots, v_N\}$ be its set of vertices, and let $\{A_n\}_{n \geq 1}$ be the sequence of matrices $A_n \in \mathbb{Z}_{\infty}^{N \times N}$, where for all $1 \leq i, j \leq N$, $(A_n)_{ij}$ is the minimal weight among all paths of length n from v_i to v_j in G. Then $\{A_n\}_{n \geq 1}$ is a periodic sequence, and its prefix, period and rates are effectively computable.*

Proof. See, e.g. Theorem 3.3 in [38]. □

[7] Since the coefficients of the DBM are minimal weight paths, the triangle inequality holds.

An important consequence of Theorem 4.17 is that, for a $*$-consistent difference bounds relation R, the sequence of sets $\{\mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}})\}_{n\geq 1}$ is definable by a periodic sequence of difference bounds matrices.

Corollary 4.18. *Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$, where $\mathbf{x} = \{x_1, \ldots, x_N\}$, be a $*$-consistent difference bounds relation. Then, for all $n \geq 1$, the difference bounds constraint $\Delta[{}^{\blacksquare}M^*_{R^n}]$ defines $\mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}})$. Moreover, the sequence $\{{}^{\blacksquare}M^*_{R^n}\}_{n\geq 1}$ is periodic, and its prefix, period and rates are all effectively computable.*

Proof. Since R is $*$-consistent, $\mathcal{G}^n_R$ does not have negative cycles, for any $n > 0$, hence the minimum $\min_{[\mathcal{G}^n_R]}\{x_i^{(0)} \to x_j^{(0)}\}$ is well defined, for all $1 \leq i, j \leq N$, $i \neq j$. Since R^n is defined by the difference bounds constraint (4.3), and since the triangle inequality:

$$\min_{[\mathcal{G}^n_R]}\{x_i^{(0)} \to x_j^{(0)}\} \leq \min_{[\mathcal{G}^n_R]}\{x_i^{(0)} \to x_k^{(0)}\} + \min_{[\mathcal{G}^n_R]}\{x_k^{(0)} \to x_j^{(0)}\}$$

holds for all pairwise distinct indices $1 \leq i, j, k \leq N$, then we have:

$$({}^{\blacksquare}M^*_{R^n})_{ij} = \min_{[\mathcal{G}^n_R]}\{x_i^{(0)} \to x_j^{(0)}\}$$

for all $1 \leq i, j \leq N$, where $i \neq j$, by the uniqueness of the closure for DBMs. Clearly,

$$({}^{\blacksquare}M^*_{R^n})_{ii} = 0$$

for all $1 \leq i \leq N$, by Definition 4.4. Then $\mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}}) = \mathrm{pre}_{R^n}(\mathbb{Z}^{\mathbf{x}})$ is defined by the constraint $\exists \mathbf{x}' \,.\, R^n(\mathbf{x}, \mathbf{x}') \Leftrightarrow \Delta[{}^{\blacksquare}M^*_{R^n}]$.

To prove that the sequence of matrices $\{{}^{\blacksquare}M^*_{R^n}\}_{n\geq 1}$ is periodic, it is enough to show that, for all $1 \leq i, j \leq N$, the sequence of integers $\{({}^{\blacksquare}M^*_{R^n})_{ij}\}_{n\geq 1}$ is periodic (by Proposition 4.15). Clearly $\{({}^{\blacksquare}M^*_{R^n})_{ii}\}_{n\geq 1}$ is periodic, because $({}^{\blacksquare}M^*_{R^n})_{ii} = 0$, for all $1 \leq i \leq N$ and all $n \geq 1$ (Definition 4.4).

Let $T_R = \langle Q, \delta, \omega \rangle$, $Q = \{q_1, \ldots, q_{5^N}\}$, be the common transition table of all zigzag automata $\mathcal{A}_{ij} = \langle T_R, I_{ij}, F \rangle$ for R. Then, by Theorem 4.17, the sequence $\{\mathcal{T}_m\}_{m\geq 0}$ is periodic, where $\mathcal{T}_m \in \mathbb{Z}^{5^N \times 5^N}$ is the matrix defined as: $(\mathcal{T}_m)_{k\ell}$ is the minimum weight among all paths of length m between q_k and q_ℓ in T_R, $1 \leq k, \ell \leq 5^N$. By Lemma 4.13, we have:

$$\begin{array}{rcl}({}^{\blacksquare}M^*_{R^n})_{ij} & = & \min\{\omega(\rho) \mid \rho \text{ is an accepting run of length } n \text{ in } \mathcal{A}_{ij}\} \\ & = & \min\{(\mathcal{T}_m)_{k\ell} \mid q_k \in I_{ij}, q_\ell \in F\}\end{array}$$

By Lemma 4.16, we obtain that the sequence $\{{}^{\blacksquare}(M^*_{R^n})_{ij}\}_{n\geq 1}$ is periodic. The effective computability of the prefix, period, and rates of the $\{{}^{\blacksquare}M^*_{R^n}\}_{n\geq 1}$ sequence follows from the constructive arguments of Theorem 4.17, Proposition 4.15 and Lemma 4.16, respectively. □

Example 4.19. Consider the difference bounds constraint $R(\mathbf{x}, \mathbf{x}') \equiv x_2 - x_1' \leq -1 \wedge x_3 - x_2' \leq 0 \wedge x_1 - x_3' \leq 0 \wedge x_4' - x_4 \leq 0 \wedge x_3' - x_4 \leq 0$ from Example 4.7. We compute the sequence $\{{}^{\blacksquare}M^*_{R^n}\}_{n\geq 0}$. Since R is $*$-consistent, the DBM ${}^{\blacksquare}M^*_{R^n}$ can be defined for each $n \geq 1$ as

$$({}^{\blacksquare}M^*_{R^n})_{ij} = \begin{cases} 0 & \text{if } i = j \\ \min\{\omega(\rho) \mid \rho \text{ is a path from } x_i^{(0)} \text{ to } x_j^{(0)} \text{ in } \mathcal{G}^n_R\} \cup \{\infty\} & \text{if } i \neq j \end{cases}$$

by (4.3) (see Fig. 1 for $\mathcal{G}^8_R$). The first 11 elements of the sequence are depicted in Figure 2. The periodic behavior can be observed for prefix $b = 3$, period $c = 3$, and rates $\Lambda_0, \Lambda_1, \Lambda_2$ defined in Figure 2. For example, ${}^{\blacksquare}M^*_{R^6} = {}^{\blacksquare}M^*_{R^3} + \Lambda_0$, ${}^{\blacksquare}M^*_{R^9} = {}^{\blacksquare}M^*_{R^6} + \Lambda_0$, etc. □

$$\begin{array}{ccccc} {}^{\blacksquare}M^*_{R^1} & x_1 & x_2 & x_3 & x_4 \\ x_1 & 0 & \infty & \infty & 0 \\ x_2 & \infty & 0 & \infty & \infty \\ x_3 & \infty & \infty & 0 & \infty \\ x_4 & \infty & \infty & \infty & 0 \end{array} \qquad \begin{array}{ccccc} {}^{\blacksquare}M^*_{R^2} & x_1 & x_2 & x_3 & x_4 \\ x_1 & 0 & \infty & \infty & 0 \\ x_2 & \infty & 0 & \infty & -1 \\ x_3 & \infty & \infty & 0 & \infty \\ x_4 & \infty & \infty & \infty & 0 \end{array}$$

$$\begin{array}{ccccc} {}^{\blacksquare}M^*_{R^3} & x_1 & x_2 & x_3 & x_4 \\ x_1 & 0 & \infty & \infty & -1 \\ x_2 & \infty & 0 & \infty & -1 \\ x_3 & \infty & \infty & 0 & -1 \\ x_4 & \infty & \infty & \infty & 0 \end{array} \qquad \begin{array}{ccccc} {}^{\blacksquare}M^*_{R^4} & x_1 & x_2 & x_3 & x_4 \\ x_1 & 0 & \infty & \infty & -1 \\ x_2 & \infty & 0 & \infty & -2 \\ x_3 & \infty & \infty & 0 & -1 \\ x_4 & \infty & \infty & \infty & 0 \end{array} \qquad \begin{array}{ccccc} {}^{\blacksquare}M^*_{R^5} & x_1 & x_2 & x_3 & x_4 \\ x_1 & 0 & \infty & \infty & -1 \\ x_2 & \infty & 0 & \infty & -2 \\ x_3 & \infty & \infty & 0 & -2 \\ x_4 & \infty & \infty & \infty & 0 \end{array}$$

$$\begin{array}{ccccc} {}^{\blacksquare}M^*_{R^6} & x_1 & x_2 & x_3 & x_4 \\ x_1 & 0 & \infty & \infty & -2 \\ x_2 & \infty & 0 & \infty & -2 \\ x_3 & \infty & \infty & 0 & -2 \\ x_4 & \infty & \infty & \infty & 0 \end{array} \qquad \begin{array}{ccccc} {}^{\blacksquare}M^*_{R^7} & x_1 & x_2 & x_3 & x_4 \\ x_1 & 0 & \infty & \infty & -2 \\ x_2 & \infty & 0 & \infty & -3 \\ x_3 & \infty & \infty & 0 & -2 \\ x_4 & \infty & \infty & \infty & 0 \end{array} \qquad \begin{array}{ccccc} {}^{\blacksquare}M^*_{R^8} & x_1 & x_2 & x_3 & x_4 \\ x_1 & 0 & \infty & \infty & -2 \\ x_2 & \infty & 0 & \infty & -3 \\ x_3 & \infty & \infty & 0 & -3 \\ x_4 & \infty & \infty & \infty & 0 \end{array}$$

$$\begin{array}{ccccc} {}^{\blacksquare}M^*_{R^9} & x_1 & x_2 & x_3 & x_4 \\ x_1 & 0 & \infty & \infty & -3 \\ x_2 & \infty & 0 & \infty & -3 \\ x_3 & \infty & \infty & 0 & -3 \\ x_4 & \infty & \infty & \infty & 0 \end{array} \qquad \begin{array}{ccccc} {}^{\blacksquare}M^*_{R^{10}} & x_1 & x_2 & x_3 & x_4 \\ x_1 & 0 & \infty & \infty & -3 \\ x_2 & \infty & 0 & \infty & -4 \\ x_3 & \infty & \infty & 0 & -3 \\ x_4 & \infty & \infty & \infty & 0 \end{array} \qquad \begin{array}{ccccc} {}^{\blacksquare}M^*_{R^{11}} & x_1 & x_2 & x_3 & x_4 \\ x_1 & 0 & \infty & \infty & -3 \\ x_2 & \infty & 0 & \infty & -4 \\ x_3 & \infty & \infty & 0 & -4 \\ x_4 & \infty & \infty & \infty & 0 \end{array}$$

$$b = 3, c = 3, \Lambda_0 = \Lambda_1 = \Lambda_2 = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

FIGURE 2. Periodic behavior of the infinite sequence $\{{}^{\blacksquare}M^*_{R^n}\}_{n\geq 1}$ where $R \Leftrightarrow x_2 - x_1' \leq -1 \wedge x_3 - x_2' \leq 0 \wedge x_1 - x_3' \leq 0 \wedge x_4' - x_4 \leq 0 \wedge x_3' - x_4 \leq 0$.

4.3. **Octagonal Constraints.** Octagonal constraints are a generalization of difference bounds constraints to conjunctions of atomic propositions of the form $\pm x \pm y \leq c$, $c \in \mathbb{Z}$. An octagonal constraint $\phi(x_1, \ldots, x_N)$ is usually represented by a difference bounds constraints $\phi(y_1, \ldots, y_{2N})$ where y_{2i-1} stands for $+x_i$ and y_{2i} stands for $-x_i$, with the implicit requirement that $y_{2i-1} = -y_{2i}$, for each $1 \leq i \leq N$. It is important to notice that this implicit condition cannot be directly represented as a difference constraint. The class of integer octagonal constraints is formally defined as follows:

Definition 4.20. A formula $\phi(\mathbf{x})$ is an *octagonal constraint* if it is a finite conjunction of terms of the form $x_i - x_j \leq a_{ij}$, $x_i + x_j \leq b_{ij}$ or $-x_i - x_j \leq c_{ij}$ where $a_{ij}, b_{ij}, c_{ij} \in \mathbb{Z}$, for all $1 \leq i, j \leq N$.

We represent octagons as difference bounds constraints over the dual 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 example, the octagonal constraint $x_1 + x_2 = 3$ is represented as $y_1 - y_4 \leq 3 \wedge y_2 - y_3 \leq -3$. In order to handle the $\mathbf{y}$ variables in the following, we define $\bar{\imath} = i - 1$, if i is even, and $\bar{\imath} = i + 1$ if i is odd. Obviously, we have $\bar{\bar{\imath}} = i$, for all $i \in \mathbb{Z}$, $i \geq 1$. We denote by $\overline{\phi}(\mathbf{y})$ the difference bounds constraint over $\mathbf{y}$ that represents $\phi(\mathbf{x})$ and which is defined as follows:

Definition 4.21. Given an octagonal constraint $\phi(\mathbf{x})$, $\mathbf{x} = \{x_1, \ldots, x_N\}$, its difference bounds representation $\overline{\phi}(\mathbf{y})$, where $\mathbf{y} = \{y_1, \ldots, y_{2N}\}$ is a conjunction of the following difference bounds constraints where $1 \leq i, j \leq N$, $c \in \mathbb{Z}$.

$$\begin{array}{lcl}
(x_i - x_j \leq c) \in Atom(\phi) & \Leftrightarrow & (y_{2i-1} - y_{2j-1} \leq c), (y_{2j} - y_{2i} \leq c) \in Atom(\overline{\phi}) \\
(-x_i + x_j \leq c) \in Atom(\phi) & \Leftrightarrow & (y_{2j-1} - y_{2i-1} \leq c), (y_{2i} - y_{2j} \leq c) \in Atom(\overline{\phi}) \\
(-x_i - x_j \leq c) \in Atom(\phi) & \Leftrightarrow & (y_{2i} - y_{2j-1} \leq c), (y_{2j} - y_{2i-1} \leq c) \in Atom(\overline{\phi}) \\
(x_i + x_j \leq c) \in Atom(\phi) & \Leftrightarrow & (y_{2i-1} - y_{2j} \leq c), (y_{2j-1} - y_{2i} \leq c) \in Atom(\overline{\phi})
\end{array}$$

An octagonal constraint ϕ is equivalently represented by the DBM $M_{\overline{\phi}} \in \mathbb{Z}_{\infty}^{2N \times 2N}$, corresponding to $\overline{\phi}$. We sometimes write M_ϕ instead of $M_{\overline{\phi}}$. We say that a DBM $M \in \mathbb{Z}_{\infty}^{2N \times 2N}$ is *coherent* iff $M_{ij} = M_{\bar{j}\bar{\imath}}$ for all $1 \leq i, j \leq 2N$. This property is needed since, for example, an atomic proposition $x_i - x_j \leq a_{ij}$, $1 \leq i, j \leq N$, can be represented as both $y_{2i-1} - y_{2j-1} \leq a_{ij}$ and $y_{2j} - y_{2i} \leq a_{ij}$. Dually, a coherent DBM $M \in \mathbb{Z}_{\infty}^{2N \times 2N}$ corresponds to the following octagonal constraint:

$$\begin{array}{lcl}
\Omega[M] & \equiv & \bigwedge_{\substack{1 \leq i,j \leq N \\ M_{2i-1,2j-1} < \infty}} x_i - x_j \leq M_{2i-1,2j-1} \wedge \\
& & \bigwedge_{\substack{1 \leq i,j \leq N \\ M_{2i-1,2j} < \infty}} x_i + x_j \leq M_{2i-1,2j} \wedge \\
& & \bigwedge_{\substack{1 \leq i,j \leq N \\ M_{2i,2j-1} < \infty}} -x_i - x_j \leq M_{2i,2j-1}
\end{array} \tag{4.4}$$

Given an octagonal constraint $\phi(\mathbf{x})$, we have the following equivalences:

$$\begin{array}{lcl}
\phi(\mathbf{x}) & \Leftrightarrow & (\exists y_2, y_4, \ldots, y_{2N} \,.\, \overline{\phi}(\mathbf{y}) \wedge \bigwedge_{i=1}^{N} y_{2i-1} = -y_{2i})[x_i/y_{2i-1}]_{i=1}^{N} \\
& \Leftrightarrow & \overline{\phi}(\mathbf{y})[x_i/y_{2i-1}, -x_i/y_{2i}]_{i=1}^{N} \\
& \Leftrightarrow & \Omega[M_{\overline{\phi}}]
\end{array} \tag{4.5}$$

A coherent DBM M is said to be *octagonal-consistent* if and only if $\Omega[M]$ is consistent.

For each octagonal constraint $\phi(\mathbf{x})$, we define $\mu(\phi)$ to be the maximal absolute value over all constants that appear in $\phi(\mathbf{x})$, formally: $\mu(\phi) \overset{def}{=} \max\{|c| \mid (\pm x_i \pm x_j \leq c) \in Atom(\phi)\}$.

Definition 4.22. An octagonal-consistent coherent DBM $M \in \mathbb{Z}_{\infty}^{2N \times 2N}$ is said to be *tightly closed* if and only if it is closed and $M_{ij} \leq \lfloor \frac{M_{i\bar{\imath}}}{2} \rfloor + \lfloor \frac{M_{\bar{j}j}}{2} \rfloor$, for all $1 \leq i, j \leq N$.

The last condition from Definition 4.22 ensures that the knowledge induced by the implicit conditions $y_i + y_{\bar{\imath}} = 0$, which cannot be represented as difference constraints, has been propagated through the DBM. Since $2y_i = y_i - y_{\bar{\imath}} \leq M_{i\bar{\imath}}$ and $-2y_j = y_{\bar{j}} - y_j \leq M_{\bar{j}j}$, we have $y_i \leq \lfloor \frac{M_{i\bar{\imath}}}{2} \rfloor$ and $-y_j \leq \lfloor \frac{M_{\bar{j}j}}{2} \rfloor$, which implies $y_i - y_j \leq \lfloor \frac{M_{i\bar{\imath}}}{2} \rfloor + \lfloor \frac{M_{\bar{j}j}}{2} \rfloor$, thus $M_{ij} \leq \lfloor \frac{M_{i\bar{\imath}}}{2} \rfloor + \lfloor \frac{M_{\bar{j}j}}{2} \rfloor$ must hold, if M is supposed to be the most precise DBM representation of an octagonal constraint. Moreover, by taking $j = \bar{\imath}$ in the previous, we have $M_{i\bar{\imath}} \leq 2\lfloor \frac{M_{i\bar{\imath}}}{2} \rfloor$, implying that $M_{i\bar{\imath}}$ is necessarily even, if M is tightly closed.

The following theorem from [2] provides an effective way of testing octagonal-consistency and computing the tight closure of a coherent DBM. Moreover, it shows that the tight closure of a given DBM is unique and can also be computed with the same worst-case time complexity as the DBM closure.

Theorem 4.23. *([2]) Let $M \in \mathbb{Z}_{\infty}^{2N \times 2N}$ be a coherent DBM. Then M is octagonal-consistent if and only if M is consistent and $\lfloor \frac{M^*_{i\bar{\imath}}}{2} \rfloor + \lfloor \frac{M^*_{\bar{\imath}i}}{2} \rfloor \geq 0$, for all $1 \leq i \leq 2N$. Moreover, if M*

is octagonal-consistent, the tight closure of M is the DBM $M^t \in \mathbb{Z}_\infty^{2N \times 2N}$ defined as:

$$M^t_{ij} = \min \left\{ M^*_{ij}, \left\lfloor \frac{M^*_{i\bar{\imath}}}{2} \right\rfloor + \left\lfloor \frac{M^*_{\bar{\jmath}j}}{2} \right\rfloor \right\}$$

for all $1 \leq i, j \leq 2N$ where $M^* \in \mathbb{Z}_\infty^{2N \times 2N}$ is the closure of M.

Corollary 4.24. *Let $\phi(\mathbf{x})$ be an octagonal constraint for some $\mathbf{x} = \{x_1, \ldots, x_N\}$ and $N \geq 1$. Then, consistency of ϕ can be decided in at most $\mathcal{O}(N^3 \cdot (N + \mu(\phi)))$ time. Moreover, it ϕ is consistent, $M^t_{\overline{\phi}}$ can be computed in at most $\mathcal{O}(N^3 \cdot (N + \mu(\phi)))$ time as well.*

Proof. An immediate consequence of Theorem 4.23 and Proposition 4.5. □

Given an octagonal-consistent coherent DBM $M \in \mathbb{Z}_\infty^{2N \times 2N}$, we denote by M^t the (unique) tightly closed DBM such that $\Omega[M] \Leftrightarrow \Omega[M^t]$. The tight closure of DBMs is needed for checking equivalence and entailment between octagonal constraints.

Proposition 4.25. *Let $\phi_1(\mathbf{x})$ and $\phi_2(\mathbf{x})$ be two consistent octagonal constraints. Then,*
(1) $\phi_1 \Leftrightarrow \phi_2$ if and only if $M^t_{\overline{\phi_1}} = M^t_{\overline{\phi_2}}$,
(2) $\phi_1 \Rightarrow \phi_2$ if and only if $M^t_{\overline{\phi_1}} \leq M^t_{\overline{\phi_2}}$.

Proof. Points (1) and (2) are Theorem 4.4.1 (points 4 and 5, respectively) in [28]. □

Moreover, the following proposition shows that octagonal constraints are closed under existential quantification.

Proposition 4.26. *Let $\phi(\mathbf{x})$, where $\mathbf{x} = \{x_1, \ldots, x_N\}$, be a consistent octagonal constraint. Further, let $1 \leq k \leq N$ and M' be the DBM obtained from $M^t_{\overline{\phi}}$ by eliminating the lines and columns $2k-1$ and $2k$. Then, M' is tightly closed, and*

- $\Omega[M'] \Leftrightarrow \exists x_k . \phi(\mathbf{x})$
- $\exists x_k \ . \ \phi(\mathbf{x}) \Leftrightarrow \big(\exists y_{2k-1}, y_{2k} \ . \ \overline{\phi}(\mathbf{y})\big)[x_i/y_{2i-1}, -x_i/y_{2i}]_{i \in \{1,\ldots,N\} \setminus \{k\}}$

Proof. For the first point, see Theorem 2 in [7]. For the second point, let us define the substitution $\sigma \overset{def}{=} [x_i/y_{2i-1}, -x_i/y_{2i}]_{i \in \{1,\ldots,N\}}$. We first prove that $\Delta[P^*][\sigma] \Leftrightarrow \Delta[P^t][\sigma]$ for every octagonal-consistent coherent DBM $P \in \mathbb{Z}_\infty^{2N \times 2N}$. By Theorem 4.23, it is sufficient to prove that for every $1 \leq i, j \leq 2N$ such that $P^*_{i\bar{\imath}} < \infty$ and $P^*_{\bar{\jmath}j} < \infty$, the following holds:

$$\Delta[M^*][\sigma] \Rightarrow \big(y_i - y_j \leq \lfloor \frac{P^*_{i\bar{\imath}}}{2} \rfloor + \lfloor \frac{P^*_{\bar{\jmath}j}}{2} \rfloor\big)[\sigma] \tag{4.6}$$

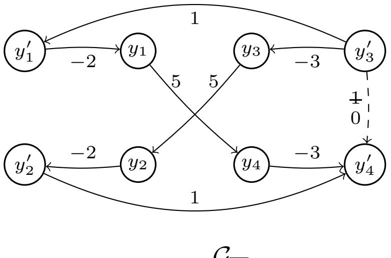
Clearly, there exists $1 \leq k, \ell \leq N$ such that either of the following holds:

$$\begin{array}{llll} (1) & i = 2k-1, \quad j = 2\ell - 1 & (3) & i = 2k, \quad j = 2\ell - 1 \\ (2) & i = 2k-1, \quad j = 2\ell & (4) & i = 2k, \quad j = 2\ell \end{array}$$

We give the proof for the first case (the other being symmetric). Then, (4.6) is equivalent to $\Delta[M^*][\sigma] \Rightarrow x_k - k_\ell \leq \lfloor \frac{P^*_{i\bar{\imath}}}{2} \rfloor + \lfloor \frac{P^*_{\bar{\jmath}j}}{2} \rfloor$. Clearly, $\Delta[P^*] \Rightarrow (y_i - y_{\bar{\imath}} \leq P^*_{i\bar{\imath}}) \ \wedge \ (y_{\bar{\jmath}} - y_j \leq P^*_{\bar{\jmath}j})$ and consequently,

$$\begin{array}{rcl} \Delta[P^*][\sigma] & \Rightarrow & (x_k + x_k \leq P^*_{i\bar{\imath}}) \ \wedge \ (-x_\ell - x_\ell \leq P^*_{\bar{\jmath}j}) \\ & \Rightarrow & x_k \leq \lfloor \frac{P^*_{i\bar{\imath}}}{2} \rfloor \ \wedge \ -x_\ell \leq \lfloor \frac{P^*_{\bar{\jmath}j}}{2} \rfloor \\ & \Rightarrow & x_k - x_\ell \leq \lfloor \frac{P^*_{i\bar{\imath}}}{2} \rfloor + \lfloor \frac{P^*_{\bar{\jmath}j}}{2} \rfloor \end{array}$$

Hence, (4.6) holds.



$\mathcal{G}_{\overline{R}}$

$$\begin{array}{c|cccccccc} & y_1 & y_2 & y_3 & y_4 & y'_1 & y'_2 & y'_3 & y'_4 \\ \hline y_1 & 0 & \infty & \infty & 5 & \infty & \infty & \infty & 2 \\ y_2 & \infty & 0 & \infty & \infty & \infty & -2 & \infty & -1 \\ y_3 & \infty & 5 & 0 & \infty & \infty & 3 & \infty & 4 \\ y_4 & \infty & \infty & \infty & 0 & \infty & \infty & \infty & -3 \\ y'_1 & -2 & \infty & \infty & 3 & 0 & \infty & \infty & 0 \\ y'_2 & \infty & \infty & \infty & \infty & \infty & 0 & \infty & 1 \\ y'_3 & -1 & 2 & -3 & 4 & 1 & 0 & 0 & 0 \\ y'_4 & \infty & \infty & \infty & \infty & \infty & \infty & \infty & 0 \end{array}$$

$M^t_{\overline{R}}$

FIGURE 3. Graph and matrix representation of the difference bounds representation $\overline{R}(\mathbf{y},\mathbf{y}')$ of an octagonal relation $R(\mathbf{x},\mathbf{x}') \equiv x_1+x_2 \leq 5 \wedge x'_1-x_1 \leq -2 \wedge x'_2 - x_2 \leq -3 \wedge x'_2 - x'_1 \leq 1$.

Let M^*_p (M^t_p, respectively) be the restriction of $M^*_{\overline{\phi}}$ (of $M^t_{\overline{\phi}}$, respectively) to $\mathbf{y}\setminus\{y_{2k-1}, y_{2k}\}$ and let $\sigma_p \stackrel{def}{=} [x_i/y_{2i-1}, -x_i/y_{2i}]_{i\in\{1,\ldots,N\}\setminus\{k\}}$. By Theorem 4.23, it is easy to see that M^t_p is the tight closure of M^*_p and thus $\Delta[M^t_p][\sigma_p] = \Delta[M^*_p][\sigma_p]$, by the previous observation. By the first point of this proposition, $\exists x_k \,.\, \phi(\mathbf{x}) \Leftrightarrow \Omega[M^t_p]$. By Proposition 4.6 (third point), $\Delta[M^*_p] \Leftrightarrow \exists y_{2k-1}, y_{2k} \,.\, \overline{\phi}(\mathbf{y})$. Next, we observe that $\Omega[P] \Leftrightarrow \Delta[P][\sigma]$ for every coherent DBM $P \in \mathbb{Z}^{2N\times 2N}_{\infty}$ and hence $\Omega[M^t_p] \Leftrightarrow \Delta[M^t_p][\sigma_p]$. Finally, we combine the equivalences:

$$\exists x_k \,.\, \phi(\mathbf{x}) \Leftrightarrow \Omega[M^t_p] \Leftrightarrow \Delta[M^t_p][\sigma_p] \Leftrightarrow \Delta[M^*_p][\sigma_p] \Leftrightarrow \big(\exists y_{2k-1}, y_{2k} \,.\, \overline{\phi}(\mathbf{y})\big)[\sigma_p] \qquad \square$$

A relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ over a set of variables is an *octagonal relation* if it can be defined by an octagonal constraint. The problem of computing the closed forms of octagonal relations has been studied first in [7], where it was shown that the transitive closures of octagonal relations are Presburger definable. In [10] we show that the sequence of tightly closed DBM encodings of the powers of an octagonal relations is periodic, in the sense of Definition 4.15. Moreover, the prefix, period and rates of this sequence of matrices are effectively computable. This result is crucial in showing that the weakest non-termination preconditions $\mathrm{wrs}(R)$ are Presburger definable and effectively computable, and moreover, that the well-foundedness problem for octagonal relations is decidable.

Example 4.27. Consider the octagonal relation $R(x_1, x_2, x'_1, x'_2) \equiv x_1 + x_2 \leq 5 \wedge x'_1 - x_1 \leq -2 \wedge x'_2 - x_2 \leq -3 \wedge x'_2 - x'_1 \leq 1$. Its difference bounds representation is $\overline{R}(\mathbf{y},\mathbf{y}') \Leftrightarrow y_1 - y_4 \leq 5 \wedge y_3 - y_2 \leq 5 \wedge y'_1 - y_1 \leq -2 \wedge y_2 - y'_2 \leq -2 \wedge y'_3 - y_3 \leq -3 \wedge y_4 - y'_4 \leq -3 \wedge y'_3 - y'_1 \leq 1 \wedge y'_2 - y'_4 \leq 1$, where $\mathbf{y} = \{y_1, \ldots, y_4\}$. Figure 3(a) shows the graph representation $\mathcal{G}_{\overline{R}}$. Note that the implicit constraint $y'_3 - y'_4 \leq 1$ (represented by a dashed edge in Figure 3(a) is not tight. The tightening step replaces the bound 1 (crossed in Figure 3(a)) with 0. Figure 3(b) shows the tightly closed DBM representation of R, denoted $M^t_{\overline{R}}$.

