Safety Problems Are NP-complete for Flat Integer Programs with Octagonal Loops

Marius Bozga[1], Radu Iosif[1], and Filip Konečný[2]

[1] VERIMAG/CNRS, Grenoble, France
[2] École Polytechnique Fédérale de Lausanne (EPFL), Switzerland

Abstract. This paper proves the NP-completeness of the reachability problem for the class of flat counter machines with difference bounds and, more generally, octagonal relations, labeling the transitions on the loops. The proof is based on the fact that the sequence of powers $\{R^i\}_{i=1}^{\infty}$ of such relations can be encoded as a periodic sequence of matrices, and that both the prefix and the period of this sequence are $2^{O(\|R\|_2)}$ in the size of the binary encoding $\|R\|_2$ of a relation R. This result allows to characterize the complexity of the reachability problem for one of the most studied class of counter machines [6,10], and has a potential impact on other problems in program verification.

1 Introduction

Counter machines are powerful abstractions of programs, commonly used in software verification. Due to their expressive power, counter machines can simulate Turing machines [18], hence, in theory, any program can be viewed as a counter machine. In practice, effective reductions to counter systems have been designed for programs with dynamic heap data structures [3], arrays [5], dynamic thread creation and shared memory [1], etc. Since counter machines with only two variables are Turing-complete [18], all their decision problems (reachability, termination) are undecidable. This early negative result motivated researchers to find classes of systems with decidable problems, such as: (branching) vector addition systems [13,17], reversal-bounded counter machines [16], Datalog programs with gap-order constraints [20], and flat counter machines [2,10,6]. Despite the fact that reachability of a set of configurations is decidable for these classes, few of them are actually supported by tools, and used for real-life verification purposes. The main reason is that the complexities of the reachability problems for these systems are, in general, prohibitive. Thus, most software verifiers rely on incomplete algorithms, which, due to the loss of precision, may raise large numbers of false alarms. Improving the precision of these tools requires mixed techniques such as combinations of *static analysis* and *acceleration* and relies on identifying subproblems for which the set of reachable states, or the transitive closure of the transition relation, can be computed precisely [14].

We study the complexity of the reachability problems for a class of *flat counter machines* (i.e., the control structure forbids nested loops), in which the transitions occurring inside loops are all labeled with *difference bounds constraints*, i.e. conjunctions of linear inequalities of the form $x - y \leq c$ where $x, y \in \mathbf{x} \cup \mathbf{x}'$ and $c \in \mathbb{Z}$ is a constant.

K.L. McMillan and X. Rival (Eds.): VMCAI 2014, LNCS 8318, pp. 242–261, 2014.

Furthermore, we extend the result to the case of octagonal relations, which are conjunctions of the form $\pm x \pm y \leq c$.

The decidability of the reachability problem for these classes relies on the fact that the transitive closures R^+ of relations R, defined by difference bounds and octagonal constraints, are expressible in Presburger arithmetic [10]. In [6], we presented a concise proof of this fact, based on the observation that any sequence of powers $\{R^i\}_{i=1}$, can be encoded as a *periodic sequence* of matrices, which can be defined by a quantifier-free Presburger formula whose size depends on the prefix and the period of the matrix sequence. In this paper we show primarily that both the prefix and period and this sequence are of the order of $2^{O(\|R\|_2)}$, where $\|R\|_2$ is the size of the binary encoding of the relation. More precisely, the quantifier-free Presburger formula defining a transitive closure (and, implicitly, the reachability problem for the counter machine) has $2^{O(\|R\|_2)}$ many disjuncts of polynomial size. A non-deterministic Turing machine that solves the reachability problem can guess, for each loop relation R, the needed disjunct of R^+, and validate its guess in NPTIME($\|R\|_2$).

Related Work. The complexity of safety, and, more generally, temporal logic properties of integer counter machines has received relatively little attention. For instance, the exact complexity of reachability for vector addition systems (VAS) is an open problem (the only known upper bound is non-primitive recursive), while the coverage and boundedness problems are EXPSPACE-complete for VAS [19], and 2EXPTIME-complete for branching VAS [13].

In [15] the authors study the functional equivalence of programs with increment, decrement and zero test, in the *reversal-bounded* case, where the counters are allowed to switch between non-decreasing and non-increasing modes a number of times which is bounded by a constant. It is found that the equivalence problem is in PSPACE, while the in-equivalence problem is NP-complete. Our model of computation is incomparable, since flat programs with non-deterministic updates are not reversal-bounded.

On what concerns counter machines with gap-order constraints (a restriction of difference bounds constraints $x - y \leq c$ to the case $c \leq 0$), reachability is PSPACE-complete [9], even in the absence of the flatness restriction on the control structure. Our result is incomparable to [9], as we show NP-completeness for flat counter machines with more general[1], difference bounds relations on loops.

The results which are probably closest to ours are the ones in [12,11], where flat counter machines with deterministic transitions of the form $\bigwedge_{j=1}^{m} \sum_{i=1}^{n} a_{ji} \cdot x_i + b_{ji} \leq 0 \wedge \bigwedge_{i=1}^{n} x_i' = x_i + c_i$ are considered. In [12] it is shown that model-checking LTL is NP-complete for these systems, matching thus our complexity for reachability with difference bounds constraints, while model-checking first-order logic and linear μ-calculus is PSPACE-complete [11], matching the complexity of CTL* model checking for gap-order constraints [9]. These results are again incomparable with ours, since (i) the linear guards are more general, while (ii) the vector addition updates are more restrictive (e.g. the direct transfer of values $x_i' = x_j$ for $i \neq j$ is not allowed).

[1] The generalization of gap-order to difference bound constraints suffices to show undecidability of non-flat counter machines, hence the restriction to flat control structures is crucial.

2 Preliminary Definitions

We denote by $\mathbb{Z}$ and $\mathbb{N}$ the sets of integers and positive integers, and let $\mathbb{Z}_\infty = \mathbb{Z} \cup \{\infty\}$. We write $[n]$ for the interval $\{0,\ldots,n-1\}$, $\mathrm{abs}(n)$ for the absolute value of the integer $n \in \mathbb{Z}$, and $lcm(n_1,\ldots,n_k)$ for the least common multiple of $n_1,\ldots,n_k \in \mathbb{N}$. Let $\mathbf{x}$ denote a nonempty set of variables, and $\mathbf{x}' = \{x' \mid x \in \mathbf{x}\}$. A *valuation* of $\mathbf{x}$ is a function $\nu : \mathbf{x} \to \mathbb{Z}$. The set of all such valuations is denoted by $\mathbb{Z}^{\mathbf{x}}$, and we denote by $\mathbb{Z}^N$ the N-times cartesian product $\mathbb{Z} \times \ldots \times \mathbb{Z}$, for some $N > 0$. We assume that the reader is familiar with Presburger arithmetic, and we denote by QFPA (quantifier-free Presburger arithmetic) the set of boolean combinations of linear inequalities and linear modulo constraints. For a QFPA formula ϕ, let $Atom(\phi)$ denote the set of atomic propositions in ϕ, and $\varphi[t/x]$ denote the formula obtained by substituting the variable x with the term t in φ.

A formula $\phi(\mathbf{x},\mathbf{x}')$ is evaluated with respect to two valuations $\nu_1,\nu_2 \in \mathbb{Z}^{\mathbf{x}}$, by replacing each occurrence of $x \in \mathbf{x}$ with $\nu_1(x)$ and each occurrence of $x' \in \mathbf{x}'$ with $\nu_2(x)$ in ϕ. The satisfaction relation is denoted by $(\nu_1,\nu_2) \models \phi(\mathbf{x},\mathbf{x}')$. A formula $\phi_R(\mathbf{x},\mathbf{x}')$ is said to *define* a relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ whenever for all $\nu_1,\nu_2 \in \mathbb{Z}^{\mathbf{x}}$, $(\nu_1,\nu_2) \in R$ if and only if $(\nu_1,\nu_2) \models \phi_R$. The composition of two relations $R_1,R_2 \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ defined by formulae $\varphi_1(\mathbf{x},\mathbf{x}')$ and $\varphi_2(\mathbf{x},\mathbf{x}')$, respectively, is the relation $R_1 \circ R_2$, defined by the formula $\exists \mathbf{y} \,.\, \varphi_1(\mathbf{x},\mathbf{y}) \wedge \varphi_2(\mathbf{y},\mathbf{x}')$. The *identity relation* $Id_{\mathbf{x}}$ is defined by the formula $\bigwedge_{x \in \mathbf{x}} x' = x$.

Definition 1. *A* class of relations *is a set $\mathcal{R}$ of QFPA formulae $\phi_R(\mathbf{x},\mathbf{x}')$ defining relations $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$, such that $Id_{\mathbf{x}}$ is $\mathcal{R}$-definable, and, for any two $\mathcal{R}$-definable relations $R_1,R_2 \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$, their composition $R_1 \circ R_2$ is $\mathcal{R}$-definable.*

Notice that any set $\mathcal{R}$ of formulae $\varphi(\mathbf{x},\mathbf{x}')$ that has quantifier elimination is a class of relations. If the class of a relation is not specified a priori, we consider it to be the set of all QFPA formulae. Given a relation R, we denote by R^i, for $i > 0$, the i-times composition of R with itself, and by R^0 the identity relation $Id_{\mathbf{x}}$. We denote by $R^+ = \bigcup_{i=1}^{\infty} R^i$ the *transitive closure* of R. Notice that, if R is an $\mathcal{R}$-definable relation, then the sequence $\{R^i\}_{i \geq 0}$ is $\mathcal{R}$-definable as well. In the following, we sometimes use the same symbol to denote a relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ and the formula $\phi_R(\mathbf{x},\mathbf{x}')$ defining it.

For a constant $c \in \mathbb{Z}$, we denote by $\|c\|_2 = \lceil \log_2(\mathrm{abs}(c)) \rceil$, if $\mathrm{abs}(c) > 2$ and $\|c\|_2 = 2$, otherwise, the *size of its binary encoding*[2]. The *binary size* of a formula is the sum of the binary sizes of its coefficients. It is known that the satisfiability problem for QFPA is NP-complete in the binary size of the formula [22]. The binary size of an $\mathcal{R}$-definable[3] relation R is $\|R\|_2^{\mathcal{R}} = \min\{\|\phi_R\|_2 \mid \phi_R \in \mathcal{R},\ \phi_R \text{ defines } R\}$. When the class of a relation is obvious from the context, it will be omitted. For space reasons, all proofs and missing material are given in [7].

[2] Abstracting from particular machine representations, we assume that at least 2 bits are needed to encode each integer.