Proposition 4.28. *Let $R(\mathbf{x},\mathbf{x}')$, where $\mathbf{x} = \{x_1, \ldots, x_N\}$, be an octagonal constraint and $\overline{R}(\mathbf{y},\mathbf{y}')$, where $\mathbf{y} = \{y_1, \ldots, y_{2N}\}$, be its difference bounds representation. Then, for each $n \geq 1$, consistency of $R^n(\mathbf{x},\mathbf{x}')$ implies consistency of $\overline{R}^n(\mathbf{y},\mathbf{y}')$. Consequently, $*$-consistency of $R(\mathbf{x},\mathbf{x}')$ implies $*$-consistency of $\overline{R}(\mathbf{y},\mathbf{y}')$.*

Proof. It follows from the definition of consistency of octagonal and difference bounds constraints that:

$$\begin{array}{rcl} R^n(\mathbf{x},\mathbf{x}') \text{ is consistent} & \Leftrightarrow & R(\mathbf{x}_0,\mathbf{x}_1) \wedge \cdots \wedge R(\mathbf{x}_{n-1},\mathbf{x}_n) \text{ is consistent} \\ & \Leftrightarrow & M_{\overline{R(\mathbf{x}_0,\mathbf{x}_1)\wedge\cdots\wedge R(\mathbf{x}_{n-1},\mathbf{x}_n)}} \text{ is octagonal-consistent} \\ & \Rightarrow & M_{\overline{R(\mathbf{x}_0,\mathbf{x}_1)\wedge\cdots\wedge R(\mathbf{x}_{n-1},\mathbf{x}_n)}} \text{ is consistent} \\ & \Leftrightarrow & \overline{R(\mathbf{x}_0,\mathbf{x}_1) \wedge \cdots \wedge R(\mathbf{x}_{n-1},\mathbf{x}_n)} \text{ is consistent} \\ & \Leftrightarrow & \overline{R(\mathbf{x}_0,\mathbf{x}_1)} \wedge \cdots \wedge \overline{R(\mathbf{x}_{n-1},\mathbf{x}_n)} \text{ is consistent} \\ & \Leftrightarrow & \overline{R(\mathbf{x},\mathbf{x}')}^{\,n} \text{ is consistent} \end{array}$$

Thus, for each $n \geq 1$, consistency of $R^n(\mathbf{x},\mathbf{x}')$ implies consistency of $\overline{R}^n(\mathbf{y},\mathbf{y}')$. Thus, if $R(\mathbf{x},\mathbf{x}')$ is $*$-consistent, then $\overline{R}(\mathbf{y},\mathbf{y}')$ is $*$-consistent too. □

The next proposition shows that the composition of two octagonal relations is octagonal, and moreover, can be computed in PTIME using the tight closure method of Theorem 4.23. If $R_1, R_2 \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ are two octagonal relations, defined by two octagonal constraints $R_1(\mathbf{x},\mathbf{x}')$ and $R_2(\mathbf{x},\mathbf{x}')$, then let $M_1, M_2 \in \mathbb{Z}^{4N\times 4N}$ be the DBM encodings of $\overline{R_1}(\mathbf{y},\mathbf{y}')$ and $\overline{R_2}(\mathbf{y},\mathbf{y}')$, respectively. Then $\mathcal{M}_{12} \in \mathbb{Z}^{6N\times 6N}$ is the matrix defined by Equation (4.2), and let $M_1 \odot_t M_2 \in \mathbb{Z}^{4N\times 4N}$ be the matrix obtained by erasing lines and columns $2N+1, \ldots, 4N$ from $\mathcal{M}_{12}^t$, if $\mathcal{M}_{12}$ is octagonal-consistent, and $\perp\!\!\!\perp^{4N}$, otherwise.

Proposition 4.29. *Let $R_1(\mathbf{x},\mathbf{x}')$ and $R_2(\mathbf{x},\mathbf{x}')$ be two octagonal constraints defining two relations $R_1, R_2 \subseteq \mathbb{Z}^{\mathbf{x}}\times\mathbb{Z}^{\mathbf{x}}$, respectively. Then the octagonal constraint $\Omega[M_{\overline{R_1}(\mathbf{y},\mathbf{y}')} \odot_t M_{\overline{R_2}(\mathbf{y},\mathbf{y}')}]$ defines the composition $R_1 \circ R_2$. Moreover, $M_{\overline{R_1}} \odot_t M_{\overline{R_2}}$ can be computed in time $\mathcal{O}(N^3 \cdot (N + \log_2(\max(\mu(R_1), \mu(R_2)))))$.*

Proof. Among the lines of the proof of Proposition 4.8. An easy check shows that, if M_1 and M_2 are coherent, then $\mathcal{M}_{12}$ is coherent as well. The consistency of $\mathcal{M}_{12}$ can be checked in time $\mathcal{O}(N^3 \cdot (N + \log_2(\max(\mu(R_1), \mu(R_2)))))$ by Algorithm 1, and its closure $\mathcal{M}_{12}^*$ can be computed during this check. The octagonal consistency of $\mathcal{M}_{12}$ is checked applying Theorem 4.23, and the same can be done to compute the tight closure $\mathcal{M}_{12}^t$. Clearly, these steps do not add to the previous complexity upper bound. Finally, the existential quantifier from $\exists \mathbf{x}''\ .\ R_1(\mathbf{x},\mathbf{x}'') \wedge R_2(\mathbf{x}'',\mathbf{x}')$ can be eliminated using Proposition 4.26. □

In general, for a DBM $M \in \mathbb{Z}_\infty^{4N\times 4N}$ encoding an octagonal constraint $R(\mathbf{x},\mathbf{x}')$, where $\mathbf{x} = \{1, \ldots, N\}$, we define $M^{\odot_t^1} = M$ and $M^{\odot_t^n} = M^{\odot_t^{n-1}} \odot_t M$, for $n > 1$. A simple inductive argument based on Proposition 4.29 shows that the n-th power R^n of the relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is defined by the octagonal constraint $\Omega[M^{\odot_t^n}]$, for all $n > 0$. In the following, we denote the formula $\Omega[M^{\odot_t^n}]$ by $R^n(\mathbf{x},\mathbf{x}')$. As usual, let $\overline{R}(\mathbf{y},\mathbf{y}')$ be the difference bounds constraint encoding $R(\mathbf{x},\mathbf{x}')$, and $\overline{R}^n(\mathbf{y},\mathbf{y}')$ be the difference bounds constraint defining the n-th power of the relation defined by $\overline{R}(\mathbf{y},\mathbf{y}')$. The following lemma establishes an essential connection between the DBMs $M^t_{\overline{R^n}}, M^t_{\overline{R}^n}, M^*_{\overline{R}^n} \in \mathbb{Z}^{4N\times 4N}$, leading to a method for the computation of the transitive closures for octagonal relations [7].

Lemma 4.30. *Let $\mathbf{x} = \{x_1, \ldots, x_N\}$ be a set of variables and $R \subseteq \mathbb{Z}^{\mathbf{x}}\times\mathbb{Z}^{\mathbf{x}}$ be a $*$-consistent octagonal relation. Then the following hold, for all integers $n > 0$:*

(1) $M^t_{\overline{R^n}} = M^t_{\overline{R}^n}$, and

(2) $(M^t_{\overline{R}^n})_{ij} = \min\left\{(M^*_{\overline{R}^n})_{ij}, \left\lfloor \frac{(M^*_{\overline{R}^n})_{i\bar{\imath}}}{2} \right\rfloor + \left\lfloor \frac{(M^*_{\overline{R}^n})_{\bar{\jmath}j}}{2} \right\rfloor\right\}$, for all $1 \leq i,j \leq 4N$.

Proof. We prove the first point by induction on $n > 0$. The base case $n = 1$ is immediate. For the induction step $n > 1$, we have $R^{n+1}(\mathbf{x}, \mathbf{x}') = \Omega[M_{\overline{R}}^{\odot_t^{n+1}}]$, hence:

$$\begin{array}{rcll} M^t_{\overline{R^{n+1}}} & = & M_{\overline{R}}^{\odot_t^{n+1}} & \\ & = & M_{\overline{R}}^{\odot_t^{n}} \odot_t M_{\overline{R}} & \\ & = & M^t_{\overline{R^n}} \odot_t M_{\overline{R}} & \\ & = & M^t_{\overline{R}^n} \odot_t M_{\overline{R}} & \text{by the induction hypothesis} \\ & = & M^t_{\overline{R}^{n+1}} & \text{by Proposition 4.29} \end{array}$$

Since R is $*$-consistent, then $M^t_{\overline{R}^n}$ is an octagonal-consistent DBM and we can directly apply Theorem 4.23 to prove the second point. □

The following result shows that the sequence $\{\mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}})\}_{n \geq 1}$, of a $*$-consistent octagonal relation R is defined by a periodic sequence of matrices.

Lemma 4.31. *Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a $*$-consistent octagonal relation. Then, for all $n \geq 1$, the octagonal constraint $\Omega[^{\blacksquare}M^t_{\overline{R^n}}]$ defines the set $\mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}})$. Moreover, the sequence $\{^{\blacksquare}M^t_{\overline{R^n}}\}_{n \geq 1}$ is periodic, and its prefix, period and rates are all effectively computable.*

Proof. By Lemma 4.30, for all $1 \leq i, j \leq 2N$ we have:

$$(M^t_{\overline{R^n}})_{ij} = \min\left\{(M^*_{\overline{R}^n})_{ij}, \left\lfloor \frac{(M^*_{\overline{R}^n})_{i\bar{\imath}}}{2} \right\rfloor + \left\lfloor \frac{(M^*_{\overline{R}^n})_{\bar{\jmath}j}}{2} \right\rfloor\right\}$$

By Corollary 4.18, the sequence of matrices $\{^{\blacksquare}M^*_{\overline{R}^n}\}_{n \geq 1}$ is periodic, hence the sequence of integers $\{(^{\blacksquare}M^*_{\overline{R}^n})_{ij}\}_{n \geq 1}$ is periodic, for all $1 \leq i, j \leq 2N$. By Lemma 4.16, the sequence of integers $(M^t_{\overline{R^n}})_{ij}$ is also periodic, hence the sequence of matrices $\{^{\blacksquare}M^t_{\overline{R^n}}\}_{n \geq 1}$ is periodic, by Proposition 4.15. The effective computability of the prefix, period, and rates of the sequence follows from the constructive arguments of Lemma 4.16 and Proposition 4.15. □

4.4. **Computing Weakest non-termination preconditions in Polynomial Time.** In the rest of this section, let $R(\mathbf{x}, \mathbf{x}')$, where $\mathbf{x} = \{x_1, \ldots, x_N\}$ for some $N \geq 1$, be an octagonal relation and $\overline{R}(\mathbf{y}, \mathbf{y}')$, where $\mathbf{y} = \{y_1, \ldots, y_{2N}\}$, be its difference bounds representation. Recall that $\mu(R) \overset{def}{=} \max\{|c| \mid (\pm x_i \pm x_j \leq c) \in \mathit{Atom}(R)\}$.

The main result of this section is an algorithm (Algorithm 3) that computes the weakest recurrent set of an octagonal relation R in at most $\mathcal{O}(N^4 \cdot (N + \log_2(\mu(R))))$ time. The main insight of the algorithm is that the Kleene sequence $\{\mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}})\}_{n \geq 1}$ either (1) never stabilizes, in which case

$$\mathrm{pre}^1_R(\mathbb{Z}^{\mathbf{x}}) \supsetneq \mathrm{pre}^2_R(\mathbb{Z}^{\mathbf{x}}) \supsetneq \mathrm{pre}^3_R(\mathbb{Z}^{\mathbf{x}}) \supsetneq \ldots$$

and $\mathrm{wrs}(R) = \emptyset$, or (2) stabilizes after at most 5^{2N} steps, in which case

$$\mathrm{wrs}(R) = \mathrm{pre}^{5^{2N}}_R(\mathbb{Z}^{\mathbf{x}}) = \mathrm{pre}^{5^{2N}+1}_R(\mathbb{Z}^{\mathbf{x}}) = \mathrm{pre}^{5^{2N}+2}_R(\mathbb{Z}^{\mathbf{x}}) = \ldots$$

Then, the stability of the sequence can be checked by checking equality between its 5^{2N}-th element with the $(5^{2N} + 1)$-th element. These elements can be computed by fast exponentiation by applying at most $\mathcal{O}(\lceil \log_2 5^{2N} + 1 \rceil) = \mathcal{O}(N)$ relational compositions. We then show that the absolute values of the coefficients of the octagonal constraint defining the set $\mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})$ is of the order $\mathcal{O}(\mu(R) \cdot N \cdot n)$. Consequently, each of the octagonal compositions performed during fast exponentiation takes at most $\mathcal{O}(N^3 \cdot (\log_2(\mu(R) \cdot N \cdot 5^{2N}))) = \mathcal{O}(N^4 \cdot (N + \log_2(\mu(R))))$ time, by Proposition 4.29. As a direct consequence of the correctness of this algorithm, one obtains a decision procedure for the termination problem with the same worst-case complexity, simply by testing the computed $\mathrm{wrs}(R)$, itself an octagonal constraint, for consistency.

The correctness argument of Algorithm 3 for $*$-consistent octagonal relations depends on Lemmas 4.33, 4.35, and 4.36. First, Lemma 4.33 proves that the weakest recurrent set of an $*$-consistent octagonal relation $R(\mathbf{x}, \mathbf{x}')$ is the limit of the Kleene sequence $\{\mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})\}_{n\geq 1}$ and moreover, that the limit is either empty or stabilizes after a finite number of steps. Next, Lemma 4.35 gives two equivalent conditions for checking well-foundedness of an arbitrary $*$-consistent difference bounds relation $R(\mathbf{x}, \mathbf{x}')$. Its main insight is that the instability of the sequence $\{\mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})\}_{n\geq 1}$ (and thus well-foundedness of R) is equivalent to existence of a negative-weight cycle in zigzag automata. Moreover, it proves that the instability manifests already after 5^N steps (5^N is an upper bound on the size of elementary cycles in zigzag automata). Then, Lemma 4.36 proves that an octagonal relation $R(\mathbf{x}, \mathbf{x}')$, where $\mathbf{x} = \{x_1, \ldots, x_N\}$, is well founded if and only if its difference bounds representation $\overline{R}(\mathbf{y}, \mathbf{y}')$, where $\mathbf{y} = \{y_1, \ldots, y_{2N}\}$, is well founded. Hence the stability stability bound of 5^{2N} applies for octagonal relations, as a consequence of Lemma 4.35.

The following proposition gives an alternative characterization of periodic sequences of matrices.

Proposition 4.32. *A sequence of matrices $\{M_k \in \mathbb{Z}_\infty^{N\times N}\}_{k=1}^{\infty}$ is periodic if and only if there exist integers $b \geq 1$, $c \geq 1$, and matrices $\Lambda_0, \ldots, \Lambda_{c-1} \in \mathbb{Z}_\infty^{m\times m}$ such that*

$$M_{nc+b+i} = n \cdot \Lambda_i + M_{b+i}$$

for all $n \geq 0$ and for all $0 \leq i < c$.

Proof. By induction on $n \geq 0$, we prove that $M_{nc+b+i} = n \cdot \Lambda_i + M_{b+i}$, for all $n \geq 0$ and for all $0 \leq i < c$. The base case trivially holds. For the induction step, observe that

$$M_{b+i+(n+1)c} = \Lambda_i + M_{b+i+nc} = \Lambda_i + n \cdot \Lambda_i + M_{b+i} = (n+1) \cdot \Lambda_i + M_{b+i}.$$

The first equality is by Definition 4.14, the second is by the induction hypothesis. □

Given a $*$-consistent octagonal relation $R(\mathbf{x}, \mathbf{x}')$ and integers $b \geq 1, c \geq 1$, we denote by $\widehat{\mathrm{pre}_{R,b,c}}(k, \mathbf{x})$ the closed form of the sequence $\{\mathrm{pre}_R^{b+nc}(\mathbb{Z}^{\mathbf{x}})\}_{n\geq 0}$. Given a $*$-consistent octagonal relation R and integers b, c such that b is the prefix and c is the period of the sequence $\{{}^{\blacksquare}M^{t}_{\overline{R^n}}\}_{n\geq 1}$, the following lemma proves that the closed form $\widehat{\mathrm{pre}_{R,b,c}}(k, \mathbf{x})$ can be computed and moreover, one can perform a simple syntactical check on $\widehat{\mathrm{pre}_{R,b,c}}(k, \mathbf{x})$ to compute the weakest recurrent set, which is either $\emptyset$ or $\mathrm{pre}_R^b(\mathbb{Z}^{\mathbf{x}})$. For a set $\mathbf{v}$ of variables, let $\mathit{OctTerm}(\mathbf{v}) = \{\pm v_1 \pm v_2 \mid v_1, v_2 \in \mathbf{v}\}$ denote the set of octagonal terms over $\mathbf{v}$.

Lemma 4.33. *Let $R(\mathbf{x}, \mathbf{x}')$ be an octagonal constraint defining a $*$-consistent relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$, let b be the prefix and c the period of $\{{}^{\blacksquare}M^{t}_{\overline{R^n}}\}_{n\geq 1}$. Then, there exists a set of octagonal terms $U \subseteq \mathit{OctTerm}(\mathbf{x})$ such that*

$$\widehat{\mathrm{pre}_{R,b,c}}(k, \mathbf{x}) \Leftrightarrow \bigwedge_{u\in U} u \leq a_u + d_u \cdot k \tag{4.7}$$

for some $a_u \in \mathbb{Z}$, $d_u \leq 0$. Moreover, the set U and the coefficients a_u, d_u, $u \in U$, are effectively computable. Furthermore,

$$\mathrm{wrs}(R) = \bigcap_{n \geq 1} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}}) = \begin{cases} \emptyset & \textit{if } d_u < 0 \textit{ for some } u \in U \\ \mathrm{pre}_R^b(\mathbb{Z}^{\mathbf{x}}) & \textit{otherwise} \end{cases}$$

Proof. The sequence $\{{}^{\blacksquare}M_{\frac{t}{R^n}}\}_{n \geq 1}$ is periodic, by Lemma 4.31. Let $\Lambda_0, \ldots, \Lambda_{c-1}$ be its rates. For each $u \in OctTerm(\mathbf{x})$, we define indices i_u, j_u as:

$$\begin{array}{lll} i_u = 2k-1, & j_u = 2\ell - 1 & \text{if } u = x_k - x_\ell \text{ for some } 1 \leq k, \ell \leq N \\ i_u = 2k-1, & j_u = 2\ell & \text{if } u = x_k + x_\ell \text{ for some } 1 \leq k, \ell \leq N \\ i_u = 2k, & j_u = 2\ell - 1 & \text{if } u = -x_k - x_\ell \text{ for some } 1 \leq k, \ell \leq N \end{array}$$

Then, the set of octagonal terms which are bounded in $pre_R^b(\mathbb{Z}^{\mathbf{x}})$ is:

$$U \overset{def}{=} \{u \in OctTerm(\mathbf{x}) \mid ({}^{\blacksquare}M_{\frac{t}{R^b}})_{i_u j_u} < \infty\}$$

Since R^n is consistent and ${}^{\blacksquare}M_{\frac{t}{R^n}}$ is coherent for all $n \geq 1$, we have:

$$\begin{array}{rcll} \mathrm{pre}_R^{b+nc}(\mathbb{Z}^{\mathbf{x}}) & \Leftrightarrow & \Omega[{}^{\blacksquare}M_{\frac{t}{R^{b+nc}}}] & \text{(by Proposition 4.26)} \\ & \Leftrightarrow & \Omega[{}^{\blacksquare}M_{\frac{t}{R^b}} + n \cdot \Lambda_0] & \text{(by Proposition 4.32)} \\ & \Leftrightarrow & \bigwedge_{u \in U} u \leq ({}^{\blacksquare}M_{\frac{t}{R^b}})_{i_u j_u} + n \cdot (\Lambda_0)_{i_u j_u} & \text{(by Equation (4.4))} \end{array} \tag{4.8}$$

for every $n \geq 0$. Clearly, $({}^{\blacksquare}M_{\frac{t}{R^b}})_{i_u j_u} < \infty$ for each $u \in U$, by definition of U. We prove that $(\Lambda_0)_{i_u j_u} \leq 0$. By contradiction, if $(\Lambda_0)_{i_u j_u} > 0$, then

$$({}^{\blacksquare}M_{\frac{t}{R^{b+c}}})_{i_u j_u} = ({}^{\blacksquare}M_{\frac{t}{R^b}})_{i_u j_u} + (\Lambda_0)_{i_u j_u} > ({}^{\blacksquare}M_{\frac{t}{R^b}})_{i_u j_u}$$

by Proposition 4.32. By Proposition 3.1, $\mathrm{pre}_R^{b+c}(\mathbb{Z}^{\mathbf{x}}) \subseteq \mathrm{pre}_R^b(\mathbb{Z}^{\mathbf{x}})$. By Proposition 4.25, we infer that ${}^{\blacksquare}M_{\frac{t}{R^{b+c}}} \leq {}^{\blacksquare}M_{\frac{t}{R^b}}$. Contradiction with $({}^{\blacksquare}M_{\frac{t}{R^{b+c}}})_{i_u j_u} > ({}^{\blacksquare}M_{\frac{t}{R^{b+c}}})_{i_u j_u}$. Hence, we can define the coefficients $a_u \in \mathbb{Z}, d_u \leq 0$ for each $u \in U$ as

$$a_u \overset{def}{=} ({}^{\blacksquare}M_{\frac{t}{R^b}})_{i_u j_u} \qquad d_u \overset{def}{=} (\Lambda_0)_{i_u j_u}$$

By Lemma 4.31, the prefix b, the period c, and the rate Λ_0 are effectively computable. Consequently, the set U and coefficients a_u, d_u, $u \in U$, defined above are effectively computable too. It follows from (4.8) that the closed form of $\{\mathrm{pre}_R^{b+nc}(\mathbb{Z}^{\mathbf{x}})\}_{n \geq 0}$ can now be defined as

$$\widehat{\mathrm{pre}_{R,b,c}}(k, \mathbf{x}) \overset{def}{=} \bigwedge_{u \in U} u \leq a_u + d_u \cdot k$$

By Proposition 3.1, $pre_R^{n_1}(\mathbb{Z}^{\mathbf{x}}) \supseteq \mathrm{pre}_R^{n_2}(\mathbb{Z}^{\mathbf{x}})$ for all $n_1 \leq n_2$. Consequently, we have that $\bigcap_{n \geq 1} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}}) = \bigcap_{n \geq 0} \mathrm{pre}_R^{b+cn}(\mathbb{Z}^{\mathbf{x}})$. The latter set can now be defined as $\forall k \geq 0 \;.\; \widehat{\mathrm{pre}_{R,b,c}}(k, \mathbf{x})$ which is equivalent to

$$\bigwedge_{u \in U} u \leq \inf\ \{a_u + d_u n \mid n \geq 0\}$$

We have

$$\inf\ \{a_u + d_u n \mid n \geq 0\} = \begin{cases} -\infty & \text{if } d_u < 0, \\ a_u & \text{otherwise.} \end{cases}$$

Hence $\bigcap_{n \geq 1} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}})$ is the empty set, if $d_u < 0$ for some $u \in U$. In this case, condition 3 of Lemma 3.7 holds. Otherwise, we obtain $\bigcap_{n \geq 1} \mathrm{pre}_R^n(\mathbb{Z}^{\mathbf{x}}) \equiv \bigwedge_{u \in U} u \leq a_u$. However, this is exactly the set $\mathrm{pre}_R^b(\mathbb{Z}^{\mathbf{x}})$, since $\bigwedge_{u \in U}(u \leq a_u) \Leftrightarrow \widehat{\mathrm{pre}_{R,b,c}}(k, \mathbf{x})[0/k]$. In this case, condition

2 of Lemma 3.7 holds. Thus, we can apply Lemma 3.7 in both cases and conclude that $\mathrm{wrs}(R) = \bigcap_{n\geq 1} \mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}})$. To summarize, $\mathrm{wrs}(R) = \emptyset$ if $d_u < 0$ for some $u \in U$. Otherwise, $\mathrm{wrs}(R) = \mathrm{pre}^b_R(\mathbb{Z}^{\mathbf{x}})$. □

The following proposition proves that the Kleene sequence $\{\mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}})\}_{n\geq 1}$ is strictly descending for arbitrary relation that is both $*$-consistent and well founded.

Proposition 4.34. *Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a $*$-consistent and well-founded relation. Then, $\mathrm{pre}^{n_1}_R(\mathbb{Z}^{\mathbf{x}}) \supsetneq \mathrm{pre}^{n_2}_R(\mathbb{Z}^{\mathbf{x}})$ for all $1 \leq n_1 < n_2$. Consequently, the sequence $\{\mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}})\}_{n\geq 1}$ is strictly descending.*

Proof. By Proposition 3.1, $\mathrm{pre}^{n_1}_R(\mathbb{Z}^{\mathbf{x}}) \supseteq \mathrm{pre}^{n_2}_R(\mathbb{Z}^{\mathbf{x}})$ for all $1 \leq n_1 < n_2$. For a proof by contraposition, suppose that $\mathrm{pre}^{n_1}_R(\mathbb{Z}^{\mathbf{x}}) = \mathrm{pre}^{n_2}_R(\mathbb{Z}^{\mathbf{x}})$ some $n_2 > n_1 \geq 1$. Then $\mathrm{wrs}(R) = \mathrm{pre}^{n_1}_R(\mathbb{Z}^{\mathbf{x}})$, by Lemma 3.7. Since R is $*$-consistent, then clearly $\mathrm{wrs}(R) = \mathrm{pre}^{n_1}_R(\mathbb{Z}^{\mathbf{x}}) \neq \emptyset$ and R is not well founded. □

The following two lemmas give several equivalent conditions for checking that a difference bounds (Lemma 4.35) or an octagonal relation (Lemma 4.36) is well founded. These conditions will later be used to design an efficient polynomial time algorithm that computes the weakest recurrent set of an octagonal relation. These conditions also provide the basis for the proof of existence of a linear ranking functions for well-founded octagonal relations, which we give in the next section.

Lemma 4.35. *Let $R(\mathbf{x}, \mathbf{x}')$, where $\mathbf{x} = \{x_1, \ldots, x_N\}$, be a difference bounds constraint defining a $*$-consistent relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ and let $T_R = \langle Q, \delta, \omega\rangle$ be the transition table of zigzag automata. Then, the following statements are equivalent:*

(1) *R is well founded,*
(2) *$\mathrm{pre}^{n_2}_R(\mathbb{Z}^{\mathbf{x}}) \subsetneq \mathrm{pre}^{n_1}_R(\mathbb{Z}^{\mathbf{x}})$ for some $n_2 > n_1 \geq 5^N$,*
(3) *there exists a zigzag automaton $\mathcal{A}_{ij} = \langle T_R, I_{ij}, F\rangle$ for some $1 \leq i, j \leq N, i \neq j$ with an accepting run $\mu.\lambda.\mu'$ where λ is a cycle such that $|\lambda| > 0$ and $\omega(\lambda) < 0$.*

Proof. $(1 \Rightarrow 2)$ Follows immediately from Proposition 4.34.

$(2 \Rightarrow 3)$ Let $n_2 > n_1 \geq 5^N$ be integers such that $\mathrm{pre}^{n_2}_R(\mathbb{Z}^{\mathbf{x}}) \subsetneq \mathrm{pre}^{n_1}_R(\mathbb{Z}^{\mathbf{x}})$. Then, ${}^{\blacksquare}M^*_{R^{n_1}} > {}^{\blacksquare}M^*_{R^{n_2}}$ by Proposition 4.6. Since R is $*$-consistent, $({}^{\blacksquare}M^*_{R^{n_1}})_{ii} = ({}^{\blacksquare}M^*_{R^{n_2}})_{ii} = 0$ for each $1 \leq i \leq N$ and hence $({}^{\blacksquare}M^*_{R^{n_1}})_{ij} > ({}^{\blacksquare}M^*_{R^{n_2}})_{ij}$ for some $1 \leq i, j \leq N, i \neq j$. By Lemma 4.13, $\mathcal{A}_{ij}$ has an accepting run π of length $|\pi| = n_2$ and weight $\omega(\pi) = ({}^{\blacksquare}M^*_{R^{n_2}})_{ij}$.