[3] The class $\mathcal{R}$ is relevant here, because the same relation can be defined by a smaller formula not in $\mathcal{R}$

3 The Reachability Problem for Flat Counter Machines

Formally, a counter machine is a tuple $M = \langle \mathbf{x}, \mathcal{L}, \ell_{init}, \ell_{fin}, \Rightarrow, \Lambda \rangle$, where $\mathbf{x}$ is a set of first-order variables ranging over $\mathbb{Z}$, $\mathcal{L}$ is a set of *control locations*, $\ell_{init}, \ell_{fin} \in \mathcal{L}$ are *initial* and *final* control locations, $\Rightarrow$ is a set of *transition rules* of the form $\ell \overset{R}{\Rightarrow} \ell'$, where $\ell, \ell' \in \mathcal{L}$ are control locations, and $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is a relation, and $\Lambda(\ell \overset{R}{\Rightarrow} \ell')$ gives the class of R. A *loop* is a path in the control graph $\langle \mathcal{L}, \Rightarrow \rangle$ of M, where the source and the destination locations are the same, and every transition rule appears only once. A counter machine is said to be *flat* if and only if every control location is the source/destination of at most one loop. The *binary size* of a counter machine M is $\|M\|_2 = \sum_{\ell \overset{R}{\Rightarrow} \ell'} \|R\|_2^{\Lambda(\ell \overset{R}{\Rightarrow} \ell')}$.

A *configuration* of M is a pair (ℓ, ν), where $\ell \in \mathcal{L}$ is a control location, and $\nu \in \mathbb{Z}^{\mathbf{x}}$ is a valuation of the counters. A *run of M to ℓ* is a sequence of configurations $(\ell_0, \nu_0), \ldots, (\ell_k, \nu_k)$, of length $k \geq 0$, where $\ell_0 = \ell_{init}$, $\ell_k = \ell$, and for each $i = 0, \ldots, k-1$, there exists a transition rule $\ell_i \overset{R_i}{\Rightarrow} \ell_{i+1}$ such that $(\nu_i, \nu_{i+1}) \in R_i$. If ℓ is not specified, we assume $\ell = \ell_{fin}$, and say that the sequence is a *run of M*.

The *reachability problem* asks, given a counter machine M, whether *there exists a run in M?* This problem is, in general, undecidable [18], and it is decidable for flat counter machines whose loops are labeled only with certain, restricted, classes of QFPA relations, such as difference bounds (Def. 7) or octagons (Def. 9). The crux of the decidability proofs in these cases is that the transitive closure of any relation of the above type can be defined in QFPA, and is, moreover, effectively computable (see [6] for an algorithm). The goal of this paper is to provide tight bounds on the complexity of the reachability problem in these decidable cases. The parameter of the decision problem is the binary size of the input counter machine M, i.e. $\|M\|_2$. The following theorem proves decidability of the reachability problem for flat counter machines, under the assumption that the composition L of the relations on every loop in a counter machine has a *QFPA-definable transitive closure*.

Theorem 1 ([8,6,2]). *The reachability problem is decidable for any class of counter machines $\mathcal{M} = \{M$ flat counter machine $\mid$ for all $q \overset{R_1}{\Rightarrow} \ldots \overset{R_n}{\Rightarrow} q$ in M, $(R_1 \circ \ldots \circ R_n)^+$ is QFPA-definable$\}$.*

4 Periodic Relations

We introduce a notion of periodicity on classes of relations that can be naturally represented as matrices. In general, an infinite sequence of integers is said to be *periodic* if the elements of the sequence beyond a certain threshold (prefix), and which are situated at equal distance (period) one from another, differ by the same quantity (rate). This notion of periodicity is lifted to matrices of integers, entry-wise. If R is a periodic relation, the sequence of powers $\{R^k\}_{k \geq 0}$ has an infinite subsequence, that can be captured by a QFPA formula, defining infinitely many powers of the relation.

Example 1. For instance, consider the relation $R \Leftrightarrow x' = y + 1 \wedge y' = x$. This relation is periodic, and we have $R^{2k+1} \Leftrightarrow x' = y + k + 1 \wedge y' = x + k$ and $R^{2k+2} \Leftrightarrow x' = x + k + 1 \wedge y' = y + k + 1$, for all $k \geq 0$.

Definition 2. *An infinite sequence of matrices* $\{A_k \in \mathbb{Z}_\infty^{m\times m}\}_{k=0}^{\infty}$ *is said to be* periodic *if and only if there exist integers* $b, c > 0$ *and matrices* $\Lambda_0, \ldots, \Lambda_{c-1} \in \mathbb{Z}_\infty^{m\times m}$ *such that* $A_{b+(k+1)c+i} = \Lambda_i + A_{b+kc+i}$, *for all* $k \geq 0$ *and* $i \in [c]$.

The smallest integers b, c are called the *prefix* and the *period* of the sequence. The matrices Λ_i, corresponding to the prefix-period pair (b, c), are called the *rates* of the sequence. A relation R is said to be $*$-*consistent* if and only if $R^n \neq \emptyset$, for all $n > 0$.

Definition 3. *A class of relations* $\mathcal{R}$ *is said to be* periodic *iff there exist two functions* $\sigma : \mathcal{R} \to \bigcup_{m>0} \mathbb{Z}_\infty^{m\times m}$ *and* $\rho : \bigcup_{m>0} \mathbb{Z}_\infty^{m\times m} \to \mathcal{R}$, *such that* $\rho(\sigma(\phi)) \Leftrightarrow \phi$, *for each formula* $\phi \in \mathcal{R}$, *and for any* $*$*-consistent relation* R *defined by a formula from* $\mathcal{R}$, *the sequence of matrices* $\{\sigma(R^i)\}_{i\geq 0}$ *is periodic.*

If R is a $*$-consistent relation, the prefix, period $b, c > 0$ and rates $\Lambda_0, \ldots, \Lambda_{c-1} \in \mathbb{Z}^{m\times m}$ of the $\{\sigma(R^i)\}_{i\geq 0}$ sequence are called the *prefix*, *period* and *rates* of R, respectively. Otherwise, if R is not $*$-consistent, we convene that its prefix is the smallest $b > 0$ such that $R^b = \emptyset$, and its period is one. Examples of mappings σ and ρ are given in Section 7.3 for difference bounds relations, and in Section 8.1 for octagonal relations.

Definition 4. *Let* $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ *be a relation. The* closed form *of* R *is the formula* $\widehat{R}(k, \mathbf{x}, \mathbf{x}')$, *where* $k \notin \mathbf{x}$, *such that the formula* $\widehat{R}[n/k]$ *defines* R^n, *for all* $n \geq 0$.

If $\mathcal{R}$ is a class of relations, let $\mathcal{R}[k]$ denote the set of closed forms of relations defined by formulae in $\mathcal{R}$[4]. Let $\mathbb{Z}[k]_\infty^{m\times m}$ be the set of matrices $M[k]$ of univariate linear terms, i.e. $M_{ij} \equiv a_{ij} \cdot k + b_{ij}$, where $a_{ij}, b_{ij} \in \mathbb{Z}$, for all $1 \leq i, j \leq m$ or $M_{ij} = \infty$. In addition to the σ and ρ functions from Def. 3, we consider a function $\pi : \bigcup_{m>0} \mathbb{Z}[k]_\infty^{m\times m} \to \mathcal{R}[k]$, mapping matrices $M[k]$ into formulae $\phi(k, \mathbf{x}, \mathbf{x}')$ such that $\pi(M)[n/k] \Leftrightarrow \rho(M[n/k])$, for all $n \geq 0$. The following lemma characterizes the closed form of a periodic relation, by defining an infinite periodic subsequence of powers of the form $\{R^{kc+b+i}\}_{k\geq 0}$, for some $b, c > 0$ and $i \in [c]$.

Lemma 1. *Let* $\mathcal{R}$ *be a periodic class of relations, and* $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ *be a* $\mathcal{R}$*-definable relation. Let* $b, c > 0$ *be integers, and* Λ_i *be matrices, for all* $i \in [c]$. *Consider the following statements, for all* $k \geq 0$ *and* $i \in [c]$*:*

1. R *is* $*$*-consistent*
2. $\widehat{R}(k \cdot c + b + i) \;\Leftrightarrow\; \pi(k \cdot \Lambda_i + \sigma(R^{b+i}))$
3. $\pi(k \cdot \Lambda_i + \sigma(R^{b+i})) \not\Leftrightarrow \mathbf{false}$
4. $\exists \mathbf{y} \,.\, \pi(k \cdot \Lambda_i + \sigma(R^{b+i}))(\mathbf{x}, \mathbf{y}) \;\wedge\; R^c(\mathbf{y}, \mathbf{x}') \;\Leftrightarrow\; \pi((k+1) \cdot \Lambda_i + \sigma(R^{b+i}))(\mathbf{x}, \mathbf{x}')$

Then (1) and (2) hold if and only if (3) and (4) hold.

[4] The closed form of a QFPA-definable relation can always be defined in first-order arithmetic, using Gödel's encoding of integer sequences, and is not, in general, equivalent to a QFPA formula.

5 Flat Counter Machines with Periodic Loops

For simplicity's sake, consider first the counter machines with the structure below:

$$\ell_{init} \xrightarrow{I(\mathbf{x}')} \overset{R(\mathbf{x},\mathbf{x}')}{\underset{\ell}{\circlearrowright}} \xrightarrow{F(\mathbf{x})} \ell_{fin} \tag{1}$$

where $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is a periodic relation (Def. 3), and $I, F \subseteq \mathbb{Z}^{\mathbf{x}}$ are QFPA-definable sets of valuations. In the following, we give sufficient conditions (Def. 6) under which the reachability problem for the counter machines (1) is NP-complete.

Definition 5. *A class of relations $\mathcal{R}$ is said to be* poly-logarithmic *if and only if there exist integer constants $p, q, r, s > 0$, depending on $\mathcal{R}$, such that, for all $P, Q, R \in \mathcal{R}$:*

1. $\|R^n\|_2 = O(\|R\|_2^p \cdot (\log_2 n)^q)$, *for all* $n > 0$
2. *the composition $P \circ Q$ can be computed in time $O((\|P\|_2 + \|Q\|_2)^r)$*
3. *the consistency $R \not\Rightarrow$ **false** can be checked in time $O(\|R\|_2^s)$*

If $\mathcal{R}$ is a poly-logarithmic class of relations, it is not difficult to see that there exists a constant $d > 0$, depending of $\mathcal{R}$, such that, for any $\mathcal{R}$-definable relation R, the n-th power R^n can be computed by a fast exponentiation algorithm in time $O((\|R\|_2 \cdot \log_2 n)^d)$.

Definition 6. *A class of periodic relations $\mathcal{R}$ is said to be* exponential *if and only if (A) $\mathcal{R}$ is poly-logarithmic, (B) the mappings σ, ρ and π (Def. 3) are computable in PTIME, and (C) for each $\mathcal{R}$-definable relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$:*

1. *there exist integer constants $p, q > 0$, depending on $\mathcal{R}$, such that the prefix and period of R are bounded by $2^{\|R\|_2^p}$ and $2^{\|R\|_2^q}$, respectively*
2. *given $i \in [c]$ and $\Lambda_i = \sigma(R^{b+c+i}) - \sigma(R^{b+i})$, points (3) and (4) of Lemma 1 can be checked in NPTIME($\|R\|_2$)*

The idea of the reduction is to show the existence of a non-deterministic Turing machine (Alg. 1) that produces, in time at most polynomial in the binary size of the input, a QFPA formula, which encodes the reachability question for the given counter machine. If the formula produced by a non-deterministic branch is satisfiable, the reachability question has a positive answer. Otherwise, if no branch of Alg. 1 returns "yes", the reachability question has a negative answer.

Since the formulae produced by Alg. 1 (lines 6 and 13) are of size at most polynomial in the size of the input (1), and that deciding whether a QFPA formula is satisfiable is an NP problem, it turns out that the reachability problem for the counter machines (1) is in NP. The general result is given in Thm. 2, which applies the idea used for single loop counter machines (1) to flat counter machines, in general.

To understand Alg. 1, observe first that the reachability problem for (1) can be stated as the satisfiability of the following formula: $I(\mathbf{x}) \wedge k \geq 0 \wedge \widehat{R}(k, \mathbf{x}, \mathbf{x}') \wedge F(\mathbf{x}')$. Since, in general, the closed form $\widehat{R}(k, \mathbf{x}, \mathbf{x}')$ is not QFPA-definable, we focus on the case where R is a periodic relation (Def. 3). We distinguish two cases. First, if R is not $*$-consistent, i.e. $R^i = \emptyset$ if and only if i is greater or equal than the prefix b of R, the reachability

Algorithm 1. Non-deterministic Algorithm for the Reachability Problem (1)

1: **function** ISREACHABLE(I,R,F)
2: **goto** 8 **or** 3 [guess whether R is $*$-consistent]
3: **choose** $0 < b < 2^{\|R\|_2^p}$
4: **assume** $R^{b-1} \neq \emptyset$ **and** $R^b = \emptyset$ [check that R is not $*$-consistent]
5: **choose** $i \in [b]$
6: **assume** $\exists \mathbf{x} \exists \mathbf{x}' \,.\, I(\mathbf{x}) \wedge R^i(\mathbf{x},\mathbf{x}') \wedge F(\mathbf{x}')$
7: **return** YES
8: **choose** $0 < b < 2^{\|R\|_2^p}$, $0 < c < 2^{\|R\|_2^q}$ **and** $j \in [c]$
9: $\Lambda \leftarrow \sigma(R^{b+c+j}) - \sigma(R^{b+j})$
10: **assume** $\forall k \geq 0 \; \exists \mathbf{x} \exists \mathbf{x}' \,.\, \pi(k \cdot \Lambda + \sigma(R^{b+j}))(\mathbf{x},\mathbf{x}')$ [check that R is $*$-consistent]
11: **assume** $\left(\begin{array}{c} \forall \mathbf{x} \forall \mathbf{x}' \forall k \geq 0 \; [\exists \mathbf{y} \,.\, \pi(k \cdot \Lambda_i + \sigma(R^{b+i}))(\mathbf{x},\mathbf{y}) \; \wedge \; R^c(\mathbf{y},\mathbf{x}')] \\ \Leftrightarrow \pi((k+1) \cdot \Lambda_i + \sigma(R^{b+i}))(\mathbf{x},\mathbf{x}') \end{array} \right)$
12: **choose** $i \in [b]$
13: **assume** $\exists \mathbf{x} \exists \mathbf{x}' \,.\, I(\mathbf{x}) \wedge [R^i(\mathbf{x},\mathbf{x}') \vee (k \geq 0 \wedge \pi(k \cdot \Lambda + \sigma(R^{b+j})))] \wedge F(\mathbf{x}')$
14: **return** YES

problem for (1) is equivalent to the satisfiability of the formula $I(\mathbf{x}) \wedge \left[\bigvee_{i=0}^{b-1} R^i(\mathbf{x},\mathbf{x}')\right] \wedge F(\mathbf{x}')$. Second, if R is $*$-consistent, the reachability problem for (1) is equivalent to the satisfiability of the following formula:

$$I(\mathbf{x}) \wedge \Big[\underbrace{\bigvee_{i=0}^{b-1} R^i(\mathbf{x},\mathbf{x}')}_{\text{prefix}} \vee \underbrace{\bigvee_{j=0}^{c-1} k \geq 0 \wedge \pi(k \cdot \Lambda_j + \sigma(R^{b+j}))}_{\text{period}} \Big] \wedge F(\mathbf{x}') \tag{2}$$

where $b,c > 0$ are integers, and $\Lambda_0, \ldots, \Lambda_{c-1}$ are matrices meeting the conditions of the second point of Lemma 1. The first disjunct above takes care of the case when the number of iterations of the loop is smaller than the prefix b, and the second one deals with the other case, when $kc+b+j$ iterations of the loop are needed, for some $k \geq 0$ and $j \in [c]$.

The first guess of Alg. 1 is whether R is $*$-consistent or not (line 2). If the guess was that R is not $*$-consistent, Alg. 1 guesses further a positive constant b, bounded by $2^{\|R\|_2^p}$, where $p > 0$ depends on the class $\mathcal{R}$ (line 3). Then it checks that b is the prefix of R, by computing R^{b-1} and R^b, and checking that $R^{b-1} \neq \emptyset$ and $R^b = \emptyset$ (line 4). By Def. 5, this check can be done in PTIME($\|R\|_2$). If the prefix check (line 4) is successful, the reachability problem can be encoded in QFPA by further guessing $i \in [B]$, and producing the QFPA formula $I(\mathbf{x}) \wedge R^i(\mathbf{x},\mathbf{x}') \wedge F(\mathbf{x}')$ (line 6). Since $\mathcal{R}$ is a poly-logarithmic class, $\|R^i\|_2 = O(\|R\|_2^r \cdot (\log_2 i)^s) = O(\|R\|_2^{r+s})$, for some $r,s > 0$, depending on $\mathcal{R}$. Thus, the binary size of this formula is polynomial in $\|I\|_2 + \|R\|_2 + \|F\|_2$, and the reachability problem, can be answered in NPTIME($\|R\|_2 + \|I\|_2 + \|F\|_2$), by checking satisfiability of this formula (line 6).

If, on the other hand, the first guess was that R is $*$-consistent, then Alg. 1 will further guess constants $0 < b < 2^{\|R\|_2^p}$ and $0 < c < 2^{\|R\|_2^q}$, for some constants $p,q > 0$ depending on $\mathcal{R}$, and $j \in [c]$ (line 8). Next, it computes the powers R^{b+j} and R^{b+c+j} in

PTIME($\|R\|_2$), using fast exponentiation, and lets $\Lambda = \sigma(R^{b+c+j}) - \sigma(R^{b+j})$. Clearly, the binary size of Λ is bounded by a polynomial in $\|R\|_2$. Further, the algorithm needs to check whether the choices of b, c, j and Λ where adequate for defining the closed form of the infinite sequence of powers $\{R^{c\cdot k+b+j}\}_{k\geq 0}$, using Lemma 1. Moreover, it also needs to check the initial guess that R is $*$-consistent, using this closed form. To this end, it must check the points (3) and (4) of Lemma 1, which by Def. 6 (point C.2) can be done in NPTIME($\|R\|_2$) (lines 10 and 11 of Alg. 1, respectively). Next, Alg. 1 outputs a QFPA formula encoding the reachability problem, using the closed form for the sequence $\{R^{c\cdot k+b+j}\}_{k\geq 0}$ (line 13). The size of this formula is polynomial in $\|I\|_2 + \|R\|_2 + \|F\|_2$, and its satisfiability status, and thus the reachability problem for the counter machine (1), can be decided in NPTIME($\|I\|_2 + \|R\|_2 + \|F\|_2$).

It is not difficult to see that the reachability problem for (1) is NP-hard, by reduction from the satisfiability problem for QFPA [22]: let $I(\mathbf{x})$ be any QFPA formula over $\mathbf{x}$, $R = \mathbf{false}$ and $F = \mathbf{true}$. Then q_f is reachable from q_i if and only if $I(\mathbf{x})$ is satisfiable. The following theorem generalizes the proof from (1) to general flat counter machines.

Theorem 2. *If $\mathcal{R}$ is a periodic exponential class of relations, the reachability problem for the class $\mathcal{M}_{\mathcal{R}} = \{M$ flat counter machine $|$ for all rules $q \overset{R}{\Rightarrow} q'$ on a loop of M, R is $\mathcal{R}$-definable$\}$ is NP-complete.*

6 The Periodicity of Tropical Matrix Powers

Weighted graphs are central to the upcoming developments. The main intuition is that the sequence of matrices representing the powers of a difference bounds relation captures *minimal weight paths* of lengths $1, 2, 3\ldots$ in a weighted graph. Formally, a *weighted digraph* is a tuple $G = \langle V, E, w\rangle$, where V is a set of vertices, $E \subseteq V \times V$ is a set of edges, and $w : E \to \mathbb{Z}$ is a weight function. A path π in G is said to be *elementary* if all vertices on π are distinct, except for the first and last vertex, which may be the same. For a path π, we denote its length by $|\pi|$, and its weight (the sum of the weights of all edges on π) by $w(\pi)$. The *average weight* of π is defined as $\overline{w}(\pi) = \frac{w(\pi)}{|\pi|}$. We assume that the reader is familiar with the notion of strongly connected component (SCC). A cycle is said to be *critical* if it has minimal average weight among all cycles in its SCC. The *cyclicity* of a SCC is the greatest common divisor of the lengths of all its elementary critical cycles, or 1, if the SCC contains no cycles.

Let $A \in \mathbb{Z}_\infty^{m\times m}$ be a square matrix, and G be any weighted graph, such that A is the incidence matrix of G. Let $(A \boxtimes B)_{ij} = \min_{k=1}^{m}(a_{ik} + b_{kj})$ denote the tropical product of A and B, $A^{\boxtimes 1} = A$ and $A^{\boxtimes k+1} = A^{\boxtimes k} \boxtimes A$, for all $k > 0$. The sequence $\{A^{\boxtimes k}\}_{k=1}^{\infty}$ of tropical powers of A gives the minimal weights of the paths of lengths $k = 1, 2, \ldots$ between any two vertices in G. The following theorem shows that any sequence of tropical matrix powers is periodic, and provides an accurate characterization of its period.

Theorem 3 ([21]). *Let $A \in \mathbb{Z}_\infty^{m\times m}$ be a matrix, $G = \langle V, E, w\rangle$ be a weighted graph whose incidence matrix is A, and $W_1, \ldots, W_n$ be the partition of G in strongly connected components. The sequence $\{A^{\boxtimes k}\}_{k=1}^{\infty}$ is periodic, and its period is $lcm(c_1, \ldots, c_n)$, where $c_1, \ldots, c_n$ are the cyclicities of $W_1, \ldots, W_n$, respectively.*

The above theorem does not give an estimate on the prefix of the sequence, which is carried out by the following theorem:

Theorem 4. *Given a matrix $A \in \mathbb{Z}_\infty^{m\times m}$, the sequence $\{A^{\boxtimes k}\}_{k=1}^{\infty}$ is periodic with prefix at most* $\max(m^4, 4\cdot M\cdot m^6)$*, where* $M = \max\{abs(A_{ij}) \mid 1 \le i,j \le m, A_{ij} < \infty\}$.