Let $\pi_0 \overset{def}{=} \pi$. We next define, iteratively for $i = 1, 2, \ldots$, an accepting run π_i by erasing an arbitrary cycle λ_i from π_{i-1}. Note that if $|\pi_{i-1}| \geq 5^N$, then π_{i-1} must contain at least one cycle λ_i, by pigeonhole principle (since 5^N is the cardinality of the set of control states in $\mathcal{A}_{ij}$). Clearly $|\pi_p| < 5^N$ for some $p \geq 1$. Let $n \overset{def}{=} |\pi_p|$. We next prove that

$$\Big(\sum_{i=1}^{p} \omega(\lambda_i)\Big) < 0$$

For a proof by contradiction, suppose that $(\sum_{i=1}^{p} \omega(\lambda_i)) \geq 0$. Then $\omega(\pi_p) \leq \omega(\pi)$, since $\omega(\pi_p) = \omega(\pi) - (\sum_{i=1}^{p} \omega(\lambda_i))$. Observe that (the first inequality is by Lemma 4.13):

$$({}^{\blacksquare}M^*_{R^n})_{ij} \leq \omega(\pi_p) \leq \omega(\pi) = ({}^{\blacksquare}M^*_{R^{n_2}})_{ij}$$

Since $n < 5^N \leq n_1 < n_2$, then $\mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}}) \supseteq \mathrm{pre}^{n_1}_R(\mathbb{Z}^{\mathbf{x}}) \supseteq \mathrm{pre}^{n_2}_R(\mathbb{Z}^{\mathbf{x}})$, by Proposition 3.1. Consequently, by Proposition 4.6:

$$({}^{\blacksquare}M^*_{R^n})_{ij} \geq ({}^{\blacksquare}M^*_{R^{n_1}})_{ij} \geq ({}^{\blacksquare}M^*_{R^{n_2}})_{ij}$$

Combining the above inequalities, we obtain that $({}^{\blacksquare}M^*_{R^n})_{ij} = ({}^{\blacksquare}M^*_{R^{n_1}})_{ij} = ({}^{\blacksquare}M^*_{R^{n_2}})_{ij}$. Contradiction with $({}^{\blacksquare}M^*_{R^{n_1}})_{ij} > ({}^{\blacksquare}M^*_{R^{n_2}})_{ij}$.

Thus, $(\sum_{i=1}^{p} \omega(\lambda_i)) < 0$ and consequently, there exists $1 \leq k \leq p$ such that $\omega(\lambda_k) < 0$. By definition of π_k, there exists μ, μ' such that $\pi_k = \mu.\lambda_k.\mu'$. Since $\omega(\lambda_k) < 0$, the run $\mu.\lambda_k.\mu'$ satisfied the requirements of the lemma.

$(3 \Rightarrow 1)$ Let us denote $d = |\mu.\mu'|$ and $e = |\lambda|$. Since $\omega(\lambda) < 0$, the infinite sequence $\{\omega(\mu.\lambda^n.\mu')\}_{n \geq 0}$ is strictly descending and thus $\inf\{\omega(\mu.\lambda^n.\mu')\}_{n\geq 0} = -\infty$. By Lemma 4.13, $({}^{\blacksquare}M^*_{R^{d+ne}})_{ij} \leq \omega(\mu.\lambda^n.\mu')$ for all $n \geq 0$ and hence, $\inf\{({}^{\blacksquare}M^*_{R^{d+ne}})_{ij}\}_{n\geq 0} = -\infty$. By Lemma 4.33, $\mathrm{wrs}(R) = \bigcap_{n\geq 1} \mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}})$. Next, observe that since R is $*$-consistent, $\Delta[{}^{\blacksquare}M^*_{R^n}]$ defines $\mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}})$ for each $n \geq 1$. Hence, any formula that defines $\mathrm{wrs}(R)$ must imply $x_i - x_j \leq \inf\{({}^{\blacksquare}M^*_{R^{d+ne}})_{ij}\}_{n\geq 0} = -\infty$. Since this formula is inconsistent, it follows that $\mathrm{wrs}(R) = \emptyset$ and R is well founded. □

Lemma 4.36. *Let $R(\mathbf{x}, \mathbf{x}')$, where $\mathbf{x} = \{x_1, \ldots, x_N\}$, be an octagonal constraint defining a $*$-consistent relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$, and let $\overline{R}(\mathbf{y}, \mathbf{y}')$, where $\mathbf{y} = \{y_1, \ldots, y_{2N}\}$, be the difference bounds encoding of $R(\mathbf{x}, \mathbf{x}')$. Then, the following statements are equivalent.*

(1) *R is well founded*
(2) *$\overline{R}$ is well founded*
(3) $\mathrm{pre}^{n_1}_R(\mathbb{Z}^{\mathbf{x}}) \supsetneq \mathrm{pre}^{n_2}_R(\mathbb{Z}^{\mathbf{x}})$ *for some integers n_1, n_2 such that $5^{2N} \leq n_1 < n_2$*

Proof. Observe that since R is $*$-consistent, $\overline{R}$ is $*$-consistent too, by Proposition 4.28.

$(1 \Rightarrow 3)$ Follows immediately from Proposition 4.34.

$(3 \Rightarrow 2)$ We first prove that $\mathrm{pre}^{n_1}_R(\mathbb{Z}^{\mathbf{x}}) \supsetneq \mathrm{pre}^{n_2}_R(\mathbb{Z}^{\mathbf{x}})$ implies that $\mathrm{pre}^{n_1}_{\overline{R}}(\mathbb{Z}^{\mathbf{y}}) \supsetneq \mathrm{pre}^{n_2}_{\overline{R}}(\mathbb{Z}^{\mathbf{y}})$. For a proof by contraposition, suppose that $\mathrm{pre}^{n_1}_{\overline{R}}(\mathbb{Z}^{\mathbf{y}}) \subseteq \mathrm{pre}^{n_2}_{\overline{R}}(\mathbb{Z}^{\mathbf{y}})$. By Proposition 3.1, $\mathrm{pre}^{n_1}_{\overline{R}}(\mathbb{Z}^{\mathbf{y}}) \supseteq \mathrm{pre}^{n_2}_{\overline{R}}(\mathbb{Z}^{\mathbf{y}})$ and consequently, $\mathrm{pre}^{n_1}_{\overline{R}}(\mathbb{Z}^{\mathbf{y}}) = \mathrm{pre}^{n_2}_{\overline{R}}(\mathbb{Z}^{\mathbf{y}})$. Then, ${}^{\blacksquare}M^*_{\overline{R}^{n_1}} = {}^{\blacksquare}M^*_{\overline{R}^{n_2}}$, by Proposition 4.6. This implies that ${}^{\blacksquare}M^t_{\overline{R}^{n_1}} = {}^{\blacksquare}M^t_{\overline{R}^{n_2}}$, by Lemma 4.30. Consequently, $\mathrm{pre}^{n_1}_R(\mathbb{Z}^{\mathbf{x}}) = \mathrm{pre}^{n_2}_R(\mathbb{Z}^{\mathbf{x}})$, by Proposition 4.25.

Since $5^{2N} \leq n_1 < n_2$ and $\mathrm{pre}^{n_1}_{\overline{R}}(\mathbb{Z}^{\mathbf{y}}) \supsetneq \mathrm{pre}^{n_2}_{\overline{R}}(\mathbb{Z}^{\mathbf{y}})$, then $\overline{R}$ is well founded, by Lemma 4.35.

$(2 \Rightarrow 1)$ The sequence $\{\mathrm{pre}^n_{\overline{R}}(\mathbb{Z}^{\mathbf{y}})\}_{n\geq 1}$ is strictly descending, by Proposition 4.34. Hence $\mathrm{pre}^1_{\overline{R}}(\mathbb{Z}^{\mathbf{y}}) \supsetneq \mathrm{pre}^2_{\overline{R}}(\mathbb{Z}^{\mathbf{y}}) \supsetneq \mathrm{pre}^3_{\overline{R}}(\mathbb{Z}^{\mathbf{y}}) \supsetneq \ldots$ and it follows from Proposition 4.6 that

$${}^{\blacksquare}M^*_{\overline{R}^1} > {}^{\blacksquare}M^*_{\overline{R}^2} > {}^{\blacksquare}M^*_{\overline{R}^3} > \ldots$$

For each $n \geq 1$, let $1 \leq i_n, j_n \leq 2N$ be arbitrary integers such that $({}^{\blacksquare}M^*_{\overline{R}^n})_{i_n j_n} > ({}^{\blacksquare}M^*_{\overline{R}^{n+1}})_{i_n j_n}$. Clearly, there exist integers $1 \leq i, j \leq 2N$ such that $i = i_n$ and $j = j_n$ for infinitely many $n \geq 1$. Consequently, for each $n \geq 1$ there exists $m > n$ such that $({}^{\blacksquare}M^*_{\overline{R}^n})_{ij} > ({}^{\blacksquare}M^*_{\overline{R}^m})_{ij}$ and hence

$$\inf\{({}^{\blacksquare}M^*_{\overline{R}^n})_{ij}\}_{n\geq 1} = -\infty$$

By Lemma 4.30, the following holds for each $n \geq 1$

$$({}^{\blacksquare}M^{t}_{\overline{R^n}})_{ij} = \min \left\{ ({}^{\blacksquare}M^{*}_{\overline{R}^n})_{ij}, \left\lfloor \frac{({}^{\blacksquare}M^{*}_{\overline{R}^n})_{i\bar{i}}}{2} \right\rfloor + \left\lfloor \frac{(M^{*}_{\overline{R}^n})_{\bar{j}j}}{2} \right\rfloor \right\}$$

Thus clearly, since $\inf\{({}^{\blacksquare}M^{*}_{\overline{R}^n})_{ij}\}_{n\geq 1} = -\infty$, then $\inf\{({}^{\blacksquare}M^{t}_{\overline{R}^n})_{ij}\}_{n\geq 1} = -\infty$ too. By Equation (4.4) and coherency of tight encoding, there exist integers $1 \leq k, \ell \leq N$ such that for each $n \geq 1$, $\Omega[{}^{\blacksquare}M^{t}_{\overline{R^n}}]$ implies:

$$\begin{array}{lll}
(1) & x_k - x_\ell \leq ({}^{\blacksquare}M^{t}_{\overline{R^n}})_{2k-1,2\ell-1} = ({}^{\blacksquare}M^{t}_{\overline{R^n}})_{ij} & \text{if } i = 2k-1, j = 2\ell - 1 \\
(2) & x_k + x_\ell \leq ({}^{\blacksquare}M^{t}_{\overline{R^n}})_{2k-1,2\ell} = ({}^{\blacksquare}M^{t}_{\overline{R^n}})_{ij} & \text{if } i = 2k-1, j = 2\ell \\
(3) & -x_k - x_\ell \leq ({}^{\blacksquare}M^{t}_{\overline{R^n}})_{2k,2\ell-1} = ({}^{\blacksquare}M^{t}_{\overline{R^n}})_{ij} & \text{if } i = 2k, j = 2\ell - 1 \\
(4) & x_\ell - x_k \leq ({}^{\blacksquare}M^{t}_{\overline{R^n}})_{2\ell-1,2k-1} = ({}^{\blacksquare}M^{t}_{\overline{R^n}})_{2k,2\ell} = ({}^{\blacksquare}M^{t}_{\overline{R^n}})_{ij} & \text{if } i = 2k, j = 2\ell
\end{array}$$

Let $u \in \mathit{OctTerm}(\mathbf{x})$ be the octagonal term from above (i.e. of the form $\pm x_k \pm x_\ell$). By Lemma 4.33, $\mathrm{wrs}(R) = \bigcap_{n\geq 1} \mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}})$. Since R is $*$-consistent, $\mathrm{pre}^n_R(\mathbb{Z}^{\mathbf{x}})$ is defined by $\Omega[{}^{\blacksquare}M^{t}_{\overline{R^n}}]$ for each $n \geq 1$. Thus, any formula that defines $\mathrm{wrs}(R)$ must imply $u \leq \inf\{({}^{\blacksquare}M^{t}_{\overline{R^n}})_{ij}\}_{n\geq 1}$. This formula is inconsistent, since $\inf\{({}^{\blacksquare}M^{t}_{\overline{R^n}})_{ij}\}_{n\geq 1} = -\infty$. Consequently, $\mathrm{wrs}(R) = \emptyset$ and R is thus well founded. □

The main result of this section is Algorithm 3 which computes the weakest non-termination precondition of an octagonal relation, in time polynomial in the number of variables and logarithmic in the maximal absolute value among all coefficients of the relation. As an auxiliary procedure, it uses Algorithm 2 to compute exponentially large powers in polynomial time.

Algorithm 2 Fast Exponentiation Algorithm

```
input An octagonal constraint $R(\mathbf{x}, \mathbf{x}')$ and an integer $n \geq 1$
output An octagonal constraint representing $R^n(\mathbf{x}, \mathbf{x}')$
function FastPower($R, n$)
    if $R \Leftrightarrow$ false then
        return false
    $P \leftarrow M^{t}_{\overline{R^0}}$
    $Q \leftarrow M^{t}_{\overline{R^1}}$
    for $i = 1, \ldots, \lceil \log_2 n \rceil$ do
        if $\Omega[Q] \Leftrightarrow$ false then
            return false
        if the $i$-th least significant bit of $n$ is 1 then
            $P \leftarrow P \odot_t Q$
        $Q \leftarrow Q \odot_t Q$                    [at this point $\Omega[Q] \Leftrightarrow R^{2^i}(\mathbf{x}, \mathbf{x}')$]
    return $\Omega[P]$
```

Lemma 4.37. *Given an octagonal constraint $R(\mathbf{x}, \mathbf{x}')$, where $\mathbf{x} = \{x_1, \cdots, \mathbf{x}_N\}$ for some $N \geq 1$, and an integer $n \geq 1$, Algorithm 2 computes $R^n(\mathbf{x}, \mathbf{x}')$ in at most $\mathcal{O}(\lceil \log_2 n \rceil \cdot N^3 \cdot (N + \log_2 \mu(R) + \lceil \log_2 n \rceil))$ time. Moreover, $\mu(R^n)$ is of the order $\mathcal{O}(\mu(R) \cdot N \cdot n)$.*

Proof. Let $\mu_{P,i}$ (respectively $\mu_{Q,i}$) be the maximal absolute value over all integer entries of P (respectively Q) before executing line 9 during the i-th iteration for $i = 1, \ldots, \lceil \log_2 n \rceil$. Further, let $n_i \geq 0$ be an integer such that $\Omega[P] \Leftrightarrow R^{n_i}(\mathbf{x}, \mathbf{x}')$ at line 7 during the i-th iteration. Notice that before executing line 7, $\Omega[Q] \Leftrightarrow R^{2^{i-1}}(\mathbf{x}, \mathbf{x}')$ and $\Omega[P] \Leftrightarrow R^{n_i}(\mathbf{x}, \mathbf{x}')$ where $n_i \leq 2^{i-1}$. It is easy to see that $\Omega[Q]$ is consistent before executing line 9. Since $n_i \leq 2^{i-1}$, it then follows that $\Omega[P]$ is consistent before executing line 10 too. Thus, compositions on lines 10 and 11 are always applied to two consistent relations.

If the test on line 7 passes, then $\Omega[Q] \Leftrightarrow R^{2^{i-1}} \Leftrightarrow$ **false** and consequently, since $2^{i-1} < n$, $R^n \Leftrightarrow$ **false** too. Thus, the algorithm returns the correct result on line 8. The correctness of the rest of the algorithm is easy to see.

Lines 2–5 take at most $\mathcal{O}(N^3 \cdot (N + \log_2 \mu(R)))$ time, by Corollary 4.24. Since the graph unfolding $\mathcal{G}^{2^i}_{\overline{R}}$, corresponding to $\overline{R}^{2^i}$ for each $i \geq 1$, has $2N \cdot 2^i$ nodes, each elementary path in this graph is of length at most $2N \cdot 2^i$. Thus, $(M^*_{\overline{R}^{2^i}})_{k\ell} \leq \mu(R) \cdot 2N \cdot 2^i$ for all $1 \leq k, \ell \leq 4N$ whenever R^{2^i} is consistent. Tightening clearly does not change this bound. Since $Q \Leftrightarrow R^{2^{i-1}} \not\Leftrightarrow$ **false** on line 9, then $\mu_{Q,i} \leq \mu(R) \cdot 2N \cdot 2^{i-1}$. By Proposition 4.29, composition on line 11 can be computed in time $\mathcal{O}(N^3 \cdot (N + \log_2(\mu_{Q,i})))$. Since $i \leq \lceil \log_2 n \rceil$, this simplifies to $\mathcal{O}(N^3 \cdot (N + \log_2 \mu(R) + \lceil \log_2 n \rceil))$. Since $n_i \leq 2^{i-1}$, then $\mu_{P,i} \leq \mu_{Q,i}$ and the same bound applies for the composition on line 10. By the definition of the composition operator $\odot_t$ and the tight closure operator, the octagonal-consistency check on line 7 can be taken care of during the preceding assignment to Q, i.e. on line 11 (composition) or on line 5 (tight closure). Thus, the overall running time of the algorithm is in the order of $\mathcal{O}(\lceil \log_2 n \rceil \cdot N^3 \cdot (N + \log_2 \mu(R) + \lceil \log_2 n \rceil))$. Finally, $\mu(R^n)$ is asymptotically bounded by $\mathcal{O}(\mu(R) \cdot N \cdot n)$. □

Algorithm 3 Weakest non-termination precondition for Octagonal Relations

```
  input An octagonal constraint $R(\mathbf{x}, \mathbf{x}')$ where $\mathbf{x} = \{x_1, \ldots, x_N\}$
  output An octagonal constraint representing wnt($R$)
1: function WNT($R$)
2:     $V(\mathbf{x}, \mathbf{x}') \leftarrow$ FastPower($R(\mathbf{x}, \mathbf{x}')$,$5^{2N}$)
3:     $W(\mathbf{x}, \mathbf{x}') \leftarrow$ FastPower($R(\mathbf{x}, \mathbf{x}')$,$5^{2N} + 1$)
4:     if $W \Leftrightarrow$ false or $^{\blacksquare}M^t_V > {}^{\blacksquare}M^t_W$ then
5:         return false
6:     else
7:         return $\Omega[{}^{\blacksquare}M^t_V]$
```

Theorem 4.38. *Let $R(\mathbf{x}, \mathbf{x}')$, where $\mathbf{x} = \{x_1, \ldots, x_N\}$ for some $N \geq 1$, be an octagonal constraint defining a relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$. Then, Algorithm 3 returns an octagonal constraint $\phi(\mathbf{x})$ that defines* wrs(R) *in at most $\mathcal{O}(N^4 \cdot (N + \log_2 \mu(R)))$ time. Also, $\mu(\phi) = \mathcal{O}(\mu(R) \cdot N \cdot 2^N)$.*

Proof. By Lemma 4.37, lines 2 and 3 of the algorithm compute $V \Leftrightarrow R^{5^{2N}}$ and $W \Leftrightarrow R^{5^{2N}+1}$ in at most $\mathcal{O}(N^4 \cdot (N + \log_2 \mu(R)))$ time and moreover, $\mu(V)$ and $\mu(W)$ are of the order $\mathcal{O}(\mu(R) \cdot N \cdot 2^N)$.

By Corollary 4.24, the test $W \Leftrightarrow$ false can be performed in at most $\mathcal{O}(N^3 \cdot (N + \log_2 \mu(W)))$ time. If the test fails, the algorithm returns **false**. Otherwise, W is consistent and moreover, since $5^{2N} < 5^{2N} + 1$, V is consistent too. Then, ${}^{\blacksquare}M^t_V$ and ${}^{\blacksquare}M^t_W$ can be computed and the test ${}^{\blacksquare}M^t_V > {}^{\blacksquare}M^t_W$ can be performed in at most $\mathcal{O}(N^3 \cdot (N + \log_2 \mu(W)))$ time, by Proposition 4.25 and Corollary 4.24. Also, $\mu(\Omega[{}^{\blacksquare}M^t_V])$ inherits the upper bound of $\mu(V)$, by Proposition 4.26.

Consider first the case when R is $*$-consistent. Then clearly $W \not\Leftrightarrow \mathsf{false}$. Notice that the test ${}^{\blacksquare}M^t_V > {}^{\blacksquare}M^t_W$ is equivalent to $\mathrm{pre}_R^{5^{2N}}(\mathbb{Z}^{\mathbf{x}}) \supsetneq \mathrm{pre}_R^{5^{2N}+1}(\mathbb{Z}^{\mathbf{x}})$. If this test passes, R is well founded, by Lemma 4.36, and the algorithm correctly returns **false**. Otherwise, if this test fails, then $\mathrm{pre}_R^{5^{2N}}(\mathbb{Z}^{\mathbf{x}}) = \mathrm{pre}_R^{5^{2N}+1}(\mathbb{Z}^{\mathbf{x}})$ and consequently, $\mathrm{wrs}(R) = \mathrm{pre}_R^{5^{2N}}(\mathbb{Z}^{\mathbf{x}})$ by Lemma 3.7 and the algorithm correctly returns $\Omega[{}^{\blacksquare}M^t_V]$.

Second, consider the case when R is not $*$-consistent. Then clearly $\mathrm{wrs}(R) = \emptyset$. Hence, if the test on line 4 passes, the algorithm returns the correct result. To see that the test on line 4 cannot fail, let us assume, by contradiction, that $\mathrm{pre}_R^{5^{2N}}(\mathbb{Z}^{\mathbf{x}}) = \mathrm{pre}_R^{5^{2N}+1}(\mathbb{Z}^{\mathbf{x}})$ and $\mathrm{pre}_R^{5^{2N}+1}(\mathbb{Z}^{\mathbf{x}}) \neq \emptyset$. Then, $\mathrm{wrs}(R) = \mathrm{pre}_R^{5^{2N}+1}(\mathbb{Z}^{\mathbf{x}})$, by Proposition 3.7. Since $\mathrm{pre}_R^{5^{2N}+1}(\mathbb{Z}^{\mathbf{x}}) \neq \emptyset$, then $\mathrm{wrs}(R) \neq \emptyset$. Contradiction with $\mathrm{wrs}(R) = \emptyset$. □

An immediate consequence of Theorem 4.38 is that the termination problem is decidable.

Theorem 4.39. *Let $R(\mathbf{x}, \mathbf{x}')$, where $\mathbf{x} = \{x_1, \ldots, x_N\}$ for some $N \geq 1$, be an octagonal constraint defining a relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$. The well-foundedness of $R(\mathbf{x}, \mathbf{x}')$ can be decided in at most $\mathcal{O}(N^4 \cdot (N + \log_2 \mu(R)))$ time.*

Proof. By Theorem 4.38, Algorithm 3 computes an octagonal constraint $\phi(\mathbf{x})$ that defines $\mathrm{wrs}(R)$ in $\mathcal{O}(N^4 \cdot (N + \log_2 \mu(R)))$ time and moreover $\mu(\phi)$ is in the order of $\mathcal{O}(\mu(R) \cdot N \cdot 2^N)$. Well-foundedness of R can be decided by checking whether $\phi(\mathbf{x})$ is consistent. This check can be performed in time $\mathcal{O}(N^3 \cdot (N + \log_2 \mu(\phi)))$, by Corollary 4.24, which simplifies to $\mathcal{O}(N^3 \cdot (N + \log(\mu(R) \cdot N \cdot 2^N))) = \mathcal{O}(N^3 \cdot (N + \log_2 \mu(R)))$. □

4.5. **On the Existence of Linear Ranking Functions.** We first define the notion of a *linear ranking function*, using the following notation: if $f(\mathbf{x})$ is a linear term over $\mathbf{x}$ of the form $f(\mathbf{x}) = a_0 + \sum_{i=1}^N a_i x_i$ where $a_0, \ldots, a_N \in \mathbb{Z}$, then $f(\mathbf{x}')$ denotes the corresponding term over $\mathbf{x}'$ defined as $f(\mathbf{x}') \overset{def}{=} a_0 + \sum_{i=1}^N a_i x'_i$.

Definition 4.40. Given a relation defined by $R(\mathbf{x}, \mathbf{x}')$, a *linear ranking function* $f : \mathbf{x} \to \mathbb{Z}$ for $R(\mathbf{x}, \mathbf{x}')$ is a linear term $f(\mathbf{x})$ such that the following holds:

$$\exists h \forall \mathbf{x} \forall \mathbf{x}' \ . \ R(\mathbf{x}, \mathbf{x}') \ \Rightarrow \ f(\mathbf{x}) > f(\mathbf{x}') \ \wedge \ f(\mathbf{x}) \geq h$$

Intuitively, $R(\mathbf{x}, \mathbf{x}') \Rightarrow f(\mathbf{x}) > f(\mathbf{x}')$ requires that f is *decreasing* and $R(\mathbf{x}, \mathbf{x}') \Rightarrow f(\mathbf{x}) \geq h$ requires that f is *bounded*.

A ranking function for a given relation R constitutes a proof of the fact that R is well founded. In this section, we show that for any well-founded octagonal relation $R(\mathbf{x}, \mathbf{x}')$, where $\mathbf{x} = \{x_1, \ldots, x_N\}$, the (strengthened) relation V defined as $V(\mathbf{x}, \mathbf{x}') \equiv R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}'. R^{5^{2N}}(\mathbf{x}, \mathbf{x}')$ has a linear ranking function if and only if R is well founded. Note that if R is well founded, then V is guaranteed to have a linear ranking function even when R alone does not have one. Moreover, we show that such a linear ranking function can be computed in polynomial time. The proof is organized as follows. First, we show in Lemma 4.41 that for each $m \geq 1$, strengthening $R(\mathbf{x}, \mathbf{x}')$ with $\exists \mathbf{x}'. R^m(\mathbf{x}, \mathbf{x}')$ preserves the (conditional) termination problem, formally: $\text{wrs}(R) = \text{wrs}(R_m)$ where R_m is defined by $R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}'.R^m(\mathbf{x}, \mathbf{x}')$. As a consequence, $\text{wrs}(R) = \text{wrs}(V)$.

In Section 4.5.1, we study the case when $R(\mathbf{x}, \mathbf{x}')$ is a well-founded difference bounds constraint. Here, we first generalize Lemma 4.35 and show that the zigzag automaton of R is guaranteed to have a negative-weight cycle, whenever the 5^N-th power of R is consistent. Lemma 4.43 and Lemma 4.47 use the structure of this cycle, representing several of the constraints in R, to show the existence of the linear ranking function for the witness relation $R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}'.R^{N^2}(\mathbf{x}, \mathbf{x}')$.

Section 4.5.2 then studies octagonal relations. Given an octagonal constraint $R(\mathbf{x}, \mathbf{x}')$, where $\mathbf{x} = \{x_1, \ldots, x_N\}$, with its difference bounds representation $\overline{R}(\mathbf{y}, \mathbf{y}')$, where $\mathbf{y} = \{y_1, \ldots, y_{2N}\}$, such that R is well founded and the 5^{2N}-th power of R is consistent, we first apply the above result and immediately infer that $\overline{R}(\mathbf{y}, \mathbf{y}') \wedge \exists \mathbf{y}'.\overline{R}^{4N^2}(\mathbf{y}, \mathbf{y}')$ has a linear ranking function $\overline{f}(\mathbf{y})$. Then, we prove in Proposition 4.50 that the function defined as $f \stackrel{def}{=} \overline{f}(\mathbf{y})[x_i/y_{2i-1}, -x_i/y_{2i}]_{i=1}^N$ is a linear ranking function for $R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}'.R^{4N^2}(\mathbf{x}, \mathbf{x}')$. For the case when the 5^{2N}-th power is not consistent, it follows easily that $R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}'.R^{4N^2}(\mathbf{x}, \mathbf{x}')$ is not consistent either and hence, trivially, has a linear ranking function. Then, since the sequence $\{\text{pre}_R^n(\mathbb{Z}^{\mathbf{x}})\}_{n \geq 1}$ is descending, it follows that $\exists \mathbf{x}'.R^{5^{2N}}(\mathbf{x}, \mathbf{x}') \Rightarrow \exists \mathbf{x}'.R^{4N^2}(\mathbf{x}, \mathbf{x}')$ and one can thus show that f is also a ranking function for V. Finally, we summarize this reasoning in Theorem 4.51 and prove that such a linear ranking function can be found in polynomial time.

Lemma 4.41. *Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a relation defined by a formula $R(\mathbf{x}, \mathbf{x}')$, and $m \geq 1$ be an integer. Then $\text{wrs}(R) = \text{wrs}(R_m)$, where R_m is the relation defined by $R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}'.R^m(\mathbf{x}, \mathbf{x}')$.*

Proof. "⊆" By Proposition 3.1, $\text{pre}_{R'}(S) \subseteq \text{pre}_R(S)$ for any set S and relations R, R' such that $R' \subseteq R$. Since $R_m \subseteq R$, then $\text{pre}_{R_m}(\mathbb{Z}^{\mathbf{x}}) \subseteq \text{pre}_R(\mathbb{Z}^{\mathbf{x}})$. Applying this argument n-times, we infer that $\text{pre}_{R_m}^n(\mathbb{Z}^{\mathbf{x}}) \subseteq \text{pre}_R^n(\mathbb{Z}^{\mathbf{x}})$. Thus, we have:

$$\begin{array}{rcll} \text{wrs}(R_m) & = & \bigcap_{n \geq 1} \text{pre}_{R_m}^n(\mathbb{Z}^{\mathbf{x}}) & \text{by Lemma 4.33} \\ & \subseteq & \bigcap_{n \geq 1} \text{pre}_R^n(\mathbb{Z}^{\mathbf{x}}) & \\ & = & \text{wrs}(R) & \text{by Lemma 4.33} \end{array}$$

"⊇" We prove the dual. Assume that $\text{wrs}(R) \neq \emptyset$, i.e. there exists an infinite sequence of valuations $\sigma = \{\nu_i \in \mathbb{Z}^x\}_{i \geq 0}$ such that $(\nu_i, \nu_{i+1}) \in R$, for all $i \geq 0$. Then each ν_i belong to the set defined by $\exists \mathbf{x}' \,.\, R^m(\mathbf{x}, \mathbf{x}')$, hence σ is an infinite sequence for the relation defined by $R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}'.R^m(\mathbf{x}, \mathbf{x}')$ as well. □

4.5.1. *Linear Ranking Function for Difference Bounds Relation.* In the rest of this section, let us fix the set of variables $\mathbf{x} = \{x_1, \ldots, x_N\}$ for some constant $N \geq 1$. We first prove the existence of a negative-weight cycle in a zigzag automaton whenever the 5^N-th power of a well-founded difference bounds relation $R(\mathbf{x}, \mathbf{x}')$ is consistent.