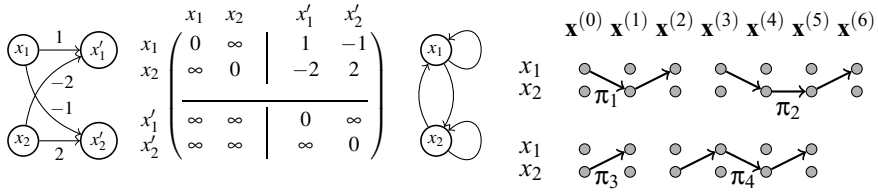
Notice that if A has only 0 and ∞ entries, then $M = 0$ and the prefix depends only on m.

7 Difference Bounds Relations

In the rest of this section, let $\mathbf{x} = \{x_1, x_2, ..., x_N\}$ be a set of variables ranging over $\mathbb{Z}$.

Definition 7. *A formula $\phi(\mathbf{x})$ is a* difference bounds constraint *if it is a finite conjunction of atomic propositions of the form $x_i - x_j \le \alpha_{ij}$, $1 \le i,j \le N$, where $\alpha_{ij} \in \mathbb{Z}$. A relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is a* difference bounds relation *if it can be defined by a difference bounds constraint $\phi_R(\mathbf{x}, \mathbf{x}')$. The class of difference bounds relations is denoted by $\mathcal{R}_{DB}$.*

Difference bounds constraints are represented either as matrices or as graphs. If $\phi(\mathbf{x})$ is a difference bounds constraint, then a *difference bounds matrix* (DBM) representing ϕ is an $N \times N$ matrix M_ϕ such that $(M_\phi)_{ij} = \alpha_{ij}$ if $x_i - x_j \le \alpha_{ij} \in Atom(\phi)$, and $(M_\phi)_{ij} = \infty$, otherwise. The *constraint graph* $\mathcal{G}_\phi = \langle \mathbf{x}, \rightarrow \rangle$ is a weighted graph, where each vertex corresponds to a variable, and there is an edge $x_i \xrightarrow{\alpha_{ij}} x_j$ in $\mathcal{G}_\phi$ if and only if there exists a constraint $x_i - x_j \le \alpha_{ij}$ in ϕ (Fig. 1(a)). Clearly, M_ϕ is the incidence matrix of $\mathcal{G}_\phi$. If R is a difference bounds relation defined by the difference bounds constraint $\phi_R(\mathbf{x}, \mathbf{x}')$, the *folded graph* of R is the graph $\mathcal{G}_R^f = \langle \mathbf{x}, \xrightarrow{f} \rangle$, which has an edge $x_i \xrightarrow{f} x_j$ whenever $x_i \xrightarrow{\alpha} x_j$, $x_i \xrightarrow{\alpha} x'_j$, $x'_i \xrightarrow{\alpha} x_j$, or $x'_i \xrightarrow{\alpha} x'_j$ in $\mathcal{G}_R$. For any two variables $x_i, x_j \in \mathbf{x}$, we write $x_i \sim_R x_j$ whenever x_i and x_j belong to the same SCC of $\mathcal{G}_R^f$ (Fig. 1(c)). If $M \in \mathbb{Z}_\infty^{N\times N}$ is



(a) $\mathcal{G}_R$ (b) M_R^* (c) $\mathcal{G}_R^f$ (d) z-paths in $\mathcal{G}_R^\omega$

Fig. 1. Let $R(x_1, x_2, x'_1, x'_2) \Leftrightarrow x_1 - x'_1 \le 1 \wedge x_1 - x'_2 \le -1 \wedge x_2 - x'_1 \le -2 \wedge x_2 - x'_2 \le 2$ be a difference bounds relation. **(a)** shows the graph representation $\mathcal{G}_R$, **(b)** the closed DBM representation of R, and **(c)** the folded graph of $\mathcal{G}_R$, where $x_1 \sim_R x_2$. **(d)** shows several odd forward z-paths: π_1 (essential and repeating), π_2 (repeating), π_3 (essential) and $\pi_4 = \pi_3.\pi_1$ (neither essential nor repeating).

a DBM, we define[5]:

$$\Phi_M^{uu} \equiv \bigwedge_{M_{ij}<\infty} x_i - x_j \leq M_{ij} \qquad \Phi_M^{pu} \equiv \bigwedge_{M_{ij}<\infty} x'_i - x_j \leq M_{ij}$$
$$\Phi_M^{up} \equiv \bigwedge_{M_{ij}<\infty} x_i - x'_j \leq M_{ij} \qquad \Phi_M^{pp} \equiv \bigwedge_{M_{ij}<\infty} x'_i - x'_j \leq M_{ij}$$

A DBM M is said to be *consistent* if and only if Φ_M^{uu} is consistent. A consistent difference bounds matrix $M \in \mathbb{Z}_\infty^{N\times N}$ is said to be *closed* if $M_{ii} = 0$, for all $1 \leq i \leq N$, and all triangle inequalities $M_{ik} \leq M_{ij} + M_{jk}$ hold, for all $1 \leq i,j,k \leq N$. Given a consistent DBM M, the (unique) closed DBM which is logically equivalent to M is denoted by M^* (Fig. 1(b)). It is well known that difference bounds constraints have quantifier elimination[6], and are thus closed under relational composition.

Lemma 2. *The class $\mathcal{R}_{DB}$ is poly-logarithmic.*

7.1 Zigzag Automata

Zigzag automata have been used in the proof of Presburger definability of transitive closures [8], and of periodicity [6], for difference bounds and octagonal relations. They are needed here for showing that difference bounds relations are exponential (Def. 6). 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 difference bounds relation, with constraint graph $\mathcal{G}_R$. Let $\Sigma_R = 2^{\mathcal{G}_R}$ denote the set of subgraphs of $\mathcal{G}_R$. A *finite word* of length $n \geq 0$ over Σ_R is a mapping $w : [n] \to \Sigma_R$. The notion of finite words over Σ_R extends naturally to infinite words $w : \mathbb{N} \to \Sigma_R$, and to bi-infinite words $w : \mathbb{Z} \to \Sigma_R$. The concatenation of two finite words $w : [n] \to \Sigma_R$ and $w' : [m] \to \Sigma_R$ is a word $w \cdot w' : [n+m] \to \Sigma_R$, defined as $(w \cdot w')(i) = w(i)$, for all $0 \leq i < n$ and $(w \cdot w')(i) = w'(i-n)$, for all $n \leq i < n+m$. The set of finite words is denoted Σ_R^*. For a finite word $w : [n] \to \Sigma_R$, we denote by ${}^{\omega}w^{\omega}$ its bi-infinite iteration, i.e. ${}^{\omega}w^{\omega}(i) = w(i \mod n)$ for all $i \in \mathbb{Z}$. For example, Fig. 2(a) shows the constraint graph $\mathcal{G}_R$ of a difference bounds relation R, and Fig. 2(b) shows several symbols $\gamma_1, \ldots, \gamma_9 \in \Sigma_R$. We associate with every finite word $w : [n] \to \Sigma$ a graph $\mathcal{H}_w = (\bigcup_{i=0}^{n} \mathbf{x}^{(i)}, \to)$, where $\mathbf{x}^{(i)} = \{x^{(i)} \mid x \in \mathbf{x}\}$, and:

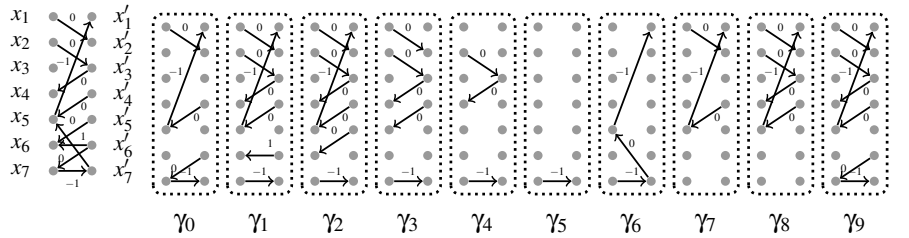
- $x_k^{(i)} \xrightarrow{\alpha} x_\ell^{(i+1)}$ in $\mathcal{H}_w$ if and only if $x_k \xrightarrow{\alpha} x'_\ell$ in $w(i)$
- $x_k^{(i+1)} \xrightarrow{\alpha} x_\ell^{(i)}$ in $\mathcal{H}_w$ if and only if $x'_k \xrightarrow{\alpha} x_\ell$ in $w(i)$

for all $1 \leq k, \ell \leq N$ and for all $0 \leq i < n$. For example, Fig. 2(c) shows the graph $\mathcal{H}_v$ corresponding to the word $v = \gamma_0.\gamma_1^2.\gamma_2.\gamma_3.\gamma_4.\gamma_5^3.\gamma_6.\gamma_7.\gamma_8^3.\gamma_9.\gamma_1.\gamma_2.\gamma_3.\gamma_4$. This notation is extended to bi-infinite words, in the obvious way. In the following, we abuse notation and denote the graph $\mathcal{H}_{\omega_{\mathcal{G}_R}\omega}$, corresponding to the bi-infinite iteration of $\mathcal{G}_R$, by ${}^{\omega}\mathcal{G}_R{}^{\omega}$.

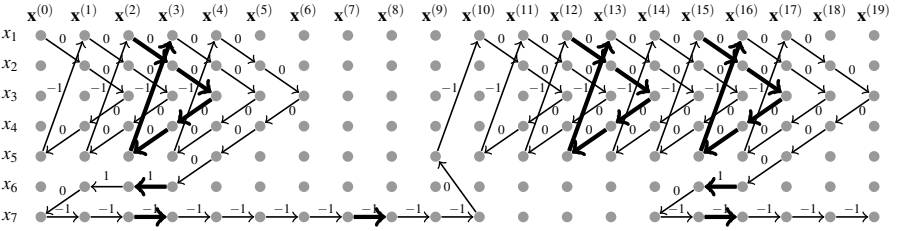
A word $w : [n] \to \Sigma_R$ is said to be *valid* if and only if each vertex of $\mathcal{H}_w$ has in-degree and out-degree at most one, and the in-degree and out-degree of each vertex from the set $\{x_k^{(i)} \mid i = 1, \ldots, n-1\}$ are equal. It is easy to see that the word v from Fig. 2(c) is valid, by inspection of the graph $\mathcal{H}_v$. The notion of validity extends from finite to bi-infinite words, in the obvious way.

[5] The superscripts u and p stand for *unprimed* and *primed*, respectively.

[6] The quantifier elimination procedure relies on the classical Floyd-Warshall closure algorithm.



(a) $\mathcal{G}_R$ (b) Symbols of the zigzag alphabet Σ_R.

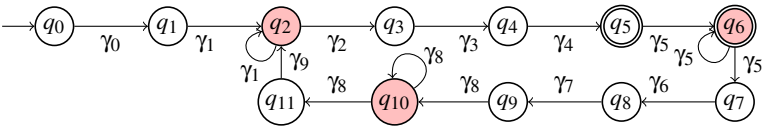


(c) A fitting odd forward z-path from $x_1^{(0)}$ to $x_7^{(19)}$ in $\mathcal{H}_{\gamma_0\cdot\gamma_1^2\cdot\gamma_2\cdot\gamma_3\cdot\gamma_4\cdot\gamma_5^3\cdot\gamma_6\cdot\gamma_7\cdot\gamma_8^3\cdot\gamma_9\cdot\gamma_1\cdot\gamma_2\cdot\gamma_3\cdot\gamma_4}$.

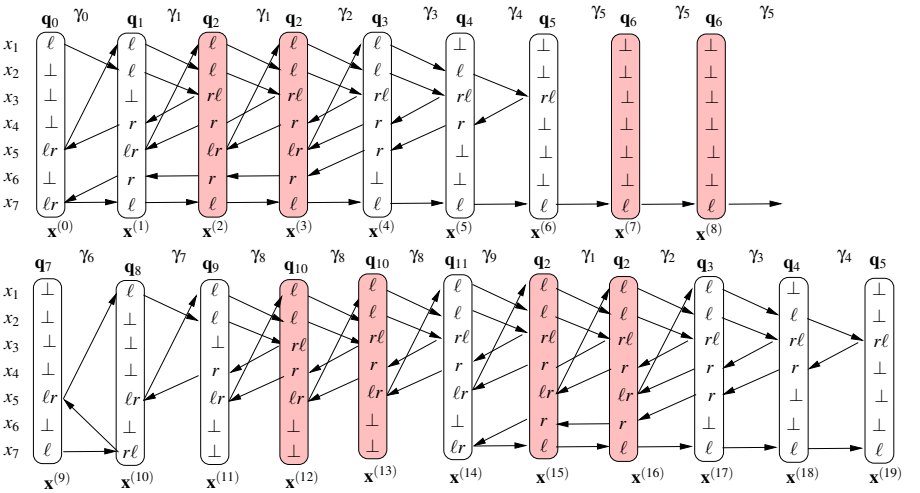
Fig. 2. Zigzag alphabet and a path in the unfolded constraint graph of a difference bounds relation $R \equiv x_1 - x'_2 \leq 0 \wedge x_2 - x'_3 \leq 0 \wedge x'_3 - x_4 \leq 0 \wedge x'_4 - x_5 \leq 0 \wedge x'_5 - x_6 \leq 0 \wedge x'_6 - x_6 \leq 1 \wedge x'_6 - x_7 \leq 0 \wedge x_7 - x'_7 \leq -1 \wedge x'_7 - x_5 \leq 0 \wedge x_5 - x'_1 \leq -1$

Given a difference bounds relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$, the set of valid finite words in Σ_R^+ is recognizable by a finite weighted automaton, called a *zigzag automaton* in the following. Let $T_R = \langle Q, \Delta, \omega \rangle$ be a weighted graph[7], called the *transition table* of the zigzag automata over Σ_R, where $Q = \{\ell, r, \ell r, r\ell, \bot\}^N$ is a set of states, $\Delta : Q \times \Sigma_R \to Q$ is a transition mapping, and $\omega : \Sigma_R \to \mathbb{Z}_\infty$ is a weight function. Intuitively, a state $\mathbf{q} = \langle \mathbf{q}_{\langle 1 \rangle}, \ldots, \mathbf{q}_{\langle N \rangle} \rangle \in Q$ describes a vertical cut in a word, as follows: for each $i = 1, \ldots, N$, $\mathbf{q}_{\langle i \rangle} = \ell$ ($\mathbf{q}_{\langle i \rangle} = r$) if there is a path in the word which traverses the cut at position i form *left* to right (*right* to left), $\mathbf{q}_{\langle i \rangle} = \ell r$ ($\mathbf{q}_{\langle i \rangle} = r\ell$) if there is a path from the right (left), which bounces to the *right* (*left*) at position i, and $\mathbf{q}_{\langle i \rangle} = \bot$ if no path in the word traverses the cut at position i (see Fig. 2(c) for an intuitive example). The transition function Δ ensures that the (local) validity condition is met. More precisely, each path $\rho : \mathbf{q}_0 \xrightarrow{\gamma_1} \mathbf{q}_1 \xrightarrow{\gamma_2} \ldots \xrightarrow{\gamma_k} \mathbf{q}_k$ in T_R, between two arbitrary states $\mathbf{q}_0, \mathbf{q}_k \in Q$, recognizes a valid word denoted as $\mathcal{G}_\rho = \gamma_1 \cdot \ldots \cdot \gamma_k$. The weight $\omega(\gamma)$ of a graph $\gamma \in \Sigma_R$ is the sum of the weights of its edges, and the weight of a path is $\omega(\rho) = \sum_{i=1}^{k} \omega(\gamma_i)$. Finally, a *zigzag automaton* is a tuple $A = \langle T_R, I, F \rangle$, where $I, F \subseteq Q$ are sets of initial and final states, respectively. We denote the *language* of A as $\mathcal{L}(A) = \{ \mathcal{G}_\rho \mid q_i \stackrel{\rho}{\Rightarrow} q_f, q_i \in I, q_f \in F \}$. For example, the zigzag automaton depicted in Fig. 3(a), with initial state q_0 and final state q_6 has a run over the word $\gamma_0 \cdot \gamma_1^2 \cdot \gamma_2 \cdot \gamma_3 \cdot \gamma_4 \cdot \gamma_5^3 \cdot \gamma_6 \cdot \gamma_7 \cdot \gamma_8^2 \cdot \gamma_9 \cdot \gamma_2 \cdot \gamma_3 \cdot \gamma_4$ (see Fig. 2(c)),

[7] For reasons of presentation, we differ slightly from the definition of a weighted graph given in the previous section – here the weight of an edge is associated with the symbol labeling that edge.



(a) The zigzag automaton $A^{of}_{1,7}$ recognizing odd forward z-paths from x_1 to x_7.



(b) A run of A^{of}_{17} over $\gamma_0.\gamma_1^2.\gamma_2.\gamma_3.\gamma_4.\gamma_5^3.\gamma_6.\gamma_7.\gamma_8^3.\gamma_9.\gamma_1.\gamma_2.\gamma_3.\gamma_4$ (Fig. 2(c))

Fig. 3. Zigzag automaton for the difference bounds relation $R \equiv x_1 - x'_2 \leq 0 \wedge x_2 - x'_3 \leq 0 \wedge x'_3 - x_4 \leq 0 \wedge x'_4 - x_5 \leq 0 \wedge x'_5 - x_6 \leq 0 \wedge x'_6 - x_6 \leq 1 \wedge x'_6 - x_7 \leq 0 \wedge x_7 - x'_7 \leq -1 \wedge x'_7 - x_5 \leq 0 \wedge x_5 - x'_1 \leq -1$ and an example of its run (Fig. 2 contd.)

depicted in Fig. 3(b). A detailed definition of zigzag automata can be found in [8]. For the purposes of the upcoming developments, we rely on the example in Fig. 3 to give the necessary intuition.

Remark 1. The transition table $T_R = \langle Q, \Delta, \omega \rangle$ of a difference bounds relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ has at most $5^{\mathrm{card}(\mathbf{x})}$ vertices, since $Q = \{\ell, r, \ell r, r\ell, \bot\}^{\mathrm{card}(\mathbf{x})}$ is a possible representation of the set of states [8].

7.2 Paths Recognizable by Zigzag Automata

This section studies the paths that occur within the words recognizable by zigzag automata. Consider the bi-infinite unfolding of $\mathcal{G}_R$, denoted as ${}^{\omega}\mathcal{G}^{\omega}_R$. A finite path $\rho : x^{(j_1)}_{i_1} \xrightarrow{\alpha_1} x^{(j_2)}_{i_2} \xrightarrow{\alpha_2} \ldots x^{(j_{k-1})}_{i_{k-1}} \xrightarrow{\alpha_{k-1}} x^{(j_k)}_{i_k}$ in ${}^{\omega}\mathcal{G}^{\omega}_R$, for $j_1, \ldots, j_k \in \mathbb{Z}$ is said to be a *z-path* whenever, for all $1 \leq p < q \leq k$, $i_p = i_q$ and $j_p = j_q$ only if $p = 1$ and $q = k$. See Fig. 1(d) or Fig. 2(c) for examples of z-paths. We say that a variable x_{i_s} *occurs* on ρ at position j_s, for all $1 \leq s \leq k$. A z-path is called a *z-cycle* if $i_1 = i_k$ and $j_1 = j_k$. A z-path is said to be *odd* if $j_1 \neq j_k$ and *even* otherwise. For instance, in

Fig. 2(c), the z-path $x_1^{(1)} \xrightarrow{0} x_2^{(2)} \xrightarrow{0} x_3^{(3)} \xrightarrow{0} x_4^{(2)} \xrightarrow{0} x_5^{(1)} \xrightarrow{-1} x_1^{(2)}$ is an odd z-path, while $x_1^{(1)} \xrightarrow{0} x_2^{(2)} \xrightarrow{0} x_3^{(3)} \xrightarrow{0} x_4^{(2)} \xrightarrow{0} x_5^{(1)}$ is an even z-path. We denote by $\|\rho\| = \mathrm{abs}(j_k - j_1)$ its *relative* length, by $w(\rho) = \sum_{i=1}^{k-1} \alpha_i$ its *weight*, and by $\overline{\overline{w}}(\rho) = \frac{w(\rho)}{\|\rho\|}$ its *relative weight*. We write $vars(\rho)$ for the set $\{x_{i_1}, \ldots, x_{i_k}\}$ of variables occurring within ρ, called the *support set* of ρ.

An even z-path is said to be *forward* if $j_1 = j_k = \min(j_1, \ldots, j_k)$ and *backward* if $j_1 = j_k = \max(j_1, \ldots, j_k)$. An even z-path is said to be *fitting* if it is either forward or backward. An odd z-path is said to be *forward* if $j_1 < j_k$ and *backward* if $j_1 > j_k$. An odd forward (backward) z-path is said to be *fitting* if $j_1 = \min(j_1, \ldots, j_k)$ and $j_k = \max(j_1, \ldots, j_k)$ ($j_1 = \max(j_1, \ldots, j_k)$ and $j_k = \min(j_1, \ldots, j_k)$). We say that a fitting z-path ρ is *encoded* by a word w, if and only if w consists of nothing but ρ and several z-cycles not intersecting with ρ. Let $Enc(w)$ be the set of z-paths encoded by a word (this set is either a singleton or the empty set), and $Enc(\mathcal{L}) = \bigcup_{w \in \mathcal{L}} Enc(w)$ for any set of words $\mathcal{L} \subseteq \Sigma_R^*$. For instance, the word $\gamma_0.\gamma_1^2.\gamma_2.\gamma_3.\gamma_4.\gamma_5^3.\gamma_6.\gamma_7.\gamma_8^3.\gamma_9.\gamma_1.\gamma_2.\gamma_3.\gamma_4$ encodes the z-path $x_1^{(0)} \to \ldots \to x_7^{(19)}$ from in Fig. 2(c).