Lemma 4.42. *Let $R(\mathbf{x}, \mathbf{x}')$ be a well-founded difference bounds relation such that $R^{5^N}(\mathbf{x}, \mathbf{x}')$ is consistent. Then, there exists a zigzag automaton $\mathcal{A}_{ij} = \langle T_R, I_{ij}, F \rangle$ for some $1 \leq i, j \leq N$ with an accepting run $\mu.\lambda.\mu'$ where λ is a cycle such that $|\lambda| > 0$ and $\omega(\lambda) < 0$.*

Proof. If $R(\mathbf{x},\mathbf{x}')$ is $*$-consistent, then the result follows immediately from Lemma 4.35. In the rest of the proof, let $R(\mathbf{x},\mathbf{x}')$ be a $*$-inconsistent relation such that $R^{5^N}(\mathbf{x},\mathbf{x}')$ is consistent. We first define $n \overset{def}{=} \min\{i \geq 1 \mid R^i(\mathbf{x},\mathbf{x}') \text{ is inconsistent}\}$. Clearly, $n > 5^N$. By Lemma 4.13, there exists $1 \leq i \leq N$ such that $\mathcal{A}_{ii}$ has an accepting run π such that $|\pi| = n$ and $\omega(\pi) < 0$. Since $n > 5^N \geq |Q|$, there must be at least one cycle λ in π, formally: $\pi = \mu.\lambda.\mu'$ for some paths μ, μ' and a cycle λ. Let us denote $m = |\mu.\mu'|$. Clearly $m < n$. We prove that $\omega(\lambda) < 0$. By contradiction, suppose that $\omega(\lambda) \geq 0$. Then $\omega(\mu.\mu') = \omega(\pi) - \omega(\lambda) < 0$ and hence, by Lemma 4.13, $R^m(\mathbf{x},\mathbf{x}')$ is not consistent. Since $m < n$, this contradicts the definition of n as the minimal inconsistent power. Thus, $\omega(\lambda) < 0$ and the run $\mu.\lambda.\mu'$ of $\mathcal{A}_{ii}$ has the property required by the lemma. □

We next prove the existence of a linear decreasing function, based on the existence of a negative-weight cycle in the zigzag automaton.

Lemma 4.43. *Let $R(\mathbf{x},\mathbf{x}')$, where $\mathbf{x} = \{x_1,\ldots,x_N\}$, be a difference bounds constraint defining a well-founded relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ such that $R^{5^N}(\mathbf{x},\mathbf{x}')$ is consistent. Then, there exists a linear function $f(\mathbf{x})$ such that $\forall \mathbf{x},\mathbf{x}' \,.\, R(\mathbf{x},\mathbf{x}') \Rightarrow f(\mathbf{x}) > f(\mathbf{x}')$ is valid.*

Proof. By Lemma 4.42, there exist integers $1 \leq i,j \leq N$ such that the zigzag automaton $\mathcal{A}_{ij}$ has an accepting run $\mu.\lambda.\mu'$ where λ is a cycle such that $|\lambda| > 0$ and $\omega(\lambda) < 0$. Let us write λ as $\lambda = q_0 \xrightarrow{G_0} q_1 \xrightarrow{G_1} q_2 \ldots q_{p-1} \xrightarrow{G_{p-1}} q_0$ where $p = |\lambda|$ and $G_j = (\mathbf{x} \cup \mathbf{x}', E_j)$ for some set of edges E_j, $0 \leq j < p$. Recall that G_j is a bipartite graph for each $0 \leq j < p$ and therefore contains edges of the form $x_i \to x'_j$ or $x'_i \to x_j$. Consider the following sum of all constraints represented by edges appearing in λ (note that the sum of weights of these edges equals $\omega(\lambda)$):

$$\sum_{\substack{0 \leq j < p \\ 1 \leq i,k \leq N \\ (x_k \to x'_i) \in E_j}} (x_k - x'_i) \;+\; \sum_{\substack{0 \leq j < p \\ 1 \leq i,k \leq N \\ (x'_k \to x_i) \in E_j}} (x'_k - x_i) \leq \sum_{\substack{0 \leq j < p \\ e \in E_j}} \omega(e) = \omega(\lambda) \tag{4.9}$$

Notice that for each $0 \leq j < p$, there exists an accepting run of the form

$$q \xrightarrow{w} q_{(j-1) \bmod p} \xrightarrow{G_{(j-1) \bmod p}} q_j \xrightarrow{G_j} q_{(j+1) \bmod p} \xrightarrow{G_{(j+1) \bmod p}} q_{(j+2) \bmod p} \xrightarrow{w'} q'$$

for some $q, q' \in Q$ and $w, w' \in \Sigma_R^*$. It follows from the definition of zigzag automata that for each edge $e_1 : x'_k \to x_i \in E_j$, there exists a unique “successor“ e_2 which is of either of the following forms:

$$\begin{array}{lll} \text{either} & e_2 : x_i \to x'_m \in E_j & \text{if } (q_j)_i = \ell r, \\ \text{or} & e_2 : x'_i \to x_m \in E_{(j-1) \bmod p} & \text{if } (q_j)_i = \ell. \end{array} \tag{4.10}$$

Dually, e_1 is said to be the unique “predecessor“ of e_2. Similarly, for each edge $e_1 : x_k \to x'_i \in E_j$, there exists a unique successor e_2 which is of either of the following forms:

$$\begin{array}{lll} \text{either} & e_2 : x'_i \to x_m \in E_j & \text{if } (q_{(j+1) \bmod p})_i = r\ell, \\ \text{or} & e_2 : x_i \to x'_m \in E_{(j+1) \bmod p} & \text{if } (q_{(j+1) \bmod p})_i = r. \end{array} \tag{4.11}$$

Consider the following sum:

$$\sum_{\substack{0\leq j<p \\ 1\leq i,k,m\leq N \\ (x_k\rightarrow x'_i)\in E_j \\ (x_i\rightarrow x'_m)\in E_{(j+1) \bmod p}}} (-x'_i+x_i) + \sum_{\substack{0\leq j<p \\ 1\leq i,k,m\leq N \\ (x_k\rightarrow x'_i)\in E_j \\ (x'_i\rightarrow x_m)\in E_j}} (-x'_i+x'_i) + \sum_{\substack{0\leq j<p \\ 1\leq i,k,m\leq N \\ (x'_k\rightarrow x_i)\in E_j \\ (x'_i\rightarrow x_m)\in E_{(j-1) \bmod p}}} (-x_i+x'_i) + \sum_{\substack{0\leq j<p \\ 1\leq i,k,m\leq N \\ (x'_k\rightarrow x_i)\in E_j \\ (x_i\rightarrow x'_m)\in E_j}} (-x_i+x_i) \tag{4.12}$$

and note that every edge $e = (x_k \rightarrow x'_i) \in E_j$, where $1 \leq i, j \leq N, 0 \leq j < p$, is considered exactly twice in (4.12), since

- e has a unique successor and therefore contributes with the $-x'_i$ term in (4.12)
- e has a unique predecessor and therefore contributes with the $+x_k$ term in (4.12)

Similarly, every edge $(x'_k \rightarrow x_i) \in E_j$ is considered twice and contributes with terms $-x_i$ and $+x'_k$. Hence, the sum (4.12) is equivalent to the left-hand side of (4.9). Clearly, the second and the fourth sum in (4.12) evaluate to zero. It follows from Equations (4.11) and (4.10) that the remaining two sums can be written equivalently as

$$\sum_{\substack{0\leq j<p \\ (q_j)_i=r}} (-x'_i + x_i) \ + \sum_{\substack{0\leq j<p \\ (q_j)_i=\ell}} (-x_i + x'_i) \tag{4.13}$$

Thus, (4.9) can be written equivalently as

$$\sum_{\substack{0\leq j<p \\ (q_j)_i=r}} (-x'_i + x_i) \ + \sum_{\substack{0\leq j<p \\ (q_j)_i=\ell}} (-x_i + x'_i) \leq \omega(\lambda) \tag{4.14}$$

Let $f(\mathbf{x})$ denote the negated sum of all unprimed terms in (4.13) and $g(\mathbf{x}')$ denote the sum of all primed terms in (4.13). Clearly, $f(\mathbf{x}) = g(\mathbf{x}')[\mathbf{x}/\mathbf{x}']$ (i.e. $g(\mathbf{x}')$ is the primed counterpart of $f(\mathbf{x})$) and (4.14) can be written as $g(\mathbf{x}') - f(\mathbf{x}) \leq \omega(\lambda)$. Recall that $f(\mathbf{x}') \stackrel{def}{=} a_0 + \sum_{i=1}^{N} a_i x'_i$ and hence $f(\mathbf{x}') = g(\mathbf{x}')$. We thus obtain:

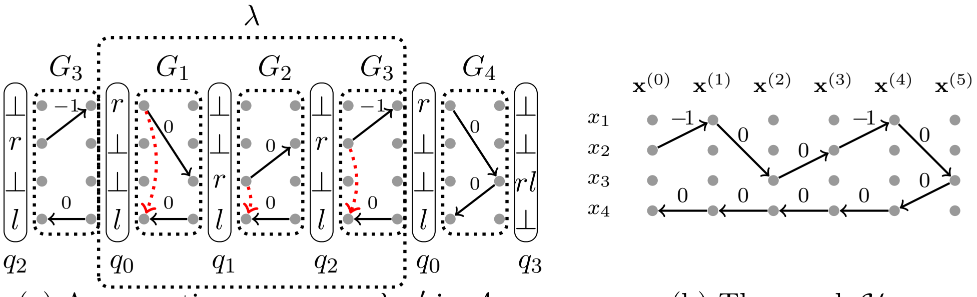
$$f(\mathbf{x}') - f(\mathbf{x}) \leq \omega(\lambda) < 0 \tag{4.15}$$

Hence, $f(\mathbf{x})$ is strictly decreasing, formally: $R(\mathbf{x}, \mathbf{x}') \Rightarrow f(\mathbf{x}) > f(\mathbf{x}')$. □

Example 4.44. (Ex. 4.7 ctd.) We illustrate the construction of a linear decreasing function for a well-founded relation $R(\mathbf{x}, \mathbf{x}') \equiv x_2 - x'_1 \leq -1 \wedge x_3 - x'_2 \leq 0 \wedge x_1 - x'_3 \leq 0 \wedge x'_4 - x_4 \leq 0 \wedge x'_3 - x_4 \leq 0$ (see also Figure 1). By Lemma 4.35, there exists an accepting run $\mu.\lambda.\mu'$ in a zigzag automaton where λ is a cycle such that $\omega(\lambda) < 0$. Figure 4 depicts such a run in $\mathcal{A}_{2,4}$ where μ, λ, and μ' are labeled with words G_3, $G_1.G_2.G_3$, and G_4, respectively. We have $\omega(\lambda) = -1$. We follow the construction from Lemma 4.43 and sum the edges that are present in λ (see the solid edges in G_1, G_2, and G_3 in Figure 4). We obtain

$$(x_1 - x'_3) + (x_3 - x'_2) + (x_2 - x'_1) + (x'_4 - x_4) + (x'_4 - x_4) + (x'_4 - x_4) \leq -1$$

which simplifies to $(x_1 + x_2 + x_3 - 3x_4) - (x'_1 + x'_2 + x'_3 - 3x'_4) \leq -1$. Letting $f(\mathbf{x}) = -(x_1 + x_2 + x_3 - 3x_4)$, we have that $R(\mathbf{x}, \mathbf{x}') \Rightarrow f(\mathbf{x}) > f(\mathbf{x}')$. □



(a) An accepting run $\pi = \mu.\lambda.\mu'$ in $\mathcal{A}_{24}$.

(b) The graph $\mathcal{H}_\pi$.

FIGURE 4. Constructing the ranking function for a relation (see also Fig. 1) $R(\mathbf{x},\mathbf{x}') \Leftrightarrow x_2 - x_1' \leq -1 \wedge x_3 - x_2' \leq 0 \wedge x_1 - x_3' \leq 0 \wedge x_4' - x_4 \leq 0 \wedge x_3' - x_4 \leq 0$. Figure (a) shows a run π that accepts word $\gamma = G_3.G_1.G_2.G_3.G_4$. Figure (b) shows $\mathcal{G}_\pi$, obtained by concatenating the symbols (graphs) of γ. $\mathcal{G}_\pi$ contains a single path ρ from $x_2^{(0)}$ to $x_4^{(0)}$.

Next, we prove that all functions of Lemma 4.43 are bounded, concluding that they are indeed ranking functions. Each run π of length $n \geq 1$ in the zigzag automaton $\mathcal{A}_{ij}$, $1 \leq i,j \leq N$, recognizes a word $w = G_0.G_1 \ldots G_{n-1}$ where $G_0, \ldots, G_{n-1} \in \Sigma_R$. Assuming that E_ℓ is the set of edges in G_ℓ for each $0 \leq \ell < n$, we define the concatenation of graphs $G_0, \ldots, G_{n-1}$ as $\mathcal{H}_\pi = (V, E)$ where $V = \bigcup_{\ell=0}^{n} \mathbf{x}^{(\ell)}$ and

$$x_p^{(\ell)} \xrightarrow{c} x_q^{(\ell+1)} \in E \quad \text{iff} \quad x_p \xrightarrow{c} x_q' \in E_\ell$$
$$x_p^{(\ell+1)} \xrightarrow{c} x_q^{(\ell)} \in E \quad \text{iff} \quad x_p' \xrightarrow{c} x_q \in E_\ell$$

for all $0 \leq \ell < n$ and $1 \leq i,j \leq N$. See Figure 4 for an illustration. Supposing that π traverses a cycle λ in $\mathcal{A}_{ij}$ (see the cycle λ in Figure 4), π can be decomposed into a prefix, the cycle itself and a suffix. By the definition of zigzag automata, $\mathcal{H}_\pi$ contains exactly one path[8] ρ from $x_i^{(0)}$ to $x_j^{(0)}$ and a (possibly empty) set of elementary cycles $\{\nu_1, \ldots, \nu_p\}, p \geq 0$. For instance, $\mathcal{H}_\pi$ from Figure 4 contains a single path ρ. The paths $\{\rho, \nu_1, \ldots, \nu_p\}$ may traverse the cycle λ several times, however each exit point from the cycle must match a subsequent entry point (the dotted edges in Figure 4(a) mark such a matching). These paths from the exit to the corresponding entries give the lower bound on $f(\mathbf{x})$, formally: $R^n(\mathbf{x},\mathbf{x}') \Rightarrow f(\mathbf{x}) \geq h$ for some $h \in \mathbb{Z}$ and sufficiently large $n \geq 1$ (Proposition 4.45). In fact, these paths appear already on graphs $\mathcal{G}_R^i$ for every $i \geq N^2$ (Lemma 4.46) and the "sufficiently large n" can be thus bounded by N^2. Hence the need for a strengthened witness $R(\mathbf{x},\mathbf{x}') \wedge \exists \mathbf{x}'.R^{N^2}(\mathbf{x},\mathbf{x}')$, as R alone is not enough for proving boundedness of $f(\mathbf{x})$. Lemma 4.47 combines all these results to prove the existence of a ranking function.

Proposition 4.45. *Let $R(\mathbf{x},\mathbf{x}')$ be a difference bounds constraint, let $\pi = q_0 \xrightarrow{G_0} q_1 \xrightarrow{G_1} \ldots \to q_{n-1} \xrightarrow{G_{n-1}} q_n$, for some $n \geq 1$, be an accepting run of a zigzag automaton $\mathcal{A}_{gh}$ for some $1 \leq g,h \leq N$, and $k \in \{0, \ldots, n-1\}$ be a constant. Then, there exists a bijection*

$$\beta : \{j \mid (q_k)_j = r\} \to \{j \mid (q_k)_j = \ell\}$$

[8] Moreover, this path is acyclic if $i \neq j$ or an elementary cycle if $i = j$.

such that for every $i \in \{j \mid (q_k)_j = r\}$, the following formula is valid:

$$\exists b \,.\, \forall \mathbf{x} \,.\, (\exists \mathbf{x}' \,.\, R^n(\mathbf{x},\mathbf{x}')) \;\Rightarrow\; x_{\beta(i)} - x_i \geq b$$

Proof. We define a shift operator that for every path ρ in $\mathcal{G}_R^m$, $m \geq 1$, of the form $\rho = x_{i_1}^{(j_1)} \xrightarrow{c_1} x_{i_2}^{(j_2)} \xrightarrow{c_2} \ldots \xrightarrow{c_{p-1}} x_{i_p}^{(j_p)}$, $p > 1$, and every $k \in \mathbb{Z}$, returns the path $\rho^{\rightarrow k}$ defined as:

$$\rho^{\rightarrow k} \stackrel{def}{=} x_{i_1}^{(j_1+k)} \xrightarrow{c_1} x_{i_2}^{(j_2+k)} \xrightarrow{c_2} \ldots \xrightarrow{c_{p-1}} x_{i_p}^{(j_p+k)}$$

Let us assume that $G_k = (\mathbf{x} \cup \mathbf{x}', E_k)$ for each $0 \leq k < n$ and let us denote by w the word $G_0.G_1 \ldots G_{n-1}$ accepted by π. Given a path ρ in $\mathcal{G}_R^n$, let V_ρ denote the set of all vertices traversed by ρ. It follows from the definition of zigzag automata that $\mathcal{H}_\pi$ contains one path ν_0 that starts in $x_g^{(0)}$ and ends in $x_h^{(0)}$. $\mathcal{H}_\pi$ may also contain a (possibly empty) set of elementary cycles $\{\nu_1, \ldots, \nu_s\}$ for some $s \geq 0$. By the definition of zigzag automata, the sets of vertices $V_{\nu_0}, \ldots, V_{\nu_p}$ are pairwise disjoint. By the definition of zigzag automata, we have:

$$|\{j \mid (q_k)_j = r\}| = |\{j \mid (q_k)_j = \ell\}|$$

Clearly, for every $1 \leq i \leq N$ such that $(q_k)_i = r$, there exists $\nu \in \{\nu_0, \ldots, \nu_s\}$ such that $x_i^{(k)} \in V_\nu$. Since $(q_k)_i = r$, ν goes to the right from $x_i^{(k)}$, but it must eventually turn left and reach $x_j^{(k)}$ such that $(q_k)_j = \ell$ for some $1 \leq j \leq N$, either in order to reach $x_h^{(0)}$ (if $\nu = \nu_0$) or in order to reach $x_i^{(k)}$ again (if $\nu \neq \nu_0$ is a cycle). Without loss of generality, let $x_j^{(k)}$ be the first such vertex reachable from $x_i^{(k)}$ and let us define $\beta(i) \stackrel{def}{=} j$. Clearly, β is a bijection from $\{j \mid (q_k)_j = r\}$ to $\{j \mid (q_k)_j = \ell\}$. Since $x_j^{(k)}$ was chosen as the first vertex reachable from $x_i^{(k)}$ such that $(q_k)_j = \ell$, it follow that the subpath ρ of ν from $x_i^{(k)}$ to $x_j^{(k)}$ traverses only vertices from $\bigcup_{m=k}^{n} \mathbf{x}^{(m)}$ (since to reach some vertex from $\bigcup_{m=0}^{k-1} \mathbf{x}^{(m)}$, the path would have to cross some component $(q_k)_t$, $1 \leq t \leq N$, such that $(q_k)_t = \ell$). Hence, ρ can be shifted by $-k$ and we obtain a path $\rho' = \rho^{\rightarrow(-k)}$ that starts in $x_i^{(0)}$ and ends in $x_j^{(0)}$. Since ρ' is a path in $\mathcal{G}_R^n$, then $R^n \Rightarrow x_i - x_j \leq \omega(\rho')$, by (4.3). Hence, $R^n(\mathbf{x},\mathbf{x}') \Rightarrow x_{\beta(i)} - x_i \geq -\omega(\rho')$ is valid. As an immediate consequence, the following formulas are valid too:

$$\begin{array}{rcl} \forall \mathbf{x} \,.\, (\exists \mathbf{x}' \,.\, R^n(\mathbf{x},\mathbf{x}')) & \Rightarrow & x_{\beta(i)} - x_i \geq -\omega(\rho') \\ \exists b \,.\, \forall \mathbf{x} \,.\, (\exists \mathbf{x}' \,.\, R^n(\mathbf{x},\mathbf{x}')) & \Rightarrow & x_{\beta(i)} - x_i \geq b \end{array}$$ □

The next lemma proves, for any two unprimed variables x_i, x_j, that if the difference $x_i - x_j$ is bounded in $R^n(\mathbf{x},\mathbf{x}')$ for some $n \geq 1$, it is bounded in $R^{N^2}(\mathbf{x},\mathbf{x}')$ too.

Lemma 4.46. *Let $R(\mathbf{x},\mathbf{x}')$ be a difference bounds constraint. Then, for each $1 \leq i, j \leq N, i \neq j$ and for each $n \geq 1$, the following is a valid formula:*

$$\begin{array}{l} \exists h \,.\, \forall \mathbf{x} \,.\, (\exists \mathbf{x}' \,.\, R^n(\mathbf{x},\mathbf{x}')) \Rightarrow (x_i - x_j \leq h) \\ \Rightarrow \\ \exists h \,.\, \forall \mathbf{x} \,.\, (\exists \mathbf{x}' \,.\, R^{N^2}(\mathbf{x},\mathbf{x}')) \Rightarrow (x_i - x_j \leq h) \end{array}$$

Proof. Let us first define, for each $n \geq 1$:

$$B_n \stackrel{def}{=} \{(i,j) \mid 1 \leq i,j \leq N \text{ and there is a path from } x_i^{(0)} \text{ to } x_j^{(0)} \text{ in } \mathcal{G}_R^n \,\}$$

Clearly, for each $n \geq 1$, $\mathcal{G}_R^n$ is a subgraph of $\mathcal{G}_R^{n+1}$ and hence $B_n \subseteq B_{n+1}$. Next observe that for every $n \geq 1$, every path ρ from $x_i^{(0)}$ to $x_j^{(0)}$ in $\mathcal{G}_R^{n+1}$ can be written as $\rho = \tau_0.\nu_1.\tau_1 \ldots \nu_p.\tau_p$

for some $p \geq 0$ such that $\tau_0, \ldots, \tau_p$ traverse only nodes from $\mathbf{x}^{(0)} \cup \mathbf{x}^{(1)}$ and $\nu_1, \ldots, \nu_p$ traverse only nodes from $\mathbf{x}^{(1)} \cup \cdots \cup \mathbf{x}^{(n+1)}$. Clearly, if ν_k, $1 \leq k \leq p$, is a path from $x_i^{(1)}$ to $x_j^{(1)}$ for some $1 \leq i, j \leq N$, then there also exists a path from $x_i^{(0)}$ to $x_j^{(0)}$ in $\mathcal{G}_R^n$ and consequently, $(i,j) \in B_n$. Hence, we have for all $n \geq 1$:

$$B_{n+1} = B_n \cup \{(i,j) \mid \begin{array}{l} 1 \leq i,j \leq N, \exists 1 \leq k_1, \ldots, k_p \leq N \,.\, (k_1,k_2),(k_3,k_4),\ldots \in B_n \text{ and } \mathcal{G}_R \\ \text{has paths } x_i^{(0)} \to^+ x_{k_1}^{(1)}, x_{k_2}^{(1)} \to^+ x_{k_3}^{(1)}, x_{k_4}^{(1)} \to^+ x_{k_5}^{(1)}, \ldots, x_{k_p}^{(1)} \to^+ x_j^{(0)} \end{array} \}$$

Hence, B_{n+1} is a function of B_n and $\mathcal{G}_R$. Consequently, if $B_n = B_{n+1}$ for some $n \geq 1$, then $B_m = B_n$ for all $m \geq n$. Clearly, $|B_n| \leq N^2$ for any $n \geq 1$. Hence, the sequence $\{B_n\}_{n \geq 1}$ stabilizes after at most N^2 steps, formally: $B_n = B_{N^2}$ for all $n \geq N^2$. Consequently, the implication

$$(i,j) \in B_n \Rightarrow (i,j) \in B_{N^2} \tag{4.16}$$

holds for all $n \geq N^2$. In fact, it is also valid for all $1 \leq n < N^2$, since we have $B_n \subseteq B_{N^2}$ in this case. Hence, (4.16) holds for all $n \geq 1$. Next, observe that:

$$\begin{array}{rll} (i,j) \in B_n & \text{iff} & \text{there exists a path } \rho \text{ from } x_i^{(0)} \text{ to } x_j^{(0)} \text{ in } \mathcal{G}_R^n \\ & \text{iff} & R^n(\mathbf{x}, \mathbf{x}') \Rightarrow (x_i - x_j \leq \omega(\rho)) \text{ is valid} \qquad\qquad\qquad\qquad \text{(by (4.3))} \\ & \text{iff} & (\exists \mathbf{x}' \,.\, R^n(\mathbf{x}, \mathbf{x}')) \Rightarrow (x_i - x_j \leq \omega(\rho)) \text{ is valid} \\ & \text{iff} & \exists h \,.\, \forall \mathbf{x} \,.\, (\exists x' \,.\, R^n(\mathbf{x}, \mathbf{x}')) \Rightarrow (x_i - x_j \leq h) \text{ is valid} \end{array}$$

Finally, we combine the above with (4.16) and conclude that for all $n \geq 1$ and for all $1 \leq i, j \leq N$, we have:

$$\begin{array}{ccc} (i,j) \in B_n & \Leftrightarrow & \exists h \,.\, \forall \mathbf{x} \,.\, (\exists x' \,.\, R^n(\mathbf{x}, \mathbf{x}')) \Rightarrow (x_i - x_j \leq h) \\ \Downarrow & & \\ (i,j) \in B_{N^2} & \Leftrightarrow & \exists h \,.\, \forall \mathbf{x} \,.\, (\exists x' \,.\, R^{N^2}(\mathbf{x}, \mathbf{x}')) \Rightarrow (x_i - x_j \leq h) \end{array}$$

Hence, the lemma holds. □

Finally, we show that each decreasing function of Lemma 4.43 is also bounded, concluding that it is a linear ranking function.