Theorem 5 ([8]). *Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a $*$-consistent difference bounds relation, where $\mathbf{x} = \{x_1, \ldots, x_N\}$, and $\mathcal{G}_R$ be its corresponding constraint graph. Then, for every $x_i, x_j \in \mathbf{x}$, there exist zigzag automata*[8] *$A_{ij}^{\bullet} = \langle T_R, I_{ij}^{\bullet}, F_{ij}^{\bullet} \rangle$, $\bullet \in \{ef, eb, of, ob\}$, where $T_R = \langle Q, \Delta, \omega \rangle$, such that $Enc(\mathcal{L}(A_{ij}^{\bullet}))$ are the sets of fitting even/odd, forward/backward z-paths, starting with $x_i^{(k)}$ and ending with $x_j^{(\ell)}$, respectively, for some $k, \ell \in \mathbb{Z}$. Moreover, for each fitting z-path ρ, $\omega(\rho) = \min\{\omega(\gamma) \mid \gamma \in \mathcal{L}(A_{ij}^{ef}) \cup \mathcal{L}(A_{ij}^{eb}) \cup \mathcal{L}(A_{ij}^{of}) \cup \mathcal{L}(A_{ij}^{ob}), \rho \in Enc(\gamma)\}$.*

In the following, we denote the concatenation of two z-paths π and ρ by $\pi.\rho$. Notice that $\pi.\rho$ is defined only if the last variable from the first z-path equals the first variable from the second z-path, and the two z-paths do not intersect in some vertex which occurs in the middle of one of them. A z-path π is said to be *repeating* if and only if the i-times concatenation of π with itself, denoted π^i, is defined, for any $i > 0$. If π is repeating, then it clearly starts and ends with the same variable, and is necessarily odd. A repeating z-path is said to be *essential* if all variables occurring on the path are distinct, with the exception of the first and last, which must be equal. The concatenation of an essential repeating z-path with itself several times is called an *essential power*. For instance, in Fig. 1(d) the z-path π_1 is essential and repeating, while π_2 is repeating but not essential. For a repeating z-path π, we denote by ${}^{\omega}\pi^{\omega}$ the bi-infinite concatenation of π with itself.

7.3 The Complexity of Acceleration for Difference Bounds Relations

In this section, we prove that difference bounds constraints induce a periodic exponential class of relations (Def. 6). First, we recall that difference bounds relations are periodic (Def. 3) [6]. If $R \subseteq \mathbb{Z}^N \times \mathbb{Z}^N$ is a difference bounds relation, let $\sigma(R) \equiv M_R$ and,

[8] Superscripts ef, eb, of and ob stand for *even forward, even backward, odd forward* and *odd backward*, respectively.

for each $M \in \mathbb{Z}_{\infty}^{2N\times 2N}$, let ${}^{\blacksquare}M$, ${}_{\blacksquare}M$, $M^{\blacksquare}$, $M_{\blacksquare} \in \mathbb{Z}^{N\times N}$ denote its top-left, bottom-left, top-right and bottom-right corners, respectively. Intuitively, ${}^{\blacksquare}M$, ${}_{\blacksquare}M$, $M^{\blacksquare}$, $M_{\blacksquare}$ capture constraints of the forms $x_i - x_j \leq c$, $x'_i - x_j \leq c$, $x_i - x'_j \leq c$ and $x'_i - x'_j \leq c$, respectively (see Fig. 1(b)). We define $\rho(M) \equiv \Phi^{uu}_{{}^{\blacksquare}M} \wedge \Phi^{up}_{M^{\blacksquare}} \wedge \Phi^{pu}_{{}_{\blacksquare}M} \wedge \Phi^{pp}_{M_{\blacksquare}}$. If $M \in \mathbb{Z}[k]_{\infty}^{2N\times 2N}$ is a matrix of univariate linear terms in k, $\pi(M)(k,\mathbf{x},\mathbf{x}')$ is defined analogously to ρ.

With these definitions, it was shown in [6], that the class of difference bounds relations is periodic (Def. 3). The reason is that the sequence of difference bounds matrices $\{M_{R^i}\}_{i=1}^{\infty}$ corresponding to the powers of a relation R is a pointwise projection of the sequence of tropical powers $\{\mathcal{M}_R^{\boxtimes i}\}_{i=1}^{\infty}$ of the incidence matrix $\mathcal{M}_R$ of the transition table T_R. By Thm. 3, any sequence of tropical powers of a matrix is periodic, which entails the periodicity of the difference bounds relation R. Recall that the number of vertices in T_R is $5^N = 2^{O(N)}$. Consequently, the prefix of a difference bounds relation can be bounded using Thm. 4:

Lemma 3. *The prefix of a difference bounds relation $R \subseteq \mathbb{Z}^N \times \mathbb{Z}^N$ is $2^{O(\|R\|_2)}$.*

A preliminary estimation of the upper bound of the period of a difference bounds relation $R \subseteq \mathbb{Z}^N \times \mathbb{Z}^N$ can be already done using Thm. 3. Since the size of the transition table T_R of the zigzag automata for R is bounded by 5^N, by definition, the cyclicity of any SCC of T_R is at most 5^N, hence, by Thm. 3, the period is bounded by $lcm(1,\ldots,5^N)$. Applying the following lemma, one shows immediately that the period is $2^{2^{O(N)}}$.

Lemma 4. *For each $n \geq 1$, $lcm(1,\ldots,n) = 2^{O(n)}$.*

We next improve the bound on periods to simply exponential (Thm. 6).

Theorem 6. *The period of a difference bounds relation $R \subseteq \mathbb{Z}^N \times \mathbb{Z}^N$ is $2^{O(N)}$.*

This leads to one of the main results of the paper:

Theorem 7. *The class $\mathcal{R}_{DB}$ is exponential, and the reachability problem for the class $\mathcal{M}_{DB} = \{M \text{ flat counter machine} \mid \text{for all } q \overset{R}{\Rightarrow} q' \text{ on a loop of } M, R \text{ is } \mathcal{R}_{DB}\text{-definable}\}$ is NP-complete.*

Before proceeding with the technical developments, we summarize the proof idea of Thm 6. Let T_R be the transition table of the zigzag automata for the difference bounds relation $R \subseteq \mathbb{Z}^N \times \mathbb{Z}^N$, and let $\mathcal{M}_R$ be its incidence matrix. The main idea is that each non-trivial SCC of T_R, which intersects a path between an initial and a final state of a zigzag automaton, contains a *critical elementary cycle* λ, whose length divides $lcm(1,\ldots,N)$. Then the cyclicity of the SCC containing λ is, by definition, the greatest common divisor of the lengths of all critical elementary cycles of the SCC, and consequently, a divisor of $lcm(1,\ldots,N)$ as well. Since this holds for any non-trivial SCC in T_R, by Thm. 3, the period of the sequence $\{\mathcal{M}_R^{\boxtimes k}\}_{k=1}^{\infty}$ of tropical powers of $\mathcal{M}_R$ is also a divisor of $lcm(1,\ldots,N)$, which is of the order of $2^{O(N)}$ (Lemma 4).

It remains to prove the existence, in each non-trivial SCC of T_R, of an elementary critical cycle of length which divides $lcm(1,\ldots,N)$. The proof consists of several steps:

1. Let $q \xrightarrow{\gamma} q$ be a critical cycle of T_R. Intuitively, a sufficiently long iteration of γ will exhibit a word z, consisting of *repeating z-paths* (and possibly several cycles), such that $\overline{w}(z) = \overline{w}(\gamma)$.

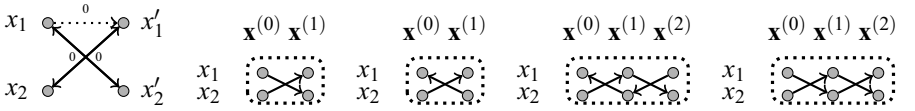
2. We define an equivalence relation on repeating z-paths (Def. 8), and define a word μ, which is obtained from z by keeping only one representative per equivalence class. Moreover, we have $\overline{w}(\mu) \leq \overline{w}(z)$ (Lemma 5), and we show that it is possible to connect μ to z both left and right, via some connecting words η and ξ, thus obtaining a valid word $z^m.\eta.\mu^n.\xi.z^p$, for every $m,n,p > 0$ (Lemma 6).
3. The word μ is further used to define a word λ, consisting only of essential powers $\pi_1^{n_1},\ldots,\pi_k^{n_k}$, where $|\pi_i| \leq N$, for all $i = 1,\ldots,k$ such that $\overline{w}(\lambda) \leq \overline{w}(\mu)$, and there exist words σ and τ, such that $\mu^q.\sigma.\lambda^r.\tau.\mu^s$ is a valid word, for all $q,r,s > 0$. Moreover, $|\lambda|$ divides $lcm(|\pi_1|,\ldots,|\pi_k|)$, and, since λ consists of essential powers $|\pi_i| \leq N$, for all $i = 1,\ldots,k$. Hence $|\lambda|$ divides $lcm(1,\ldots,N)$.
4. Finally, for sufficiently large $m,n,p,q,r > 0$, the word $z^m.\eta.\mu^n.\sigma.\lambda^p.\tau.\mu^q.\xi.z^r$ is mapped back into a path of the form: $q \to \ell \xrightarrow{\lambda} \ell \to q$, which traverses a cycle from the same SCC as the initial cycle $q \xrightarrow{\gamma} q$ (Lemma 7).

Multipaths and Reducts. A *multipath* is a (possibly empty) finite set of z-paths from ${}^{\omega}\mathcal{G}_R{}^{\omega}$, which all start and end on the same positions (see Fig. 4). Formally, a multipath $\mu = \{\pi_1,\ldots,\pi_n\}$ is a set of z-paths such that there exist integers $k < \ell$ such that, for all $i = 1,\ldots,n$, either (i) π_i is a forward (backward) odd z-path from k to ℓ (from ℓ to k), (ii) π_i is an even z-path from k to k (ℓ to ℓ), or (iii) π_i is a z-cycle whose set of positions of variable occurrences is included in the interval $[k,\ell]$, and (iv) no two z-paths in μ intersect each other. The relative length of a multipath μ, is defined as $\|\mu\| = \ell - k$ if $\mu \neq \emptyset$, or $\|\mu\| = 0$ if $\mu = \emptyset$.

For a multipath μ, we denote by μ^{ac} the set of acyclic z-paths in μ. The weight of μ is defined as $w(\mu) = \sum_{\pi\in\mu}^{n} w(\pi)$, and its average weight is $\overline{\overline{w}}(\mu) = \frac{w(\mu)}{\|\mu\|}$ if $\|\mu\| \neq 0$, or $\overline{\overline{w}}(\mu) = 0$ if $\|\mu\| = 0$. The support set of a multipath is denoted as $vars(\mu) = \bigcup_{\pi\in\mu} vars(\pi)$. The concatenation $\mu_1.\mu_2$ of two multipaths μ_1 and μ_2 is defined as the union of the two graphs, only if the result is a valid multipath. A multipath μ is *iterable* if it can be concatenated with itself any number of times, i.e. μ^i is a valid multipath, for all $i > 0$ (Fig. 4 (b,d,e)). A *repeating multipath* is an iterable multipath in which all acyclic z-paths are repeating (Fig. 4 (d,e)) – an empty multipath is repeating, by convention. A repeating multipath is said to be *essential* if every acyclic z-path is an essential power. A multipath μ is said to be *fitting* if every acyclic z-path in μ is fitting (Fig. 4 (b-e)).