Lemma 4.47. *Let $R(\mathbf{x}, \mathbf{x}')$ be a difference bounds constraint defining a well-founded relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ such that $R^{5^N}(\mathbf{x}, \mathbf{x}')$ is consistent. Then, there exists a linear ranking function for $R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}'.R^{N^2}(\mathbf{x}, \mathbf{x}')$.*

Proof. Let $\mu.\lambda.\mu'$ be an accepting run from Lemma 4.43 where λ is a negative-weight cycle of the form $\lambda = q_0 \xrightarrow{G_0} q_1 \xrightarrow{G_1} q_2 \ldots q_{p-1} \xrightarrow{G_{p-1}} q_0$ where $p = |\lambda|$. Let $n = |\mu.\lambda.\mu'|$. Further, let $f(\mathbf{x})$ be the the corresponding linear decreasing function constructed in Lemma 4.43 from λ. Recall that $f(\mathbf{x})$ denotes the negated sum of all unprimed terms in

$$\sum_{\substack{0 \leq j < p \\ (q_j)_i = r}} (-x_i' + x_i) \;+\; \sum_{\substack{0 \leq j < p \\ (q_j)_i = \ell}} (-x_i + x_i')$$

Hence, for each $0 \leq j < p$ and $1 \leq i \leq N$, $(q_j)_i$ contributes to $f(\mathbf{x})$ with terms:

$$\begin{array}{cl} \{-x_i\} & \text{if } (q_j)_i = r, \\ \{+x_i\} & \text{if } (q_j)_i = \ell, \\ \emptyset & \text{otherwise.} \end{array}$$

Let $n \overset{def}{=} |\mu.\lambda.\mu'|$. By Proposition 4.45, for each $0 \leq j < p$, there exists a bijection

$$\beta_j : \{i \mid (q_j)_i = r\} \to \{i \mid (q_j)_i = \ell\}$$

such that, for each $k \in \{i \mid (q_j)_i = r\}$:

$$\exists h \ . \ \forall \mathbf{x} \ . \ (\exists \mathbf{x}' \ . \ R^n(\mathbf{x}, \mathbf{x}')) \Rightarrow (x_{\beta_j(k)} - x_k \geq h)$$

By Lemma 4.46, we then have:

$$\exists h \ . \ \forall \mathbf{x} \ . \ (\exists \mathbf{x}' \ . \ R^{N^2}(\mathbf{x}, \mathbf{x}')) \Rightarrow (x_{\beta_j(k)} - x_k \geq h)$$

Clearly:

$$f(\mathbf{x}) = \sum_{0 \leq j < p} \sum_{\substack{1 \leq k \leq N \\ (q_j)_k = r}} (x_{\beta_j(k)} - x_k)$$

Thus, since each term $x_{\beta_j(i)} - x_i$ in the above sum is bounded in $\exists \mathbf{x}' \ . \ R^{N^2}(\mathbf{x}, \mathbf{x}')$, it follows that the sum of these terms is bounded too:

$$\exists h \ . \ \forall \mathbf{x} \ . \ (\exists \mathbf{x}' \ . \ R^{N^2}(\mathbf{x}, \mathbf{x}')) \Rightarrow f(\mathbf{x}) \geq h \tag{4.17}$$

By Lemma 4.43, we have:

$$\forall \mathbf{x}, \mathbf{x}' \ . \ R(\mathbf{x}, \mathbf{x}') \Rightarrow f(\mathbf{x}) > f(\mathbf{x}') \tag{4.18}$$

Since strengthening the hypothesis of any implication preserves its validity, we can infer from (4.17) and (4.18) that:

$$\exists h \ . \ \forall \mathbf{x}, \mathbf{x}' \ . \ R(\mathbf{x}, \mathbf{x}') \wedge (\exists \mathbf{x}'.R^{N^2}(\mathbf{x}, \mathbf{x}')) \ \Rightarrow \ f(\mathbf{x}) > f(\mathbf{x}') \ \wedge \ f(\mathbf{x}) \geq h$$

Thus, $f(\mathbf{x})$ is a linear ranking function for $R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}'.R^{N^2}(\mathbf{x}, \mathbf{x}')$. □

Example 4.48. (Ex. 4.44 ctd.) We illustrate the boundedness of $f = -(x_1 + x_2 + x_3 - 3x_4)$, by following the arguments of Lemma 4.47 and Proposition 4.45. The cycle λ traverses control states q_0, q_1, q_2 (see Figure 4). Let us consider the following bijections $\beta_0, \beta_1, \beta_2$:

$$\beta_0 = \{(1, 4)\}, \beta_1 = \{(3, 4)\}, \beta_2 = \{(2, 4)\}$$

(the dotted edges in Figure 4(a) mark these bijections). Next, we define the paths ρ_0, ρ_1, ρ_2 as subpaths of ρ from Figure 4(b)

$$\begin{array}{lcl}
\rho_0 & \overset{def}{=} & x_1^{(1)} \xrightarrow{0} x_3^{(2)} \xrightarrow{0} x_2^{(3)} \xrightarrow{-1} x_1^{(4)} \xrightarrow{0} x_3^{(5)} \xrightarrow{0} x_4^{(4)} \xrightarrow{0} x_4^{(3)} \xrightarrow{0} x_4^{(2)} \xrightarrow{0} x_4^{(1)} \\
\rho_1 & \overset{def}{=} & x_3^{(2)} \xrightarrow{0} x_2^{(3)} \xrightarrow{-1} x_1^{(4)} \xrightarrow{0} x_3^{(5)} \xrightarrow{0} x_4^{(4)} \xrightarrow{0} x_4^{(3)} \xrightarrow{0} x_4^{(2)} \\
\rho_2 & \overset{def}{=} & x_2^{(3)} \xrightarrow{-1} x_1^{(4)} \xrightarrow{0} x_3^{(5)} \xrightarrow{0} x_4^{(4)} \xrightarrow{0} x_4^{(3)}
\end{array}$$

Note that

$$\begin{array}{lcll}
\rho_0 & = & x_1^{(1)} \to \ldots \to x_{\beta(1)}^{(1)} & V_{\rho_0} \subseteq \bigcup_{\ell=1}^{5} \mathbf{x}^{(\ell)} \\
{\rho_0}^{\to(-1)} & = & x_1^{(0)} \to \ldots \to x_{\beta(1)}^{(0)} & V_{{\rho_0}^{\to(-1)}} \subseteq \bigcup_{\ell=0}^{5} \mathbf{x}^{(\ell)}
\end{array}$$

According to Equation (4.3), existence of the path ${\rho_0}^{\to(-1)}$ implies that $R^4(\mathbf{x}, \mathbf{x}') \Rightarrow (x_1 - x_{\beta_0(1)}) \leq \omega({\rho_0}^{\to(-1)}) = -1$. Clearly, it follows that $(\exists \mathbf{x}' \ . \ R^4(\mathbf{x}, \mathbf{x}')) \Rightarrow (x_{\beta_0(1)} - x_1) \geq 1$. The bijection β_0 therefore satisfies the required properties. Next, we apply Proposition 4.46 and infer that $(\exists \mathbf{x}' \ . \ R^{N^2}(\mathbf{x}, \mathbf{x}')) \Rightarrow (x_{\beta_0(1)} - x_1) \geq c_0$ for some $c_0 \in \mathbb{Z}$. By analogical reasoning, we infer that

$$\begin{array}{ll}
(\exists \mathbf{x}' \ . \ R^{N^2}(\mathbf{x}, \mathbf{x}')) \Rightarrow (x_{\beta_1(3)} - x_3) \geq c_1 & \text{for some } c_1 \in \mathbb{Z} \\
(\exists \mathbf{x}' \ . \ R^{N^2}(\mathbf{x}, \mathbf{x}')) \Rightarrow (x_{\beta_2(2)} - x_2) \geq c_2 & \text{for some } c_2 \in \mathbb{Z}
\end{array}$$

Then, we infer:

$$\begin{array}{rl} & (x_{\beta_0(1)} - x_1) \geq c_0 \ \wedge \ (x_{\beta_1(3)} - x_3) \geq c_1 \ \wedge \ (x_{\beta_2(2)} - x_2) \geq c_2 \\ \Leftrightarrow & (x_4 - x_1) \geq c_0 \ \wedge \ (x_4 - x_3) \geq c_1 \ \wedge \ (x_4 - x_2) \geq c_2 \\ \Rightarrow & (x_4 - x_1) + (x_4 - x_3) + (x_4 - x_2) \geq c_0 + c_1 + c_2 \\ \Leftrightarrow & f(\mathbf{x}) \geq c_0 + c_1 + c_2 \end{array}$$

Hence, $(\exists \mathbf{x}' \ . \ R^{N^2}(\mathbf{x}, \mathbf{x}')) \Rightarrow f(\mathbf{x}) \geq c_0 + c_1 + c_2$ and thus, $f(\mathbf{x})$ is bounded. Example 4.44 demonstrated that $f(\mathbf{x})$ is decreasing. We conclude that $f(\mathbf{x})$ is a ranking function.

As an experiment, we have tried the iRankFinder [4] tool (complete for integer linear ranking functions), which failed to discover a ranking function on this example. This comes with no surprise, since no linear decreasing function that is bounded after the first iteration exists. However, iRankFinder finds a linear ranking function for the witness relation $R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}'.R^{N^2}(\mathbf{x}, \mathbf{x}')$ instead. Interestingly, the linear ranking function found by iRankFinder differs from the one computed in this example only by a constant. □

4.5.2. *Linear Ranking Functions for Octagonal Relations.* In the rest of this section, let us fix the sets of variables $\mathbf{x} = \{x_1, \ldots, x_N\}$ and $\mathbf{y} = \{y_1, \ldots, y_{2N}\}$ for some constant $N \geq 1$. The following proposition gives a way to construct a linear ranking function for an octagonal relation $R(\mathbf{x}, \mathbf{x}')$ from any linear ranking function for its difference bounds representation $\overline{R}(\mathbf{y}, \mathbf{y}')$.

Proposition 4.49. *Let $R(\mathbf{x}, \mathbf{x}')$ be an octagonal constraint, $\overline{R}(\mathbf{y}, \mathbf{y}')$ be its difference bounds encoding and let $\overline{f}(\mathbf{y})$ be a linear ranking function for $\overline{R}(\mathbf{y}, \mathbf{y}')$. Then, the function $f(\mathbf{x}) \overset{def}{=} \overline{f}(\mathbf{y})[x_i/y_{2i-1}, -x_i/y_{2i}]_{i=1}^{N}$, is a linear ranking function for $R(\mathbf{x}, \mathbf{x}')$.*

Proof. Clearly, $f(\mathbf{x})$ is linear by definition. We have the following equivalences:

$$\begin{array}{rll} R(\mathbf{x}, \mathbf{x}') \Leftrightarrow & \overline{R}(\mathbf{y}, \mathbf{y}')[x_i/y_{2i-1}, -x_i/y_{2i}]_{i=1}^{N} & \text{(by Equation (4.5))} \\ f(\mathbf{x}) = & \overline{f}(\mathbf{y})[x_i/y_{2i-1}, -x_i/y_{2i}]_{i=1}^{N} & \text{(by definition of } f(\mathbf{x})\text{)} \end{array}$$

Since $\overline{f}(\mathbf{y})$ is a linear ranking function for $\overline{R}(\mathbf{y}, \mathbf{y}')$, the following formula is valid:

$$\exists h \ . \ \forall \mathbf{y}, \mathbf{y}' \ . \ \overline{R}(\mathbf{y}, \mathbf{y}') \ \Rightarrow \ \overline{f}(\mathbf{y}) > \overline{f}(\mathbf{y}') \ \wedge \ \overline{f}(\mathbf{y}) \geq h$$

Clearly, its validity is preserved under the substitution $[x_i/y_{2i-1}, -x_i/y_{2i}]_{i=1}^{N}$ and thus

$$\exists h \ . \ \forall \mathbf{x}, \mathbf{x}' \ . \ \forall R(\mathbf{x}, \mathbf{x}') \ \Rightarrow \ f(\mathbf{x}) > f(\mathbf{x}') \ \wedge \ f(\mathbf{x}) \geq h$$

is valid too. Hence, $f(\mathbf{x})$ is a linear ranking function for $R(\mathbf{x}, \mathbf{x}')$. □

The next proposition generalizes Proposition 4.50 and shows how to construct a linear ranking function for an octagonal relation $R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}'.R^n(\mathbf{x}, \mathbf{x}')$ from any linear ranking function for the difference bounds relation $\overline{R}(\mathbf{y}, \mathbf{y}') \wedge \exists \mathbf{y}' \ . \ \overline{R}^n(\mathbf{y}, \mathbf{y}')$.

Proposition 4.50. *Let $R(\mathbf{x}, \mathbf{x}')$ be an octagonal constraint, $\overline{R}(\mathbf{y}, \mathbf{y}')$ be its difference bounds encoding and let $\overline{f}(\mathbf{y})$ be a linear ranking function for $\overline{R}(\mathbf{y}, \mathbf{y}') \wedge \exists \mathbf{y}' \ . \ \overline{R}^n(\mathbf{y}, \mathbf{y}')$, for a fixed $n \geq 1$. Then, $f(\mathbf{x}) \overset{def}{=} \overline{f}(\mathbf{y})[x_i/y_{2i-1}, -x_i/y_{2i}]_{i=1}^{N}$ is a linear ranking function for $R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}'.R^n(\mathbf{x}, \mathbf{x}')$.*

Proof. Let us first define the following substitution

$$\sigma \overset{def}{=} [x_i^{(0)}/y_{2i-1}^{(0)}, -x_i^{(0)}/y_{2i}^{(0)}, x_i^{(n)}/y_{2i-1}^{(n)}, -x_i^{(n)}/y_{2i-1}^{(n)}]_{i=1}^{2N}$$

Next, observe that (the second equivalence is by Proposition 4.26)

$$\begin{array}{rcl} R^n(\mathbf{x}^{(0)}, \mathbf{x}^{(n)}) & \Leftrightarrow & \exists \mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(n-1)} \ . \ \bigwedge_{i=0}^{n-1} R(\mathbf{x}^{(i)}, \mathbf{x}^{(i+1)}) \\ & \Leftrightarrow & \left[\exists \mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(n-1)} \ . \ \bigwedge_{i=0}^{n-1} \overline{R}(\mathbf{y}^{(i)}, \mathbf{y}^{(i+1)})\right][\sigma] \\ & \Leftrightarrow & \overline{R}^n(\mathbf{y}^{(0)}, \mathbf{y}^{(n)})[\sigma] \end{array}$$

Consequently, we have:

$$\overline{R^n}(\mathbf{y}, \mathbf{y}') \Leftrightarrow \overline{R}^n(\mathbf{y}, \mathbf{y}') \tag{4.19}$$

Observe that

$$\begin{array}{rcll} \overline{\exists \mathbf{x}' \ . \ R^n(\mathbf{x}, \mathbf{x}')} & \Leftrightarrow & \overline{\big(\exists \mathbf{y}' \ . \ \overline{R^n}(\mathbf{y}, \mathbf{y}')\big)[x_i/y_{2i-1}, -x_i/y_{2i}]_{i=1}^N} & \text{(by Proposition 4.26)} \\ & \Leftrightarrow & \exists \mathbf{y}' \ . \ \overline{R^n}(\mathbf{y}, \mathbf{y}') & \\ & \Leftrightarrow & \exists \mathbf{y}' \ . \ \overline{R}^n(\mathbf{y}, \mathbf{y}') & \text{(by Equation (4.19))} \end{array} \tag{4.20}$$

Consequently, we have:

$$\begin{array}{rcll} \overline{R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}' \ . \ R^n(\mathbf{x}, \mathbf{x}')} & \Leftrightarrow & \overline{R}(\mathbf{y}, \mathbf{y}') \wedge \overline{\exists \mathbf{x}' \ . \ R^n(\mathbf{x}, \mathbf{x}')} & \\ & \Leftrightarrow & \overline{R}(\mathbf{y}, \mathbf{y}') \wedge \exists \mathbf{y}' \ . \ \overline{R}^n(\mathbf{y}, \mathbf{y}') & \text{(by Equation (4.20))} \end{array}$$

Thus, since $\overline{f}(\mathbf{y})$ is a linear ranking function for $\overline{R}(\mathbf{y}, \mathbf{y}') \wedge \exists \mathbf{y}' \ . \ \overline{R}^n(\mathbf{y}, \mathbf{y}')$, then $f(\mathbf{x})$ is a linear ranking function for $R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}' \ . \ R^n(\mathbf{x}, \mathbf{x}')$, by Proposition 4.49. □

Finally, we can combine the above results into the main theorem.

Theorem 4.51. *Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a relation defined by an octagonal constraint $R(\mathbf{x}, \mathbf{x}')$ and let $V \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a relation defined by*

$$V(\mathbf{x}, \mathbf{x}') \ \equiv \ R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}'. R^{5^{2N}}(\mathbf{x}, \mathbf{x}')$$

Then, R is well founded if and only if V is well founded if and only if $V(\mathbf{x}, \mathbf{x}')$ has a linear ranking function. Moreover, both $V(\mathbf{x}, \mathbf{x}')$ and the linear ranking function are computable in polynomial time.

Proof. The fact that $R(\mathbf{x}, \mathbf{x}')$ is well founded if and only if $V(\mathbf{x}, \mathbf{x}')$ is well founded follows from Lemma 4.41. Thus, if $R(\mathbf{x}, \mathbf{x}')$ is not well founded, neither is $V(\mathbf{x}, \mathbf{x}')$ and hence, $V(\mathbf{x}, \mathbf{x}')$ has no (linear) ranking function. In the rest of the proof, we show that if $R(\mathbf{x}, \mathbf{x}')$ is well founded, then there exists a linear ranking function for $V(\mathbf{x}, \mathbf{x}')$. As a first subcase, suppose that $R^{5^{2N}}(\mathbf{x}, \mathbf{x}')$ is inconsistent. Then clearly, $V(\mathbf{x}, \mathbf{x}')$ is inconsistent too and, trivially, $V(\mathbf{x}, \mathbf{x}')$ has a linear ranking function. As a second subcase, suppose that $R^{5^{2N}}(\mathbf{x}, \mathbf{x}')$ is consistent. By Proposition 4.28, $\overline{R}^{5^{2N}}(\mathbf{y}, \mathbf{y}')$ is consistent too. Since R is well founded, $\overline{R}$ is well founded too, by Lemma 4.36. Then, by Lemma 4.47, there exists a linear ranking function $\overline{f}$ for $\overline{R}(\mathbf{y}, \mathbf{y}') \wedge \exists \mathbf{y}'. \overline{R}^{4N^2}(\mathbf{y}, \mathbf{y}')$. By Proposition 4.50, the function defined as $f \overset{def}{=} \overline{f}[x_i/y_{2i-1}, -x_i/y_{2i}]_{i=1}^N$ is a linear ranking function for $R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}'. R^{4N^2}(\mathbf{x}, \mathbf{x}')$, formally:

$$\exists h \ . \ \forall \mathbf{x}, \mathbf{x}' \ . \ R(\mathbf{x}, \mathbf{x}') \wedge (\exists \mathbf{x}'. R^{4N^2}(\mathbf{x}, \mathbf{x}')) \ \Rightarrow \ f(\mathbf{x}) > f(\mathbf{x}') \ \wedge \ f(\mathbf{x}) \geq 0 \tag{4.21}$$

Since $4N^2 < 5^{2N}$ for all $N \geq 1$, then $\mathrm{pre}_R^{4N^2}(\mathbb{Z}^{\mathbf{z}}) \supseteq \mathrm{pre}_R^{5^{2N}}(\mathbb{Z}^{\mathbf{x}})$, by Proposition 3.1. Consequently, $\exists \mathbf{x}' \, . \, R^{5^{2N}}(\mathbf{x}, \mathbf{x}') \Rightarrow \exists \mathbf{x}' \, . \, R^{4N^2}(\mathbf{x}, \mathbf{x}')$ and therefore

$$R(\mathbf{x}, \mathbf{x}') \wedge (\exists \mathbf{x}'.R^{5^{2N}}(\mathbf{x}, \mathbf{x}')) \Rightarrow R(\mathbf{x}, \mathbf{x}') \wedge (\exists \mathbf{x}'.R^{4N^2}(\mathbf{x}, \mathbf{x}')) \tag{4.22}$$

Combining (4.21) with (4.22), we infer that $f(\mathbf{x})$ is a linear ranking function for $R(\mathbf{x}, \mathbf{x}') \wedge \exists \mathbf{x}'.R^{5^{2N}}(\mathbf{x}, \mathbf{x}')$.

By Lemma 4.37, V can be computed in at most $\mathcal{O}(N^4 \cdot (N + \log_2 \mu(R)))$ time and moreover, $\mu(V)$ is of the order $\mathcal{O}(\mu(R) \cdot N \cdot 2^N)$. Consistency of $V(\mathbf{x}, \mathbf{x}')$ can then be checked in at most $\mathcal{O}(N^3 \cdot (N + \log_2 \mu(V))) = \mathcal{O}(N^3 \cdot (N + \log_2 \mu(R)))$ time, by Corollary 4.24. If $V \Leftrightarrow$ **false**, one can return an arbitrary linear function $f(\mathbf{x})$. Otherwise, if $V \not\Leftrightarrow$ **false**, one can compute $\overline{V} \equiv \overline{R}(\mathbf{y}, \mathbf{y}') \wedge \exists \mathbf{y}'.\overline{R}^{4N^2}(\mathbf{y}, \mathbf{y}')$, again in at most $\mathcal{O}(N^3 \cdot (N + \log_2 \mu(R)))$ time, as a consequence of Proposition 4.26, Proposition 4.25, and Corollary 4.24. Then, a linear ranking function for $\overline{R}$ can be computed in time that is polynomial in the bit-size of $V(\mathbf{x}, \mathbf{x}')$, as proved in [4] (see Corollary 4.8 in Section 4.1). It follows easily from Definition 4.20 that $V(\mathbf{x}, \mathbf{x}')$ can be represented using $\mathcal{O}(\log_2(\mu(V)) \cdot 3 \cdot (2N)^2) = \mathcal{O}(N^2 \cdot (\log_2 N + \log_2 \mu(R)))$ bits. Thus, the time needed to compute $\overline{f}$ is polynomial in μ_R and N. Finally, one computes $f \stackrel{def}{=} \overline{f}[x_i/y_{2i-1}, -x_i/y_{2i}]_{i=1}^N$, again in polynomial time. □

5. Linear Affine Relations

The previous section was concerned with computing weakest non-termination preconditions for non-deterministic integer relations (octagonal relations). Here, we present linear affine relations which are a general model of deterministic transition relations. Linear affine relations are conjunctions of equalities of the form $x' = a_1 x_1 + \ldots + a_n x_n + b$, where $a_1, \ldots, a_n \in \mathbb{Z}$ are integer coefficients, and Presburger definable conditions on the unprimed variables $x_1, \ldots, x_n$. First, we show that the weakest recurrent set of a linear affine relation R can be computed as the limit of a descending Kleene sequence $pre_R(\mathbb{Z}^{\mathbf{x}}) \supseteq pre_R^2(\mathbb{Z}^{\mathbf{x}}) \supseteq \ldots$. Second, this set can be defined in Presburger arithmetic for a subclass of affine relations with the *finite monoid property* (Section 5.3). Finally, we relax the finite monoid condition and describe a method for generating sufficient termination conditions, i.e. sets $S \in \mathbb{Z}^{\mathbf{x}}$ such that $S \cap \mathrm{wrs}(R) = \emptyset$, for the class of *polynomially bounded* affine relations (Section 5.4).

Definition 5.1. Let $\mathbf{x} = \langle x_1, \ldots, x_N \rangle$ be a vector of variables ranging over $\mathbb{Z}$. A relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is said to be an *affine relation* if it can be defined by a formula $R(\mathbf{x}, \mathbf{x}')$ of the form:

$$R(\mathbf{x}, \mathbf{x}') \;\Leftrightarrow\; \mathbf{x}' = A \times \mathbf{x} + \mathbf{b} \;\wedge\; \phi(\mathbf{x}) \tag{5.1}$$

where $A \in \mathbb{Z}^{N \times N}$, $\mathbf{b} \in \mathbb{Z}^N$, and ϕ is a quantifier-free Presburger formula over unprimed variables only, called the *guard* of R. The formula $\mathbf{x}' = A \times \mathbf{x} + \mathbf{b}$, defining a linear transformation, is called the *update* of R.

5.1. **Background on Linear Algebra.** We first recall several notions of linear algebra, needed in the following. For a comprehensive textbook on linear algebra, we refer to [37]. A complex number r is said to be a *root of the unity* if $r^d = 1$ for some integer $d > 0$. If $A \in \mathbb{Z}^{n\times n}$ is a square matrix, and $\mathbf{v} \in \mathbb{Z}^n$ is a column vector of integer constants, then any complex number $\lambda \in \mathbb{C}$ such that $A\mathbf{v} = \lambda\mathbf{v}$, for some complex vector $\mathbf{v} \in \mathbb{C}^n$, is called an *eigenvalue* of A. The vector $\mathbf{v}$ in this case is called an *eigenvector* of A. It is known that the eigenvalues of A are the roots of the *characteristic polynomial* $P_A(x) = \det(A - xI_n) = 0$, which is an effectively computable univariate polynomial. The *minimal polynomial* of A is the polynomial μ_A of lowest degree such that $\mu_A(A) = 0$. By the Cayley-Hamilton Theorem, the minimal polynomial always divides the characteristic polynomial, i.e. the roots of the former are root of the latter.

If $\lambda_1, \ldots, \lambda_m$ are the eigenvalues of A, then $\lambda_1^p, \ldots, \lambda_m^p$ are the eigenvalues of A^p, for all integers $p > 0$. A matrix is said to be *diagonalizable* if and only if there exists a non-singular matrix $U \in \mathbb{C}^{N\times N}$ and a diagonal matrix with the eigenvalues $\lambda_1, \ldots, \lambda_m$ occurring on the main diagonal, such that $A = U \times D \times U^{-1}$. This is the case if and only if μ_A has only roots of multiplicity one.[9]

5.2. **Termination Preconditions for Deterministic Relations.** First, we show that the pre-image function of a deterministic relation is $\cap$-continuous. Since affine transformations are deterministic, this means that their weakest non-termination preconditions can be computed as limits of descending Kleene sequences. Let $\mathbf{x}$ be a set of variables in the following.

Lemma 5.2. *Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a deterministic relation. Then,* pre_R *is $\cap$-continuous.*

Proof. Let $I = \{0, \ldots, d\}$, $d \in \mathbb{N}_\infty$, and $\{S_i \subseteq \mathbb{Z}^{\mathbf{x}}\}_{i\in I}$ be a potentially infinite collection of sets. We prove that:

$$\mathrm{pre}_R(\textstyle\bigcap_{i\in I} S_i) = \bigcap_{i\in I} \mathrm{pre}_R(S_i).$$

"$\subseteq$" By the monotonicity of pre_R (Proposition 3.1), we have $\mathrm{pre}_R(\bigcap_{i\in I} S_i) \subseteq \mathrm{pre}_R(S_i)$ for all $i \in I$ and hence, $\mathrm{pre}_R(\bigcap_{i\in I} S_i) \subseteq \bigcap_{i\in I} \mathrm{pre}_R(S_i)$.

"$\supseteq$" Let $v \in \bigcap_{i\in I} \mathrm{pre}_R(S_i)$. Then, there exists $v_i \in S_i$ such that $(v, v_i) \in R$ for all $i \in I$. Since R is deterministic, then $v_0 = v_i$ for all $i \in I$ and hence $v_0 \in \bigcap_{i\in I} S_i$. Consequently, $v \in \mathrm{pre}_R(\bigcap_{i\in I} S_i)$. □

For the rest of this section, we extend the notion of *closed form* (Definition 3.8) from sequences of sets $S \subseteq \mathbb{Z}^{\mathbf{x}}$ to sequences of powers of relations $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$.

Definition 5.3. Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a relation. The *closed form* of R is a formula $\widehat{R}(k, \mathbf{x}, \mathbf{x}')$ such that, for all $n \geq 1$ and all $\nu, \nu' \in \mathbb{Z}^{\mathbf{x}}$:

$$(\nu, \nu') \in R^n \Leftrightarrow (\nu, \nu') \models \widehat{R}[n/k]$$

Next, we prove that the closed form of a deterministic relation can be defined in Presburger arithmetic whenever the closed form of its update can be defined in Presburger arithmetic. Concretely, whenever the logical definition of a relation R can be split into a guard and a deterministic update, and the closed form of R can be computed based on the closed form of the update.

[9] See e.g. Thm 8.47 in [5].

Lemma 5.4. *Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$, $\mathbf{x} = \{x_1, \ldots, x_N\}$, be a deterministic relation and $\varphi(\mathbf{x})$ be a guard. Then the closed form of the relation defined by the formula $R(\mathbf{x}, \mathbf{x}') \wedge \varphi(\mathbf{x})$ is:*

$$(\widehat{R \wedge \varphi})(k, \mathbf{x}, \mathbf{x}') \Leftrightarrow \widehat{R}(k, \mathbf{x}, \mathbf{x}') \wedge \forall 1 \leq \ell < k \ \exists \mathbf{y} \ . \ \widehat{R}(\ell, \mathbf{x}, \mathbf{y}) \wedge \varphi(\mathbf{y})$$

where $\widehat{R}$ is the closed form of R and $\mathbf{y} = \{y_1, \ldots, y_N\}$.

Proof. "⇒" Let $\nu, \nu' \in \mathbb{Z}^{\mathbf{x}}$ be a pair of valuations, such that $(\nu, \nu') \models (R \wedge \varphi)^n$, for some integer $n \geq 1$. Then we also have $(\nu, \nu') \models (\widehat{R \wedge \varphi})[n/k]$. Consequently, there exists a sequence of valuations $\nu = \nu_0, \nu_1, \ldots, \nu_n = \nu' \in \mathbb{Z}^{\mathbf{x}}$, such that $(\nu_i, \nu_{i+1}) \models R \wedge \varphi$. By Definition 5.3, we have that $(\nu_0, \nu_n) \models \widehat{R}[n/k]$ and $(\nu_0, \nu_i) \models (\widehat{R} \wedge \varphi)[i/k]$, for all $i = 0, \ldots, n-1$.

"⇐" Let $\nu, \nu' \in \mathbb{Z}^{\mathbf{x}}$ be two valuations such that:

- $(\nu, \nu') \models \widehat{R}[n/k]$ for some $n \geq 1$ and,
- for all $i = 0, \ldots, n-1$ there exists a valuation $\nu_i \in \mathbb{Z}^{\mathbf{x}}$ such that $(\nu, \nu_i) \models \widehat{R}[i/k]$ and $\nu_i \models \varphi$.

Since $\widehat{R}[n/k]$ defines R^n, by Definition 5.3, there exists a sequence of valuations $\nu = \nu'_0, \nu'_1, \ldots, \nu'_n = \nu' \in \mathbb{Z}^{\mathbf{x}}$ such that $(\nu'_i, \nu'_{i+1}) \models R$. By the fact that R was assumed to be deterministic, we have $\nu_i = \nu'_i$ for all $i = 0, \ldots, n-1$, hence $\nu'_i \models \varphi$, for all $i = 0, \ldots, n-1$. Clearly then $(\nu, \nu') \models (\widehat{R \wedge \varphi})[n/k]$. □

Since linear affine relations are deterministic (Definition 5.1), by Lemma 5.2 they are also ∩-continuous, and the weakest recurrent set of an arbitrary linear affine relation R can be computed as $\mathrm{wrs}(R) = \bigcap_{m \geq 0} \mathrm{pre}_R^m(\mathbb{Z}^{\mathbf{x}})$, by Lemma 3.7. Hence, the weakest recurrent set can be defined using the closed form of R:

$$(\mathrm{wrs}(R))(\mathbf{x}) \Leftrightarrow \forall k \geq 1 \ . \ \exists \mathbf{x}' \ . \ \widehat{R}(k, \mathbf{x}, \mathbf{x}')$$

Considering that the formula defining R is of the form $R_u(\mathbf{x}, \mathbf{x}') \wedge \varphi(\mathbf{x})$ where $R_u(\mathbf{x}, \mathbf{x}')$ is a deterministic update and $\varphi(\mathbf{x})$ is a Presburger guard, we can write the closed form of R as:

$$\widehat{R}(k, \mathbf{x}, \mathbf{x}') \Leftrightarrow \widehat{R_u}(k, \mathbf{x}, \mathbf{x}') \wedge \forall 1 \leq \ell < k \ \exists \mathbf{y} \ . \ \widehat{R_u}(\ell, \mathbf{x}, \mathbf{y}) \wedge \varphi(\mathbf{y})$$

by Lemma 5.4. Then, the definition of the weakest recurrent set of a linear affine relation is (after the elimination of the trailing existential quantifier and renaming ℓ with k and $\mathbf{y}$ with $\mathbf{x}'$):

$$(\mathrm{wrs}(R))(\mathbf{x}) \ \Leftrightarrow \ \forall k \geq 1 \ . \ \exists \mathbf{x}' \ . \ \widehat{R_u}(k, \mathbf{x}, \mathbf{x}') \wedge \varphi(\mathbf{x}') \tag{5.2}$$

5.3. **Finite Monoid Affine Relations.** The class of finite monoid affine relations was the first class of integer relations for which the transitive closure has been shown to be Presburger definable, by Boigelot [5]. Informally, an affine relation is a finite monoid relation if the set of powers of its transformation matrix is finite. Originally, Boigelot characterized this class by two decidable conditions in [5] (we report on these conditions in Theorem 5.5). Later, Finkel and Leroux noticed in [21] that Boigelot's conditions correspond to the finite monoid property, which is also known to be decidable [27].