Definition 8. *Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a difference bounds relation, and $\mathcal{G}_R$ be its constraint graph. Let π_1 and π_2 be repeating z-paths in ${}^{\omega}\mathcal{G}_R^{\omega}$. We say that π_1* may join *π_2, denoted $\pi_1 \bowtie_R \pi_2$, if and only if (i) there exists an SCC S of the folded graph $\mathcal{G}_R^f$, such that $vars(\pi_1) \cup vars(\pi_2) \subseteq S$ and (ii) there exists a path in ${}^{\omega}\mathcal{G}_R^{\omega}$ from some vertex in ${}^{\omega}\pi_1{}^{\omega}$ to some vertex in ${}^{\omega}\pi_2{}^{\omega}$.*

It is not hard to show that $\bowtie_R$ is an equivalence relation. For a repeating multipath μ, we denote by $\mu^{ac}_{/\bowtie_R}$ the partition of the set of acyclic paths μ^{ac} in equivalence classes of the $\bowtie_R$ relation. An *sc-multipath* (for strongly connected multipath) is a repeating multipath whose repeating z-paths belong to the same equivalence class of the $\bowtie_R$ relation (see Fig. 4). A repeating multipath ν is said to be a *reduct* of a repeating multipath μ if and



(a) $\mathcal{G}_R$ (b) μ_1 (c) μ_2 (d) μ_3 (e) μ_4

Fig. 4. Examples of multipaths. R is $x_1 = x_2' \wedge x_2 = x_1'$ and $\mathcal{G}_R$ is shown in **(a)**. μ_1 is iterable but not repeating, μ_2 is not iterable. Both μ_3 and μ_4 are fitting, iterable, repeating, and they consist of two balanced sc-multipaths each. If R is $x_1 = x_2' \wedge x_2 = x_1' \wedge x_1 \leq x_1'$ instead (the dotted edge $x_1 \xrightarrow{0} x_1'$), then μ_3 is a balanced sc-multipath and μ_4 is an unbalanced sc-multipath, since $\tau_1 \bowtie_R \tau_2$ for the two forward repeating z-paths $\tau_1, \tau_2 \in \mu_4$.

only if $\nu \subseteq \mu$ and, for each equivalence class $C \in \mu^{ac}_{/\bowtie_R}$: if the difference between the number of repeating forward (backward) z-paths and the number of repeating backward (forward) z-paths in C equals $k \geq 0$, then $\nu \cap C$ contains exactly k repeating forward (backward) z-paths and no repeating backward (forward) z-path.

Example 2. Consider for instance, in Fig. 2(c), the highlighted sc-multipath $\mu = \{\pi_1 : x_1^{(2)} \xrightarrow{0} x_2^{(3)} \xrightarrow{0} x_3^{(4)} \xrightarrow{0} x_4^{(3)} \xrightarrow{0} x_5^{(2)} \xrightarrow{-1} x_1^{(3)}, \pi_2 : x_6^{(3)} \xrightarrow{1} x_6^{(2)}, \pi_3 : x_7^{(2)} \xrightarrow{-1} x_7^{(3)}\}$. Notice that $\pi_1 \bowtie_R \pi_2 \bowtie_R \pi_3$, since all variables $x_1, \ldots, x_7$ are in the same SCC of the folded graph $\mathcal{G}_R^f$ of the difference bounds relation, and, e.g. $x_5^{(5)} \xrightarrow{0} x_6^{(4)}$ connects ${}^{\omega}\pi_1{}^{\omega}$ to ${}^{\omega}\pi_2{}^{\omega}$, while $x_6^{(2)} \xrightarrow{0} x_7^{(1)}$ connects ${}^{\omega}\pi_2{}^{\omega}$ to ${}^{\omega}\pi_3{}^{\omega}$ in ${}^{\omega}\mathcal{G}_R{}^{\omega}$. Moreover, since π_1, π_3 are forward z-paths, and π_2 is a backward z-path, $\nu_1 = \{\pi_1\}$ and $\nu_2 = \{\pi_3\}$ are the only reducts of μ.

Lemma 5. *Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a $*$-consistent difference bounds relation, and $\mathcal{G}_R$ be its constraint graph. Let μ be an sc-multipath in ${}^{\omega}\mathcal{G}_R^{\omega}$ and ν be a reduct of μ. Then $\overline{\overline{w}}(\nu) \leq \overline{\overline{w}}(\mu)$.*

Example 3. (contd. from Ex. 2) For instance, for the multipaths μ, ν_1 and ν_2 from Ex. 2, we have $\overline{\overline{w}}(\nu_1) = \overline{\overline{w}}(\nu_2) = \overline{\overline{w}}(\mu) = -1$. See the highlighted edges in Fig. 2(c).

Balanced SC-Multipaths and Strongly Connected Zigzag Cycles. An sc-multipath μ is said to be *balanced* if and only if the difference between the number of forward repeating and backward repeating z-paths in μ is either 1, 0, or -1. Let us observe that each reduct of a balanced sc-multipath contains at most one repeating z-path. For instance, the multipath μ from Ex. 2 is balanced, and its reducts ν_1 and ν_2 contain one z-path each.

Lemma 6. *Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a $*$-consistent difference bounds relation, $\mathcal{G}_R$ be its constraint graph and μ be a balanced sc-multipath in ${}^{\omega}\mathcal{G}_R^{\omega}$. Then there exists an essential sc-multipath, $\tau = \{\tau_0\}$, such that τ_0 is an essential repeating z-path, $\overline{\overline{w}}(\tau) \leq \overline{\overline{w}}(\mu)$, and two sc-multipaths ξ and ζ such that $\mu^m.\xi.\tau^n.\zeta.\mu^p$ is a valid sc-multipath for all $m, n, p \geq 0$.*

Example 4. (contd. from Ex. 2) For instance, the multipath μ from Ex. 2 can be connected with its reducts ν_1 and ν_2, and back (see Fig. 2(c)).

The motivation for defining and studying balanced sc-multipaths can be found when examining the words generated by the iterations of a cycle $q \xrightarrow{\gamma} q$ in a zigzag automaton. Without losing generality, we assume that the state q is both *reachable* (from an initial state) and *co-reachable* (a final state is reachable from q). With this assumption, it is possible to prove that sufficiently many iterations of the γ cycle will exhibit a subgraph composed only of balanced sc-multipaths. Details can be found in [7].

Example 5. (contd. from Ex. 2) For instance, for the γ_1 cycle in the zigzag automaton in Fig. 3(a), the balanced sc-multipath is μ, defined in Ex. 2, and highlighted in Fig. 2(c), and the connecting multipaths are $\eta = \{x_2^{(3)} \xrightarrow{0} x_3^{(4)} \xrightarrow{0} x_4^{(3)}\}$ and $\xi = \{x_1^{(3)} \xrightarrow{0} x_2^{(4)},\ x_4^{(4)} \xrightarrow{0} x_5^{(3)} \xrightarrow{-1} x_1^{(4)},\ x_6^{(4)} \xrightarrow{1} x_6^{(3)},\ x_7^{(3)} \xrightarrow{-1} x_7^{(4)}\}$. We have $\gamma_1^n = \eta.\mu^{n-2}.\xi$, for all $n \geq 2$.

The next lemma maps this graph, composed only of balanced sc-multipaths, back into another critical elementary loop $q' \xrightarrow{\lambda} q'$ of the zigzag automaton, belonging to the same SCC as γ, such that λ is composed of essential powers, and $\overline{w}(\lambda) = \overline{w}(\gamma)$. Since λ is composed of essential powers, and the length of an essential power is bounded by the number of variables N in the arithmetic representation of R, we have that $|\lambda|$ is a divisor of $lcm(1,\ldots,N)$. This is the final step needed to conclude the proof of Thm. 6.

Lemma 7. *Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a difference bounds relation, where $\mathbf{x} = \{x_1,\ldots,x_N\}$, $T_R = \langle Q, \Delta, \omega \rangle$ be its transition table, and $A = \langle T_R, I, F \rangle$ be one of the zigzag automata from Thm. 5. If $q \in Q$ is a reachable and co-reachable state of A, and $q \xrightarrow{\gamma} q$ is a cycle, then there exists a state $q' \in Q$, a cycle $q' \xrightarrow{\lambda} q'$, and paths $q \to q'$ and $q' \to q$ in T_R, such that (i) $\overline{w}(\lambda) \leq \overline{w}(\gamma)$, and (ii) $|\lambda| \mid lcm(1,\ldots,N)$.*

Example 6. (contd. from Ex. 2 and 5) Consider the zigzag automaton depicted in Fig. 3(a). The (reachable and co-reachable) cycle $\mathbf{q}_2 \xrightarrow{\gamma_1} \mathbf{q}_2$ is a critical cycle of average weight -1. The balanced sc-multipath μ, defined in Ex. 2 is obtained by the unfolding of the $\mathbf{q}_2 \xrightarrow{\gamma_1} \mathbf{q}_2$ cycle, and has relative average weight of -1 as well. The reduct ν_1 of μ (Ex. 2) consists of one essential repeating path $\pi_1 : x_1^{(2)} \xrightarrow{0} x_2^{(3)} \xrightarrow{0} x_3^{(4)} \xrightarrow{0} x_4^{(3)} \xrightarrow{0} x_5^{(2)} \xrightarrow{-1} x_1^{(3)}$, which appears in the unfolding of another critical cycle $\mathbf{q}_{10} \xrightarrow{\gamma_8} \mathbf{q}_{10}$ of the zigzag automaton. Moreover, the latter cycle is from the same SCC as $\mathbf{q}_2 \xrightarrow{\gamma_1} \mathbf{q}_2$. The fact that both cycles belong to the same SCC is witnessed by the fact that the multipath μ can be connected to its reduct ν_1, and back, via two connecting multipaths.

8 Octagonal Relations

The class of integer octagonal constraints is defined as follows:

Definition 9. *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 $1 \leq i, j \leq N$. A relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is an* octagonal relation *if it can be defined by an octagonal constraint $\phi_R(\mathbf{x}, \mathbf{x}')$.*

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 $i \in \mathbb{N}$. We denote by $\overline{\phi}(\mathbf{y})$ the difference bounds constraint over $\mathbf{y}$ that represents $\phi(\mathbf{x})$:

Definition 10. *Given an octagonal constraint* $\phi(\mathbf{x})$, $\mathbf{x} = \{x_1, \ldots, x_N\}$, *its* difference bounds representation $\overline{\phi}(\mathbf{y})$, *over* $\mathbf{y} = \{y_1, \ldots, y_{2N}\}$, *is a conjunction of the following difference bounds constraints, where* $1 \leq i, j \leq N$, $c \in \mathbb{Z}$.