Given a vector $\mathbf{x} = \langle x_1, \ldots, x_N \rangle$ of variables, an affine transformation

$$R(\mathbf{x}, \mathbf{x}') \ \Leftrightarrow \ \mathbf{x}' = A \times \mathbf{x} + \mathbf{b} \ \wedge \ \varphi(\mathbf{x})$$

where $A \in \mathbb{Z}^{N \times N}$, $\mathbf{b} \in \mathbb{Z}^N$, is said to have the *finite monoid property* [5, 21] if the monoid of powers of A, denoted as $\langle \mathcal{M}_A, \times \rangle$, where $\mathcal{M}_A = \{A^i \mid i \geq 0\}$, is finite. Here $A^0 = I_N$

and $A^i = A \times A^{i-1}$, for $i > 0$. It has been shown in [21] that the finite monoid property can be equivalently characterized by the following two conditions.

Theorem 5.5 ([5, 21])**.** *An affine transformation $R(\mathbf{x}, \mathbf{x}') \Leftrightarrow A \times \mathbf{x} + \mathbf{b} \wedge \varphi(\mathbf{x})$, where $A \in \mathbb{Z}^{N \times N}$ and $\mathbf{b} \in \mathbb{Z}^N$, has the finite monoid property if and only if there exists $p > 0$ such that the following hold:*

(1) *every eigenvalue of A^p belongs to the set $\{0, 1\}$, and*
(2) *the minimal polynomial $\mu_{A^p}(x)$ of A^p belongs to the set $\{0, x, x-1, x(x-1)\}$ (or, equivalently, A^p is diagonalizable).*

Both conditions in the above theorem are decidable [5, 27]. It was shown in [5, 21, 10] that the closed form of (the update part of) a linear affine transformation with the finite monoid property is Presburger definable. This entails the decidability of the universal termination problem for finite monoid affine relations.

Theorem 5.6. *The weakest non-termination precondition of a finite monoid affine relation is Presburger definable and effectively computable. Consequently, the termination problem is decidable for finite monoid affine relations.*

Proof. Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a finite monoid affine relation defined by a formula $R_u(\mathbf{x}, \mathbf{x}') \wedge \varphi(\mathbf{x})$. By Equation (5.2) we have:

$$(\text{wrs}(R))(\mathbf{x}) \Leftrightarrow \forall k \geq 1 \;.\; \exists \mathbf{x}' \;.\; \widehat{R}_u(k, \mathbf{x}, \mathbf{x}') \wedge \varphi(\mathbf{x}')$$

Since both $\widehat{R}_u(k, \mathbf{x}, \mathbf{x}')$ and $\varphi(\mathbf{x}')$ are Presburger formulas, $\text{wrs}(R)(\mathbf{x})$ is a Presburger formula as well. Since Presburger arithmetic is decidable [35], the termination problem can be decided by checking whether $\text{wrs}(R) = \emptyset$. □

5.4. **Polynomially Bounded Affine Relations.** In the following, we study another subclass of affine relations with linear guards and transformation matrices whose eigenvalues are either zero or roots of the unity.

Definition 5.7. If $\mathbf{x} = \langle x_1, \ldots, x_N \rangle$ is a vector of variables ranging over $\mathbb{Z}$, a *polynomially bounded affine relation* is a relation defined by a formula of the form:

$$R(\mathbf{x}, \mathbf{x}') \;\Leftrightarrow\; \mathbf{x}' = A \times \mathbf{x} + \mathbf{b} \;\wedge\; C\mathbf{x} \geq \mathbf{d} \tag{5.3}$$

where $A \in \mathbb{Z}^{N \times N}$, $C \in \mathbb{Z}^{P \times N}$ are matrices, and $\mathbf{b} \in \mathbb{Z}^N$, $\mathbf{d} \in \mathbb{Z}^P$ are column vectors of integer constants, for some $P > 0$, and moreover, all eigenvalues of A are either zero or roots of the unity.

Note that, if A is a finite monoid matrix, then all eigenvalues of A are either zero or roots of the unity. Thus, the condition on A is weaker for polynomially bounded affine relations. However, since the guard of finite monoid relations is more general (Presburger), the two classes are incomparable.

The closed form of polynomially bounded affine relations cannot be defined in Presburger arithmetic[10], thus we renounce defining $\text{wrs}(R)$ precisely, and content ourselves with the discovery of *sufficient conditions for termination.* Basically, given a linear affine relation

[10] The closed form $\widehat{R}(k, \mathbf{x}, \mathbf{x}')$ of a polynomially bounded affine relation is defined by polynomial functions in k, of arbitrary degrees. It is possible to show that a polynomial function of degree greater than one is not Presburger definable [23]) .

R, we aim at finding a disjunction $\phi(\mathbf{x})$ of linear constraints on $\mathbf{x}$, such that $\phi \wedge \mathrm{wrs}(R)$ is inconsistent without explicitly computing $\mathrm{wrs}(R)$. For this, we use several existing results from linear algebra (see, e.g., [20]). In the following, it is convenient to work with the equivalent homogeneous form:

$$R(\mathbf{x},\mathbf{x}') \equiv C_h\mathbf{x}_h \geq \mathbf{0} \;\wedge\; \mathbf{x}'_h = A_h\mathbf{x}_h \;\wedge\; x_{N+1} = 1$$

$$A_h = \begin{pmatrix} A & \mathbf{b} \\ 0 & 1 \end{pmatrix} \; C_h = \begin{pmatrix} C & -\mathbf{d} \end{pmatrix} \; \mathbf{x}_h = \begin{pmatrix} \mathbf{x} \\ x_{N+1} \end{pmatrix} \qquad (5.4)$$

The weakest recurrent set of R can be then defined as:

$$(\mathrm{wrs}(R))(\mathbf{x}) \;\equiv\; \exists x_{N+1} \;.\; \forall k \geq 0 \;.\; C_h A_h^k \mathbf{x}_h \geq \mathbf{0} \;\wedge\; x_{N+1} = 1 \qquad (5.5)$$

Definition 5.8. A function $f : \mathbb{N} \to \mathbb{C}$ is said to be a *C-finite recurrence* if and only if:

$$f(n+d) = a_{d-1}f(n+d-1) + \ldots + a_1 f(n+1) + a_0 f(n),\ \forall n \geq 0$$

for some $d \in \mathbb{N}$ and $a_0, a_1, \ldots, a_{d-1} \in \mathbb{C}$, with $a_{d-1} \neq 0$. The polynomial $x^d - a_{d-1}x^{d-1} - \ldots a_1 x - a_0$ is called the *characteristic polynomial* of f.

A C-finite recurrence always admits a closed form.

Theorem 5.9 ([20])**.** *The closed form of a C-finite recurrence is:*

$$f(n) = p_1(n)\lambda_1^n + \ldots + p_s(n)\lambda_s^n$$

where $\lambda_1, \ldots, \lambda_s \in \mathbb{C}$ are non-zero distinct roots of the characteristic polynomial of f, and $p_1, \ldots, p_s \in \mathbb{C}[n]$ are polynomials of degree less than the multiplicities of $\lambda_1, \ldots, \lambda_s$, respectively.

Next, we define the closed form for the sequence of powers of A.

Corollary 5.10. *Given a square matrix $A \in \mathbb{Z}^{N \times N}$, we have, for all $n > 0$:*

$$(A^n)_{i,j} = p_{1,i,j}(n)\lambda_1^n + \ldots + p_{s,i,j}(n)\lambda_s^n$$

where $\lambda_1, \ldots, \lambda_s \in \mathbb{C}$ are non-zero distinct eigenvalues of A, and $p_{1,i,j}, \ldots, p_{s,i,j} \in \mathbb{C}[n]$ are polynomials of degree less than the multiplicities of $\lambda_1, \ldots, \lambda_s$, respectively.

Proof. If $\det(A - xI_n) = x^d - a_{d-1}x^{d-1} - \ldots - a_1 x - a_0$ is the characteristic polynomial of A, then we have

$$A^d - a_{d-1}A^{d-1} - \ldots - a_1 A - a_0 = 0$$

by the Cayley-Hamilton Theorem. If we define $f_{i,j}(n) = (A^n)_{i,j}$, for all $n > 0$, by multiplying the above equality with A^n, we obtain:

$$\begin{array}{rcl} A^{n+d} & = & a_{d-1}A^{n+d-1} + \ldots + a_1 A^{n+1} + a_0 A^n \\ f_{i,j}(n+d) & = & a_{d-1}f_{i,j}(n+d-1) + \ldots + a_1 f_{i,j}(n+1) + a_0 f_{i,j}(n) \end{array}$$

By Theorem 5.9, we have that

$$(A^n)_{i,j} = p_{1,i,j}(n)\lambda_1^n + \ldots + p_{s,i,j}(n)\lambda_s^n$$

for some polynomials $p_{1,i,j}, \ldots, p_{s,i,j} \in \mathbb{C}[n]$ of degrees less than the multiplicities of $\lambda_1, \ldots, \lambda_s$, respectively. □

Lemma 5.11. *Given a square matrix $A \in \mathbb{Z}^{N \times N}$, whose non-zero eigenvalues are all roots of the unity. Then $(A^n)_{i,j} \in \mathbb{Q}[n]$, for all $1 \leq i,j \leq N$, are effectively computable polynomials with rational coefficients.*

Proof. Assume from now on that all non-zero eigenvalues $\lambda_1, \ldots, \lambda_s$ of A are such that $\lambda_1^{d_1} = \ldots = \lambda_s^{d_s} = 1$, for some integers $d_1, \ldots, d_s > 0$. The method given in [5] for testing the finite monoid condition for A gives also bounds for $d_1, \ldots, d_s$. Then we have $\lambda_1^L = \ldots \lambda_s^L = 1$, where $L = \mathrm{lcm}(d_1, \ldots, d_s)$. As $d_1, \ldots, d_s$ are effectively bounded, so is L. By Corollary 5.10, we have that, if n is a multiple of L, then $(A^n)_{i,j} = p_{i,j}(n)$ for some effectively computable polynomial $p_{i,j} \in \mathbb{C}[n]$, of degree $d_{ij} > 0$, i.e. for n multiple of L, A^n is polynomially definable. But since $p_{i,j}(n)$ assumes real values in an infinity of points $n = kL,\ k > 0$, it must be that its coefficients are all real numbers, i.e. $p_{i,j} \in \mathbb{R}[n]$. Moreover, these coefficients are the solutions of the integer system:

$$\left\{ \begin{array}{ccc} p_{i,j}(L) & = & (A^L)_{i,j} \\ & \ldots & \\ p_{i,j}((d_{ij}+1)L) & = & (A^{(d_{ij}+1)L})_{i,j} \end{array} \right.$$

Clearly, since $A \in \mathbb{Z}^{N \times N}$, $A^p \in \mathbb{Z}^{N \times N}$, for any $p > 0$. Hence $p_{i,j} \in \mathbb{Q}[n]$. □

We turn now back to the problem of defining wrs(R) for linear affine relations R of the form (5.5). First notice that, if all non-zero eigenvalues of A are roots of the unity, then the same holds for A_h (5.4). By Lemma 5.11, one can find rational polynomials $p_{i,j}(k)$ defining $(A_h^k)_{i,j}$, for all $1 \leq i,j \leq N$. The condition (5.5) becomes a conjunction of the form:

$$(\mathrm{wrs}(R))(\mathbf{x}) \equiv \bigwedge_{i=1}^{n} \forall k \geq 1 \ .\ P_i(k, \mathbf{x}) \geq 0 \tag{5.6}$$

where each $P_i = a_{i,d}(\mathbf{x}) \cdot k^d + \ldots + a_{i,1}(\mathbf{x}) \cdot k + a_{i,0}(\mathbf{x})$ is a polynomial in k whose coefficients are the linear combinations $a_{i,d} \in \mathbb{Q}[\mathbf{x}]$. We are looking for a sufficient condition for termination, which is, in this case, any set of valuations of $\mathbf{x}$ that would invalidate (5.6). The following proposition gives sufficient invalidating clauses for each conjunct above. By taking the disjunction of all these clauses we obtain a sufficient termination condition for R.

Lemma 5.12. *Given a polynomial $P(k, \mathbf{x}) = a_d(\mathbf{x}) \cdot k^d + \ldots + a_1(\mathbf{x}) \cdot k + a_0(\mathbf{x})$, for each valuation $\nu \in \mathbb{Z}^{\mathbf{x}}$ there exists an integer $n > 0$ such that $P(n, \nu(\mathbf{x})) < 0$ if, for some $i = 0, 1, \ldots, d$, we have $a_{d-i}(\nu(\mathbf{x})) < 0$ and $a_d(\nu(\mathbf{x})) = a_{d-1}(\nu(\mathbf{x})) = \ldots = a_{d-i+1}(\nu(\mathbf{x})) = 0$.*

Proof. Assuming that:

$$a_{d-i}(\nu(\mathbf{x})) < 0 \text{ and } a_d(\nu(\mathbf{x})) = a_{d-1}(\nu(\mathbf{x})) = \ldots = a_{d-i+1}(\nu(\mathbf{x})) = 0$$

for some $0 \leq i \leq d$, we have $P(k, \nu(\mathbf{x})) = a_{d-i}(\nu(\mathbf{x})) \cdot k^d + \ldots + a_1(\nu(\mathbf{x})) \cdot k + a_0(\nu(\mathbf{x}))$. Since the dominant coefficient $a_{d-i}(\nu(\mathbf{x}))$ is negative, the polynomial will assume only negative values, from some point on. □

Example 5.13. Consider the following program [16], and its linear transformation matrix A.

```
while ($x \geq 0$)
    $x' = x + y$
    $y' = y + z$
```

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \qquad A^k = \begin{pmatrix} 1 & k & \frac{k(k-1)}{2} \\ 0 & 1 & k \\ 0 & 0 & 1 \end{pmatrix}$$

The characteristic polynomial of A is $\det(A-\lambda I_3) = (1-\lambda)^3$, hence the only eigenvalue is 1, with multiplicity 3. Then we compute A^k (see above), and $x' = x + k \cdot y + \frac{k(k-1)}{2} z$ gives the value of x after k iterations of the loop. Since only x occurs within the guard of the loop, the weakest non-termination precondition is: $\forall k \geq 1 \,.\, \frac{z}{2} \cdot k^2 + (y - \frac{z}{2}) \cdot k + x \geq 0$. Lemma 5.12 gives a sufficient condition for termination: $(z < 0) \vee (z = 0 \wedge y < 0) \vee (z = 0 \wedge y = 0 \wedge x < 0)$.

We can generalize this method further to the case where all eigenvalues of A are of the form $q \cdot r$, with $q \in \mathbb{R}$ and $r \in \mathbb{C}$ being a root of the unity[11]. The main reason for not using this condition from the beginning is that we are, to this point, unaware of its decidability status. With this condition instead, it is sufficient to consider only the eigenvalues with the maximal absolute value, and the polynomials obtained as sums of the polynomial coefficients of these eigenvalues. The result of Lemma 5.11 and the sufficient condition of Lemma 5.12 carry over when using these polynomials instead.

6. Termination Analysis of Integer Programs

In this section, we extend the computation of weakest non-termination preconditions from simple conjunctive loops to programs with possibly nested loops. The method described here applies the *transition invariants* technique, initially developed for proving program termination [34], to the computation of termination preconditions.

The method can be summarized as follows. Suppose that R is the (possibly disjunctive) transition relation of a program. Our method first computes (1) a *reachability relation*, defined as an over-approximation of a restriction of the transitive closure of the transition relation R^+ to a set Init of initial program configurations, formally $\mathit{Reach} \supseteq \{(\nu, \nu') \mid (\nu, \nu') \in R^+, \nu \in \mathit{Init}\}$, and (2) a *transition invariant*, defined as an over-approximation of the transitive closure of R restricted to states reachable from the set of initial configurations, formally $\mathit{TInv} \supseteq \{(\nu, \nu') \mid (\nu, \nu') \in R^+, \nu \in R^*(\mathit{Init})\}$. Then, TInv is over-approximated with a union $R_1 \cup \cdots \cup R_m$, $m \geq 1$, of octagonal relations. Next, the weakest non-termination precondition $\mathrm{wnt}(R_i)$, $1 \leq i \leq m$, can be computed using techniques from Sections 4 and 5. The weakest non-termination precondition of the program is then over-approximated by the pre-image of $\mathrm{wnt}(R_1) \cup \ldots \cup \mathrm{wnt}(R_m)$ via the reachability relation, formally $\mathit{Reach}^{-1}(\mathrm{wnt}(R_1) \cup \ldots \cup \mathrm{wnt}(R_m))$, or equivalently, $\bigcup_{i=1}^{m} \mathit{Reach}^{-1}(\mathrm{wnt}(R_i))$. The complement of this set is then a valid termination precondition.

The technique presented in this section can be further applied to programs with (recursive) procedure calls, by using the program transformation described in [18], which turns a program P with recursive procedure calls into a program P' without procedures such that $\mathrm{wrs}(P) \subseteq \mathrm{wrs}(P')$. The main ingredient of this technique is the *summarization* of procedures, i.e. computing (an over-approximation of) the relation between the values of the input parameters and the values returned by the procedure.

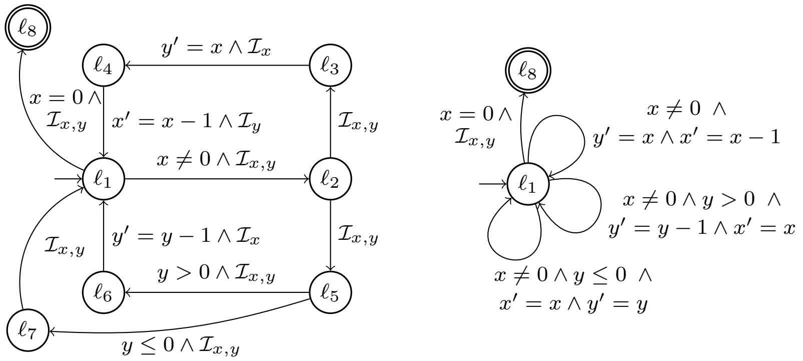
6.1. **Example.** Consider the non-deterministic integer program in Figure 5(a). If $x = 0$ initially, the program does not enter the main loop, and terminates trivially. Otherwise, the program may enter an infinite computation. If $y \leq 0$ initially, the program can iterate the third branch of the main loop infinitely many times. Otherwise, if $y > 0$ initially, the

[11] A complex number $r = \cos(\theta) + i \sin(\theta)$, of absolute value $|r| = 1$, is a root of the unity if and only if $\theta = \frac{a\pi}{b}$, for some $a, b \in \mathbb{N}$, $b \neq 0$.

program can iterate the second branch y times and then iterate the third branch infinitely many times.

```
    int x,y;
1.  while (x != 0) {
2.      if (*) {
3.          y = x;
4.          x = x-1;
5.      } else if (y>0) {
6.          y = y-1;
        } else {
7.          skip;
        }
8.  }
```

(a)



ℓ_8
ℓ_4
$y' = x \wedge \mathcal{I}_x$
ℓ_3
$x = 0 \wedge$
$\mathcal{I}_{x,y}$
$x' = x - 1 \wedge \mathcal{I}_y$
$\mathcal{I}_{x,y}$
$x \neq 0 \wedge \mathcal{I}_{x,y}$
ℓ_1
ℓ_2
$\mathcal{I}_{x,y}$
$y' = y - 1 \wedge \mathcal{I}_x$
$\mathcal{I}_{x,y}$
$y > 0 \wedge \mathcal{I}_{x,y}$
ℓ_6
ℓ_5
ℓ_7
$y \leq 0 \wedge \mathcal{I}_{x,y}$
ℓ_8
$x = 0 \wedge$
$\mathcal{I}_{x,y}$
$x \neq 0 \wedge$
$y' = x \wedge x' = x - 1$
ℓ_1
$x \neq 0 \wedge y > 0 \wedge$
$y' = y - 1 \wedge x' = x$
$x \neq 0 \wedge y \leq 0 \wedge$
$x' = x \wedge y' = y$

(b) (c)

FIGURE 5. An integer program and its control flow graph

We view programs as control flow graphs labeled with arithmetic formulas. Figure 5(b) depicts the control flow graph of the program in Figure 5(a). We write $\mathcal{I}_{x_1,\ldots,x_m}$ as a shorthand for $\bigwedge_{i=1}^{m} x_i' = x_i$. The mechanics of our algorithm computing the weakest non-termination precondition applied on the above example are described in the following. First, we reduce the three loops $\ell_1 \to \ell_2 \to \ell_3 \to \ell_4 \to \ell_1$, $\ell_1 \to \ell_2 \to \ell_5 \to \ell_6 \to \ell_1$ and $\ell_1 \to \ell_2 \to \ell_5 \to \ell_7 \to \ell_1$ in Figure 5(b) into self-loops, obtaining a reduced control flow graph in Figure 5(c). Then, we compute the transitive summary relation induced by all non-trivial runs of the program starting and ending at ℓ_1 (this notion is formally defined in the next section). This relation is given in disjunctive normal form:

$$\begin{array}{lcl}
[\![P]\!]^+(\ell_1,\ell_1) & \Leftrightarrow & R_1 \vee R_2 \vee R_3 \vee R_4 \vee R_5 \vee R_6 \vee R_7 \\
 & & \\
R_1 & \Leftrightarrow & x \leq -1 \wedge y' \leq x \wedge y' = x' + 1 \\
R_2 & \Leftrightarrow & y' \geq 1 \wedge y' \leq x \wedge y' = x' + 1 \\
R_3 & \Leftrightarrow & y' \geq 0 \wedge y' \leq y - 1 \wedge x' = x \wedge x' \leq -1 \\
R_4 & \Leftrightarrow & x' \geq 1 \wedge x' = x \wedge y' \geq 0 \wedge y' \leq y - 1 \\
R_5 & \Leftrightarrow & x' = x \wedge x' \leq -1 \wedge y' = y \wedge y' \leq 0 \\
R_6 & \Leftrightarrow & x' \geq 1 \wedge x' = x \wedge y' = y \wedge y' \leq 0 \\
R_7 & \Leftrightarrow & x' \geq 1 \wedge y' \geq 0 \wedge x' \leq x - 1 \wedge y' \leq x'
\end{array}$$

Notice that, since ℓ_1 is the initial control state of the program, the set of valuations reached at ℓ_1 is the universal set $\mathbb{Z}^{\mathbf{x}}$. A *transition invariant* of the program is the restriction of the summary relation to the reachable states, which, in this case, is $[\![P]\!]^{TInv}(\ell_1,\ell_1) = [\![P]\!]^+(\ell_1,\ell_1)$. Next, we compute the weakest non-termination precondition of each disjunct of the transition invariant, obtaining the formulas $\mathrm{wnt}(R_1), \ldots, \mathrm{wnt}(R_7)$ below:

$$\begin{array}{lcl}
\mathrm{wnt}(R_1) & \Leftrightarrow & x \leq -1 \\
\mathrm{wnt}(R_2) & \Leftrightarrow & \mathbf{false} \\
\mathrm{wnt}(R_3) & \Leftrightarrow & \mathbf{false} \\
\mathrm{wnt}(R_4) & \Leftrightarrow & \mathbf{false} \\
\mathrm{wnt}(R_5) & \Leftrightarrow & x \leq -1 \wedge y \leq 0 \\
\mathrm{wnt}(R_6) & \Leftrightarrow & x \geq 1 \wedge y \leq 0 \\
\mathrm{wnt}(R_7) & \Leftrightarrow & \mathbf{false}
\end{array}$$

The disjunction of these non-termination precondition defines a set of configurations of the program, from which infinite runs, starting at ℓ_1, are guaranteed to exist:

$$\mathrm{wnt}(R_1) \vee \cdots \vee \mathrm{wnt}(R_7) \Leftrightarrow (x \leq -1) \vee (x \geq 1 \wedge y \leq 0)$$

Finally, we compute the pre-image of this set via the (reflexive and transitive) reachability relation defined as $[\![P]\!]^*(\ell_1, \ell_1) = [\![P]\!]^+(\ell_1, \ell_1) \vee \mathcal{I}_{\mathbf{x}}$, obtaining thus the weakest non-termination precondition of the program:

$$\begin{array}{rcl} ([\![P]\!]^*(\ell_1, \ell_1))^{-1}(\mathrm{wnt}(R_1) \vee \cdots \vee \mathrm{wnt}(R_7)) & \Leftrightarrow & \\ (x \geq 1 \wedge y \leq 0) \vee (x \geq 1 \wedge y \geq 1) \vee (x \geq 2) \vee (x \leq -1) & \Leftrightarrow & x \neq 0 \end{array}$$

This result matches the intuition. Indeed, the program will terminate if and only if $x = 0$, in which case the `while` loop is never entered. For $x \neq 0$, the program enters the `while` loop and may get stuck into an infinite loop, for every initial value of y.

6.2. **Syntax and Semantics.** In the following, we abstract from specific programming language constructs and assume that programs are represented by control flow graphs whose edges are labeled by quantifier-free Presburger arithmetic formulas defining relations. Formally, an *integer program* is a tuple $P = \langle \mathbf{x}, Q, q_{init}, \Delta \rangle$, where:

- $\mathbf{x}$ is the set of variables of P
- Q are the *control states* of P
- Δ is a set of *transition rules* $q \xrightarrow{R(\mathbf{x},\mathbf{x}')} q'$, where $q, q' \in Q$ are the source and destination states, and $R(\mathbf{x}, \mathbf{x}')$ is a quantifier-free Presburger formula
- q_{init} is the *initial* control state of P

Example 6.1. The program whose control flow graph is shown in Figure 5(b) can be formalized as $P = \langle \mathbf{x}, Q, \ell_1, \Delta \rangle$, where $\mathbf{x} = \{x, y\}$, $Q = \{\ell_1, \ldots, \ell_8\}$, $\Delta = \{t_1, \ldots, t_{10}\}$, and

$$\begin{array}{rclrclrcl} t_1 & = & \ell_1 \xrightarrow{x \neq 0 \ \wedge \ \mathcal{I}_{x,y}} \ell_2 & t_5 & = & \ell_2 \xrightarrow{\mathcal{I}_{x,y}} \ell_5 & t_8 & = & \ell_5 \xrightarrow{y \leq 0 \ \wedge \ \mathcal{I}_{x,y}} \ell_7 \\ t_2 & = & \ell_2 \xrightarrow{\mathcal{I}_{x,y}} \ell_3 & t_6 & = & \ell_5 \xrightarrow{y > 0 \ \wedge \ \mathcal{I}_{x,y}} \ell_6 & t_9 & = & \ell_7 \xrightarrow{\mathcal{I}_{x,y}} \ell_1 \\ t_3 & = & \ell_3 \xrightarrow{y' = x \ \wedge \ \mathcal{I}_x} \ell_4 & t_7 & = & \ell_6 \xrightarrow{y' = y - 1 \ \wedge \ \mathcal{I}_x} \ell_1 & t_{10} & = & \ell_1 \xrightarrow{x = 0 \ \wedge \ \mathcal{I}_{x,y}} \ell_8 \\ t_4 & = & \ell_4 \xrightarrow{x' = x - 1 \ \wedge \ \mathcal{I}_y} \ell_1 & & & & & & \end{array}$$

□

A *configuration* of a program $P = \langle \mathbf{x}, Q, q_{init}, \Delta \rangle$ is a pair $\langle q, \nu \rangle$, where $q \in Q$ is a control state and $\nu \in \mathbb{Z}^{\mathbf{x}}$ is a valuation of the variables. Given two configurations $\langle q, \nu \rangle$ and $\langle q', \nu' \rangle$ of a program P, the configuration $\langle q', \nu' \rangle$ is said to be an *immediate successor* of $\langle q, \nu \rangle$ if and only if $q \xrightarrow{R(\mathbf{x},\mathbf{x}')} q' \in \Delta$ and $(\nu, \nu') \models R$. For any $k \geq 0$, a *run* of length k of the program P from q to q' is a finite sequence $\langle q_0, \nu_0 \rangle \to \langle q_1, \nu_1 \rangle \to \ldots \to \langle q_k, \nu_k \rangle$, such that $q = q_0$, $q' = q_k$, and $\langle q_{i+1}, \nu_{i+1} \rangle$ is an immediate successor of $\langle q_i, \nu_i \rangle$, for all $0 \leq i < k$. Given two configurations $\langle q, \nu \rangle$ and $\langle q', \nu' \rangle$ of a program P, the configuration $\langle q', \nu' \rangle$ is said to be a *successor* of $\langle q, \nu \rangle$ if there exists a run of length $k \geq 0$ from $\langle q, \nu \rangle$ to $\langle q', \nu' \rangle$. An *infinite run* of a program P from a control state q is an infinite sequence $\langle q_0, \nu_0 \rangle \to \langle q_1, \nu_1 \rangle \to \ldots$ such that $q = q_0$ and $\langle q_{i+1}, \nu_{i+1} \rangle$ is an immediate successor of $\langle q_i, \nu_i \rangle$ for all $i \geq 0$. The transitive closure of the transition relation $[\![P]\!]^+ : (Q \times Q) \to 2^{\mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}}$, the reflexive and transitive closures of the transition relation $[\![P]\!]^* : (Q \times Q) \to 2^{\mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}}$, and the weakest non-termination precondition $[\![P]\!]^{wnt} : Q \to 2^{\mathbb{Z}^{\mathbf{x}}}$ of the program P are defined for each $q, q' \in Q$

as follows:

$$\begin{array}{lcl}
[\![P]\!]^{+}(q,q') & \stackrel{def}{=} & \{\langle \nu,\nu' \rangle \mid \langle q,\nu\rangle \rightarrow \ldots \rightarrow \langle q',\nu'\rangle \text{ is a run of } P \text{ of length } k \geq 1\} \\
[\![P]\!]^{*}(q,q') & \stackrel{def}{=} & \{\langle \nu,\nu' \rangle \mid \langle q,\nu\rangle \rightarrow \ldots \rightarrow \langle q',\nu'\rangle \text{ is a run of } P \text{ of length } k \geq 0\} \\
[\![P]\!]^{wnt}(q) & \stackrel{def}{=} & \{\nu \mid \langle q,\nu\rangle \rightarrow \ldots \text{ is an infinite run of } P\}
\end{array}$$

Note that the set of configurations with control state q that are reachable from q_{init}, can be defined as the post-image of $\mathbb{Z}^{\mathbf{x}}$ via $[\![P]\!]^{*}(q_{init},q)$, i.e. $[\![P]\!]^{*}(q_{init},q)(\mathbb{Z}^{\mathbf{x}})$. With this notation, the *strongest transition invariant* $[\![P]\!]^{TInv} : (Q \times Q) \rightarrow 2^{\mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}}$ of a program P is defined for each $q, q' \in Q$ as the restriction of the transitive closure of the transition relation to the set of reachable configurations:

$$[\![P]\!]^{TInv}(q,q') \stackrel{def}{=} \{\langle \nu,\nu'\rangle \in [\![P]\!]^{+}(q,q') \mid \nu \in \big([\![P]\!]^{*}(q_{init},q)\big)(\mathbb{Z}^{\mathbf{x}})\}$$

When $[\![P]\!]^{+}$, $[\![P]\!]^{*}$, $[\![P]\!]^{TInv}$, or $[\![P]\!]^{wnt}$ is not computable, one may content oneself with computing the following over-approximations:

$$\begin{array}{lcllcl}
[\![P]\!]^{+}_{\sharp} & : & (Q \times Q) \rightarrow 2^{\mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}}, & [\![P]\!]^{TInv}_{\sharp} & : & (Q \times Q) \rightarrow 2^{\mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}}, \\
[\![P]\!]^{*}_{\sharp} & : & (Q \times Q) \rightarrow 2^{\mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}}, & [\![P]\!]^{wnt}_{\sharp} & : & Q \rightarrow 2^{\mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}},
\end{array}$$

These are arbitrary mappings such that:

$$\begin{array}{lcllcl}
[\![P]\!]^{+}_{\sharp}(q,q') & \supseteq & [\![P]\!]^{+}(q,q'), & [\![P]\!]^{TInv}_{\sharp}(q,q') & \supseteq & [\![P]\!]^{TInv}(q,q'), \\
[\![P]\!]^{*}_{\sharp}(q,q') & \supseteq & [\![P]\!]^{*}(q,q'), & [\![P]\!]^{wnt}_{\sharp}(q) & \supseteq & [\![P]\!]^{wnt}(q),
\end{array}$$

for all $q, q' \in Q$. Any set $[\![P]\!]^{TInv}_{\sharp}$ that satisfies the above inclusion is called a *transition invariant.*

6.3. **Computing Termination Preconditions for Integer Programs.** The following theorem is used to compute a termination precondition of an integer program, using a set of precomputed transition invariants. In fact we compute an over-approximation of the weakest non-termination precondition. The complement of this set is a termination precondition, i.e. a set of initial configurations from which the program is guaranteed to terminate.