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

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 say that a DBM $M \in \mathbb{Z}_\infty^{2N \times 2N}$ is *coherent*[9] iff $M_{ij} = M_{\bar{j}\bar{\imath}}$ for all $1 \leq i, j \leq 2N$. Dually, for a coherent DBM $M \in \mathbb{Z}_\infty^{2N \times 2N}$, we define:

$$
\begin{array}{l}
\Psi_M^{uu} \equiv \bigwedge_{1 \leq i,j \leq N} x_i - x_j \leq M_{2i-1,2j-1} \wedge x_i + x_j \leq M_{2i-1,2j} \wedge -x_i - x_j \leq M_{2i,2j-1} \\
\Psi_M^{up} \equiv \bigwedge_{1 \leq i,j \leq N} x_i - x'_j \leq M_{2i-1,2j-1} \wedge x_i + x'_j \leq M_{2i-1,2j} \wedge -x_i - x'_j \leq M_{2i,2j-1} \\
\Psi_M^{pu} \equiv \bigwedge_{1 \leq i,j \leq N} x'_i - x_j \leq M_{2i-1,2j-1} \wedge x'_i + x_j \leq M_{2i-1,2j} \wedge -x'_i - x_j \leq M_{2i,2j-1} \\
\Psi_M^{pp} \equiv \bigwedge_{1 \leq i,j \leq N} x'_i - x'_j \leq M_{2i-1,2j-1} \wedge x'_i + x'_j \leq M_{2i-1,2j} \wedge -x'_i - x'_j \leq M_{2i,2j-1}
\end{array}
$$

A coherent DBM M is said to be *octagonal-consistent* if and only if Ψ_M^{uu} is consistent.

Definition 11. *An octagonal-consistent coherent DBM* $M \in \mathbb{Z}_\infty^{2N \times 2N}$ *is said to be* tightly closed *iff it is closed and, for all* $1 \leq i, j \leq 2N$, $M_{i\bar{\imath}}$ *is even, and* $M_{ij} \leq \lfloor \frac{M_{i\bar{\imath}}}{2} \rfloor + \lfloor \frac{M_{\bar{\jmath}j}}{2} \rfloor$.

Intuitively the conditions of Def. 11 ensure that all knowledge induced by the triangle inequality and the $y_{2i-1} = -y_{2i}$ constraints has been propagated in the DBM. Given an octagonal-consistent coherent DBM $M \in \mathbb{Z}^{2N} \times \mathbb{Z}^{2N}$, we denote the (unique) logically equivalent tightly closed DBM by M^t. Octagonal constraints are closed under existential quantification, thus octagonal relations are closed under composition [4]. Tight closure of octagonal-consistent DBMs is needed for quantifier elimination. The set of octagonal constraints forms therefore a class, denoted further $\mathcal{R}_{OCT}$.

Lemma 8. *The class* $\mathcal{R}_{OCT}$ *is poly-logarithmic.*

8.1 The Complexity of Acceleration for Octagonal Relations

The proof idea for the periodicity of $\mathcal{R}_{OCT}$ is the following. Since any power R^i of an octagonal relation R is obtained by quantifier elimination, and since quantifier elimination for octagons uses the tight closure of the DBM representation, then the sequence

[9] DBM coherence is needed because $x_i - x_j \leq c$ can be represented as both $y_{2i-1} - y_{2j-1} \leq c$ and $y_{2j} - y_{2i} \leq c$.

$\{R^i\}_{i>0}$ is defined by the sequence $\{M^t_{\overline{R^i}}\}_{i>0}$ of tightly closed DBMs. In [6] we prove that this sequence of matrices is periodic, using the result from Thm. 8, below. If $R \subseteq \mathbb{Z}^N \times \mathbb{Z}^N$ is an octagonal relation, let $\sigma(R) \equiv M_{\overline{R}}$ be the characteristic DBM of its difference bounds representation, and for a coherent DBM $M \in \mathbb{Z}_\infty^{4N\times 4N}$, we define $\rho(M) \equiv \Psi^{uu}_{\blacksquare M} \wedge \Psi^{up}_{M\blacksquare} \wedge \Psi^{pu}_{\blacksquare M} \wedge \Psi^{pp}_{M\blacksquare}$. Analogously, $\pi(M)$ is defined in the same way as ρ, for each matrix $M \in \mathbb{Z}[k]_\infty^{4N\times 4N}$ of univariate linear terms. With these definitions, periodicity of $\mathcal{R}_{OCT}$ has been shown in [6], using the periodicity of $\mathcal{R}_{DB}$ and the following theorem [4], establishing the following relation between $M^t_{\overline{R^m}}$ (the tightly closed octagonal DBM corresponding to the m-th iteration of R) and $M^*_{\overline{R}^m}$ (the closed DBM corresponding to the m-th iteration of the difference bounds relation $\overline{R}$), for all $m > 0$:

Theorem 8. *[4] Let $R \subseteq \mathbb{Z}^N \times \mathbb{Z}^N$, be a $*$-consistent octagonal relation. Then, for all $m > 0$ and $1 \leq i, j \leq 4N$: $(M^t_{\overline{R^m}})_{ij} = \min\left\{(M^*_{\overline{R}^m})_{ij}, \left\lfloor \frac{(M^*_{\overline{R}^m})_{\bar{i}i}}{2} \right\rfloor + \left\lfloor \frac{(M^*_{\overline{R}^m})_{\bar{j}j}}{2} \right\rfloor\right\}$.*

In the rest of this section, we show that the periodic class $\mathcal{R}_{OCT}$ is also exponential, which proves NP-completness of the reachability problem for flat counter machines with octagonal constraints labeling their loops.

Lemma 9. *Let $\{s_m\}_{m=1}^\infty$ and $\{t_m\}_{m=1}^\infty$ be two periodic sequences. Then the sequences $\{\min(s_m, t_m)\}_{m=1}^\infty$, $\{s_m + t_m\}_{m=1}^\infty$ and $\left\{\left\lfloor \frac{s_m}{2} \right\rfloor\right\}_{m=1}^\infty$ are periodic as well. Moreover, the prefixes and periods of these sequences are linear in the prefixes and periods of $\{s_m\}_{m=1}^\infty$ and $\{t_m\}_{m=1}^\infty$.*

A consequence of Thm. 8 and Lemma 9 is that the asymptotic bounds on the prefix and period and an octagonal relation match the ones of its difference bounds representation, which uses twice as many variables (Def. 10).

Lemma 10. *Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$, where $\mathbf{x} = \{x_1, \ldots, x_N\}$, be an octagonal relation. The prefix and period of R are $2^{O(\|R\|_2)}$ and $2^{O(N)}$, respectively.*

The previous lemma provides the bounds on the prefix and periods of octagonal relations, needed for the next theorem, which gives the second main result of the paper:

Theorem 9. *The class $\mathcal{R}_{DB}$ is exponential, and the reachability problem for the class $\mathcal{M}_{OCT} = \{M \text{ flat counter machine} \mid \text{for all } q \overset{R}{\Rightarrow} q' \text{ on a loop of } M, R \text{ is } \mathcal{R}_{OCT}\text{-definable}\}$ is NP-complete.*

9 Conclusions and Future Work

We prove that the verification of reachability properties for flat counter machines with difference bounds and octagonal relations on loops is NP-complete. Future work includes the extension of this result to finite monoid affine relations [6], and the investigation of temporal logic properties of flat counter machines with transitions defined using these classes of relations.

References

1. Bansal, K., Koskinen, E., Wies, T., Zufferey, D.: Structural counter abstraction. In: Piterman, N., Smolka, S.A. (eds.) TACAS 2013. LNCS, vol. 7795, pp. 62–77. Springer, Heidelberg (2013)

2. Boigelot, B.: Symbolic Methods for Exploring Infinite State Spaces. PhD, Univ. de Liège (1999)
3. Bouajjani, A., Bozga, M., Habermehl, P., Iosif, R., Moro, P., Vojnar, T.: Programs with lists are counter automata. In: Ball, T., Jones, R.B. (eds.) CAV 2006. LNCS, vol. 4144, pp. 517–531. Springer, Heidelberg (2006)
4. Bozga, M., Gîrlea, C., Iosif, R.: Iterating octagons. In: Kowalewski, S., Philippou, A. (eds.) TACAS 2009. LNCS, vol. 5505, pp. 337–351. Springer, Heidelberg (2009)
5. Bozga, M., Habermehl, P., Iosif, R., Konečný, F., Vojnar, T.: Automatic verification of integer array programs. In: Bouajjani, A., Maler, O. (eds.) CAV 2009. LNCS, vol. 5643, pp. 157–172. Springer, Heidelberg (2009)
6. Bozga, M., Iosif, R., Konečný, F.: Fast acceleration of ultimately periodic relations. In: Touili, T., Cook, B., Jackson, P. (eds.) CAV 2010. LNCS, vol. 6174, pp. 227–242. Springer, Heidelberg (2010)
7. Bozga, M., Iosif, R., Konečný, F.: Safety problems are NP-complete for flat integer programs with octagonal loops. Tech. Rep. arXiv 1307.5321 (2013), http://arxiv.org/abs/1307.5321
8. Bozga, M., Iosif, R., Lakhnech, Y.: Flat parametric counter automata. Fundamenta Informaticae 91(2), 275–303 (2009)
9. Bozzelli, L., Pinchinat, S.: Verification of gap-order constraint abstractions of counter systems. In: Kuncak, V., Rybalchenko, A. (eds.) VMCAI 2012. LNCS, vol. 7148, pp. 88–103. Springer, Heidelberg (2012)
10. Comon, H., Jurski, Y.: Multiple counters automata, safety analysis and presburger arithmetic. In: Hu, A.J., Vardi, M.Y. (eds.) CAV 1998. LNCS, vol. 1427, pp. 268–279. Springer, Heidelberg (1998)
11. Demri, S., Dhar, A.K., Sangnier, A.: On the complexity of verifying regular properties on flat counter systems, In: Fomin, F.V., Freivalds, R., Kwiatkowska, M., Peleg, D. (eds.) ICALP 2013, Part II. LNCS, vol. 7966, pp. 162–173. Springer, Heidelberg (2013)
12. Demri, S., Dhar, A.K., Sangnier, A.: Taming past LTL and flat counter systems. In: Gramlich, B., Miller, D., Sattler, U. (eds.) IJCAR 2012. LNCS, vol. 7364, pp. 179–193. Springer, Heidelberg (2012)
13. Demri, S., Jurdzinski, M., Lachish, O., Lazic, R.: The covering and boundedness problems for branching vector addition systems. J. Comput. Syst. Sci. 79(1), 23–38 (2013)
14. Gawlitza, T.M., Monniaux, D.: Invariant generation through strategy iteration in succinctly represented control flow graphs. Logical Methods in Computer Science 8(3) (2012)
15. Gurari, E.M., Ibarra, O.H.: The complexity of the equivalence problem for simple programs. J. ACM 28(3), 535–560 (1981)
16. Ibarra, O.H.: Reversal-bounded multicounter machines and their decision problems. J. ACM 25(1), 116–133 (1978)
17. Leroux, J.: Vector addition system reachability problem: a short self-contained proof. In: POPL, pp. 307–316 (2011)
18. Minsky, M.: Computation: Finite and Infinite Machines. Prentice-Hall (1967)
19. Rackoff, C.: The covering and boundedness problems for vector addition systems. Theor. Comput. Sci. 6, 223–231 (1978)
20. Revesz, P.Z.: A closed-form evaluation for Datalog queries with integer (gap)-order constraints. Theor. Comput. Sci. 116(1&2), 117–149 (1993)
21. Schutter, B.D.: 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)
22. Verma, K.N., Seidl, H., Schwentick, T.: On the complexity of equational Horn clauses. In: Nieuwenhuis, R. (ed.) CADE 2005. LNCS (LNAI), vol. 3632, pp. 337–352. Springer, Heidelberg (2005)