Theorem 6.2. *Let $P = \langle \mathbf{x}, Q, q_{init}, \Delta\rangle$ be a program, $[\![P]\!]^{*}_{\sharp} \supseteq [\![P]\!]^{*}$ be an over-approximation of the reflexive and transitive closure of the transition relation, $[\![P]\!]^{TInv}_{\sharp} \supseteq [\![P]\!]^{TInv}$ be a transition invariant and, for each $q \in Q$, let $R_{q,1}, \ldots, R_{q,p_q} \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be relations, such that $[\![P]\!]^{TInv}_{\sharp}(q,q) = \bigcup_{k=1}^{p_q} R_{q,k}$, for some $p_q \geq 1$. Let*

$$\mathcal{N} \stackrel{def}{=} \bigcup_{q \in Q} \left(\big([\![P]\!]^{*}_{\sharp}(q_{init},q)\big)^{-1} \left(\bigcup_{k=1}^{p_q} \mathrm{wnt}(R_{q,k}) \right) \right)$$

Then, $[\![P]\!]^{wnt}(q_{init}) \subseteq \mathcal{N}$. Moreover, if $[\![P]\!]^{TInv}_{\sharp} = [\![P]\!]^{TInv}$ and $[\![P]\!]^{*}_{\sharp} = [\![P]\!]^{*}$, then $\mathcal{N} = [\![P]\!]^{wnt}(q_{init})$.

Proof. We first prove that $[\![P]\!]^{wnt}(q_{init}) \subseteq \mathcal{N}$. Let $\nu_0 \in [\![P]\!]^{wnt}(q_{init})$ be a valuation, and let $\rho_1 = \langle q_{init}, \nu_0\rangle\langle q_1,\nu_1\rangle\langle q_2,\nu_2\rangle \ldots$ be an infinite run of P starting with ν_0. Since the set of control states Q is finite, there exists $q \in Q$, and infinitely many integers $1 \leq \ell_1 < \ell_2 < \ell_3 < \ldots$ such that $q = q_{\ell_1} = q_{\ell_2} = q_{\ell_3} = \ldots$ It follows from the definition of $[\![P]\!]^{TInv}_{\sharp}$

that $\langle \nu_{\ell_j}, \nu_{\ell_{j+1}} \rangle \in [\![P]\!]_\sharp^{TInv}(q,q)$ for all $j \geq 1$. Let μ_i denote ν_{ℓ_i}, for all $i \geq 1$. Then $\rho_2 = \langle q_{init}, \nu_0 \rangle \langle q, \mu_1 \rangle \langle q, \mu_2 \rangle \ldots$ is an infinite subsequence of ρ_1.

Since $[\![P]\!]_\sharp^{TInv}(q,q) = \bigcup_{k=1}^{p_q} R_{q,k}$, it follows from the definition of $[\![P]\!]_\sharp^{TInv}$ that for each $1 \leq k < \ell$, there exists $1 \leq j \leq p_q$ such that $\langle \mu_k, \mu_\ell \rangle \in R_{q,j}$. Consequently, there exists a function $f : \{(k,\ell) \mid 1 \leq k < \ell\} \to \{R_{q,1}, \ldots, R_{q,p_q}\}$ such that $\langle \mu_k, \mu_\ell \rangle \in f(k,\ell)$ for all $1 \leq k < \ell$. Let $\sim_f$ be the kernel of f, i.e. the equivalence relation defined as $\langle k, \ell \rangle \sim_f \langle k', \ell' \rangle$ if and only if $f(k,\ell) = f(k',\ell')$. Clearly, $\sim_f$ has finite index, since the range of f is finite. Consequently, by the Ramsey theorem [36], there exists an infinite sequence of integers $1 \leq k_1 < k_2 < k_3 < \ldots$ and an equivalence class $[(m,n)]_{\sim_f}$ for some $1 \leq m < n$ such that $\langle k_i, k_{i+1} \rangle \sim_f \langle m, n \rangle$ for all $i \geq 1$. Thus, there exists $1 \leq j \leq p_q$ such that $f(k_i, k_{i+1}) = R_{q,j}$ for all $i \geq 1$. Consequently, $\mu_{k_1} \mu_{k_2} \ldots$ is an infinite run of $R_{q,j}$ and hence, $\mu_{k_1} \in \mathrm{wnt}(R_{q,j})$. Since $\langle \nu_0, \mu_{k_1} \rangle \in [\![P]\!]_\sharp^*(q_{init}, q)$, by the definition of $[\![P]\!]_\sharp^*$, it follows that

$$\nu_0 \in \left([\![P]\!]_\sharp^*(q_{init}, q)\right)^{-1} \left(\mathrm{wnt}(R_{q,j})\right) \subseteq \left([\![P]\!]_\sharp^*(q_{init}, q)\right)^{-1} \left(\bigcup_{k=1}^{p} \mathrm{wnt}(R_{q,k})\right) \subseteq \mathcal{N}$$

hence $\nu_0 \in \mathcal{N}$, i.e. $[\![P]\!]^{wnt}(q_{init}) \subseteq \mathcal{N}$.

Next, we prove that $[\![P]\!]^{wnt}(q_{init}) \supseteq \mathcal{N}$ under the assumption that $[\![P]\!]_\sharp^{TInv} = [\![P]\!]^{TInv}$ and $[\![P]\!]_\sharp^* = [\![P]\!]^*$. Together with the previous point, this is sufficient to prove that $[\![P]\!]^{wnt}(q_{init}) = \mathcal{N}$. Let $\nu \in \mathcal{N}$. By the definition of $\mathcal{N}$ and since $[\![P]\!]_\sharp^* = [\![P]\!]^*$, there exists $q \in Q$, $\nu_0 \in \mathbb{Z}^{\mathbf{x}}$, and $k \in \{1, \ldots, p_q\}$ such that (i) there exists a run ρ from the configuration $\langle q_{init}, \nu \rangle$ to the configuration $\langle q, \nu_0 \rangle$, and (ii) $\nu_0 \in \mathrm{wnt}(R_{q,j})$ for some $j \in \{1, \ldots, p_q\}$. Since $\nu_0 \in \mathrm{wnt}(R_{q,j})$, there exist infinitely many valuations $\nu_1, \nu_2, \ldots$ such that $\langle \nu_i, \nu_{i+1} \rangle \in R_{q,j}$ for all $i \geq 0$. Since $[\![P]\!]^{TInv}(q,q) = [\![P]\!]_\sharp^{TInv}(q,q) = \bigcup_{k=1}^{p_q} R_{q,k}$, we have that $R_{q,j} \subseteq [\![P]\!]^{TInv}(q,q) \subseteq [\![P]\!]^+(q,q)$, by the definition of the strongest transition invariant $[\![P]\!]^{TInv}(q,q)$. But then, for each $i \geq 0$ there exists a run ρ_i of strictly positive length from $\langle q, \nu_i \rangle$ to $\langle q, \nu_{i+1} \rangle$. Consequently, $\rho.\rho_1.\rho_2 \ldots$ is an infinite run of P and hence, $\nu \in [\![P]\!]^{wnt}(q_{init})$. □

Algorithm 4 computes a sound over-approximation of the weakest non-termination precondition of an integer program. It uses a function $\mathrm{WNT}(R)$ to compute the weakest non-termination precondition of an octagonal, finite monoid or polynomially bounded affine relation. Based on our previous results, $\mathrm{WNT}(R)$ is precisely the weakest non-termination precondition, if R is octagonal (Algorithm 3) or finite monoid affine (Theorems 4.38 and 5.6, respectively), and $\mathrm{WNT}(R)$ is an over-approximation of the above, if R is a polynomially bounded affine relation (Equation (5.6) and Lemma 5.12). Let $P = \langle \mathbf{x}, Q, q_{init}, \Delta \rangle$ be an integer program, for which we would like to compute a non-termination precondition $[\![P]\!]_\sharp^{wnt}(q_{init})$. Since the set of control states of P is finite, any infinite computation of P will eventually iterate through the same state $q \in Q$ infinitely often. Hence we must compute non-termination preconditions for all states $q \in Q$, i.e. sets of configurations from which a computation iterating q infinitely often is possible. For reasons of precision, here we distinguish two cases:

- If q occurs within only one elementary cycle, then every infinite run involving q infinitely often must iterate this cycle. If, moreover, the composition of the relations on the cycle defines an:

  - octagonal relation or a finite monoid affine relation R, then we can compute $\mathrm{wnt}(R)$ precisely (see Theorems 4.38 and 5.6, respectively).
  - polynomially bounded affine relation R, then we can compute an over-approximation of $\mathrm{wnt}(R)$ (see Equation (5.6) and Lemma 5.12).

  Notice that equivalence of a formula with an octagonal constraint can be decided using integer linear programming [37], whereas the finite monoid and polynomial boundedness of an affine relation can be decided using Theorem 5.5 and the decidability of its preconditions [5, 27].
- Otherwise, we compute a transition invariant $[\![P]\!]_\sharp^{TInv}(q,q)$ and over-approximate it with a set of octagonal relations $R'_1,\ldots,R'_p$, for some $p \geq 1$. Since we can compute $\mathrm{wnt}(R'_i)$ for each such octagonal relation, we can apply Theorem 6.2 to obtain $[\![P]\!]^{wnt}(q_{init})$.

Alternatively, one can see the first case above (lines 4-8 of Algorithm 4) as a special case of Theorem 6.2, in which the transition invariant $[\![P]\!]^{TInv}(q,q)$ can be safely replaced by the weakest non-termination precondition $\mathrm{wnt}(R)$, since R is the only cycle that can be iterated infinitely often. Since we consider the pre-image of this set via the reflexive and transitive closure of the reachability relation $[\![P]\!]_\sharp^*(q_{init},q)$, we are guaranteed to iterate this loop only through reachable configurations.

Any procedure for computing transition invariants can be used for the purposes of this algorithm. For reasons of self-containment, Section 6.4 describes an algorithm for computing reflexive and transitive closures of the transition relations $[\![P]\!]_\sharp^*(q_{init},q)$, and transition invariants $[\![P]\!]_\sharp^{TInv}(q)$, for every $q \in Q$. A version of this algorithm was implemented in the Flata tool [22], and is guaranteed to return the exact reflexive and transitive closures of the transition relations $[\![P]\!]^*(q_{init},q)$, and the strongest transition invariants of the program $[\![P]\!]^{TInv}(q)$, for a specific class of programs, called *flat* (see Section 6.5). A formal proof of correctness of Algorithm 4 is given in Section 6.5.

Algorithm 4 Computing a Non-termination Precondition for a Program

```
  input A program $P = \langle \mathbf{x}, Q, q_{init}, \Delta \rangle$
  output A non-termination precondition $[\![P]\!]_\sharp^{wnt}(q_{init})$
1: function NT_PROGRAM(P)
2:     $\mathcal{N} \leftarrow \emptyset$
3:     for each $q \in Q$ do
4:         if $q \xrightarrow{R_1} \ldots \xrightarrow{R_n} q$ is the only elementary cycle involving $q$ in $P$ then
5:             $R \leftarrow \exists \mathbf{x}_1 \ldots \exists \mathbf{x}_{n-1} \,.\, R_1(\mathbf{x},\mathbf{x}_1) \wedge \ldots R_n(\mathbf{x}_{n-1},\mathbf{x}')$
6:             if $R$ defines an octagonal, fin. monoid or poly. bounded affine relation then
7:                 $\mathcal{N} \leftarrow \mathcal{N} \cup \left([\![P]\!]_\sharp^*(q_{init},q)\right)^{-1}\left(\mathrm{WNT}(R)\right)$
8:                 continue
9:         find octagonal relations $R'_1,\ldots,R'_p$ s.t. $[\![P]\!]^{TInv}(q,q) \subseteq \left(R'_1 \cup \cdots \cup R'_p\right)$
10:        $\mathcal{N} \leftarrow \mathcal{N} \cup \left([\![P]\!]_\sharp^*(q_{init},q)\right)^{-1}\left(\bigcup_{j=1}^{p} \mathrm{WNT}(R'_j)\right)$
11:    return $\mathcal{N}$
```

Algorithm 5 Procedure Summary Algorithm

```
    input A program $P = \langle \mathbf{x}, Q, q_{init}, \Delta \rangle$, and distinct control states $q_{in}, q_{out} \in Q$
    output An over-approximated transitive closure $[\![P]\!]_{\sharp}^{+}(q_{in}, q_{out})$
 1: function TransitiveRelation($P, q_{in}, q_{out}$)
 2:     $\overline{P} = \langle \mathbf{x}, Q \cup \{\bar{q}_{in}, \bar{q}_{out}\}, \bar{q}_{in}, \Delta \cup \{\bar{q}_{in} \xrightarrow{\mathcal{I}_{\mathbf{x}}} q_{in}, q_{out} \xrightarrow{\mathcal{I}_{\mathbf{x}}} \bar{q}_{out}\} \rangle$
 3:     for each $q \in \overline{Q} \setminus \{\bar{q}_{in}, \bar{q}_{out}\}$ with self-loops $q \xrightarrow{R_1} q, \ldots, q \xrightarrow{R_k} q \in \overline{\Delta}$ do
 4:         if $k = 0$ then
 5:             $T \leftarrow \mathcal{I}_{\mathbf{x}}$
 6:         else
 7:             if $k = 1$ and $R_1$ is a finite monoid affine relation then
 8:                 $H \leftarrow R_1$
 9:             else
10:                 $H \leftarrow$ OctagonalHull($R_1 \vee \ldots \vee R_k$)
11:             $T \leftarrow$ ReflexiveTransitiveClosure($H$)
12:         for each $q_1 \xrightarrow{P} q$ and $q \xrightarrow{Q} q_2$ such that $q \notin \{q_1, q_2\}$ do
13:             $\overline{\Delta} \leftarrow \overline{\Delta} \cup \{q_1 \xrightarrow{\exists \mathbf{x}_1 \exists \mathbf{x}_2 . P(\mathbf{x},\mathbf{x}_1) \wedge T(\mathbf{x}_1,\mathbf{x}_2) \wedge Q(\mathbf{x}_2,\mathbf{x}')} q_2\}$
14:         $\overline{Q} \leftarrow \overline{Q} \setminus \{q\}$
15:         $\overline{\Delta} \leftarrow \overline{\Delta} \setminus \{q_1 \xrightarrow{R} q_2 \mid q \in \{q_1, q_2\}\}$
16:     return $\bigvee \{R \mid (\bar{q}_{in} \xrightarrow{R} \bar{q}_{out}) \in \overline{\Delta}\}$
```

6.4. **Computing Transition Invariants.** The core of the method for computing transition invariants, needed by the non-termination precondition Algorithm 3, is a procedure that computes, for any two control states $q, q' \in Q$ of an integer program $P = \langle \mathbf{x}, Q, q_{init}, \Delta \rangle$, an over-approximation $[\![P]\!]_{\sharp}^{+}(q, q')$ of the transitive closure $[\![P]\!]^{+}(q, q')$. The reflexive and transitive closure $[\![P]\!]_{\sharp}^{*}(q, q')$ can be computed using the alternative definition: $[\![P]\!]_{\sharp}^{*}(q, q') = [\![P]\!]_{\sharp}^{+}(q, q')$, if $q \neq q'$, and $[\![P]\!]_{\sharp}^{*}(q, q) = [\![P]\!]_{\sharp}^{+}(q, q) \cup \mathcal{I}_{\mathbf{x}}$. Using the reflexive and transitive closure, one can compute an over-approximation of the reachable set, at any control state $q \in Q$, as: $Reach_P^{\sharp}(q) = [\![P]\!]_{\sharp}^{*}(q_{init}, q)(\mathbb{Z}^{\mathbf{x}})$. The transition invariant $[\![P]\!]_{\sharp}^{TInv}(q, q')$ given by the transitive closure $[\![P]\!]_{\sharp}^{+}(q, q')$ restricted to values from $Reach_P^{\sharp}(q)$ only: $[\![P]\!]_{\sharp}^{TInv}(q, q') = \{\langle \nu, \nu' \rangle \in [\![P]\!]_{\sharp}^{+}(q, q') \mid \nu \in Reach_P^{\sharp}(q)\}$.

Algorithm 5 computes the over-approximated transitive closures $[\![P]\!]_{\sharp}^{+}(q, q')$, that are the key of our method for computing non-termination preconditions. The idea of this algorithm is to eliminate control states which are neither initial or final, while introducing new transitions labeled with compositions of relations between the remaining states.[12] In the beginning (line 2) we create a working copy $\overline{P}$ of the program by adding two fresh control states $\bar{q}_{in}, \bar{q}_{out} \notin Q$ and two copy transitions $\bar{q}_{in} \xrightarrow{\mathcal{I}_{\mathbf{x}}} q_{in}$ and $q_{out} \xrightarrow{\mathcal{I}_{\mathbf{x}}} \bar{q}_{out}$. This ensures that $\bar{q}_{in}$ and $\bar{q}_{out}$ do not occur within loops in $\overline{P}$. Then we iterate the following steps, until no more states can be eliminated. For each control state with (possibly zero) self-loops labeled with relations $R_1, \ldots, R_k$, we compute an over-approximation of the reflexive and transitive closure $T = (R_1 \vee \ldots \vee R_k)^*$. Three situations may arise:

- if there is no such loop, i.e. $k = 0$, T is the identity relation.

[12] The algorithm resembles the schoolbook method for converting finite automata into regular expressions.

- if there is only one such loop labeled with a finite monoid affine relation R_1, $T = R_1^*$ can be computed using one of the techniques from [21, 5, 10].
- otherwise, we compute first the *octagonal hull* $H = (R_1 \vee \ldots \vee R_k)^{oct}$, and then the reflexive and transitive closure of the octagonal hull $T = H^*$, using the algorithm described in [10]. The octagonal hull of a set is the strongest octagonal constraint that defines an over-approximation of that set. In general, the octagonal hull of a Presburger-definable set can be computed using integer linear programming [37].

Next, we compose the relation of each incoming transition $q_1 \xrightarrow{R} q$ with T, and with the relation of each outgoing transition $q \xrightarrow{Q} q_2$. We replace the pair of incoming and outgoing transitions with the transition $q_1 \xrightarrow{P \circ T \circ Q} q_2$, which does not involve q (line 13), and, finally, we eliminate q and all transitions involving it from the program (lines 14-15). The result is the disjunction of all relations occurring on the remaining transitions between the q_{in} and q_{out} states (line 16), which defines $[\![P]\!]^+_\sharp(q_{in}, q_{out})$.

The argument for proving the soundness of Algorithm 5 is that the following invariant holds, at each iteration of the main loop of the algorithm: after each elimination of a control state q from a program P (line 14), the transitive closure of the remaining program P' is an over-approximation of the previous one, i.e. for all $q_1, q_2 \in Q \setminus \{q\}$, $[\![P]\!]^+(q_1, q_2) \subseteq [\![P']\!]^+(q_1, q_2)$. This is the case because the summary relation:

$$S_P^q(q_1, q_2) = \{\langle \nu_1, \nu_2 \rangle \mid \text{there is a run } \langle q_1, \nu_1 \rangle \to \ldots \to \langle q, \nu \rangle \to \ldots \langle q_2, \nu_2 \rangle \text{ in } P\}$$

induced by the set of runs between two configurations $\langle q_1, \nu_1 \rangle$ and $\langle q_2, \nu_2 \rangle$, which visits q, is over-approximated by the composition of P, T and Q (line 13):

$$S_P^q(q_1, q_2) \Rightarrow \exists \mathbf{x}_1 \exists \mathbf{x}_2 \;.\; P(\mathbf{x}, \mathbf{x}_1) \wedge T(\mathbf{x}_1, \mathbf{x}_2) \wedge Q(\mathbf{x}_2, \mathbf{x}')$$

It is to be noticed that each transition $q_1 \to q_2$ introduced at line 13 in the algorithm corresponds to a path between q_1 and q_2 in the original control flow graph of the program, which visits at least once the state q removed at line 14. A formal proof of soundness is given in Lemma 6.4.

6.5. **Flat Integer Programs.** In this section, we define a class of integer programs for which our method computes precisely the weakest non-termination preconditions, as formulas in Presburger arithmetic. As a consequence of the decidability of the satisfiability problem for Presburger arithmetic [35], the universal termination problem is decidable for this class. A recent result [9, 8] shows that the *reachability problem*, i.e. the existence of a finite run between two control states, in a flat program whose transitions occurring within loops are labeled by octagonal constraints, is NP-complete. As a byproduct, we show that the non-termination problem, i.e. the existence of an infinite computation, for these programs is NP-complete as well.

Definition 6.3. Let $P = \langle \mathbf{x}, Q, q_{init}, \Delta \rangle$ be an integer program. For any elementary cycle $\pi : q_1 \xrightarrow{R_1} q_2 \xrightarrow{R_2} \ldots q_n \xrightarrow{R_n} q_1$, let $\lambda(\pi)$ denote the formula $\exists \mathbf{x}_1, \ldots, \mathbf{x}_{n-1} \;.\; R_1(\mathbf{x}, \mathbf{x}_1) \wedge \ldots \wedge R_n(\mathbf{x}_{n-1}, \mathbf{x})$. Then P is said to be *flat* if and only if:

(1) each control state $q \in Q$ belongs to at most one elementary cycle,
(2) for each elementary cycle π in P, $\lambda(\pi)$ defines an octagonal, or a finite monoid affine relation.

Example 1. Figure 6 depicts a flat integer programs P and its control flow graph. For simplicity, the elementary cycles have been already reduced to one transition, by composition of all the relations labeling the transitions within them. Since the labels of the self-loops are octagonal constraints, we can compute their reflexive and transitive closures precisely:

$$\begin{array}{lcl} R^*_{2,2} & \Leftrightarrow & \mathcal{I}_{x,y,m,n,y_0} \vee (x' - x = y' - y \wedge x' \geq x + 1 \wedge m \geq x' \wedge \mathcal{I}_{m,n,y_0}) \\ R^*_{5,5} & \Leftrightarrow & \mathcal{I}_{x,y,m,n,y_0} \vee (x' - x = y - y' \wedge x' \geq x + 1 \wedge n \geq x' \wedge \mathcal{I}_{m,n,y_0}) \end{array}$$

$$\mathrm{wnt}(R_{2,2}) \Leftrightarrow \textbf{false} \qquad \mathrm{wnt}(R_{5,5}) \Leftrightarrow \textbf{false} \qquad \mathrm{wnt}(R_{8,8}) \Leftrightarrow y = y_0$$

Following the computation of Algorithm 4, the weakest non-termination precondition of the integer program is:

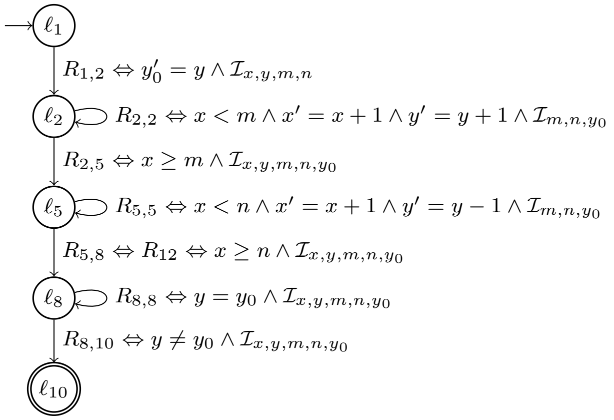
$$\mathrm{wnt}(P) \Leftrightarrow \begin{array}{ll} \exists \mathbf{x}' \,.\, R_{1,2}(\mathbf{x}, \mathbf{x}') \wedge \mathrm{wnt}(R_{2,2})(\mathbf{x}') & \vee \\ \exists \mathbf{x}' \,.\, (R_{1,2} \circ R^*_{2,2} \circ R_{2,5})(\mathbf{x}, \mathbf{x}') \wedge \mathrm{wnt}(R_{5,5})(\mathbf{x}') & \vee \\ \exists \mathbf{x}' \,.\, (R_{1,2} \circ R^*_{2,2} \circ R_{2,5} \circ R^*_{5,5} \circ R_{5,8})(\mathbf{x}, \mathbf{x}') \wedge \mathrm{wnt}(R_{9,9})(\mathbf{x}') & \end{array}$$

Since $\mathrm{wnt}(R_{2,2}) \Leftrightarrow \mathrm{wnt}(R_{5,5}) \Leftrightarrow$ **false**, the first two disjuncts are equivalent to **false**. The third disjunct, and hence $\mathrm{wnt}(P)$, is equivalent to

$$\mathrm{wnt}(P) \Leftrightarrow (n = 2m - x \wedge m \geq x + 1 \wedge n \geq m + 1) \vee (m \leq x \wedge n \leq x) \qquad \square$$

```
      int x,y,y0,m,n;
1.    y0 = y;
2.    while (x < m) {
3.        x=x+1;
4.        y=y+1;
      }
5.    while (x < n) {
6.        x=x+1;
7.        y=y-1;
      }
8.    while (y = y0) {
9.        skip;
10.   }
```

(a)


ℓ_1
$R_{1,2} \Leftrightarrow y'_0 = y \wedge \mathcal{I}_{x,y,m,n}$
ℓ_2
$R_{2,2} \Leftrightarrow x < m \wedge x' = x + 1 \wedge y' = y + 1 \wedge \mathcal{I}_{m,n,y_0}$
$R_{2,5} \Leftrightarrow x \geq m \wedge \mathcal{I}_{x,y,m,n,y_0}$
ℓ_5
$R_{5,5} \Leftrightarrow x < n \wedge x' = x + 1 \wedge y' = y - 1 \wedge \mathcal{I}_{m,n,y_0}$
$R_{5,8} \Leftrightarrow R_{12} \Leftrightarrow x \geq n \wedge \mathcal{I}_{x,y,m,n,y_0}$
ℓ_8
$R_{8,8} \Leftrightarrow y = y_0 \wedge \mathcal{I}_{x,y,m,n,y_0}$
$R_{8,10} \Leftrightarrow y \neq y_0 \wedge \mathcal{I}_{x,y,m,n,y_0}$
ℓ_{10}

(b)

FIGURE 6. A flat integer program and its simplified control flow graph

If $P = \langle \mathbf{x}, Q, q_{init}, \Delta \rangle$ is a flat program, then Algorithm 5 can be shown to return the precise transitive closures $[\![P]\!]^+(q, q')$, for any $q, q' \in Q$. Intuitively, this is the case because during the state elimination process, at any step, a state $q \in Q$ that is chosen to be removed can have at most one self-loop (line 7 in Algorithm 5), which corresponds to the (at most one) elementary cycle involving q in Δ. Since, moreover the label of this cycle denotes an octagonal or finite monoid affine relation, the transitive closure of this relation can be computed as a Presburger formula, without loss of information, using the algorithm from e.g. [10]. As a direct consequence, $[\![P]\!]^*(q, q')$ can also be computed without loss of precision, if the program is flat.

Lemma 6.4. *Let $P = \langle \mathbf{x}, Q, q_{init}, \Delta \rangle$ be an integer program. Then, the result of Algorithm 5 is a Presburger formula $\phi(\mathbf{x}, \mathbf{x}')$ that defines an over-approximation of $[\![P]\!]^+(q_{in}, q_{out})$. If, moreover, P is flat, $\phi(\mathbf{x}, \mathbf{x}')$ defines precisely $[\![P]\!]^+$.*

Proof. Let $\overline{P}_i = \langle \mathbf{x}, \overline{Q}_i, \bar{q}_{in}, \overline{\Delta}_i \rangle$ be the program $\overline{P}$ at the i-th iteration of the main loop of the algorithm, $i \geq 0$, and $\overline{P}_0 = \overline{P}$. Since for all $i \geq 0$, $\overline{Q}_{i+1} \subset \overline{Q}_i$ (line 14) it is sufficient to prove that, for all $i \geq 0$ we have $[\![\overline{P}_i]\!]^+(\bar{q}_{in}, \bar{q}_{out}) \subseteq [\![\overline{P}_{i+1}]\!]^+(\bar{q}_{in}, \bar{q}_{out})$. Moreover, $\overline{P}_0 = \overline{P}$ (line 2) and $[\![P]\!]^+ = [\![\overline{P}]\!]^+$ is an easy exercise. Then we obtain that, for all $i \geq 0$, $[\![P]\!]^+(q_{in}, q_{out}) \subseteq [\![\overline{P}_i]\!]^+(\bar{q}_{in}, \bar{q}_{out})$. The algorithm is bound to terminate, by the fact that the set of control states Q is finite and the for loop at line 3 is executed once for each control state $q \in \overline{Q} \setminus \{\bar{q}_{in}, \bar{q}_{out}\}$. Hence the result is an over-approximation of $[\![P]\!]^+$.

Let $q \in \overline{Q}_{i-1}$ be a control state chosen at line 3, $R_1, \ldots, R_k$ be the labels of the self-loops of q, and let H be the relation computed by the algorithm. For some $i > 0$, let π be a run between two configurations $\langle \bar{q}_{in}, \nu' \rangle$ and $\langle \bar{q}_{out}, \nu'' \rangle$ in $\overline{P}_{i-1}$, for some valuations $\nu', \nu'' \in \mathbb{Z}^{\mathbf{x}}$. It is sufficient to show that each sub-run ρ of π of the form $\langle q_0, \nu_0 \rangle \rightarrow \ldots \rightarrow \langle q_n, \nu_n \rangle$, where $n \geq 2$, $q_1 = \cdots = q_{n-1} = q$, $q_0 \neq q$, and $q_n \neq q$, can be replaced with a sub-run $\rho' : \langle q_0, \nu_0 \rangle \rightarrow \langle q_n, \nu_n \rangle$ in $\overline{P}_i$ of length 1, thus obtaining a run π' between $\langle \bar{q}_{in}, \nu' \rangle$ and $\langle \bar{q}_{out}, \nu'' \rangle$ in $\overline{P}_i$. Consequently, we have:

$$\langle \nu', \nu'' \rangle \in [\![\overline{P}_{i-1}]\!]^+(\bar{q}_{in}, \bar{q}_{out}) \Rightarrow \langle \nu', \nu'' \rangle \in [\![\overline{P}_i]\!]^+(\bar{q}_{in}, \bar{q}_{out})$$

and hence $[\![P]\!]^+(q_{in}, q_{out}) \subseteq [\![\overline{P}_{i-1}]\!]^+(\bar{q}_{in}, \bar{q}_{out}) \subseteq [\![\overline{P}_i]\!]^+(\bar{q}_{in}, \bar{q}_{out})$.

Let us consider any sub-run ρ of the above form. Since $R_j \subseteq H$ for each $1 \leq j \leq k$, we have that $(\nu_\ell, \nu_{\ell+1}) \in H$ for each $1 \leq \ell < n-1$, and hence $(\nu_1, \nu_{n-1}) \in H^{n-2} \subseteq H^* = T$. Let $q_0 \xrightarrow{P} q$ and $q \xrightarrow{Q} q_n$ be transitions in $\overline{\Delta}_{i-1}$ such that $(\nu_0, \nu_1) \in P$ and $(\nu_{n-1}, \nu_n) \in Q$. Since $(\nu_0, \nu_1) \models P$, $(\nu_1, \nu_{n-1}) \models T$ and $(\nu_{n-1}, \nu_n) \models Q$, we can choose ρ' as the transition labeled by $\exists \mathbf{x}_1 \exists \mathbf{x}_2 . P(\mathbf{x}, \mathbf{x}_1) \wedge T(\mathbf{x}_1, \mathbf{x}_2) \wedge Q(\mathbf{x}_2, \mathbf{x}')$, added at line 13.

For the second part of the proof, suppose that the program P is flat. For some arbitrary $i \geq 0$ and two configurations $\nu', \nu'' \in \mathbb{Z}^{\mathbf{x}}$, let π be a run from $\langle \bar{q}_{in}, \nu' \rangle$ to $\langle \bar{q}_{out}, \nu'' \rangle$ in $\overline{P}_i$. We show that there exists a run in $\overline{P}_{i-1}$ between the same configurations, proving thus that $[\![\overline{P}]\!]_i^+(\bar{q}_{in}, \bar{q}_{out}) \subseteq [\![\overline{P}]\!]_{i-1}^+(\bar{q}_{in}, \bar{q}_{out})$. By the previous point, we obtain $[\![\overline{P}]\!]_i^+(\bar{q}_{in}, \bar{q}_{out}) = [\![\overline{P}]\!]_{i-1}^+(\bar{q}_{in}, \bar{q}_{out})$, and since the choice of $i \geq 0$ was arbitrary, we conclude that $[\![\overline{P}]\!]_i^+(\bar{q}_{in}, \bar{q}_{out}) = [\![P]\!]^+(q_{in}, q_{out})$.

Let $\langle q_1, \nu_1 \rangle \rightarrow \langle q_2, \nu_2 \rangle$ be a step of π such that $(\nu_1, \nu_2) \models V$ for some transition $t = (q_1 \xrightarrow{V} q_2) \in (\overline{\Delta}_i \setminus \overline{\Delta}_{i-1})$, and let $t_1 = q_1 \xrightarrow{P} q$ and $t_2 = q \xrightarrow{Q} q_2$ be the transitions in $\overline{\Delta}_{i-1}$ used to construct t. Since P is flat, there is at most 1 self-loop involving the control state q. If there is no such self-loop, the algorithm computes $T = \mathcal{I}_{\mathbf{x}}$, hence $V(\mathbf{x}, \mathbf{x}') \Leftrightarrow \exists \mathbf{z} . P(\mathbf{x}, \mathbf{z}) \wedge Q(\mathbf{z}, \mathbf{x}')$. Consequently, there exists a valuation $\eta \in \mathbb{Z}^{\mathbf{x}}$ such that $(\nu_1, \eta) \models P$, $(\eta, \nu_2) \models Q$ and thus, there is a run $\langle q_1, \nu_1 \rangle \rightarrow \langle q, \eta \rangle \rightarrow \langle q_2, \nu_2 \rangle$ in $\overline{P}_{i-1}$. If there is one self-loop, then the algorithm computes precisely the reflexive and transitive closure $T = R_1^*$ and hence, $V(\mathbf{x}, \mathbf{x}') \Leftrightarrow \exists \mathbf{z}, \mathbf{z}' . P(\mathbf{x}, \mathbf{z}) \wedge R_1^*(\mathbf{z}, \mathbf{z}') \wedge Q(\mathbf{z}', \mathbf{x}')$. Since $(\nu_1, \nu_2) \models V$, there exists $n \geq 0$, such that $(\nu_1, \nu_2) \models \exists \mathbf{z}, \mathbf{z}' . P(\mathbf{x}, \mathbf{z}) \wedge R_1^n(\mathbf{z}, \mathbf{z}') \wedge Q(\mathbf{z}', \mathbf{x}')$. If $n = 0$, $R^0 = \mathcal{I}_{\mathbf{z}}$ and we obtain a run in $\overline{P}_{i-1}$ similarly as in the case with no self-loop. If $n \geq 1$, there exist valuations $\eta_0, \ldots, \eta_n \in \mathbb{Z}^{\mathbf{x}}$ such that $(\eta_\ell, \eta_{\ell+1}) \in R_1$ for each $0 \leq \ell < n$, $(\nu_1, \eta_0) \in P$, and $(\eta_n, \nu_2) \in Q$. Hence we obtain the run $\langle q_1, \nu_1 \rangle \rightarrow \langle q, \eta_0 \rangle \rightarrow \ldots \rightarrow \langle q, \eta_n \rangle \rightarrow \langle q_2, \nu_2 \rangle$ in $\overline{P}_{i-1}$. We obtain thus:

$$\langle \nu', \nu'' \rangle \in [\![\overline{P}_i]\!]^+(\bar{q}_{in}, \bar{q}_{out}) \Rightarrow \langle \nu', \nu'' \rangle \in [\![\overline{P}_{i-1}]\!]^+(\bar{q}_{in}, \bar{q}_{out})$$

and consequently, $[\![\overline{P}_i]\!]^+(\bar{q}_{in}, \bar{q}_{out}) \subseteq [\![\overline{P}_{i-1}]\!]^+(\bar{q}_{in}, \bar{q}_{out})$.

Since the transitive closure of octagonal and finite monoid affine relations is Presburger definable (see e.g. [10]), Presburger arithmetic is closed under existential quantification, and since the octagonal hull of a Presburger formula can be computed using integer linear programming [37], it follows that the algorithm manipulates and returns only Presburger formulas. □

Moreover, Algorithm 4 will also compute the weakest non-termination precondition for flat programs. Since every state occurs within at most one elementary cycle, the test on line 4 of the algorithm will succeed for every state on a loop, and since the formula defining the composition R of all relations along the cycle is equivalent to an octagonal or a finite monoid affine relation, the test on line 6 will also succeed. In this case, $\mathrm{WNT}(R)$ is bound to return the weakest non-termination precondition of R, thus the result of Algorithm 4 is the weakest non-termination precondition of the entire program.

Lemma 6.5. *Let $P = \langle \mathbf{x}, Q, q_{init}, \Delta \rangle$ be an integer program. Then, the result of Algorithm 4 is a Presburger formula $\phi(\mathbf{x}, \mathbf{x}')$ that defines an over-approximation of $[\![P]\!]^{wnt}(q_{init})$. If, moreover, P is flat, $\phi(\mathbf{x}, \mathbf{x}')$ defines precisely $[\![P]\!]^{wnt}(q_{init})$.*

Proof. Consider the iteration of the for-loop during which the control state $q \in Q$ is chosen. First, suppose that the test at line 4 fails. In this case the algorithm enters line 10, and the correctness of the assignment at this line follows from Theorem 6.2. Second, suppose that the test at 4 succeeds. In this case, there is a unique elementary cycle of the form $q \xrightarrow{R_1} \ldots \xrightarrow{R_n} q$, where $n \geq 1$. Let $R \overset{def}{=} R_1 \circ \cdots \circ R_n$. Then, it follows from the definition of $[\![P]\!]^{TInv}$ that:

$$\begin{array}{rl} & ([\![P]\!]^*(q_{init}, q))^{-1}([\![P]\!]^{TInv}(q, q)) \\ = & \left\{ \nu_0 \in \mathbb{Z}^{\mathbf{x}} \mid \begin{array}{l} \exists \text{ valuations } \{\nu_i \in \mathbb{Z}^{\mathbf{x}}\}_{i \geq 1} \text{ and runs } \pi_0 = \langle q_{init}, \nu_0 \rangle \to^* \langle q, \nu_1 \rangle, \\ \pi_i = \langle q, \nu_i \rangle \to^+ \langle q, \nu_{i+1} \rangle \text{ for each } i \geq 1 \end{array} \right\} \\ = & \left\{ \nu_0 \in \mathbb{Z}^{\mathbf{x}} \mid \begin{array}{l} \exists \text{ valuations } \{\nu_i \in \mathbb{Z}^{\mathbf{x}}\}_{i \geq 1} \text{ and run } \pi_0 = \langle q_{init}, \nu_0 \rangle \to^* \langle q, \nu_1 \rangle \\ \text{such that } (\nu_i, \nu_{i+1}) \in R^+ \text{ for each } i \geq 1 \end{array} \right\} \\ = & \left\{ \nu_0 \in \mathbb{Z}^{\mathbf{x}} \mid \begin{array}{l} \exists \text{ valuations } \{\nu_i \in \mathbb{Z}^{\mathbf{x}}\}_{i \geq 1} \text{ and run } \pi_0 = \langle q_{init}, \nu_0 \rangle \to^* \langle q, \nu_1 \rangle \\ \text{such that } (\nu_i, \nu_{i+1}) \in R \text{ for each } i \geq 1 \end{array} \right\} \\ = & \left\{ \nu_0 \in \mathbb{Z}^{\mathbf{x}} \mid \begin{array}{l} \exists \text{ valuation } \nu_1 \in \mathbb{Z}^{\mathbf{x}} \text{ and run } \pi_0 = \langle q_{init}, \nu_0 \rangle \to^* \langle q, \nu_1 \rangle \\ \text{such that } \nu_1 \in \mathrm{wnt}(R) \text{ for each } i \geq 1 \end{array} \right\} \\ = & ([\![P]\!]^*(q_{init}, q))^{-1}(\mathrm{wnt}(R)) \end{array}$$

Then, the correctness of line 4 follows from Theorem 6.2. Consequently, the algorithm always returns an over-approximation of $[\![P]\!]^{wnt}(q_{init})$.

Next, suppose that P is flat. Moreover, line 10 is reached if and only if there is no cycle that involves q, in which case $[\![P]\!]^+(q, q) = \emptyset$. Consequently, $[\![P]\!]^{TInv}(q, q) = \emptyset$ and hence, the algorithm can always choose $R_1' \Leftrightarrow \mathbf{false}$ before executing line 10. Previously, we argued that

$$([\![P]\!]^*(q_{init}, q))^{-1}([\![P]\!]^{TInv}(q, q)) = ([\![P]\!]^*(q_{init}, q))^{-1}(\mathrm{wnt}(R))$$

Since P is flat, $[\![P]\!]^*(q_{init}, q)$ can be computed precisely as a Presburger formula, by Lemma 6.4. Moreover, R is an octagonal or a finite monoid affine relations and hence, $\mathrm{wnt}(R)$ can be computed precisely as a Presburger formula too, by Theorem 4.38 and 5.6. Hence, the algorithm returns a Presburger formula that precisely defines $[\![P]\!]^{wnt}(q_{init})$. □

If we restrict the class of flat integer programs further, by considering that only octagonal constraints appear as labels within the loops of the program, we can characterize the complexity class for the problem asking for the existence of an infinite run, within this class of programs. The result is based on a characterization of the *reachability problem* in this class of programs. Given a program $P = \langle \mathbf{x}, Q, q_{init}, \Delta \rangle$ and a control state $q \in Q$, the reachability problem asks for the existence of a run of P from q_{init} to q.

Theorem 6.6 ([9])**.** *The reachability problem for the class of programs:*

$$\mathcal{P}_{OCT} = \left\{ P \textit{ flat program} \mid \begin{array}{l} \textit{if } q \xrightarrow{R} q' \textit{ is in a cycle, } R \textit{ is an octagonal constraint} \\ \textit{otherwise, } R \textit{ is a quantifier-free Presburger formula} \end{array} \right\}$$

is NP-complete.

This result can be used in conjunction with Theorem 4.38 to obtain the following:

Theorem 6.7. *The problem asking for the existence of an infinite run is NP-complete for the class of programs $\mathcal{P}_{OCT}$.*

Proof. Let $P = \langle \mathbf{x}, Q, q_{init}, \Delta \rangle$ be an instance of the $\mathcal{P}_{OCT}$ class. Since P is a flat program, each strongly connected component consists of at most one cycle, which is elementary. Let $C_1, \ldots, C_k$ be the non-trivial elementary cycles of P, and let $q_1, \ldots, q_k$ be arbitrary control states belonging to each of these cycles, respectively. Let R_i be the composition of all octagonal relations on C_i starting from q_i, for all $i = 1, \ldots, k$, respectively. Since all of these relations are defined by octagonal constraints, their composition can be computed in PTIME, according to Corollary 4.24. Since PTIME $\subseteq$ PSPACE, the sizes of $R_1, \ldots, R_k$ are at most polynomial in the size of P. Then one uses Algorithm 3 to compute $\mathrm{wnt}(R_1), \ldots, \mathrm{wnt}(R_k)$ in PTIME, respectively (Theorem 4.38). Clearly, the sizes of $\mathrm{wnt}(R_1), \ldots, \mathrm{wnt}(R_k)$ are also polynomial in the size of P. Finally, we construct $P' = \langle \mathbf{x}, Q \cup \{q_{nt}\}, q_{init}, \Delta' \rangle$, where $q_{nt} \notin Q$ is a fresh control state, and:

$$\Delta' = \Delta \cup \{q_i \xrightarrow{\mathrm{wnt}(R_i)} q_{nt} \mid i = 1, \ldots, k\}$$

The size of P' is bounded by a polynomial in the size of P, and, moreover, P has an infinite run if and only if the control state q_{nt} is reachable by a finite run of P'. Hence the existence of an infinite run is in NP.

To show NP-hardness, let $\varphi(\mathbf{x})$ be an arbitrary quantifier-free Presburger formula, and consider the following integer program:

$$q_{init} \xrightarrow{\varphi(\mathbf{x}')} \overset{\overset{\textbf{true}}{\curvearrowright}}{q} \tag{6.1}$$

Clearly, the program (6.1) has an infinite run if and only if $\varphi(\mathbf{x})$ is satisfiable. However, this is an NP-complete problem, since φ is an arbitrary quantifier-free Presburger formula. □

7. Experiments

We have validated the methods described in this paper by automatically finding preconditions for termination of all the octagonal running examples, and of several integer programs synthesized from (i) programs with lists obtained using the translation scheme from [6] which generates an integer program from a program manipulating dynamically allocated single-selector linked lists, (ii) VHDL designs such as hardware counter and synchronous

Table 1. Weakest Non-termination Preconditions for Integer Programs.

Model	Size			Time [s]	Weakest Non-termination Preconditions
	$\|\mathbf{x}\|$	$\|Q\|$	$\|\Delta\|$		
(i) Examples from L2CA [6]					
listcounter	4	31	35	1.2	$false$
listreversal	7	97	107	32.6	$false$
(ii) VHDL models from [39]					
counter	2	6	13	0.8	$true$
register	2	10	49	1.4	$true$
synlifo	3	43	1006	1016.4	$true$
(iii) Examples from [25]					
anubhav	29	20	25	3.2	$i < 0$
cousot	29	31	34	4.0	$true$
(iv) Examples from [41]					
leq	3	5	6	0.6	$false$
leq.modif	3	5	6	2.4	$x < 0 \wedge y < 0$
plus	3	7	9	0.7	$false$
plus.modif	3	7	9	0.9	$x < 0 \vee y < 0$

Table 2. Termination preconditions for several program fragments from [16]

Program	Cook et al. [16]	Linear Affine Loops

if (lvar $\geq$ 0)
  while (lvar $< 2^{30}$)
    lvar = lvar $\ll$ 1;
	$lvar > 0 \vee lvar < 0 \vee lvar \geq 2^{30}$	$\neg(lvar{=}0) \vee lvar{\geq}2^{30}$

while (x $\geq$ N)
  x = -2*x + 10;
	$x > 5 \vee x + y \geq 0$	$x \neq \frac{10}{3} \Leftrightarrow$ true

//@ requires $n > 200$
x = 0;
while (1)
  if (x < n) { x=x+y;
    if (x $\geq$ 200) break; }
	$y > 0$	$y{>}0$

LIFO [39], (iii) small C programs with challenging loops and (iv) small recursive Java programs from [41] translated to non-recursive programs using the procedure summarization method described in [18].

We have computed the weakest non-termination preconditions reported in Table 1 using the methods from Section 4 and 6 which we implemented in the Flata tool [22]. By computing octagonal abstractions of disjuncts of a transition invariant, we have verified universal termination of the ListCounter and ListReversal programs. Next, we have verified the Counter and SynLifo programs by computing the precise transition invariant and then the weakest non-termination precondition, which was empty in both cases. Thus, these models have infinite runs for any input values, which is to be expected as they encode the behavior of synchronous reactive circuits. Similarly, we have computed the weakest non-termination preconditions for numerical programs anubhav, cousot, leq, and plus.

Second, we have compared (Table 2) our method for termination of polynomially bounded linear affine loops from Section 5 with the examples given in [16], and found the same termination preconditions as they do, with one exception, in which we can prove universal termination in integer input values (row 3 of Table 2).

8. Conclusion

We have presented several methods for deciding conditional termination of several classes of program loops manipulating integer variables. The universal termination problem has been found to be decidable for octagonal relations and linear affine loops with the finite monoid property. For the class of polynomially bounded linear affine loops, we give sufficient termination conditions. Further, we extend the computation of weakest non-termination preconditions from simple loops to general programs, and define a class of programs, called flat, for which this computation yields precise results. Finally, we have implemented our method in the Flata tool [22] and performed a number of preliminary experiments.

Acknowledgments The authors wish to thank the anonymous reviewers for their important contribution to improving the quality of this paper.

References

[1] R. Alur and D. L. Dill. The theory of timed automata. In *Proc. of REX Workshop*, volume 600 of *LNCS*, pages 45–73, Berlin, Heidelberg, 1991. Springer Verlag.

[2] R. Bagnara, P. M. Hill, and E. Zaffanella. An improved tight closure algorithm for integer octagonal constraints. In *Proc. of VMCAI*, volume 4905 of *LNCS*, pages 8–21, Berlin, Heidelberg, 2008. Springer Verlag.

[3] A. M. Ben-Amram. Size-change termination with difference constraints. *ACM Trans. Program. Lang. Syst.*, 30(3):1–16, 2008.

[4] A. M. Ben-Amram and S. Genaim. On the linear ranking problem for integer linear-constraint loops. In *POPL*, pages 51–62, 2013.

[5] B. Boigelot. *Symbolic Methods for Exploring Infinite State Spaces.* PhD Thesis. Université de Liège, 1999.

[6] A. Bouajjani, M. Bozga, P. Habermehl, R. Iosif, P. Moro, and T. Vojnar. Programs with lists are counter automata. In *Proc. of CAV*, volume 4144 of *LNCS*, pages 517–531, Berlin, Heidelberg, 2006. Springer Verlag.

[7] M. Bozga, C. Gîrlea, and R. Iosif. Iterating octagons. In *Proc. of TACAS*, volume 5505 of *LNCS*, pages 337–351, Berlin, Heidelberg, 2009. Springer Verlag.

[8] M. Bozga, R. Iosif, and F. Konecný. Safety problems are np-complete for flat integer programs with octagonal loops. *CoRR*, abs/1307.5321, 2013.

[9] M. Bozga, R. Iosif, and F. Konecný. Safety problems are np-complete for flat integer programs with octagonal loops. In *VMCAI*, pages 242–261, 2014.

[10] M. Bozga, R. Iosif, and F. Konečný. Fast acceleration of ultimately periodic relations. In *Proc. of CAV*, volume 6174 of *LNCS*, pages 227–242, Berlin, Heidelberg, 2010. Springer Verlag.

[11] M. Bozga, R. Iosif, and F. Konečný. Deciding conditional termination. In *Proc. of TACAS*, volume 7214 of *LNCS*, pages 252–266, Berlin, Heidelberg, 2012. Springer Verlag.

[12] M. Bozga, R. Iosif, and Y. Lakhnech. Flat parametric counter automata. *Fundamenta Informaticae*, 91(2):275–303, 2009.

[13] A. R. Bradley, Z. Manna, and H. B. Sipma. Linear ranking with reachability. In *Proc. of CAV*, volume 3576 of *LNCS*, pages 491–504, Berlin, Heidelberg, 2005. Springer Verlag.

[14] M. Braverman. Termination of integer linear programs. In *Proc. of CAV*, volume 4144 of *LNCS*, pages 372–385, Berlin, Heidelberg, 2006. Springer Verlag.

[15] H. Comon and Y. Jurski. Multiple counters automata, safety analysis and presburger arithmetic. In *Proc. of CAV*, volume 1427 of *LNCS*, pages 268–279, Berlin, Heidelberg, 1998. Springer Verlag.

[16] B. Cook, S. Gulwani, T. Lev-Ami, A. Rybalchenko, and M. Sagiv. Proving conditional termination. In *Proc. of CAV*, volume 5123 of *LNCS*, pages 328–340, Berlin, Heidelberg, 2008. Springer Verlag.

[17] B. Cook, A. Podelski, and A. Rybalchenko. Termination proofs for systems code. *SIGPLAN Not.*, 41(6):415–426, June 2006.

[18] B. Cook, A. Podelski, and A. Rybalchenko. Summarization for termination: no return! *Formal Methods in System Design*, 35:369–387, 2009.

[19] T. H. Cormen, C. Stein, R. L. Rivest, and C. E. Leiserson. *Introduction to Algorithms*. McGraw-Hill Higher Education, 2nd edition, 2001.

[20] G. Everest. *Recurrence sequences*. American Mathematical Soc., 2003.

[21] A. Finkel and J. Leroux. How to compose presburger-accelerations: Applications to broadcast protocols. In *Proc. of FST TCS*, volume 2556 of *LNCS*, pages 145–156, Berlin, Heidelberg, 2002. Springer Verlag.

[22] Flata: a tool for the analysis of integer programs. `http://nts.imag.fr/index.php/Flata`.

[23] S. Ginsburg and E. H. Spanier. Semigroups, presburger formulas, and languages. *Pacific Journal of Mathematics*, 16:285 – 296, 1966.

[24] A. Gupta, T. A. Henzinger, R. Majumdar, A. Rybalchenko, and R. Xu. Proving non-termination. In *Proc. of POPL*, pages 147–158, New York, NY, USA, 2008. ACM.

[25] R. Jhala and K. L. McMillan. A practical and complete approach to predicate refinement. In *Proc. of TACAS*, volume 3920 of *LNCS*, pages 459–473, Berlin, Heidelberg, 2006. Springer Verlag.

[26] S. C. Kleene. *Introduction to Metamathematics*. North Holland Publishing Company, 1952.

[27] A. Mandel and I. Simon. On finite semigroups of matrices. *Theoretical Computer Science*, 5(2):101–111, 1977.

[28] A. Miné. *Weakly Relational Numerical Abstract Domains*. PhD Thesis, Ecole Polytechnique, Palaiseau, France, 2004.

[29] A. Miné. The octagon abstract domain. *Higher-Order and Symbolic Computation*, 19(1):31–100, 2006.

[30] F. Nielson, H. R. Nielson, and C. Hankin. *Principles of Program Analysis*. Springer Verlag, 1999.

[31] J. Ouaknine and J. Worrell. Decision problems for linear recurrence sequences. In *RP*, pages 21–28, 2012.

[32] E. Payet and F. Mesnard. Non-termination inference for constraint logic programs. In *Proc. of SAS*, volume 3148 of *Lecture Notes in Computer Science*, pages 377–392. Springer Berlin Heidelberg, 2004.

[33] A. Podelski and A. Rybalchenko. A complete method for the synthesis of linear ranking functions. In *Proc. of VMCAI*, volume 2937 of *LNCS*, pages 465–486, Berlin, Heidelberg, 2004. Springer Verlag.

[34] A. Podelski and A. Rybalchenko. Transition invariants. In *LICS'04*, pages 32–41, 2004.

[35] M. Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. *Comptes rendus du I Congrés des Pays Slaves*, pages 92–101, 1929.

[36] F. P. Ramsey. On a problem of formal logic. *Proc. of the London Mathematical Society*, 30:264–285, 1930.

[37] A. Schrijver. *Theory of Linear and Integer Programming*. Wiley, 1986.

[38] B. De Schutter. On the ultimate behavior of the sequence of consecutive powers of a matrix in the max-plus algebra. *Linear Algebra and its Applications*, 307:103–117, 2000.

[39] A. Smrcka and T. Vojnar. Verifying parametrised hardware designs via counter automata. In *Proc. of HVC*, volume 4899 of *LNCS*, pages 51–68, Berlin, Heidelberg, 2007. Springer Verlag.

[40] K. Sohn and A. Van Gelder. Termination detection in logic programs using argument sizes. In *Proc. of PODS*, pages 216–226, New York, NY, USA, 1991. ACM.

[41] Termination Competition 2011. `http://termcomp.uibk.ac.at/termcomp/home.seam`.

[42] A. Tiwari. Termination of linear programs. In *Proc. of CAV*, volume 3114 of *LNCS*, pages 70–82, Berlin, Heidelberg, 2004. Springer Verlag.

[43] A. M. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, 42:230–265, 1936.

[44] K. N. Verma, H. Seidl, and T. Schwentick. On the Complexity of Equational Horn Clauses. In *CADE-20*, volume 3632 of *LNCS*, pages 337–352, 2005.